acunetix

v12 Product Manual

http://www.acunetix.com
info@acunetix.com

Document version 12
Last updated: 3rd July 2018

Table of Contents

Introduction to Acunetix

Why You Need To Secure Your Web Applications

Website security is today's most overlooked aspect of securing an enterprise and should be a priority in any organization. Increasingly, hackers are concentrating their efforts on web-based applications – shopping carts, forms, login pages, dynamic content, etc. Accessible 24/7 from anywhere in the world, insecure web applications provide easy access to backend corporate databases and also allow hackers to perform illegal activities using the attacked sites. A victim's website can be used to launch criminal activities such as hosting phishing sites or to transfer illicit content, while abusing the website's bandwidth and making its owner liable for these unlawful acts.

Hackers already have a wide repertoire of attacks that they regularly launch against organizations including SQL Injection, Cross Site Scripting, Directory Traversal Attacks, Parameter Manipulation (e.g., URL, Cookie, HTTP headers, web forms), Authentication Attacks, Directory Enumeration and other exploits.
The hacking community is also very close-knit; newly discovered web application intrusions, known as Zero Day exploits, are posted on a number of forums and websites known only to members of that exclusive underground group. Postings are updated daily and are used to propagate and facilitate further hacking.

Web applications – shopping carts, forms, login pages, dynamic content, and other bespoke applications – are designed to allow your website visitors to retrieve and submit dynamic content including varying levels of personal and sensitive data.
If these web applications are not secure, then your entire database of sensitive information is at serious risk. A Gartner Group study reveals that 75% of cyber-attacks are done at the web application level.

Why are web applications vulnerable?

- Websites and web applications are easily available via the internet 24 hours a day, 7 days a week to customers, employees, suppliers and therefore also hackers.
- Firewalls and SSL provide no protection against web application hacking, simply because access to the website has to be made public.
- Web applications often have direct access to backend data such as customer databases.
- Most web applications are custom-made and, therefore, involve a lesser degree of testing than off-the-shelf software. Consequently, custom applications are more susceptible to attack.
- Various high-profile hacking attacks have proven that web application security remains the most critical. If your web applications are compromised, hackers will have complete access to your backend data even though your firewall is configured correctly and your operating system and applications are patched repeatedly.
- Network security defense provides no protection against web application attacks since these are launched on port 80 which has to remain open to allow regular

operation of the business. It is therefore imperative that you regularly and consistently audit your web applications for exploitable vulnerabilities.

The need for automated web application security scanning

Manual vulnerability auditing of all your web applications is complex and time-consuming, since it generally involves processing a large volume of data. It also demands a high level of expertise and the ability to keep track of considerable volumes of code used in a web application. In addition, hackers are constantly finding new ways to exploit your web application, which means that you would have to constantly monitor the security communities, and find new vulnerabilities in your web application code before hackers discover them.

Automated vulnerability scanning allows you to focus on the already challenging task of building a web application. An automated web application scanner is always on the lookout for new attack paths that hackers can use to access your web application or the data behind it.

Within minutes, an automated web application scanner can scan your web application, identify all the files accessible from the internet and simulate hacker activity in order to identify vulnerable components.

In addition, an automated vulnerability scanner can also be used to assess the code which makes up a web application, allowing it to identify potential vulnerabilities which might not be obvious from the internet, but still exist in the web application, and can thus still be exploited.

Acunetix Vulnerability Management

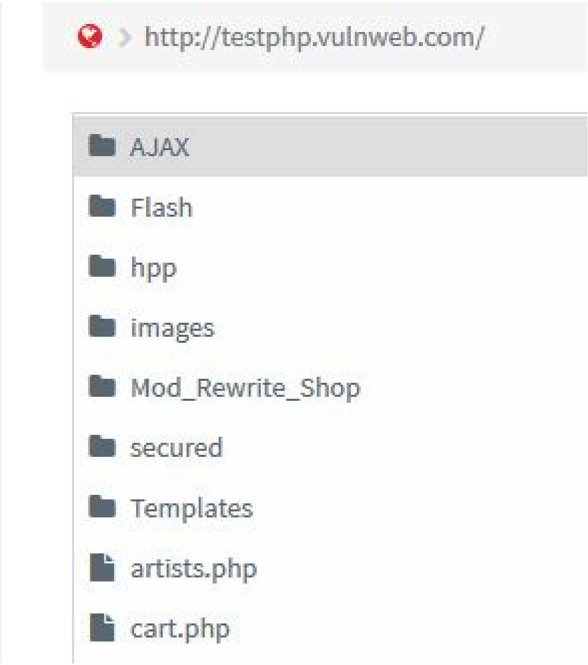
Acunetix is an automated web application security testing tool that audits your web applications by checking for vulnerabilities like SQL Injection, Cross site scripting and other exploitable vulnerabilities. In general, Acunetix scans any website or web application that is accessible via a web browser and uses the HTTP/HTTPS protocol.

Acunetix offers a strong and unique solution for analyzing off-the-shelf and custom web applications including those utilizing JavaScript, AJAX and Web 2.0 web applications. Acunetix has an advanced crawler that can find almost any file. This is important since what is not found cannot be checked.

How Acunetix Works

Acunetix works in the following manner:

1. Acunetix DeepScan analyses the entire website by following all the links on the site, including links which are dynamically constructed using JavaScript, and links found in robots.txt and sitemap.xml (if available). The result is a map of the site, which Acunetix will use to launch targeted checks against each part of the site.

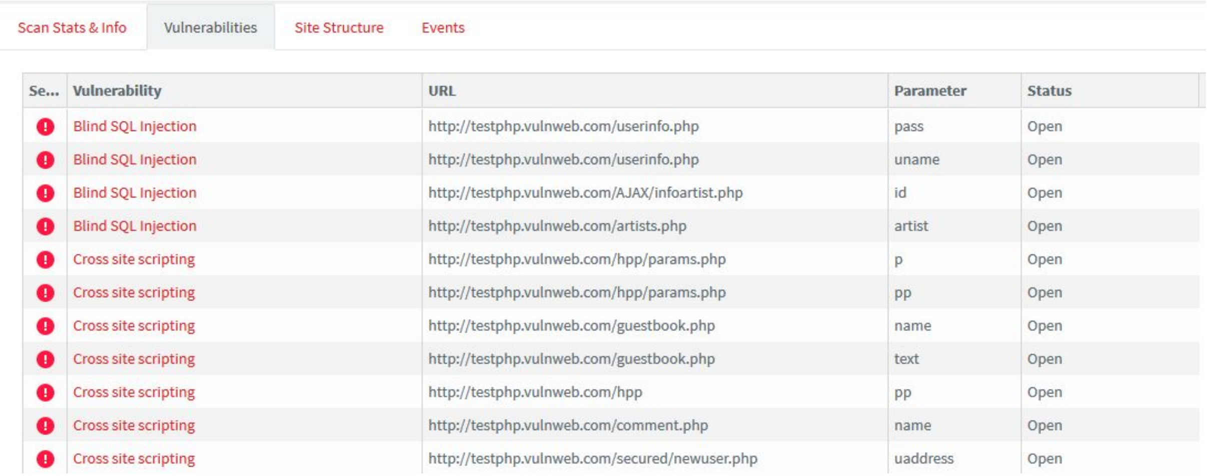


http://testphp.vulnweb.com/

- AJAX
- Flash
- hpp
- images
- Mod_Rewrite_Shop
- secured
- Templates
- artists.php
- cart.php

Screenshot - Crawler Results

2. If Acunetix AcuSensor Technology is enabled, the sensor will retrieve a listing of all the files present in the web application directory and add the files not found by the crawler to the crawler output. Such files usually are not discovered by the crawler as they are not accessible from the web server, or not linked through the website. Acunetix AcuSensor also analyses files which are not accessible from the internet, such as *web.config*.
3. After the crawling process, the scanner automatically launches a series of vulnerability checks on each page found, in essence emulating a hacker. Acunetix also analyses each page for places where it can input data, and subsequently attempts all the different input combinations. This is the Automated Scan Stage. If the AcuSensor Technology is enabled, a series of additional vulnerability checks are launched against the website. More information about AcuSensor is provided in the following section.



Se...	Vulnerability	URL	Parameter	Status
!	Blind SQL Injection	http://testphp.vulnweb.com/userinfo.php	pass	Open
!	Blind SQL Injection	http://testphp.vulnweb.com/userinfo.php	uname	Open
!	Blind SQL Injection	http://testphp.vulnweb.com/AJAX/infoartist.php	id	Open
!	Blind SQL Injection	http://testphp.vulnweb.com/artists.php	artist	Open
!	Cross site scripting	http://testphp.vulnweb.com/hpp/params.php	p	Open
!	Cross site scripting	http://testphp.vulnweb.com/hpp/params.php	pp	Open
!	Cross site scripting	http://testphp.vulnweb.com/guestbook.php	name	Open
!	Cross site scripting	http://testphp.vulnweb.com/guestbook.php	text	Open
!	Cross site scripting	http://testphp.vulnweb.com/hpp	pp	Open
!	Cross site scripting	http://testphp.vulnweb.com/comment.php	name	Open
!	Cross site scripting	http://testphp.vulnweb.com/secured/newuser.php	uaddress	Open

Screenshot - Scan Results

4. The vulnerabilities identified are shown in the Scan Results. Each vulnerability alert contains information about the vulnerability such as POST data used, affected item, HTTP response of the server and more.
5. If AcuSensor Technology is used, details such as source code line number, stack trace or affected SQL query which lead to the vulnerability are listed. Recommendations on how to fix the vulnerability are also shown.
6. Various reports can be generated on completed scans, including Executive Summary report, Developer report and various compliance reports such as PCI DSS or ISO 270001.

Acunetix AcuSensor Technology

Acunetix' unique AcuSensor Technology allows you to identify more vulnerabilities than other Web Application Scanners, whilst generating less false positives. Acunetix AcuSensor indicates exactly where in your code the vulnerability is and reports additional debug information.

The increased accuracy, available for PHP, .NET and JAVA web applications, is achieved by combining black box scanning techniques with feedback from sensors placed inside the source code. Black box scanning does not know how the application reacts and source code analyzers do not understand how the application will behave while it is being attacked. AcuSensor technology combines both techniques to achieve significantly better results than using source code analyzers and black box scanning independently.

AcuSensor can be installed in .NET, PHP and JAVA code transparently.

AcuSensor can be installed into pre-compiled .NET and JAVA assemblies, even if they are signed (strong-named), therefore, neither .NET or JAVA source code, nor a compiler (or any other dependencies) are required.In case of PHP web applications, the source is readily available. To date, Acunetix is the only web vulnerability security solution to implement this technology.

Advantages of using AcuSensor Technology

- Allows you to locate and fix the vulnerability faster because of the ability to provide more information about the vulnerability, such as source code line number, stack trace, affected SQL query, etc.
- Significantly reduces false positives when scanning a website because it understands the behavior of the web application better.
- Alerts you to web application configuration problems which can result in a security misconfiguration, or expose sensitive information. E.g. If ‘custom errors’ are enabled in .NET, this could expose sensitive application details to a malicious user.
- Advises you how to better secure your web server settings, e.g. if write access is enabled on the web server.
- Detects more SQL injection vulnerabilities. Previously SQL injection vulnerabilities could only be found if database errors were reported, whereas now the source code can be analyzed for improved detection.
- Ability to detect SQL injection vulnerabilities in all SQL statements, including in SQL INSERT statements. Using a black box scanner such SQL injection vulnerabilities

cannot be found. This significantly increases the ability for Acunetix to find vulnerabilities.

- Scans run using AcuSensor run a back-end crawl, presenting all files accessible through the web server to the scanner; even if these files are not linked through the front-end application. This ensures 100% coverage of the application, and alerts users of any backdoor files that might have been maliciously uploaded by an attacker.
- AcuSensor Technology is able to intercept all web application inputs and build a comprehensive list with all possible inputs in the website and test them.
- Ability to test for arbitrary file creation and deletion vulnerabilities. E.g. Through a vulnerable script a malicious user can create a file in the web application directory and execute it to have privileged access, or delete sensitive web application files.

Network Vulnerability Scanning

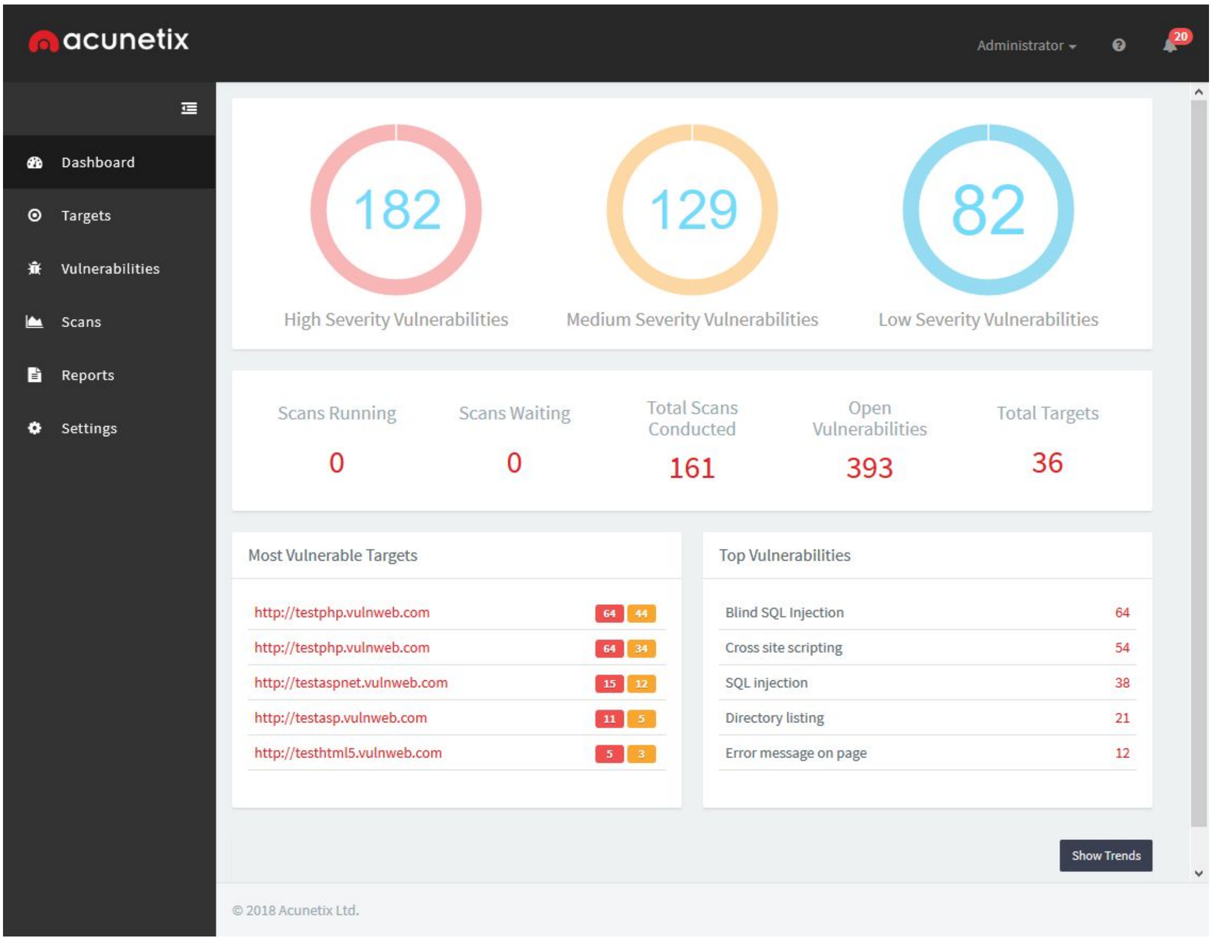
As part of a website audit, the online version of Acunetix will execute a network security audit of the server hosting the website. This network security scan will identify any services running on the scanned server by running a port scan on the system. Acunetix will report the operating system and the software hosting the services detected. This process will also identify Trojans which might be lurking on the server.

The network vulnerability scan assesses the security of popular protocols such as FTP, DNS, SMTP, IMAP, POP3, SSH, SNMP and Telnet. Apart from testing for weak or default passwords, Acunetix will also check for misconfiguration in the services detected which could lead to a security breach. Acunetix will also check that any other servers running on the machine are not using any deprecated protocols. All these lead to an insecure system, which would allow an intruder to damage your web site and your reputation.

Acunetix Online also integrates the popular OpenVAS network scanner to check for over 50,000 network vulnerabilities. During a network scan, Acunetix makes use of various port probing and OS fingerprinting techniques to identify a vast number of devices, Operating Systems and server products. Numerous security checks are then launched against the products identified running on the scanned server, allowing you to detect all the vulnerabilities that exist on your perimeter servers.

Acunetix Overview

Acunetix allows you to secure your websites and web applications quickly and efficiently, while making it easy to manage the vulnerabilities detected. It consists of the following components:



High Severity Vulnerabilities	Medium Severity Vulnerabilities	Low Severity Vulnerabilities
182	129	82

Scans Running	Scans Waiting	Total Scans Conducted	Open Vulnerabilities	Total Targets
0	0	161	393	36

Most Vulnerable Targets

http://testphp.vulnweb.com	64	44
http://testphp.vulnweb.com	64	34
http://testaspnet.vulnweb.com	15	12
http://testasp.vulnweb.com	11	5
http://testhtml5.vulnweb.com	5	3

Top Vulnerabilities

Blind SQL Injection	64
Cross site scripting	54
SQL injection	38
Directory listing	21
Error message on page	12

Screenshot - Acunetix dashboard

Acunetix Web Interface

Acunetix ships with an easy to use web interface, allowing multiple users to use Acunetix from a standard web browser. After logging in, users are taken to the Dashboard which provides a bird's-eye view of the security of the organisation’s assets. From here, users can access the inbuilt-in vulnerability management features including:

- Configure Targets once and scan them as often as needed. Acunetix keeps track of the security status of each target by aggregating and keeping track of the vulnerabilities identified for each target;
- All the vulnerabilities identified by Acunetix are shown in one page, making it easy to prioritise the vulnerabilities identified across all the organisation. Vulnerabilities can be filtered to show only what is required or grouped either by the severity of the vulnerability or the business criticality assigned to each target;

- Acunetix makes it easy to review scan results of ongoing or completed scans. New scans can be configured to occur either instantly or on a schedule;
- Reports can be generated for targets, scans or a set of vulnerabilities;

Web Scanner

The Web Scanner launches an automatic security audit of a website. A website security scan typically consists of two phases:

1. Crawling – Making use of Acunetix DeepScan, Acunetix automatically analyzes and crawls the website in order to build the site's structure. The crawling process enumerates all files, folders and inputs and is vital to ensure that all your website is scanned.
2. Scanning – Acunetix launches a series of web vulnerability checks against each component in your web application – in effect, emulating a hacker. The results of a scan include comprehensive details of all the vulnerabilities found within the website.

AcuSensor Technology Agent

Acunetix AcuSensor Technology is a unique technology that allows you to identify more vulnerabilities than a traditional black-box web security scanner, and is designed to further reduce false positives. Additionally, it also indicates the line of code where the vulnerability was found. This increased accuracy is achieved by combining black-box scanning techniques with interactive code analysis whilst the source code is being executed. For Acunetix AcuSensor to work, an agent must be installed on your website to enable communication between Acunetix and AcuSensor. Acunetix AcuSensor can be used with PHP, JAVA and .NET web applications.

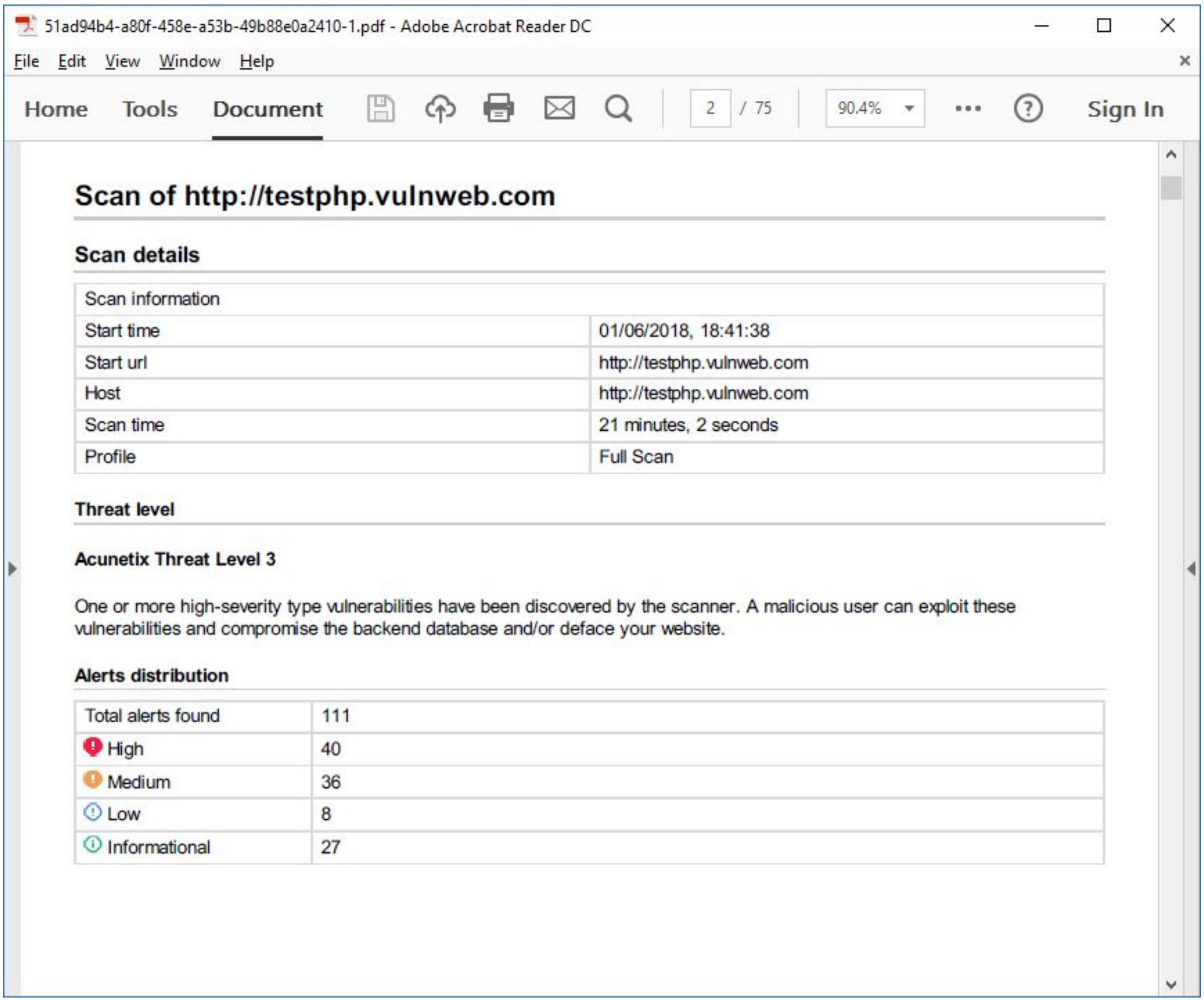
AcuMonitor Technology

Some vulnerabilities can only be detected using an intermediate service. Acunetix AcuMonitor allows Acunetix to detect such vulnerabilities. Depending on the vulnerability, AcuMonitor can either report the vulnerability immediately during a scan, or send a notification email directly to the user if the vulnerability is identified after the scan has finished. More information on the AcuMonitor Service can be found at http://www.acunetix.com/vulnerability-scanner/acumonitor-blind-xss-detection/

The AcuMonitor Service is fully integrated in Acunetix, and is enabled for all the targets configured in Acunetix.

Reporter

The Reporter allows you to generate reports for Scans, Targets and all the vulnerabilities detected. Various report templates are available, including executive summaries, detailed reports and a wide variety of compliance reports.



51ad94b4-a80f-458e-a53b-49b88e0a2410-1.pdf - Adobe Acrobat Reader DC
File Edit View Window Help
Home Tools Document
2 / 75
90.4%
Sign In

Scan of http://testphp.vulnweb.com

Scan details

Scan information	
Start time	01/06/2018, 18:41:38
Start url	http://testphp.vulnweb.com
Host	http://testphp.vulnweb.com
Scan time	21 minutes, 2 seconds
Profile	Full Scan

Threat level

Acunetix Threat Level 3

One or more high-severity type vulnerabilities have been discovered by the scanner. A malicious user can exploit these vulnerabilities and compromise the backend database and/or deface your website.

Alerts distribution

Total alerts found	111
High	40
Medium	36
Low	8
Informational	27

Screenshot - Typical Report Summary

Installing Acunetix

Minimum System Requirements

- Operating system: Microsoft Windows 7 or Windows 2008 R2 and later
- CPU: 64 bit processor
- System memory: minimum of 2 GB RAM
- Storage: 200 MB of available hard-disk space.
  This does not include the storage required to save the scan results - this will depend on the level of usage of Acunetix.

Installation

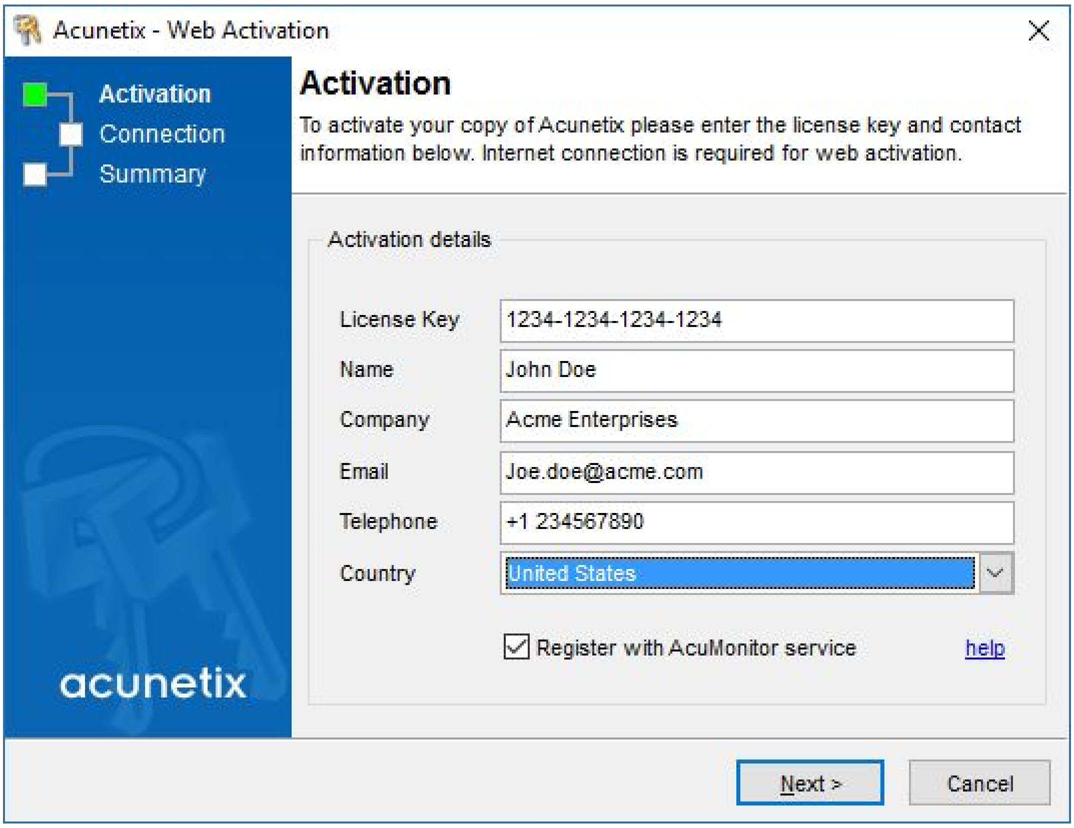
1. Download the latest version of Acunetix from the download location provided when you purchased the license.
2. Double click the installation file to launch the Acunetix installation wizard and click Next when prompted.
3. Review and accept the License Agreement.
4. Provide credentials for the Administrative user account. These will be used to access and configure Acunetix.
5. Configure how the Acunetix Web UI is accessed, and if remote UI access is allowed.
6. Review the installation tasks, and click Install to start the installation.
7. Setup will now copy all files and install the Acunetix services.
8. Click Finish when ready.

Activating your Acunetix Installation

After the installation, Acunetix needs to be activated using your license key. This can be done using the Acunetix Activation utility which can be loaded from the Acunetix program group. Insert your License key and your details and proceed with the product activation.

At this stage, you can also choose to Register your installation with the AcuMonitor service. AcuMonitor is used to detect certain type of vulnerabilities, such Blind XSS, SSRF, XXE and other out of band vulnerabilities which can only be detected using an intermediary service. More information on AcuMonitor can be found at http://www.acunetix.com/vulnerability-scanner/acumonitor-blind-xss-detection/.

Product activation requires a connection to the internet.



Activation

To activate your copy of Acunetix please enter the license key and contact information below. Internet connection is required for web activation.

Activation details

License Key	1234-1234-1234-1234
Name	John Doe
Company	Acme Enterprises
Email	Joe.doe@acme.com
Telephone	+1 234567890
Country	United States

☑ Register with AcuMonitor service

Installing AcuSensor in your web application

If you need to scan a .NET, JAVA or PHP web application, you should install Acunetix AcuSensor on your web application in order to improve the detection of vulnerabilities, get the line in the source code where vulnerabilities are located and decrease false positives.

Upgrading Acunetix

To upgrade from Acunetix version 11 to Acunetix version 12:

1. Close all instances of Acunetix (and related utilities such as the Login Sequence Recorder)
2. Optionally backup the Acunetix data folder which includes the Acunetix database and other settings. These are all found in <C:\ProgramData\Acunetix>
3. You can run the Acunetix 12 installation on the machine running Acunetix 11. The installation will detect the older version, and will proceed with upgrading it to the latest version. All your settings will be retained.

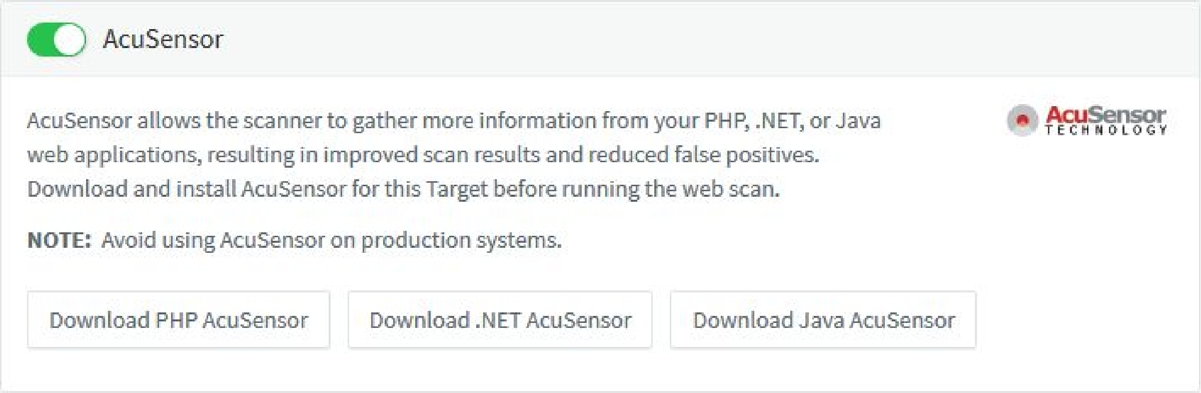
Installing AcuSensor

Acunetix AcuSensor increases the accuracy of an Acunetix scan by improving the crawling, detection and reporting of vulnerabilities, while decreasing false positives. Acunetix AcuSensor can be used on .NET, JAVA and PHP web applications.

Installing the AcuSensor Agent

NOTE: Installing the AcuSensor Agent is optional. Acunetix is still best in class as a black-box scanner, but the AcuSensor Agent improves accuracy and vulnerability results when scanning .NET, JAVA and PHP web applications.
The unique Acunetix AcuSensor Technology identifies more vulnerabilities than a black-box Web Application Scanner while generating less false positives. In addition, it indicates exactly where vulnerabilities are detected in your code and also reports debug information

Acunetix AcuSensor requires an agent to be installed on your website. This agent is generated uniquely for each website for security reasons. From the configuration of each Target, change to the General tab, and toggle the AcuSensor option. From here, you can download the AcuSensor generated for the Target. Choose between the .NET, JAVA or PHP AcuSensor agent, depending on the web technology used on your site, and proceed with the installation steps below.


AcuSensor

AcuSensor allows the scanner to gather more information from your PHP, .NET, or Java web applications, resulting in improved scan results and reduced false positives. Download and install AcuSensor for this Target before running the web scan.

NOTE: Avoid using AcuSensor on production systems.

Screenshot – Acunetix AcuSensor configuration

Installing the AcuSensor agent for PHP websites

First, you need to download the AcuSensor agent for your Target.

This section describes how to install AcuSensor in a PHP web application.

1. Locate the PHP AcuSensor file of the website you want to install AcuSensor on. Copy the **acu_phpaspect.php** file to the remote web server hosting the web application. The AcuSensor agent file should be in a location where it can be accessed by the web server software. Acunetix AcuSensor Technology works on websites using PHP version 5 and up.
2. There are 2 methods to install the AcuSensor agent, one method can be used for Apache web server, and the other method can be used for IIS, nginx and Apache web servers.

Method 1: Apache web Server - .htaccess file

Create a .htaccess file in the website directory and add the following directive:
php_value auto_prepend_file '[path to acu_phpaspect.php file]'.

Note: For Windows use 'C:\sensor\acu_phpaspect.php' and for Linux use '/Sensor/acu_phpaspect.php' path declaration formats. If Apache web server does not execute *.htaccess* files, it must be configured to do so. Refer to the following configuration guide: http://httpd.apache.org/docs/2.0/howto/htaccess.html. The above directive can also be configured in the *httpd.conf* file.

Method 2: IIS, Apache and nginx - php.ini

1. Locate the file 'php.ini' on the server by using *phpinfo()* function.
2. Search for the directive **auto_prepend_file**, and specify the path to the acu_phpaspect.php file. If the directive does not exist, add it in the php.ini file: **auto_prepend_file="/path/to/acu_phpaspect.php"**
3. Save all changes and restart the web server for the above changes to take effect.

Disabling and uninstalling AcuSensor for PHP

To uninstall and disable the sensor from your web site:

1. If method 1 (.htaccess file) was used to install the PHP AcuSensor, delete the directive: **php_value auto_prepend_file="/path/to/acu_phpaspect.php"** from .htaccess
2. If method 2 was used to install the PHP AcuSensor, delete the directive: **auto_prepend_file="/path/to/acu_phpaspect.php"** from php.ini.
3. Finally, delete the Acunetix AcuSensor PHP file: acu_phpaspect.php.

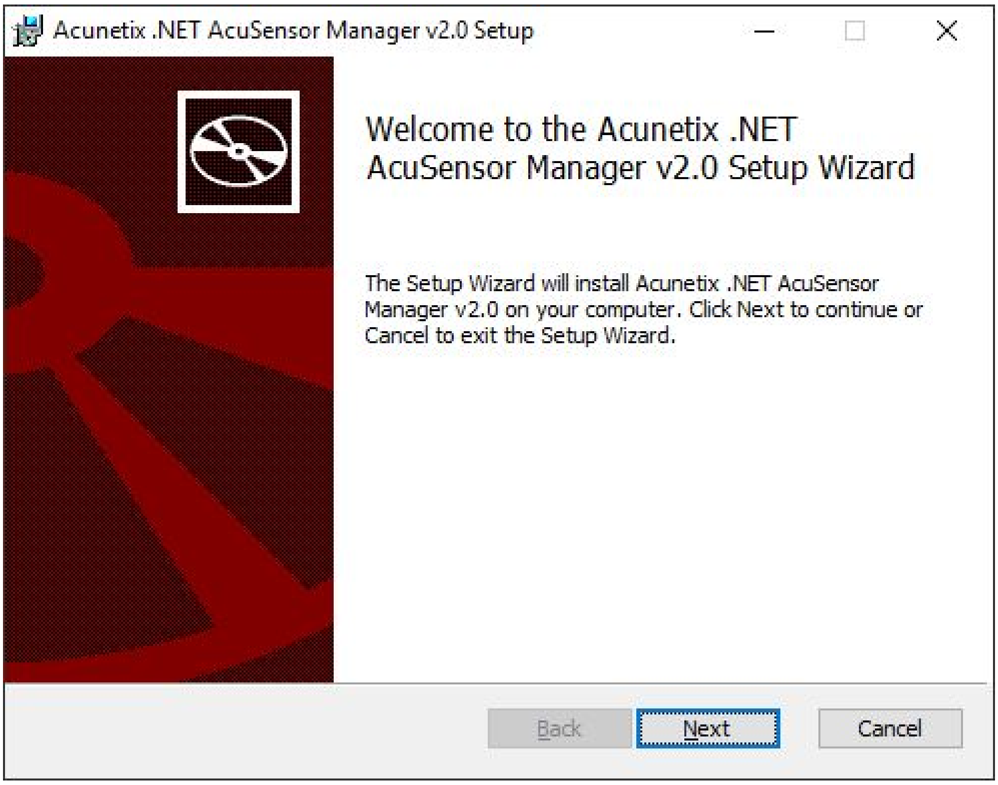
Note: Although the Acunetix AcuSensor agent are secured with a strong password, it is recommended that the AcuSensor client files are uninstalled and removed from the web application if they are no longer in use.

Installing the AcuSensor agent for ASP .NET Websites

First, you need to download the AcuSensor agent for your Target.

The AcuSensor agent will need to be installed in your web application. This section describes how to install AcuSensor in an ASP.NET web application.

1. **Install Prerequisites on the server hosting the website:** The AcuSensor installer application requires Microsoft .NET Framework 3.5 or higher.
2. Copy the AcuSensor installation files to the server hosting the .NET website.



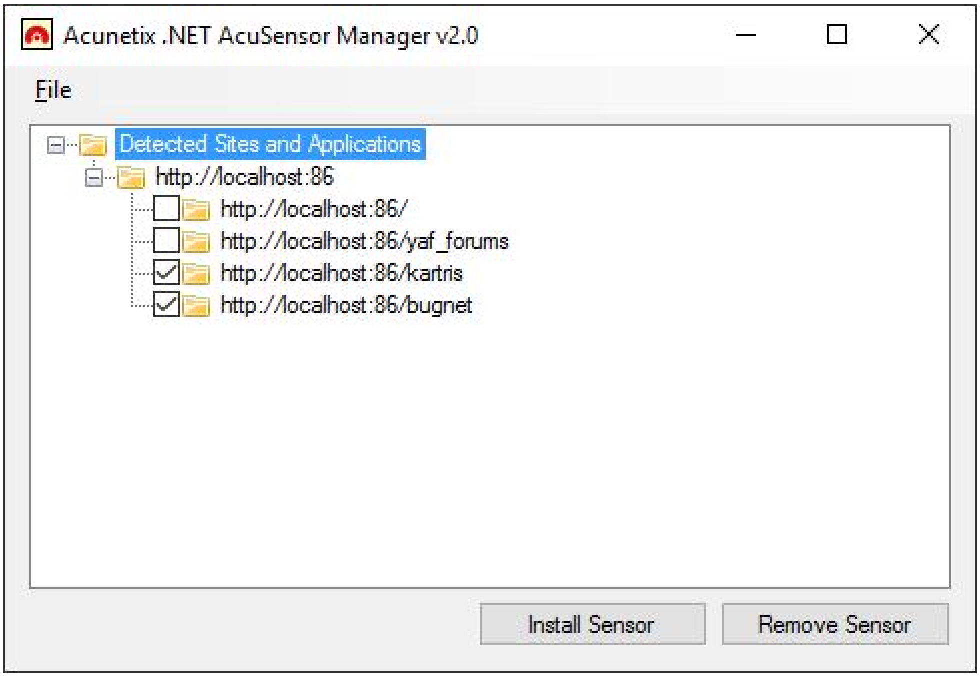
Acunetix .NET AcuSensor Manager v2.0 Setup

Welcome to the Acunetix .NET AcuSensor Manager v2.0 Setup Wizard

The Setup Wizard will install Acunetix .NET AcuSensor Manager v2.0 on your computer. Click Next to continue or Cancel to exit the Setup Wizard.

Screenshot – Acunetix .NET AcuSensor installation

3. Double click **AcuSensorInstaller.exe** to install the Acunetix .NET AcuSensor agent and proceed through the installation wizard.
4. You will be asked to insert the AcuSensor password. This should match the one that you used in the Acunetix settings.
5. After the installation is complete, you will be prompted to launch the Acunetix .NET AcuSensor Manager.



Detected Sites and Applications
- http://localhost:86
  - □ http://localhost:86/
  - □ http://localhost:86/yaf_forums
  - ☑ http://localhost:86/kartris
  - ☑ http://localhost:86/bugnet

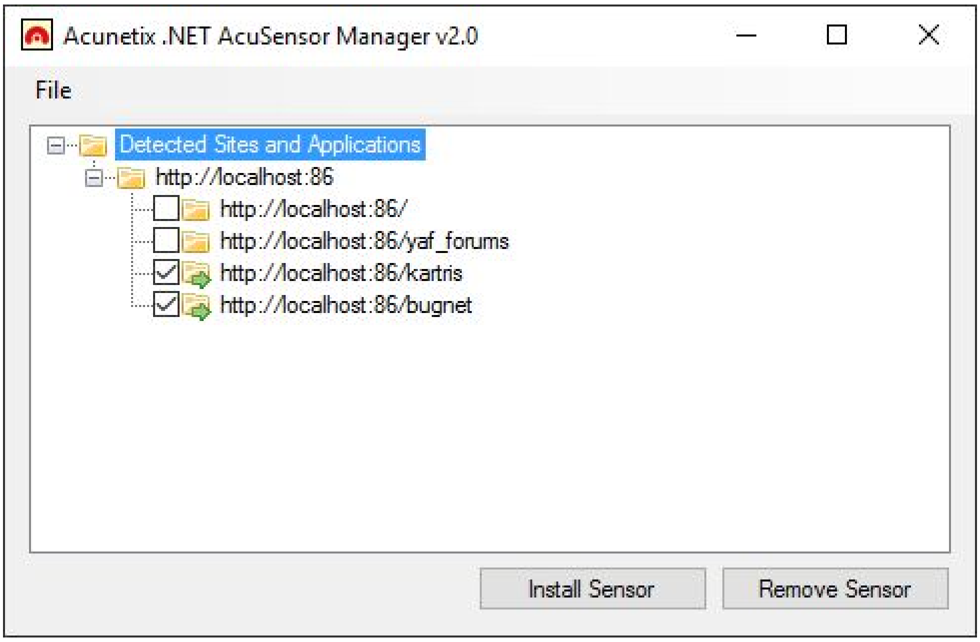
Screenshot – Acunetix .NET AcuSensor Manager

6. On start-up, the Acunetix .NET AcuSensor Manager will retrieve a list of .NET applications installed on your server. Select which applications you would like to enhance with the AcuSensor Technology and click **Install Sensor** to install the AcuSensor Technology sensor in the selected .NET applications. Once the sensor has been installed, close the confirmation window and also the AcuSensor manager.

Disabling and uninstalling AcuSensor for ASP .NET websites

To uninstall and disable the sensor from your web site:

1. From Start > Programs, open the Acunetix .NET AcuSensor Manager



Detected Sites and Applications
- http://localhost:86
  - □ http://localhost:86/
  - □ http://localhost:86/yaf_forums
  - ☑ http://localhost:86/kartris
  - ☑ http://localhost:86/bugnet

Screenshot - Select website and click Remove Sensor

2. Select the website where the AcuSensor agent is installed and click **Remove Sensor** to remove the AcuSensor Agent from the site.
3. Close the Acunetix .NET AcuSensor Manager.
4. If needed, you can also uninstall the Acunetix .NET AcuSensor Manager from the Add/Remove Programs Control Panel.

Note: Although the Acunetix AcuSensor agent are secured with a strong password, it is recommended that the AcuSensor client files are uninstalled and removed from the web application if they are no longer in use.

Installing the AcuSensor agent for JAVA websites

First, you need to download the AcuSensor agent for your Target.

The AcuSensor agent will need to be installed in your web application. This section describes how to install AcuSensor in a JAVA web application.

Acunetix JAVA Acusensor requires Tomcat (7+) and Java (1.7+)

1. Download the Acunetix JAVA AcuSensor from the Acunetix UI.

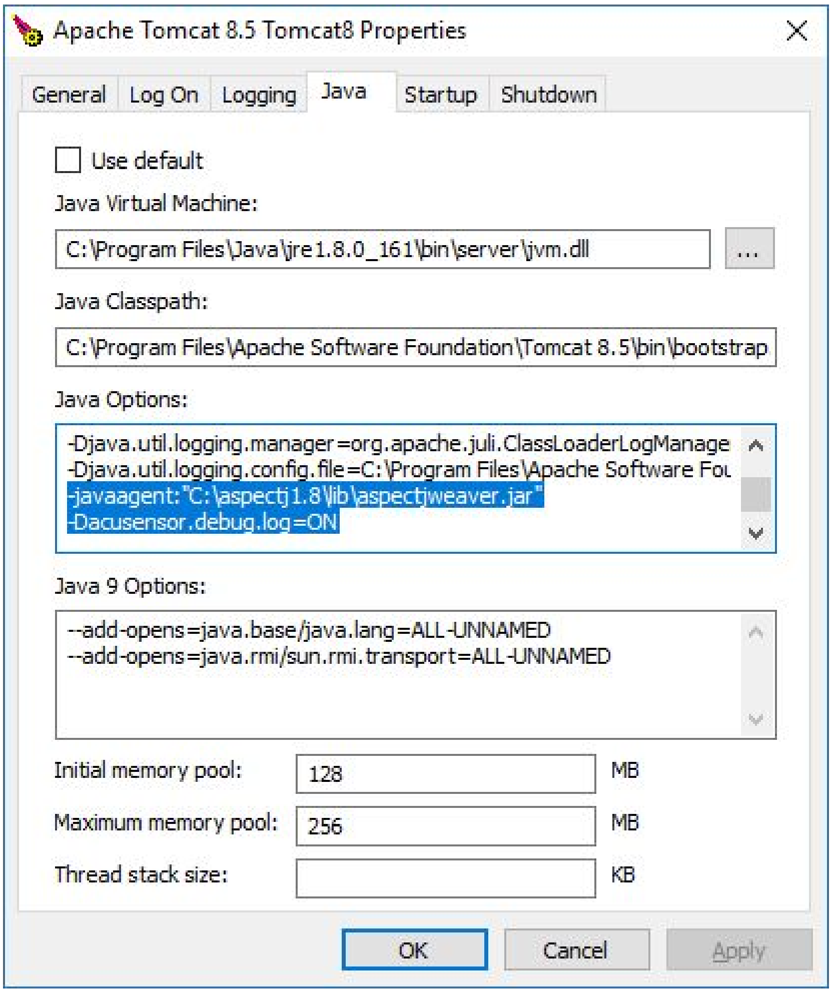
2. Copy the Acunetix JAVA AcuSensor (AcuSensor.jar) to %TOMCAT-HOME%\lib

3. Copy aspectjweaver.jar (included in the zip with this document) to any folder, e.g.: C:\aspectj1.8\lib

4. Launch Tomcat with Load Time Weaving enabled. This can be done by adding a **-javaagent** parameter with the path to aspectjweaver.jar when launching Tomcat as shown below in bold:

   ```
   java -javaagent:C:\aspectj1.8\lib\aspectjweaver.jar
   -Djava.util.logging.config.file=C:\apache-tomcat-8.5.15\conf\logging.properties
   -Djava.util.logging.manager=org.apache.juli.ClassLoaderLogManager
   "-Djdk.tls.ephemeralDHKeySize=2048"
   "-Djava.protocol.handler.pkgs=org.apache.catalina.webresources" -classpath
   "C:\apache-tomcat-8.5.15\bin\bootstrap.jar;C:\apache-tomcat-
   8.5.15\bin\tomcat-juli.jar" -Dcatalina.base=C:\apache-tomcat-8.5.15
   -Dcatalina.home=C:\apache-tomcat-8.5.15 -Djava.io.tmpdir=C:\apachetomcat-
   8.5.15\temp org.apache.catalina.startup.Bootstrap start
   ```

4. If Tomcat is started as a Windows service, you will need to specify the javaagent from Apache Tomcat Configuration > JAVA options tab.



□ Use default

Java Virtual Machine: C:\Program Files\Java\jre1.8.0_161\bin\server\jvm.dll

Java Classpath: C:\Program Files\Apache Software Foundation\Tomcat 8.5\bin\bootstrap

Java Options:

```
-Djava.util.logging.manager=org.apache.juli.ClassLoaderLogManage
-Djava.util.logging.config.file=C:\Program Files\Apache Software Fou
-javaagent:"C:\aspectj1.8\lib\aspectjweaver.jar"
-Dacusensor.debug.log=ON
```

Java 9 Options:

```
--add-opens=java.base/java.lang=ALL-UNNAMED
--add-opens=java.rmi/sun.rmi.transport=ALL-UNNAMED
```

Initial memory pool: 128 MB

Maximum memory pool: 256 MB

Thread stack size: KB

5. To enable extra debug logging add the following parameter when running tomcat *-Dacusensor.debug.log=ON*
   This will output AcuSensor logging in the Tomcat logs starting with: [Acunetix-debug]

Disabling and uninstalling AcuSensor for JAVA

To uninstall and disable the sensor from your website you need to revert the changes done during the installation of the Agent.:

1. Remove the Acunetix JAVA AcuSensor (AcuSensor.jar) to %TOMCAT-HOME%\lib
2. Remove aspectjweaver.jar from the folder where it was copied to
3. Stop launching Tomcat with Load Time Weaving enabled. This can be done by removing the **-javaagent** parameter with the path to aspectjweaver.jar
4. If Tomcat is started as a Windows service, you will need to remove the javaagent parameter from Apache Tomcat Configuration > JAVA options tab

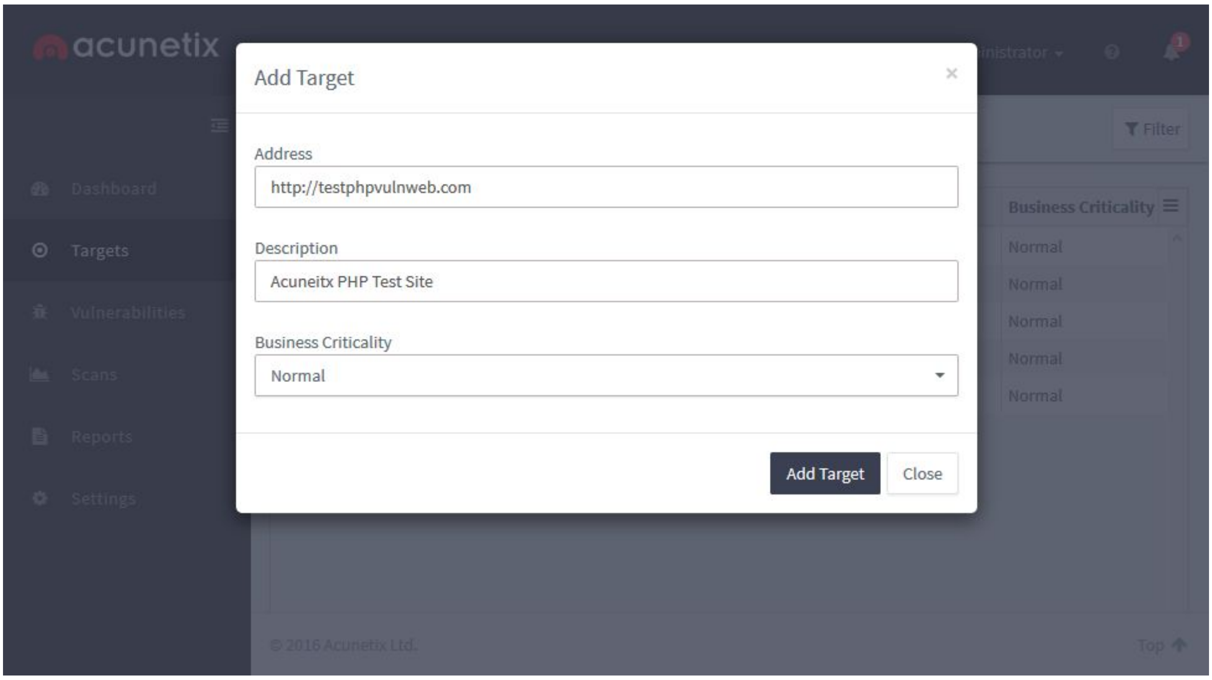
Note: Although the Acunetix AcuSensor agent are secured with a strong password, it is recommended that the AcuSensor client files are uninstalled and removed from the web application if they are no longer in use.

Configuring Targets

Targets are the websites and web applications that you would like to scan using Acunetix. In Acunetix Online, you can also configure Network assets as Targets. These will need to be configured in Acunetix before they can be scanned. Once configured, a Target can be scanned as often as required.

Change to the Targets page to configure a new website to scan.:

1. From the Targets' page, select 'Add Target'.



Add Target

Address: http://testphpvulnweb.com

Description: Acuneitx PHP Test Site

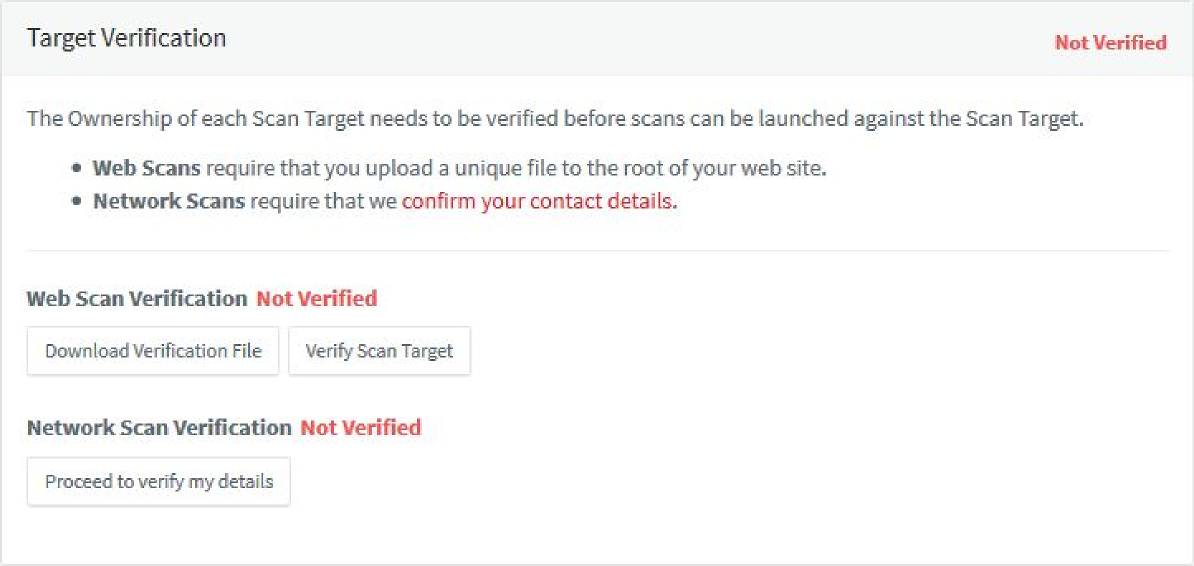
Business Criticality: Normal

Screenshot - Add Target

2. Provide the address of the asset to scan
3. Optionally, enter a short description that will allow you to easily identify this target.
4. Click 'Add Target' when done.
5. You will be taken to the Target's options, where you can configure other options if needed.

Verifying Scan Target Ownership (Acunetix Online only)

Once you create a new Target, you will be asked to verify ownership of the Target. Target verification will depend on the type of scans that you intend to launch against the Target.
In summary, web vulnerability scans require a unique verification file to be present in the root of the web server before a scan starts. This is required for all your Targets against which you wish to run web scans.
Network vulnerability scans require that we verify your account details; a one-time process where you may be contacted by an Acunetix representative.



Target Verification **Not Verified**

The Ownership of each Scan Target needs to be verified before scans can be launched against the Scan Target.

- **Web Scans** require that you upload a unique file to the root of your web site.
- **Network Scans** require that we confirm your contact details.

Web Scan Verification **Not Verified**

Network Scan Verification **Not Verified**

Screenshot - Scan Target Verification required

Web Scan Verification

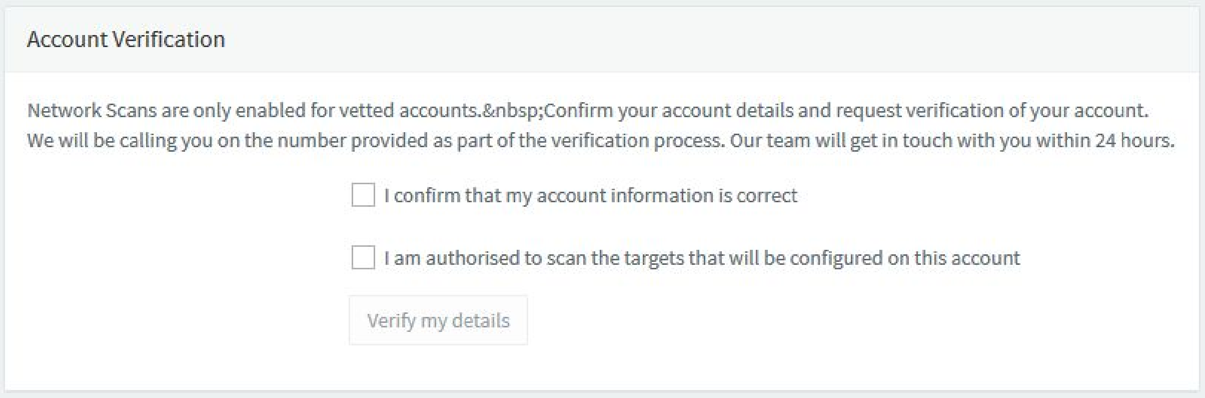
Web scan verification is a 3 step process.

1. Download the unique verification file assigned to your new Target.
2. Upload the verification file to the root of the site (using FTP for example).
3. From the configuration of the Target in Acunetix Online, click on 'Verify Scan Target' to complete the verification process.

Note: The verification file needs to be kept in the root of the site, since Acunetix Online will check the verification file each time it scans the server.

Network Scan Verification

1. For network scans you will need to verify that your account details are correct, and request verification of your account by an Acunetix representative.
2. From within the configuration of your scan target, in the Network Scan Verification, click ‘Proceed to verify my details’, or you can go directly to Account Settings > Profile.
3. Confirm that your account details are correct, and update as needed.



Account Verification

Network Scans are only enabled for vetted accounts. Confirm your account details and request verification of your account. We will be calling you on the number provided as part of the verification process. Our team will get in touch with you within 24 hours.

☐ I confirm that my account information is correct

☐ I am authorised to scan the targets that will be configured on this account

Screenshot - Verify account details

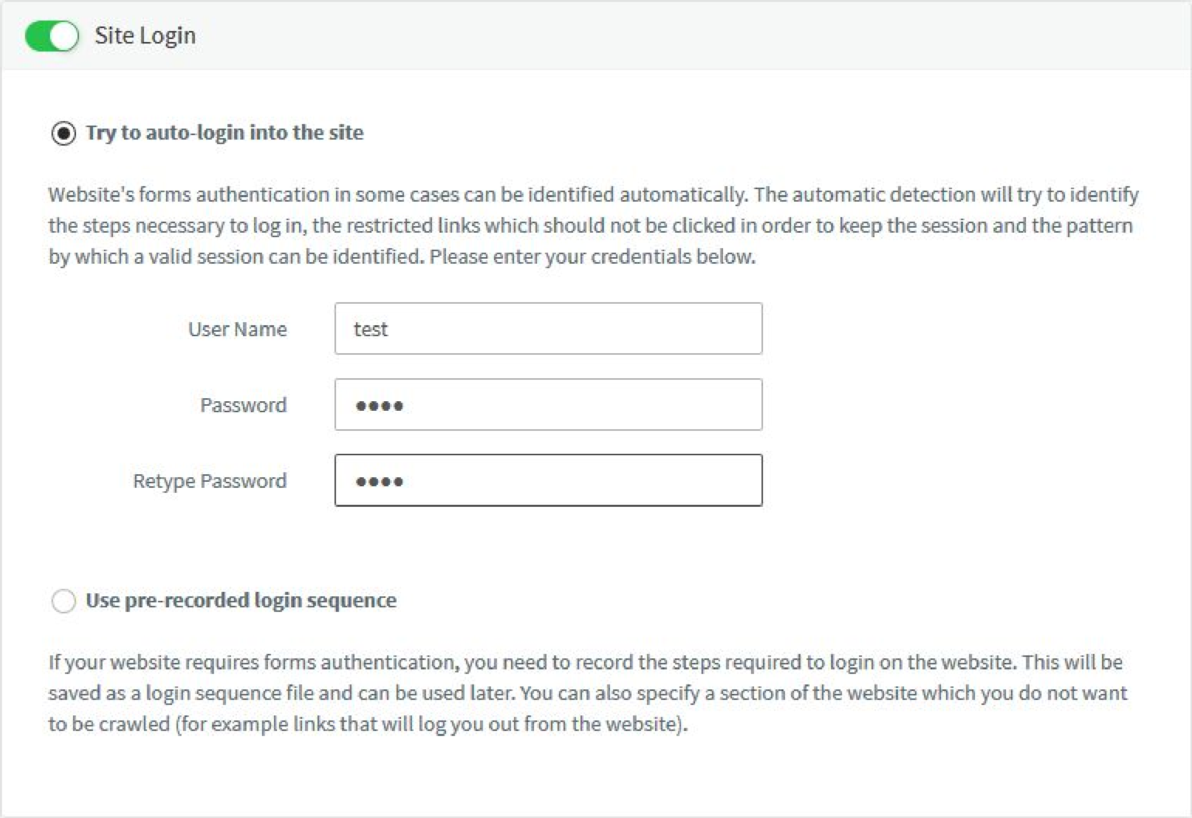
4. From within the Account Verification section, you can request the verification of your account details.

5. You will immediately receive an automatic call to the phone number specified, and will be given a one time code. You will need to enter this code into Acunetix as part of the account verification process.
6. An Acunetix representative may get in touch with you within 24 hours to complete the verification.
7. Once your account details have been verified, you can launch network vulnerability scans on all your scan targets.

Contact us at support@acunetix.com if you require help with the verification process.

Configuring Site Login

You may need to scan restricted areas within the web application configured as a Target in Acunetix. The information used to access the restricted area can be configured from the Site Login options found in the General Settings within the Target's configuration.



Site Login

● **Try to auto-login into the site**

Website's forms authentication in some cases can be identified automatically. The automatic detection will try to identify the steps necessary to log in, the restricted links which should not be clicked in order to keep the session and the pattern by which a valid session can be identified. Please enter your credentials below.

User Name: test

Password: ••••

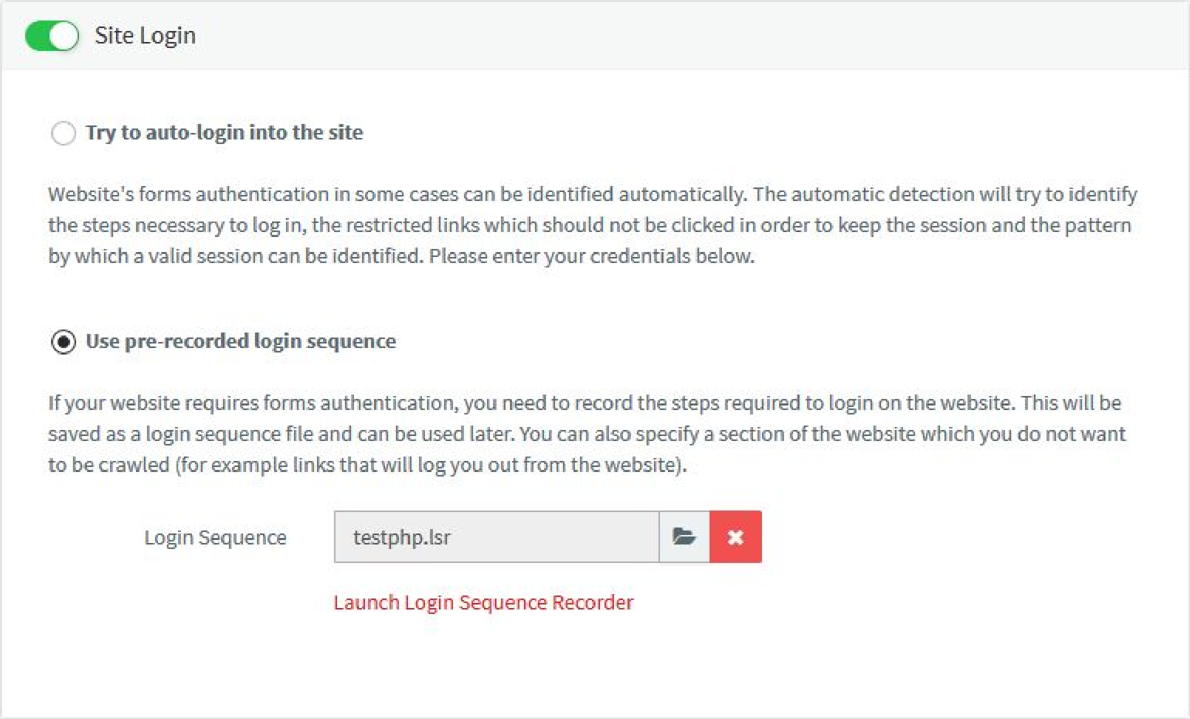
Retype Password: ••••

○ **Use pre-recorded login sequence**

If your website requires forms authentication, you need to record the steps required to login on the website. This will be saved as a login sequence file and can be used later. You can also specify a section of the website which you do not want to be crawled (for example links that will log you out from the website).

Screenshot - Form-based Authentication - Automated Login

In most cases, you can select to have Acunetix try to auto-login into the site. This will work for most web applications which use a simple login process. You need to provide the Username and Password to access the restricted area. The scanner will automatically detect the login link, the logout link and the mechanism used to maintain the session active.



Site Login

○ **Try to auto-login into the site**

Website's forms authentication in some cases can be identified automatically. The automatic detection will try to identify the steps necessary to log in, the restricted links which should not be clicked in order to keep the session and the pattern by which a valid session can be identified. Please enter your credentials below.

● **Use pre-recorded login sequence**

If your website requires forms authentication, you need to record the steps required to login on the website. This will be saved as a login sequence file and can be used later. You can also specify a section of the website which you do not want to be crawled (for example links that will log you out from the website).

Login Sequence: testphp.lsr

Screenshot - Form-based Authentication using Login Sequence Recorder

For more complex web applications, which might be using a more elaborate login mechanism, you would need to Launch the Login Sequence Recorder and record a login sequence (*.lsr file), which can then be uploaded and saved with your Target settings. Information on how to use the Login Sequence Recorder can be found at http://www.acunetix.com/blog/docs/acunetix-wvs-login-sequence-recorder/

Generating and Installing AcuSensor

AcuSensor improves the scan results provided by Acunetix by being able to identify all the pages on your website, increases the information about the vulnerabilities detected and decreases false positives. Check the previous section on how to install AcuSensor.

Other Advanced Options

For each Target, you can configure other options, including:

- Crawling options, such as using a custom User-Agent
- Paths to be excluded when scanning the specific target
- HTTP Authentication
- Client Certificates
- Custom Headers
- Custom Cookies
- List of Allowed hosts, which will be scanned when scanning the specific Target. Note that these need to pre-configured as separate Targets beforehand.

- Excluded Hours profile

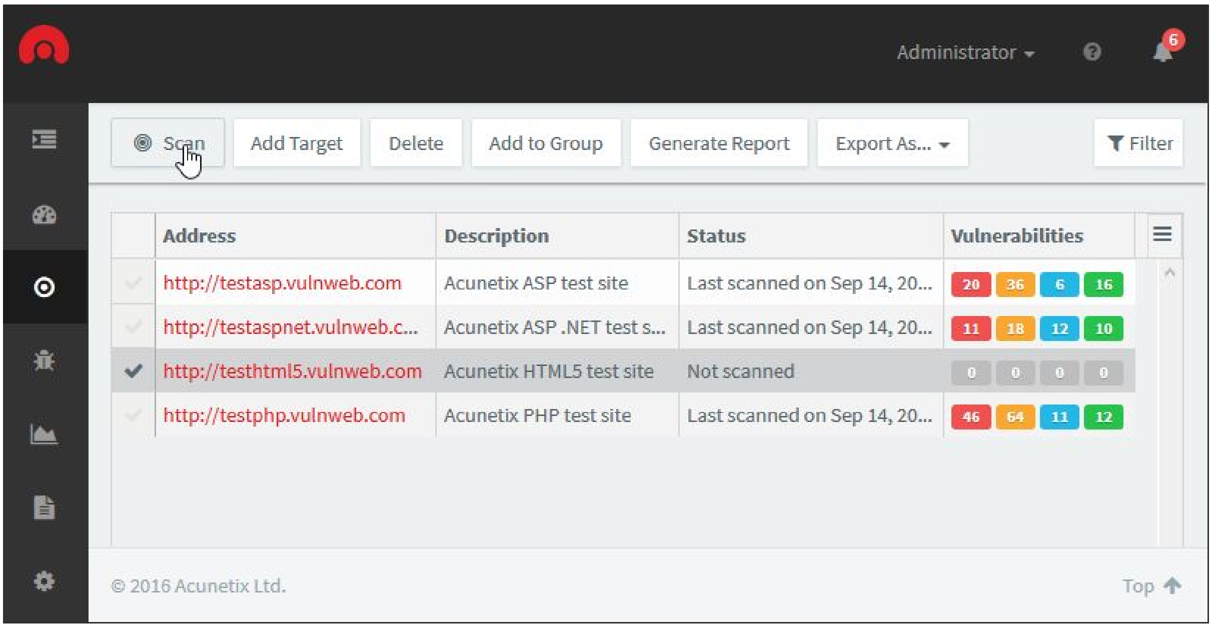
Launching Scans

NOTE: DO NOT SCAN A WEBSITE WITHOUT PROPER AUTHORIZATION!

The web server logs will show your IP address and all the attacks made by Acunetix. If you are not the sole administrator of the website or web application, please make sure to warn other administrators before performing a scan. Some scans might cause a website to crash, requiring a restart of the website.

After configuring your Targets, you are ready to launch Scans and start identifying any vulnerabilities that exist in the web applications. There are multiple ways to start a Scan, which include:

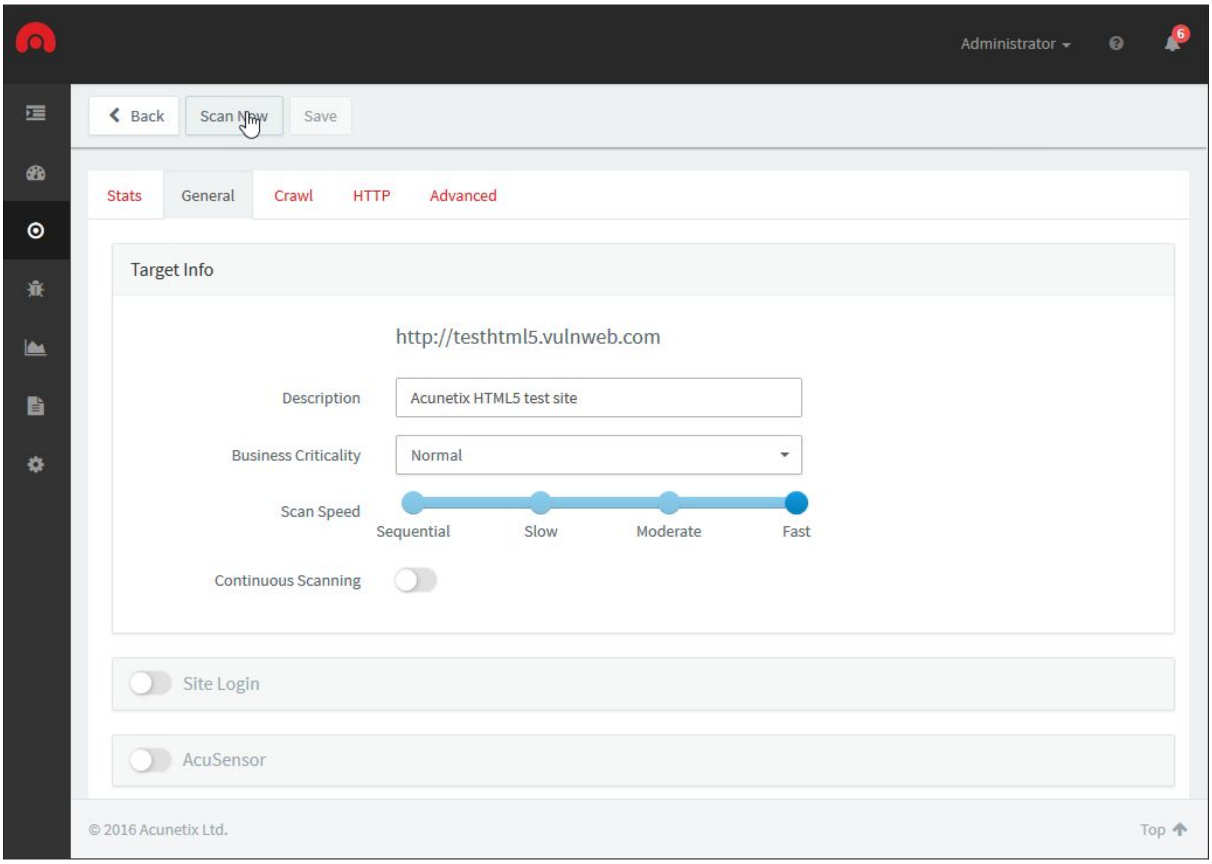
1. From the Targets list, select the Targets to scan, and click the Scan button



	Address	Description	Status	Vulnerabilities
	http://testasp.vulnweb.com	Acunetix ASP test site	Last scanned on Sep 14, 20...	20 36 6 16
	http://testaspnet.vulnweb.c...	Acunetix ASP .NET test s...	Last scanned on Sep 14, 20...	11 18 12 10
✓	http://testhtml5.vulnweb.com	Acunetix HTML5 test site	Not scanned	0 0 0 0
	http://testphp.vulnweb.com	Acunetix PHP test site	Last scanned on Sep 14, 20...	46 64 11 12

Screenshot - Select Target and click Scan

2. From within the Target’s settings, click the Scan Now button



http://testhtml5.vulnweb.com

Description: Acunetix HTML5 test site

Business Criticality: Normal

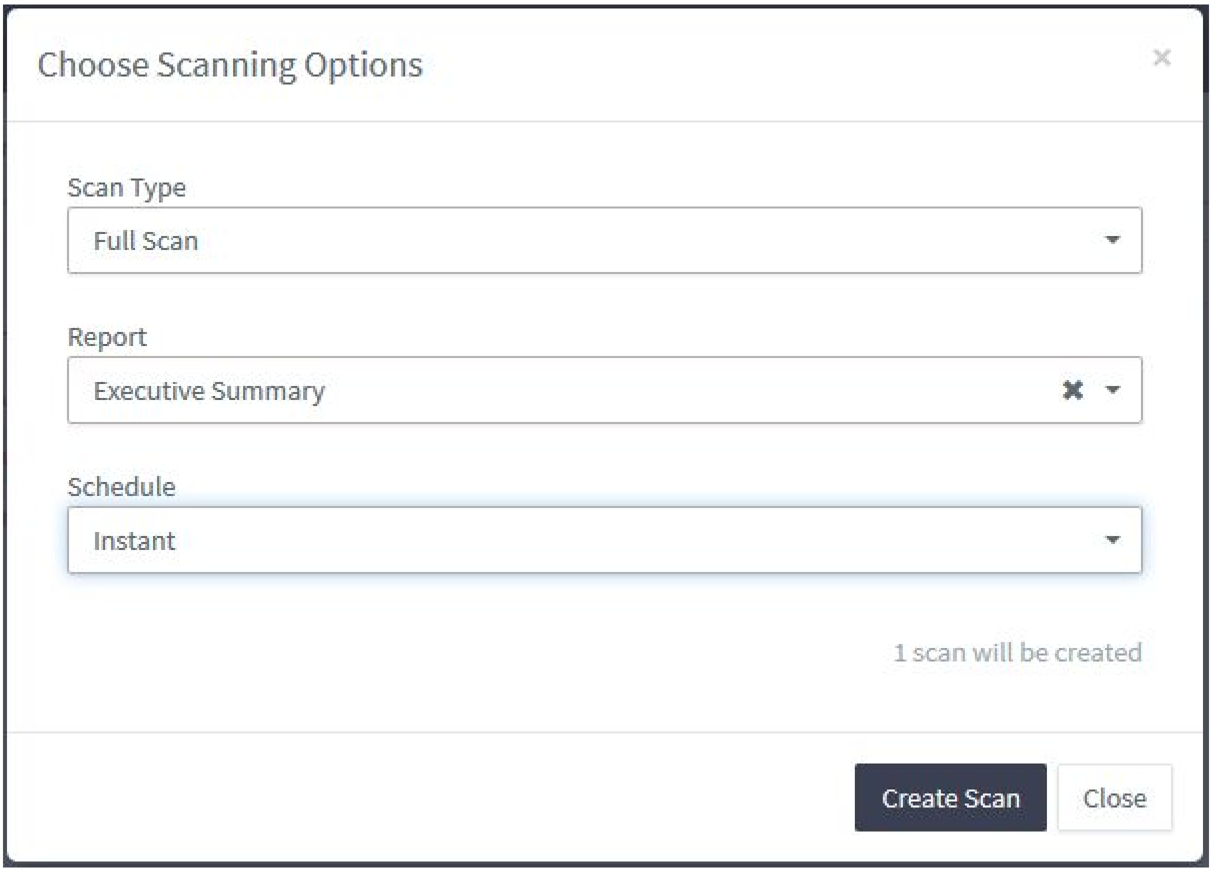
Scan Speed: ○ Sequential ○ Slow ○ Moderate ● Fast

Continuous Scanning

Screenshot - Select Target and click Scan

3. From the Scans page, click on New Scan. You will be asked to select the Targets to Scan.

After choosing the Target(s) to scan, configure the scan options to be used for the Scan.



Choose Scanning Options

Scan Type: Full Scan

Report: Executive Summary

Schedule: Instant

1 scan will be created

Screenshot - Choose scanning options

- **Scan Type** - Choose between Full Scan or a scanning profile which will scan for specific vulnerabilities, such as High Risk Vulnerabilities only. The Scan Types are described below
- **Report** - You can request that a report is automatically generated after the scan is completed. Here is a description of all the Reports
- **Schedule** - Select if the scan should start instantly, or if the scan should be scheduled for a future date / time. You can also configure to have a recurrent scan.

Scan Types

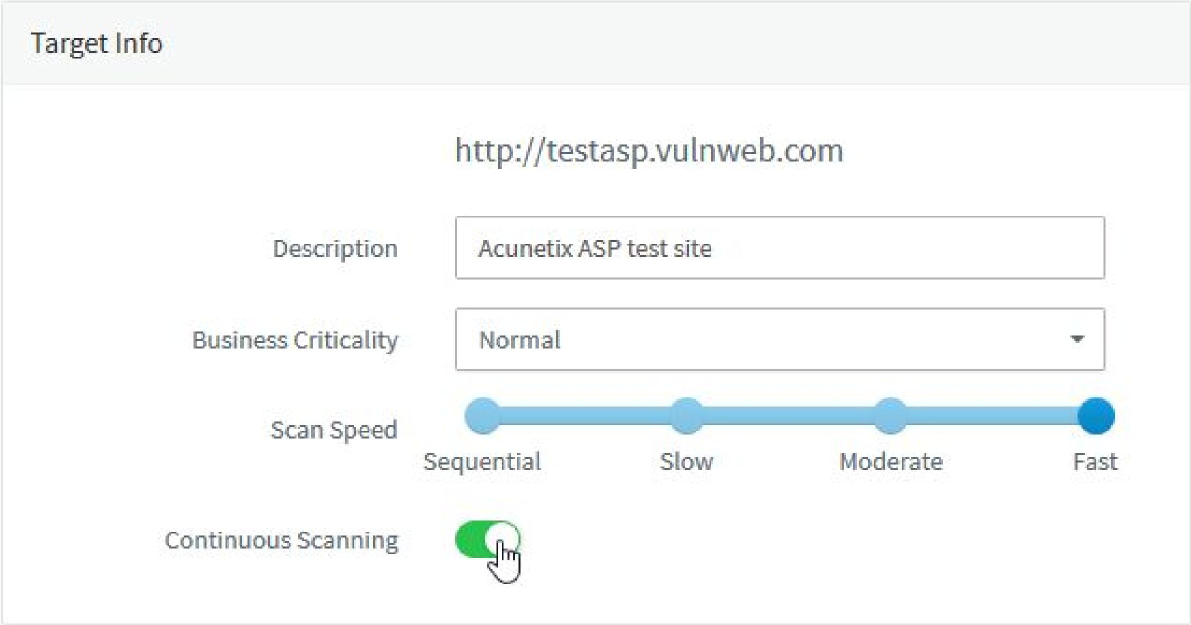
The Scan Types is a logical grouping of checks that Acunetix performs to scan for a specific category of vulnerabilities (such as Cross-Site Scripting, SQL Injection, etc.). Below is a list of scanning types available in Acunetix with a short description about each:

- **Full Scan -** Use the Full Scan profile to launch a scan using all the checks available in Acunetix.
- **High Risk Vulnerabilities** - The High Risk Alerts scanning profile will only check for the most dangerous web vulnerabilities.
- **Cross-Site Scripting (XSS)** - The XSS scanning profile will only check for Cross-Site Scripting vulnerabilities.
- **SQL Injection** - The SQL Injection scanning profile will only check for SQL Injection vulnerabilities.

- **Weak Passwords -** The Weak Passwords Scanning profile will identify forms which accept a username and password and will attack these forms.
- **Crawl Only -** The crawl only scan will only crawl the site and builds the structure of the site without running any vulnerability checks.

Continuous Scanning

After running the initial scan, identifying and fixing the vulnerabilities detected, and making sure that your Targets do not contain vulnerabilities, you need to ensure that they remain secure. Enable Continuous Scanning on a Target to have Acunetix scan the Target on a daily basis and report back any new vulnerabilities immediately. New vulnerabilities can be introduced by web developers making updates to the site or by administrators making changes the web server's configuration. In addition, Acunetix is often updated to detect new vulnerabilities.



Target Info

http://testasp.vulnweb.com

Description: Acunetix ASP test site

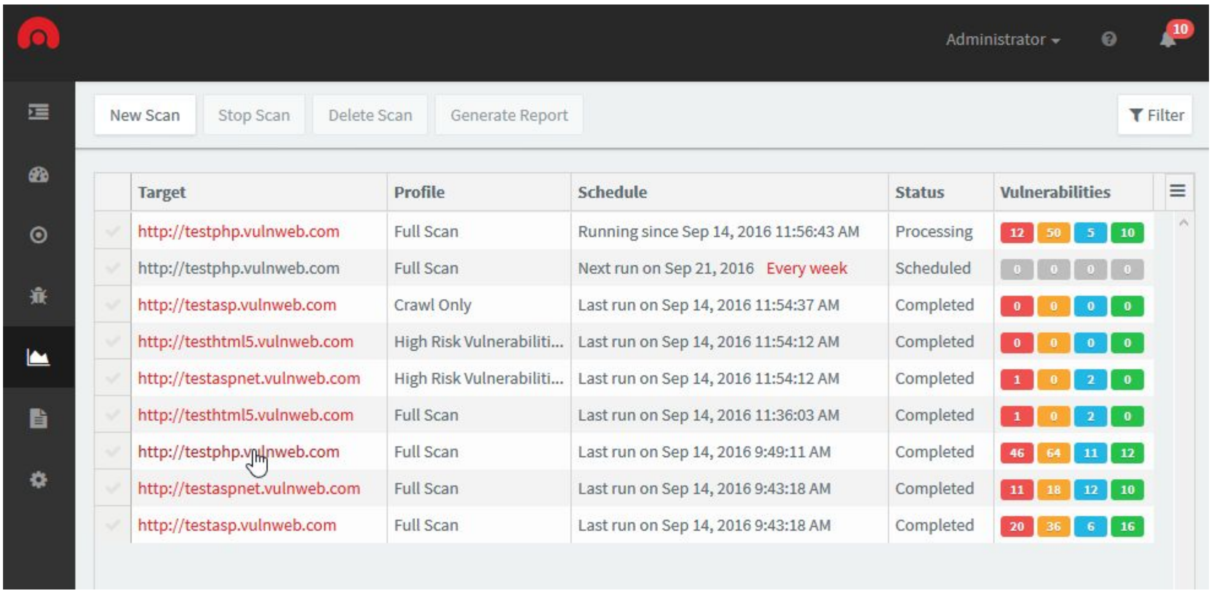
Business Criticality: Normal

Scan Speed: Fast

Continuous Scanning

Continuous Scanning performs a full scan once a week. This scan is augmented by a daily quick scan, which only scans for critical vulnerabilities. Continuous scans updates the vulnerabilities for the Target, and these can be accessed from the Vulnerabilities page. You will be notified by email and in the notification area when new vulnerabilities are identified.

Review Scan Results



Target	Profile	Schedule	Status	Vulnerabilities
http://testphp.vulnweb.com	Full Scan	Running since Sep 14, 2016 11:56:43 AM	Processing	12 50 5 10
http://testphp.vulnweb.com	Full Scan	Next run on Sep 21, 2016 Every week	Scheduled	0 0 0 0
http://testasp.vulnweb.com	Crawl Only	Last run on Sep 14, 2016 11:54:37 AM	Completed	0 0 0 0
http://testhtml5.vulnweb.com	High Risk Vulnerabiliti...	Last run on Sep 14, 2016 11:54:12 AM	Completed	0 0 0 0
http://testaspnet.vulnweb.com	High Risk Vulnerabiliti...	Last run on Sep 14, 2016 11:54:12 AM	Completed	1 0 2 0
http://testhtml5.vulnweb.com	Full Scan	Last run on Sep 14, 2016 11:36:03 AM	Completed	1 0 2 0
http://testphp.vulnweb.com	Full Scan	Last run on Sep 14, 2016 9:49:11 AM	Completed	46 64 11 12
http://testaspnet.vulnweb.com	Full Scan	Last run on Sep 14, 2016 9:43:18 AM	Completed	11 18 12 10
http://testasp.vulnweb.com	Full Scan	Last run on Sep 14, 2016 9:43:18 AM	Completed	20 36 6 16

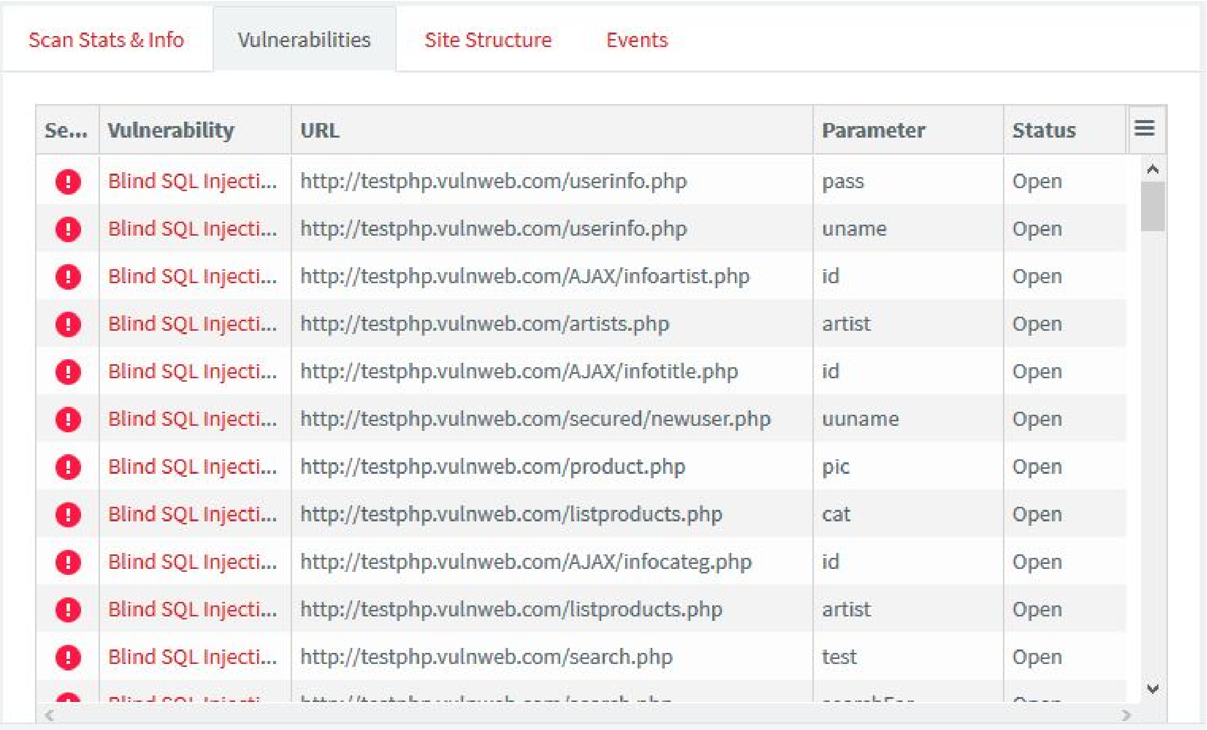
Screenshot - Scan List

Once the scan has finished, Acunetix will send you an email with a summary of the results and a link allowing you to access the scan results directly. The scan results show the start and end date of the scan, the duration of the scan and all the alerts that have been identified during the scan. The AcuSensor logo is also displayed when the scan detects and makes use of AcuSensor during a web scan.

The scan results consists of 4 sections:

- **Scan Stats & Info -** this provides an overview of the Target as detected by the scan, and information about the Scan, such as scan duration, average response time and the number of files scanned.

- **Vulnerabilities -** This is the list of vulnerabilities detected ordered by severity.

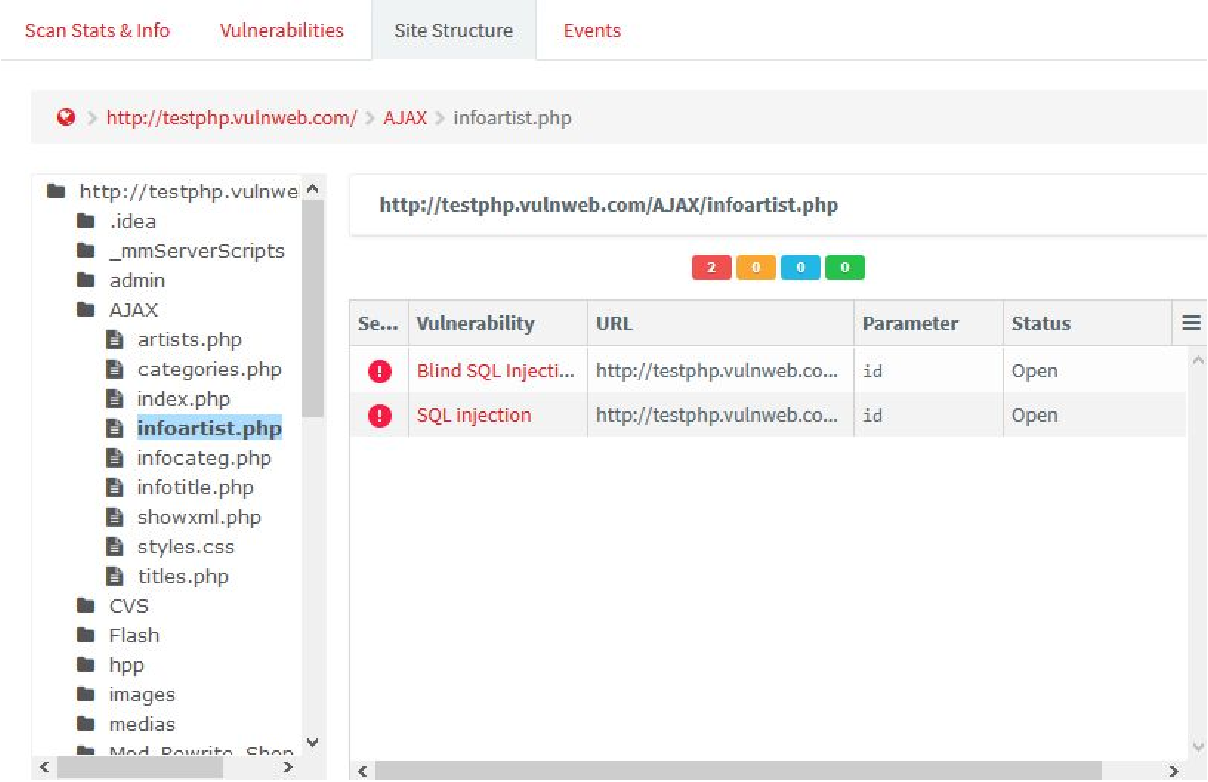


Scan Stats & Info | Vulnerabilities | Site Structure | Events

Se...	Vulnerability	URL	Parameter	Status
!	Blind SQL Injecti...	http://testphp.vulnweb.com/userinfo.php	pass	Open
!	Blind SQL Injecti...	http://testphp.vulnweb.com/userinfo.php	uname	Open
!	Blind SQL Injecti...	http://testphp.vulnweb.com/AJAX/infoartist.php	id	Open
!	Blind SQL Injecti...	http://testphp.vulnweb.com/artists.php	artist	Open
!	Blind SQL Injecti...	http://testphp.vulnweb.com/AJAX/infotitle.php	id	Open
!	Blind SQL Injecti...	http://testphp.vulnweb.com/secured/newuser.php	uuname	Open
!	Blind SQL Injecti...	http://testphp.vulnweb.com/product.php	pic	Open
!	Blind SQL Injecti...	http://testphp.vulnweb.com/listproducts.php	cat	Open
!	Blind SQL Injecti...	http://testphp.vulnweb.com/AJAX/infocateg.php	id	Open
!	Blind SQL Injecti...	http://testphp.vulnweb.com/listproducts.php	artist	Open
!	Blind SQL Injecti...	http://testphp.vulnweb.com/search.php	test	Open
!	Blind SQL Injecti...	http://testphp.vulnweb.com/search.php	searchFor	Open

Screenshot - List of Vulnerabilities detected by a scan

- **Site Structure -** You can use the site structure to ensure that Acunetix has covered all the site, and to identify vulnerabilities affecting a specific file or folder of the site scanned. Click on the folder icon to expand the site structure tree.



Scan Stats & Info | Vulnerabilities | Site Structure | Events

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

- http://testphp.vulnwe
  - .idea
  - _mmServerScripts
  - admin
  - AJAX
    - artists.php
    - categories.php
    - index.php
    - infoartist.php
    - infocateg.php
    - infotitle.php
    - showxml.php
    - styles.css
    - titles.php
  - CVS
  - Flash
  - hpp
  - images
  - medias
  - Mod_Rewrite_Shop

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

2 0 0 0

Se...	Vulnerability	URL	Parameter	Status
!	Blind SQL Injecti...	http://testphp.vulnweb.co...	id	Open
!	SQL injection	http://testphp.vulnweb.co...	id	Open

Screenshot - Site Structure

- **Events -** A list of events related to scan. This will show when the scan started and finished, and if any errors have been encountered during the scan.

Alerts (vulnerabilities) discovered

One of the key components of the scan results is the list of all vulnerabilities found in the scan target during the scan. Depending on the type of scan, these can be either Web Alerts or Network Alerts, and the alerts are categorized according to 4 severity levels:

High High Risk Alert Level 3 – Vulnerabilities categorized as the most dangerous, which put the scan target at maximum risk for hacking and data theft.

Medium Medium Risk Alert Level 2 – Vulnerabilities caused by server misconfiguration and site-coding flaws, which facilitate server disruption and intrusion.

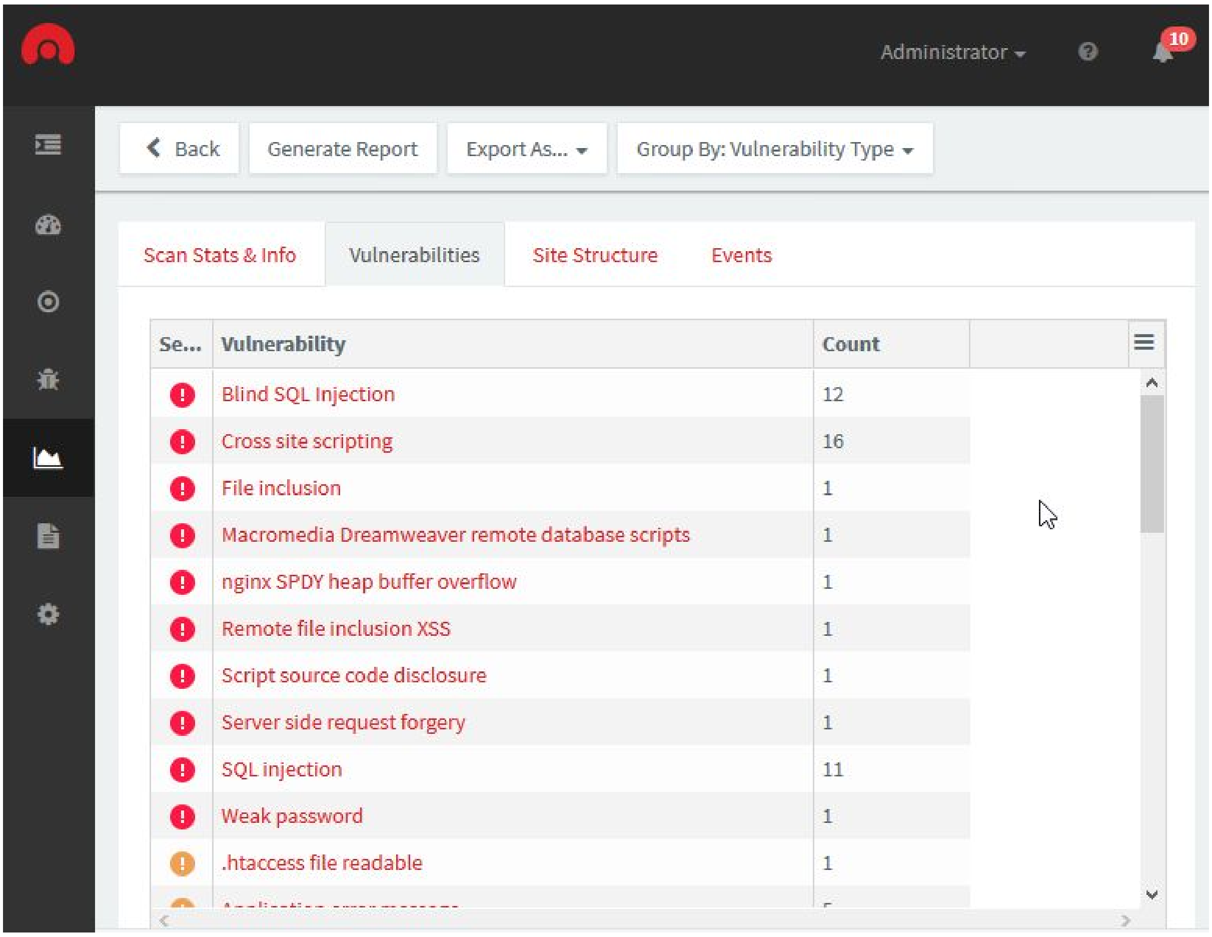
Low Low Risk Alert Level 1 – Vulnerabilities derived from lack of encryption of data traffic or directory path disclosures.

Informational Informational Alert – These are items which have been discovered during a scan and which are deemed to be of interest, e.g. the possible disclosure of an internal IP address or email address, or matching a search string found in the Google Hacking Database, or information on a service that has been discovered during the scan.

Depending on the type of vulnerability, additional information about the vulnerability is shown when you click on an alert category node:

- **Vulnerability description** - A description of the discovered vulnerability.
- **Affected items** - The list of files or components which are affected by the alert.
- **The impact of this vulnerability** – Level of impact on the website, web server or perimeter server if this vulnerability is exploited.
- **Attack details** - Details about the parameters and variables used to test for this vulnerability. E.g. for a Cross Site Scripting alert, the name of the exploited input variable and the string it was set to will be displayed. You can also find the HTTP request sent to the web server and the response sent back by the web server (including the HTML response).
- **How to fix this vulnerability** - Guidance on how to fix the vulnerability.
- **Classification** - Apart from the Acunetix classification, this section provides classification by CVSS (v2 and v3) score and CWE enumeration id.
- **Detailed information** - More information on what is causing the reported vulnerability, with examples where applicable.
- **Web references** - A list of web links to external sources providing more information on the vulnerability to help you understand and fix it.

Grouping of Vulnerabilities



Se...	Vulnerability	Count
!	Blind SQL Injection	12
!	Cross site scripting	16
!	File inclusion	1
!	Macromedia Dreamweaver remote database scripts	1
!	nginx SPDY heap buffer overflow	1
!	Remote file inclusion XSS	1
!	Script source code disclosure	1
!	Server side request forgery	1
!	SQL injection	11
!	Weak password	1
!	.htaccess file readable	1
!	Application error message	5

Screenshot – Grouping of vulnerabilities

The list of vulnerabilities detected can be grouped by the vulnerability type. If the same type of vulnerability is detected on multiple pages, the scanner will group them under one alert node. Clicking on one of the vulnerabilities will filter the list to show only the instances for the specific vulnerability.

Vulnerabilities Detected by AcuMonitor

An Acunetix scan makes use of AcuMonitor to detect certain vulnerabilities such as Blind XSS, Email Header Injection, and certain types of SSRF, XXE and Host Header Attacks. AcuMonitor can only detect some of these vulnerabilities after the scan has finished. When this happens, AcuMonitor will update the scan results with the new vulnerabilities detected and you will receive an email notifying you that the scan results have been updated. More information on AcuMontor can be found at http://www.acunetix.com/vulnerability-scanner/acumonitor-blind-xss-detection/.

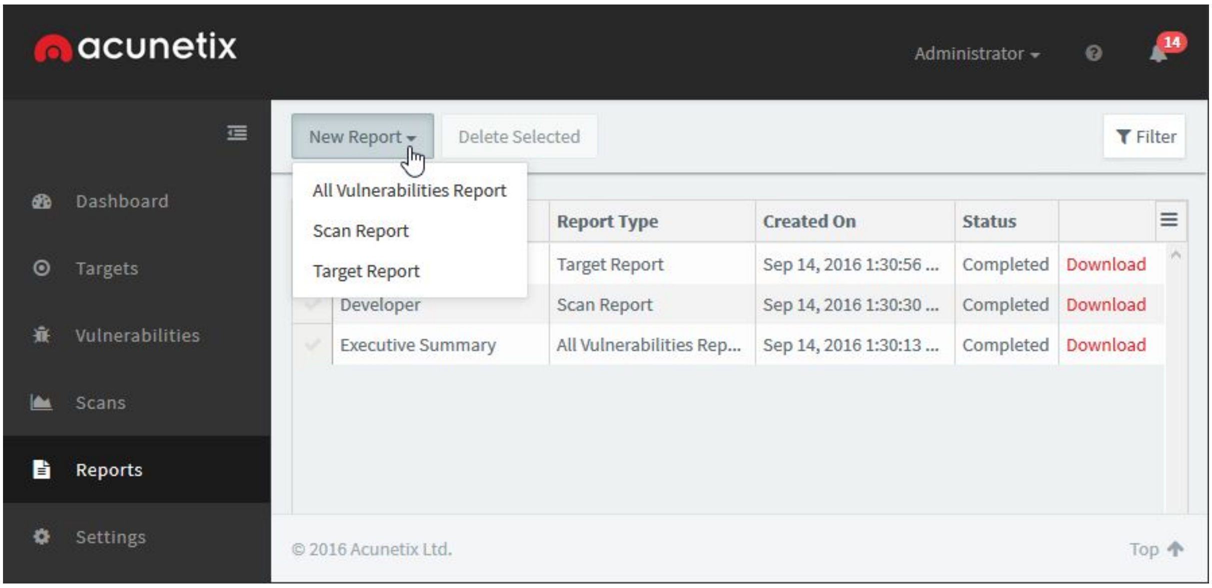
Exporting Scan Results to WAFs

The detection of vulnerabilities on a web application is the first step. Ideally these vulnerabilities are fixed as soon as possible, however experience shows that this is not always the case. In this case, it is ideal if the risk that vulnerabilities create is mitigated.

An Acunetix scan can be exported to a format supported by the most popular Web Application Firewalls (WAFs), including:

- F5 Big-IP Application Security Manager (ASM)
- Imperva SecureSphere WAF
- Fortinet Fortiweb
- Generic XML export

Generating Reports



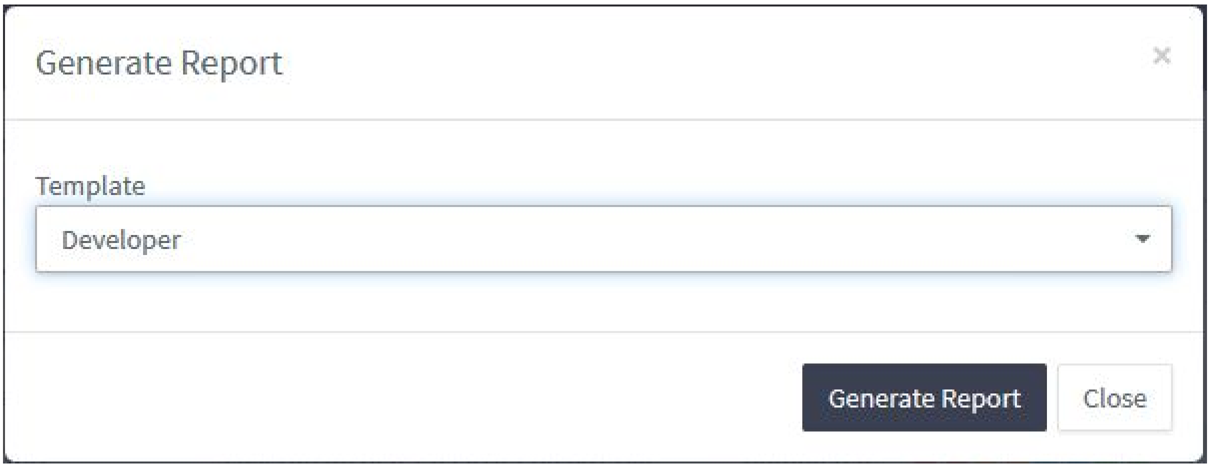
	Report Type	Created On	Status	
	Target Report	Sep 14, 2016 1:30:56 ...	Completed	Download
Developer	Scan Report	Sep 14, 2016 1:30:30 ...	Completed	Download
Executive Summary	All Vulnerabilities Rep...	Sep 14, 2016 1:30:13 ...	Completed	Download

Screenshot - Create a new report

From the Reports page, there are 3 types of reports that can be generated:

- **All Vulnerabilities report -** report on all the vulnerabilities detected on all the Targets configured in Acunetix
- **Scan Report -** report on the vulnerabilities detected by one or multiple scans. When 2 scans for the same Target are selected, you will be given the option to compare the scans when generating the report (by selecting the Scan Comparison report template)
- **Target Report -** report on all the vulnerabilities detected on one or multiple Targets taking into consideration all the scans done on the target(s).

Reports can also be generated directly from the Targets page, the Vulnerabilities page or the Scans page.



Generate Report

Template: Developer

Screenshot - Generate a Report

After choosing what to report on, you will need to choose a report template. The format of the report, the detail included, and the grouping used in the report are determined by the report template. Report templates are described in the next section.

After choosing to generate the report, you will then be taken to the Saved Reports. The report might take a few seconds to generate. The PDF or HTML report can be downloaded by clicking on the Download link, which becomes available when Acunetix has finished generating the report.

Acunetix Reports

The following is a list of the reports that can be generated in Acunetix:

Affected Items Report

The Affected Items report shows the files and locations where vulnerabilities have been detected during a scan. The report shows the severity of the vulnerability detected, together with other details about how the vulnerability has been detected.

Developer Report

The Developer Report is targeted to developers who need to work on the website in order to address the vulnerabilities discovered by Acunetix. The report provides information on the files which have a long response time, a list of external links, email addresses, client scripts and external hosts, together with remediation examples and best practice recommendations for fixing the vulnerabilities.

Executive Report

The Executive Report summarizes the vulnerabilities detected in a website and gives a clear overview of the severity level of vulnerabilities found in the website.

Quick Report

The Quick Report provides a detailed listing of all the vulnerabilities discovered during the scan.

Scan Comparison

The Scan Comparison report allows you to compare two scans on the same Target, highlighting the differences between the scans. This report template will only become available when 2 scans for the same Target are selected.

Compliance Reports

Compliance Reports are available for the following compliance bodies and standards:

CWE / SANS - Top 25 Most Dangerous Software Errors

This report shows a list of vulnerabilities that have been detected in your website which are listed in the CWE / SANS top 25 most dangerous software errors. These errors are often easy to find and exploit and are dangerous because they will often allow attackers to take over the website or steal data. More information can be found at http://cwe.mitre.org/top25/.

The Health Insurance Portability and Accountability Act (HIPAA)

Part of the HIPAA Act defines the policies, procedures and guidelines for maintaining the privacy and security of individually identifiable health information. This report identifies the vulnerabilities that might be infringing these policies. The vulnerabilities are grouped by the sections as defined in the HIPAA Act.

International Standard - ISO 27001

ISO 27001, part of the ISO / IEC 27000 family of standards, formally specifies a management system that is intended to bring information security under explicit management control. This report identifies vulnerabilities which might be in violation of the standard and groups the vulnerabilities by the sections defined in the standard.

NIST Special Publication 800-53

NIST Special Publication 800-53 covers the recommended security controls for the Federal Information Systems and Organizations. Once again, the vulnerabilities identified during a scan are grouped by the categories as defined in the publication.

OWASP Top10 2017

The Open Web Application Security Project (OWASP) is web security project led by an international community of corporations, educational institutions and security researchers. OWASP is renown for its work in web security, specifically through its list of top 10 web security risks to avoid. This report shows which of the detected vulnerabilities are found on the OWASP top 10 vulnerabilities.

Payment Card Industry (PCI) standards

The Payment Card Industry Data Security Standard (PCI DSS) is an information security standard, which applies to organizations that handle credit card holder information. This report identifies vulnerabilities which might breach parts of the standard and groups the vulnerabilities by the requirement that has been violated.

Sarbanes Oxley Act

The Sarbanes Oxley Act was enacted to prevent fraudulent financial activities by corporations and top management. Vulnerabilities which are detected during a scan which might lead to a breach in sections of the Act are listed in this report.

DISA STIG Web Security

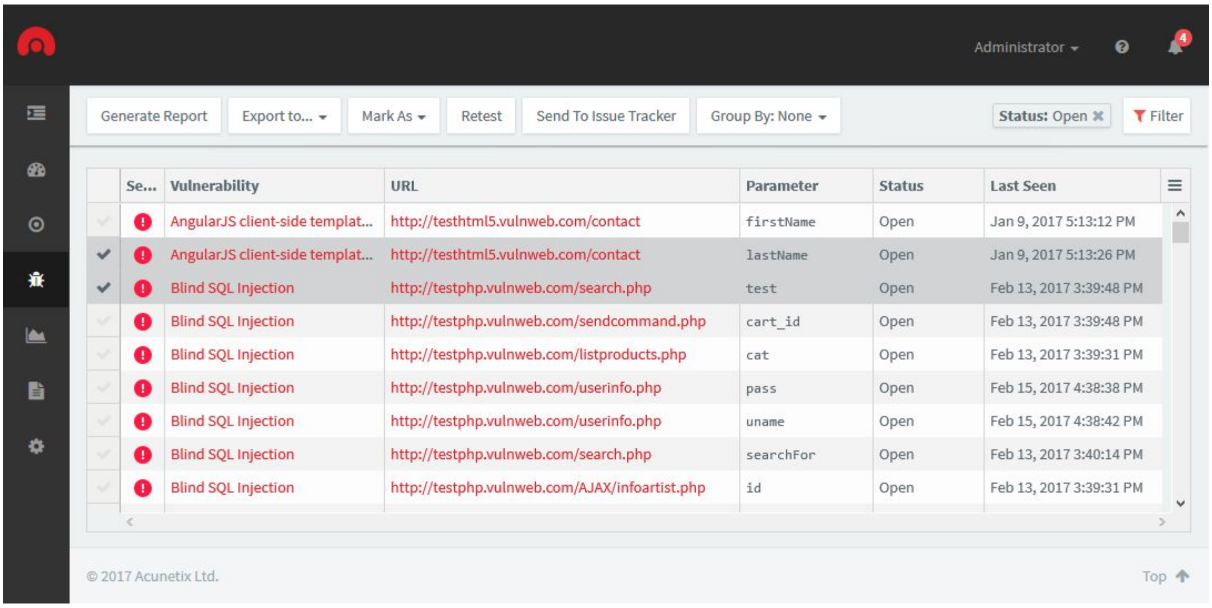
The Security Technical Implementation Guide (STIG) is a configuration guide for computer software and hardware defined by the Defense Information System Agency (DISA), which part of the United States Department of Defense. This report identifies vulnerabilities which violate sections of STIG and groups the vulnerabilities by the sections of the STIG guide which are being violated.

Web Application Security Consortium (WASC) Threat Classification

The Web Application Security Consortium (WASC) is a non-profit organization made up of an international group of security experts, which has created a threat classification system for web vulnerabilities. This report groups the vulnerabilities identified on your site using the WASC threat classification system.

Managing Vulnerabilities

The detection of vulnerabilities is the first step to securing your web applications. The vulnerabilities detected need to be managed and eventually fixed. Acunetix provides the means to help you prioritise and manage vulnerabilities.

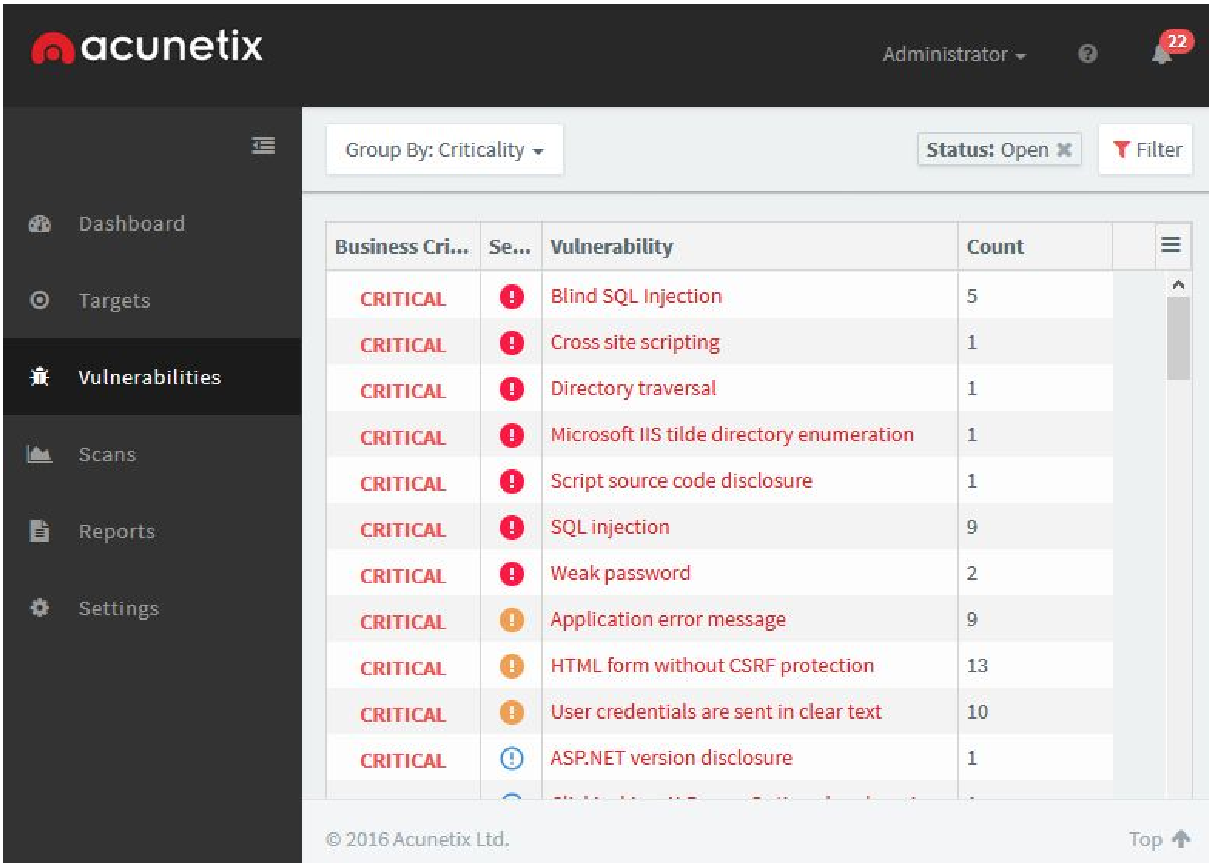


	Se...	Vulnerability	URL	Parameter	Status	Last Seen
	!	AngularJS client-side templat...	http://testhtml5.vulnweb.com/contact	firstName	Open	Jan 9, 2017 5:13:12 PM
✓	!	AngularJS client-side templat...	http://testhtml5.vulnweb.com/contact	lastName	Open	Jan 9, 2017 5:13:26 PM
✓	!	Blind SQL Injection	http://testphp.vulnweb.com/search.php	test	Open	Feb 13, 2017 3:39:48 PM
	!	Blind SQL Injection	http://testphp.vulnweb.com/sendcommand.php	cart_id	Open	Feb 13, 2017 3:39:48 PM
	!	Blind SQL Injection	http://testphp.vulnweb.com/listproducts.php	cat	Open	Feb 13, 2017 3:39:31 PM
	!	Blind SQL Injection	http://testphp.vulnweb.com/userinfo.php	pass	Open	Feb 15, 2017 4:38:38 PM
	!	Blind SQL Injection	http://testphp.vulnweb.com/userinfo.php	uname	Open	Feb 15, 2017 4:38:42 PM
	!	Blind SQL Injection	http://testphp.vulnweb.com/search.php	searchFor	Open	Feb 13, 2017 3:40:14 PM
	!	Blind SQL Injection	http://testphp.vulnweb.com/AJAX/infoartist.php	id	Open	Feb 13, 2017 3:39:31 PM

Screenshot - Vulnerabilities List

The Vulnerabilities page provides a list of all the vulnerabilities detected by Acunetix. By default, the vulnerabilities are sorted by Business Criticality of the target the vulnerability was detected on, and the severity assigned to the vulnerability by Acunetix. This will help you focus on the most important vulnerabilities, without losing sight of the less important ones.

Grouping and Filtering Vulnerabilities



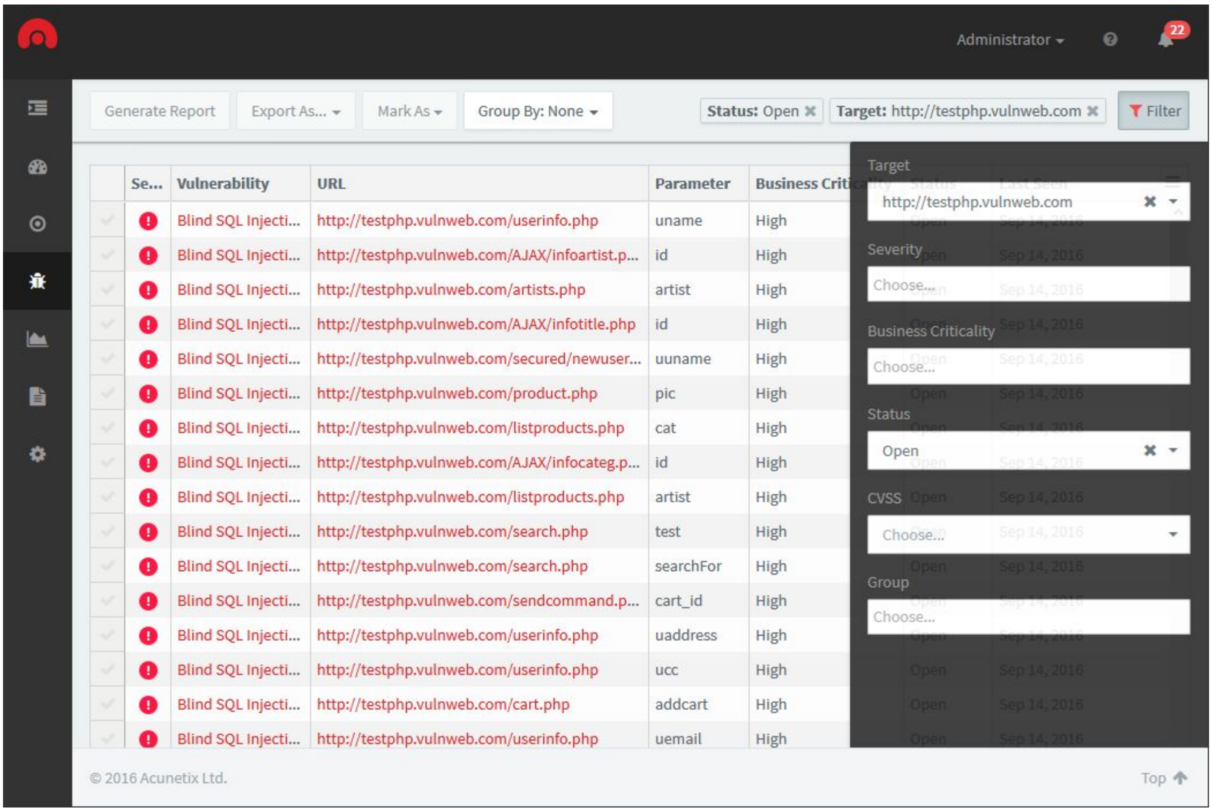
Business Cri...	Se...	Vulnerability	Count
CRITICAL	!	Blind SQL Injection	5
CRITICAL	!	Cross site scripting	1
CRITICAL	!	Directory traversal	1
CRITICAL	!	Microsoft IIS tilde directory enumeration	1
CRITICAL	!	Script source code disclosure	1
CRITICAL	!	SQL injection	9
CRITICAL	!	Weak password	2
CRITICAL	!	Application error message	9
CRITICAL	!	HTML form without CSRF protection	13
CRITICAL	!	User credentials are sent in clear text	10
CRITICAL	!	ASP.NET version disclosure	1

Screenshot - Grouping by Business Criticality

As the amount of vulnerabilities detected increases, the list of vulnerabilities can become cumbersome to manage. For this reason, the vulnerabilities can be grouped or filtered.

Vulnerabilities can be grouped either by **Business Criticality** or by **Vulnerability Type**. Grouping by Business Criticality gives priority the vulnerabilities occurring on web applications which are of higher importance to the organisation. Grouping by Vulnerability Type prioritises the vulnerabilities using the severity assigned by Acunetix.

Vulnerabilities can be filtered by Target, Severity, Target's Business Criticality, Status, CVSS, and Target Group. The list allows for multiple flexible filters, e.g. show all the high severity Vulnerabilities, identified on a specific Target, which are still open.



Status: Open ✖ Target: http://testphp.vulnweb.com ✖

Se...	Vulnerability	URL	Parameter	Business Criti
!	Blind SQL Injecti...	http://testphp.vulnweb.com/userinfo.php	uname	High
!	Blind SQL Injecti...	http://testphp.vulnweb.com/AJAX/infoartist.p...	id	High
!	Blind SQL Injecti...	http://testphp.vulnweb.com/artists.php	artist	High
!	Blind SQL Injecti...	http://testphp.vulnweb.com/AJAX/infotitle.php	id	High
!	Blind SQL Injecti...	http://testphp.vulnweb.com/secured/newuser...	uuname	High
!	Blind SQL Injecti...	http://testphp.vulnweb.com/product.php	pic	High
!	Blind SQL Injecti...	http://testphp.vulnweb.com/listproducts.php	cat	High
!	Blind SQL Injecti...	http://testphp.vulnweb.com/AJAX/infocateg.p...	id	High
!	Blind SQL Injecti...	http://testphp.vulnweb.com/listproducts.php	artist	High
!	Blind SQL Injecti...	http://testphp.vulnweb.com/search.php	test	High
!	Blind SQL Injecti...	http://testphp.vulnweb.com/search.php	searchFor	High
!	Blind SQL Injecti...	http://testphp.vulnweb.com/sendcommand.p...	cart_id	High
!	Blind SQL Injecti...	http://testphp.vulnweb.com/userinfo.php	uaddress	High
!	Blind SQL Injecti...	http://testphp.vulnweb.com/userinfo.php	ucc	High
!	Blind SQL Injecti...	http://testphp.vulnweb.com/cart.php	addcart	High
!	Blind SQL Injecti...	http://testphp.vulnweb.com/userinfo.php	uemail	High

Target: http://testphp.vulnweb.com

Severity: Choose...

Business Criticality: Choose...

Status: Open

CVSS: Choose...

Group: Choose...

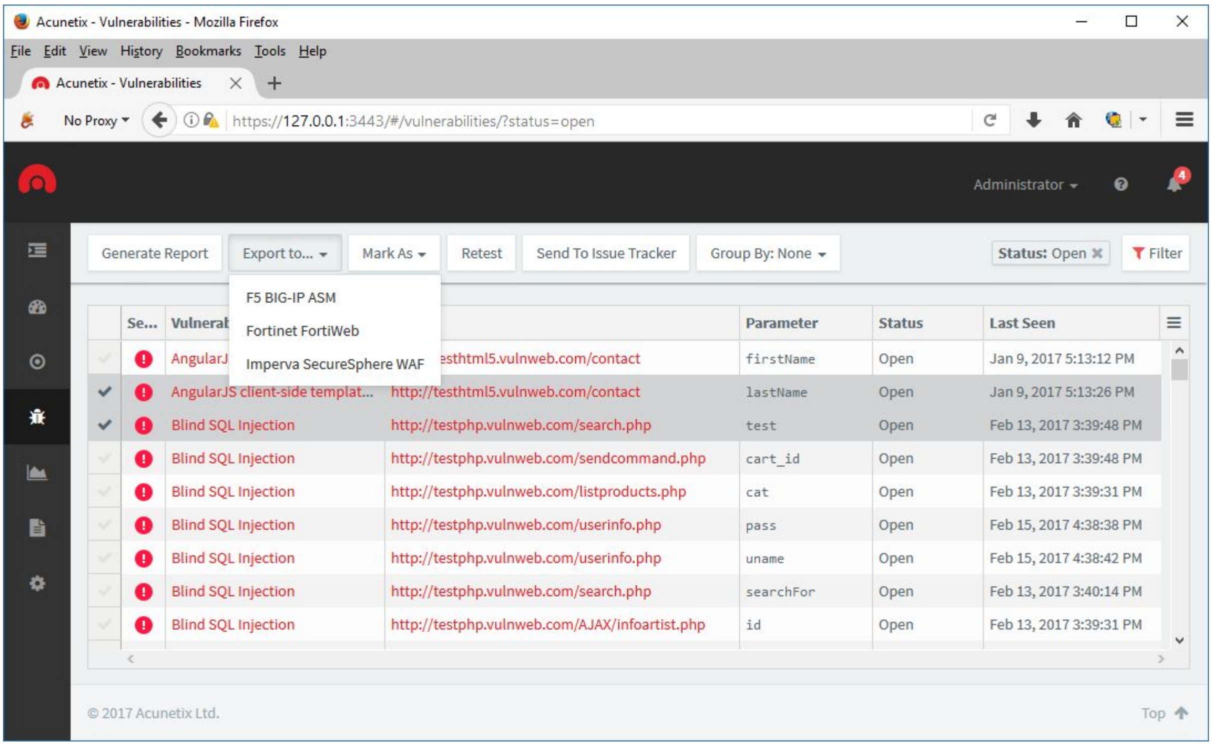
© 2016 Acunetix Ltd.

Screenshot - Filtered vulnerabilities

Import vulnerabilities into your Web Application Firewall (WAF)

Ideally, vulnerabilities are fixed as soon as possible. Unfortunately, it often takes months to fix a vulnerability. If you make use of a Web Application Firewall (WAF) supported by Acunetix, you can export vulnerabilities from Acunetix and import them into your WAF. Your WAF will be able to provide virtual patching for the vulnerability.

Acunetix supports exporting vulnerabilities for F5 BIG-IP ASM, Fortinet FortiWeb and Imperva SecureSphere WAF.



Se...	Vulnerab		Parameter	Status	Last Seen
	AngularJ	esthtml5.vulnweb.com/contact	firstName	Open	Jan 9, 2017 5:13:12 PM
✓	AngularJS client-side templat...	http://testhtml5.vulnweb.com/contact	lastName	Open	Jan 9, 2017 5:13:26 PM
✓	Blind SQL Injection	http://testphp.vulnweb.com/search.php	test	Open	Feb 13, 2017 3:39:48 PM
	Blind SQL Injection	http://testphp.vulnweb.com/sendcommand.php	cart_id	Open	Feb 13, 2017 3:39:48 PM
	Blind SQL Injection	http://testphp.vulnweb.com/listproducts.php	cat	Open	Feb 13, 2017 3:39:31 PM
	Blind SQL Injection	http://testphp.vulnweb.com/userinfo.php	pass	Open	Feb 15, 2017 4:38:38 PM
	Blind SQL Injection	http://testphp.vulnweb.com/userinfo.php	uname	Open	Feb 15, 2017 4:38:42 PM
	Blind SQL Injection	http://testphp.vulnweb.com/search.php	searchFor	Open	Feb 13, 2017 3:40:14 PM
	Blind SQL Injection	http://testphp.vulnweb.com/AJAX/infoartist.php	id	Open	Feb 13, 2017 3:39:31 PM

Sending Vulnerabilities to an Issue Tracker

For a developer, vulnerabilities are considered as bugs in the web application. Acunetix provides to means to send the vulnerabilities to the issue tracker used by the organisation, allowing for better tracking of vulnerabilities by the development team.

You will first need to configure the issue tracker in the Acunetix settings, and assign the Issue Tracker to the Target. You will then be able to send vulnerabilities detected for the specific Target to the Issue Tracker.

Acunetix supports GitHub, Jira and Microsoft TFS issue trackers

Retesting Vulnerabilities

When a vulnerability has been fixed, you can have Acunetix confirm the fix by selecting the vulnerability and clicking on the Retest option. This will create a new scan using a custom scanning profile restricted to the specific vulnerability.

Closing Vulnerabilities

Vulnerabilities detected by Acunetix remain in the vulnerabilities list until they are marked as not open. You can remove vulnerabilities from the list of open vulnerabilities by marking them as:

Fixed - This status is given to vulnerabilities that are fixed by the developers. If the vulnerability is found again by Acunetix, the vulnerability will be re-opened, and marked as Rediscovered
False Positive - There are situations where a vulnerability is incorrectly detected by Acunetix. The vulnerability will not be reported again in future scans.
Ignored - This status can be used for vulnerabilities which are not False Positives, but which for some reason should be ignored in future scans.

Vulnerabilities marked as False Positives or Ignored can be re-opened manually at any time.

Configuring General Settings

From the general settings page, you can configure product updates settings, proxy settings, notification settings, users and target groups.

Product Updates

Acunetix frequently releases updates which consist of new features, bug fixes and updates to the vulnerabilities database. You can configure Acunetix to Download and install updates automatically, or have Acunetix notify you when new updates are available.

Proxy Settings

You can configure Acunetix to use a proxy server if this is required to connect to the Internet. This will affect product updates, license activation requests and AcuMonitor requests. Specify the protocol, proxy address and port and optionally username and password to be used to connect to the proxy server.

Notification Settings

The mail server settings are used by Acunetix to send email notifications such as when a scan is complete, license notifications, or forgot password emails. Here you can configure the SMTP server’s address, port, from address, security protocol used, and any authentication if needed.

Users

The management of Acunetix users is explained here.

Target Groups

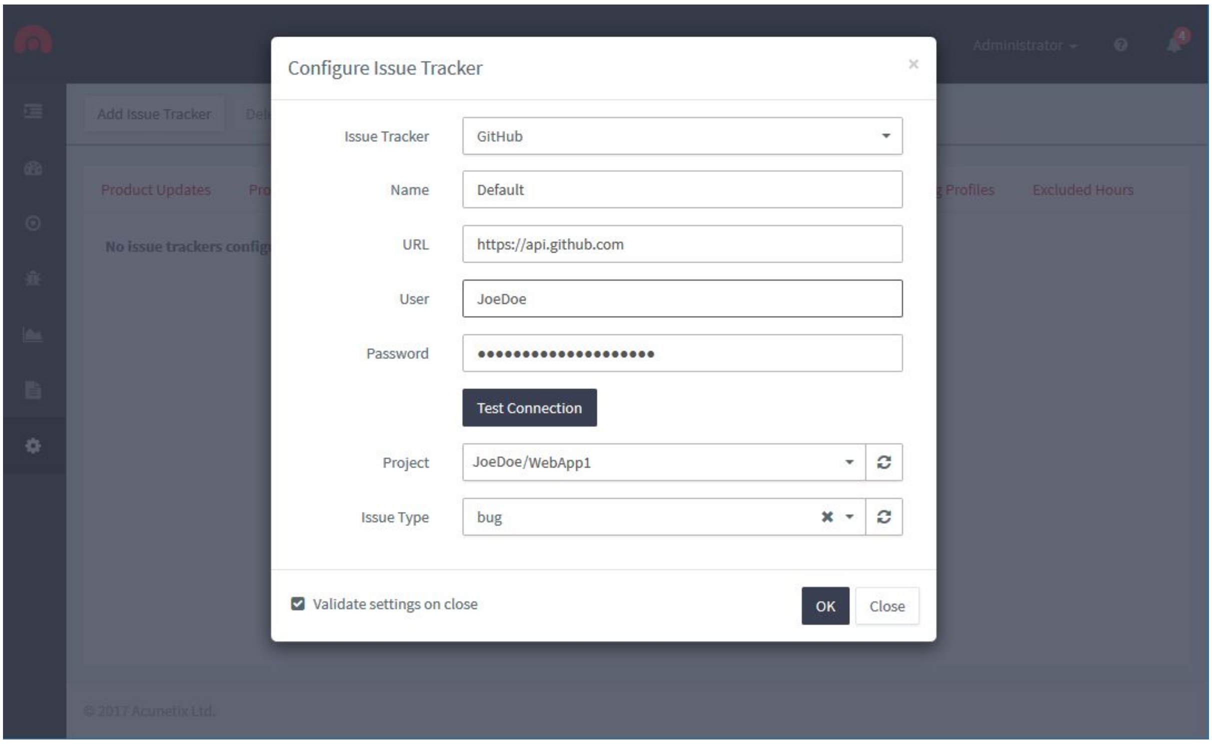
Targets can be grouped for easier management. For example, from the Vulnerabilities page, you can filter for the vulnerabilities of one Target Group, or in the Scan page, you can filter for scans of a specific Target Group. Users accounts are also given access to specific Target Groups.

You will first need to create the Target Group, after which, you can configure target group membership for the Target Group.

Issue Trackers

Acunetix supports sending vulnerabilities to an issue tracker. You will first need to configure the settings of the issue tracker in Acunetix. Proceed as follows:

1. Select the Issue Tracker you are using
2. Provide a Name for the issue tracker. This name will be used to when selecting the issue tracker for the Target
3. Provide the URL and credentials to access the issue tracker, and click Test Connection
4. Select the Project in which issues should be logged.
5. Select the Issue Type to be used by Acunetix when logging an issue.



Configure Issue Tracker

Issue Tracker: GitHub

Name: Default

URL: https://api.github.com

User: JoeDoe

Password: ••••••••••••••••••••

Project: JoeDoe/WebApp1

Issue Type: bug

☑ Validate settings on close

Screenshot - Configure Issue Tracker

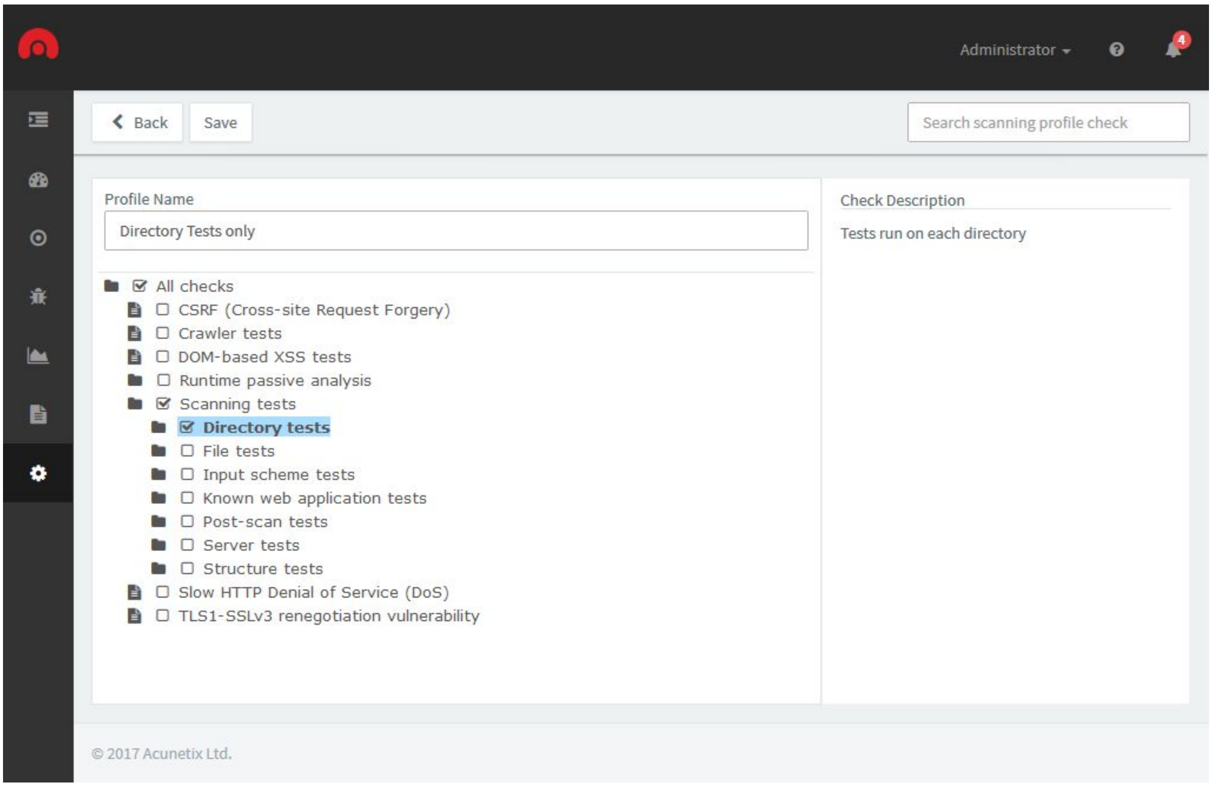
After configuring the issue tracker, you can assign the issue tracker to a Target from the target’s settings.

Acunetix supports sending issues to Github, Jira and Microsoft TFS.

Scan Types

Acunetix installs with a default set of Scanning Profiles, which allow you to scan for specific types of vulnerabilities. If you need to be more granular in your scans, you can create your own custom scanning profiles which check for specific vulnerabilities. Proceed as follows:

1. Click the Create Profile button
2. Provide a name for the profile.
3. Select the vulnerabilities as needed.
   You can search for vulnerabilities using the search field. You can also click on the folder icons to expand the folders.
4. Click Save when done.



Profile Name: Directory Tests only

Check Description: Tests run on each directory

- ☑ All checks
  - ☐ CSRF (Cross-site Request Forgery)
  - ☐ Crawler tests
  - ☐ DOM-based XSS tests
  - ☐ Runtime passive analysis
  - ☑ Scanning tests
    - ☑ Directory tests
    - ☐ File tests
    - ☐ Input scheme tests
    - ☐ Known web application tests
    - ☐ Post-scan tests
    - ☐ Server tests
    - ☐ Structure tests
  - ☐ Slow HTTP Denial of Service (DoS)
  - ☐ TLS1-SSLv3 renegotiation vulnerability

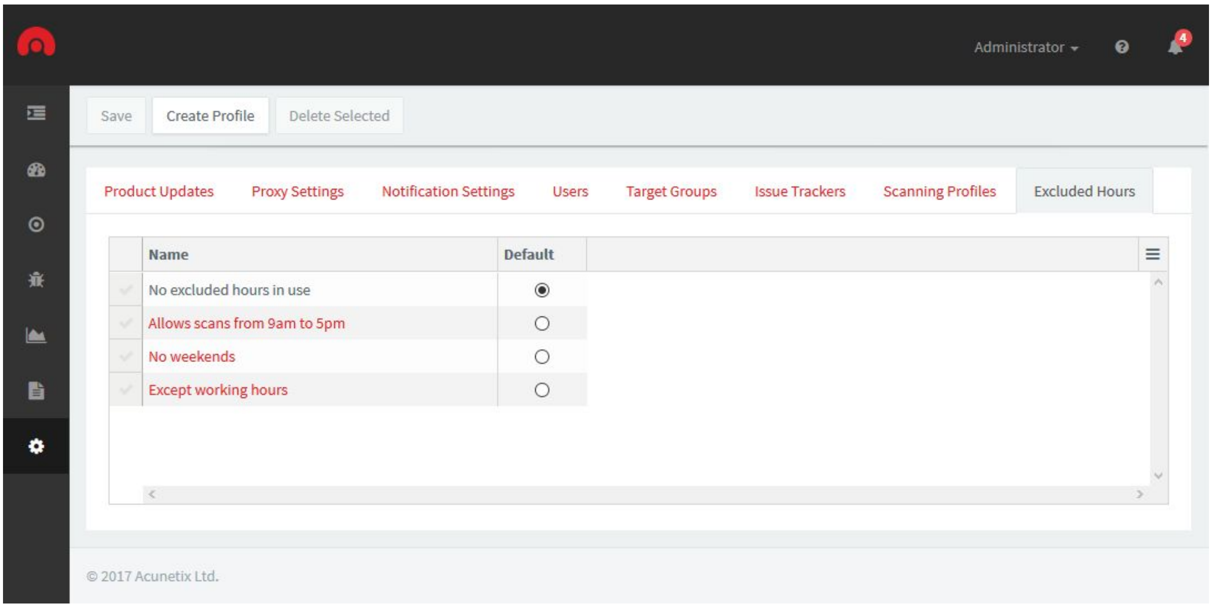
© 2017 Acunetix Ltd.

Screenshot - Custom Scanning Profile

When starting a new scan, you can choose your custom scanning profiles in the Scan Type selection..

Excluded Hours

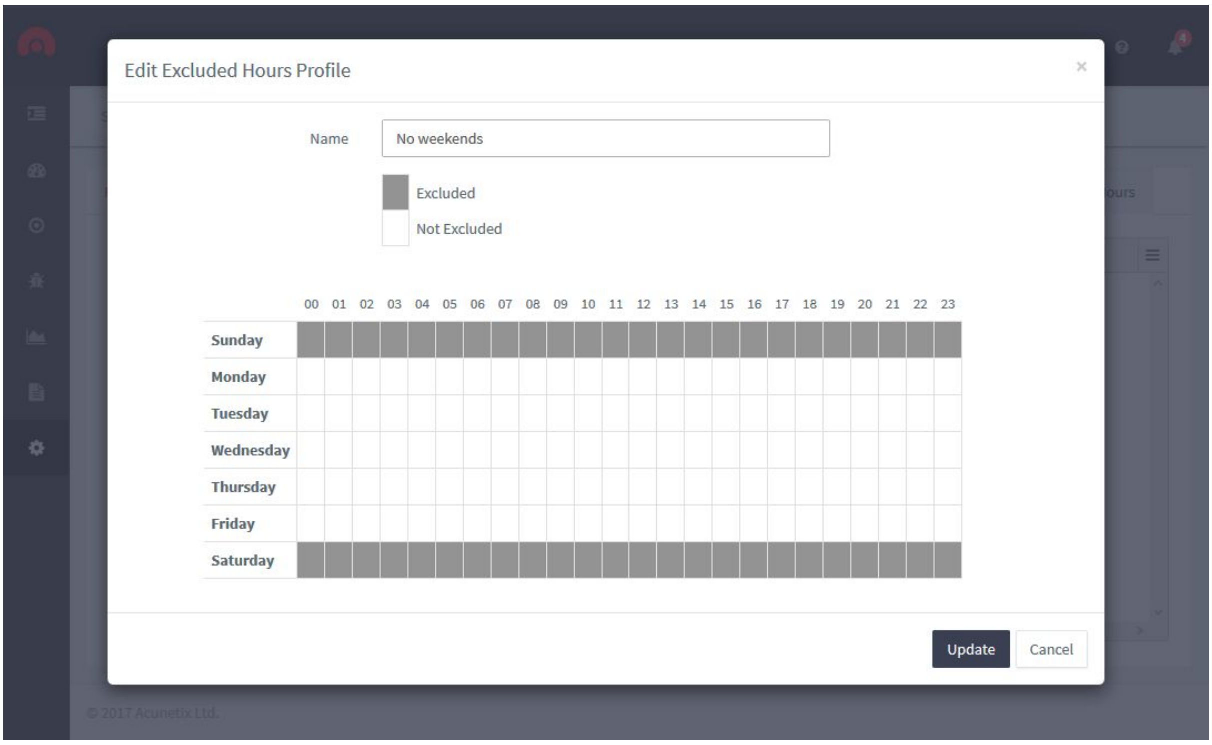
There are times when you do not want to scan a Target. For example, you might want to scan your site when during your workday so you can monitor the site while it is being scanned. Alternatively, you can scan your web application during the weekend when nobody is using it.



Name	Default
No excluded hours in use	●
Allows scans from 9am to 5pm	○
No weekends	○
Except working hours	○

Screenshot - Excluded hours list

Excluded hours allow you to configure the times when no scans should be done by Acunetix. The default excluded hours profile is assigned to all new Targets, however this can be changed to a different excluded hours profile for each Target. You can also create your custom excluded hours profile if needed.



Name: No weekends

▨ Excluded

□ Not Excluded

	00	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23
Sunday	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨
Monday																								
Tuesday																								
Wednesday																								
Thursday																								
Friday																								
Saturday	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨

Screenshot - Edit an excluded hours profile

Note: Any scans that are running at the start or an excluded hours period will be stopped. Any scans that are scheduled to start during an excluded hour period will be delayed till after the excluded hour period.

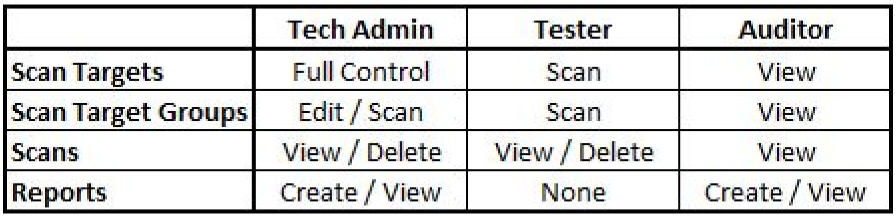
Configuring Users

Depending on your license, the scanning and reporting tasks of scan targets can be delegated to other people within the organisation using additional user accounts. These user accounts can be given permissions on specific Target Groups, and they will be able to create new targets, scan them or report on the targets within the group. The account created during the installation is the only account that can configure users within Acunetix.

Note: This feature is only available to Enterprise licensed users and in Acunetix Online.

User Account Roles

When creating a user account, you need to select a role for the user. There are 3 roles that you can choose from, which are Tech Admin, Tester or Auditor. Depending on the role selected, the user will be able to create, edit, scan and delete Targets, view scans and generate reports. The following table summarises the permissions available for each role



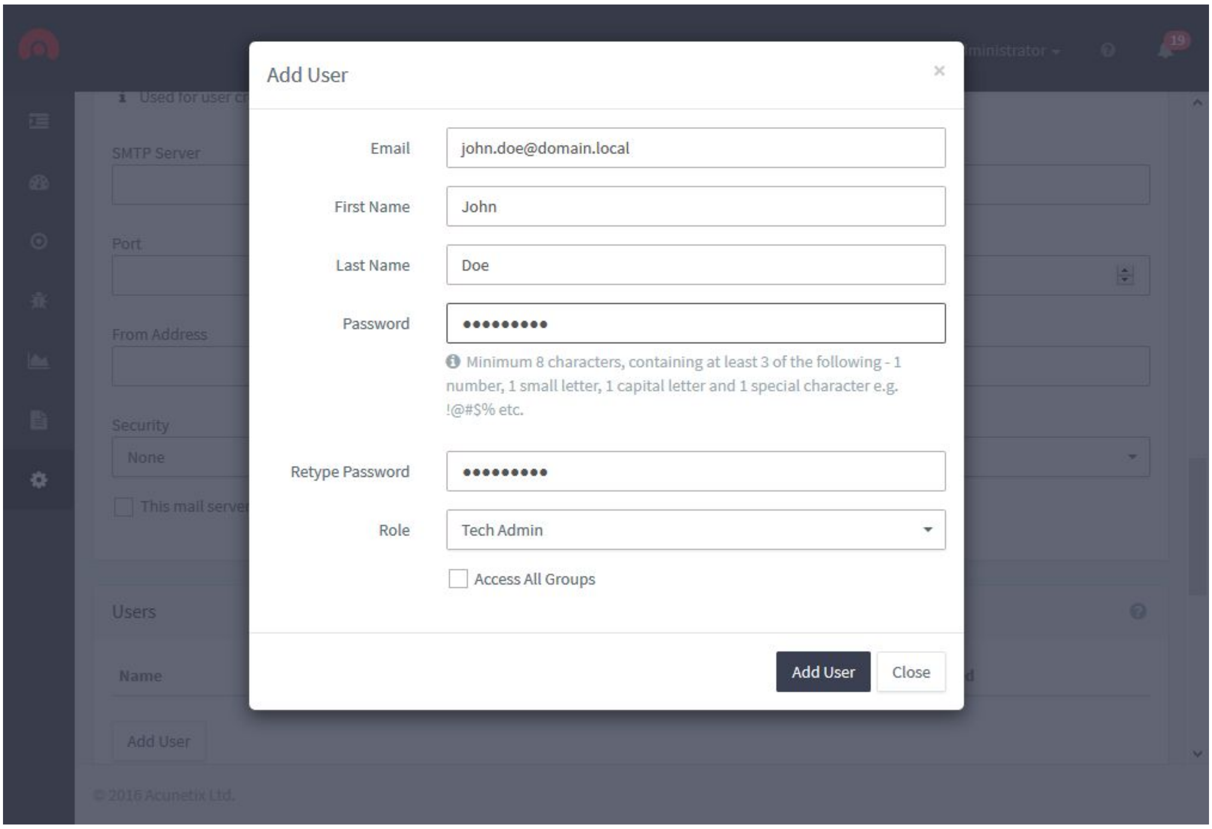
	Tech Admin	Tester	Auditor
Scan Targets	Full Control	Scan	View
Scan Target Groups	Edit / Scan	Scan	View
Scans	View / Delete	View / Delete	View
Reports	Create / View	None	Create / View

Note: The Tech Admin role can create new Targets if the user is assigned access to all Targets.

Creating a User Account

To create a user account:

1. From Settings, move to the Users Section..
2. Click the Add User button to create a new user



Add User

Email: john.doe@domain.local

First Name: John

Last Name: Doe

Password: •••••••••

Minimum 8 characters, containing at least 3 of the following - 1 number, 1 small letter, 1 capital letter and 1 special character e.g. !@#$% etc.

Retype Password: •••••••••

Role: Tech Admin

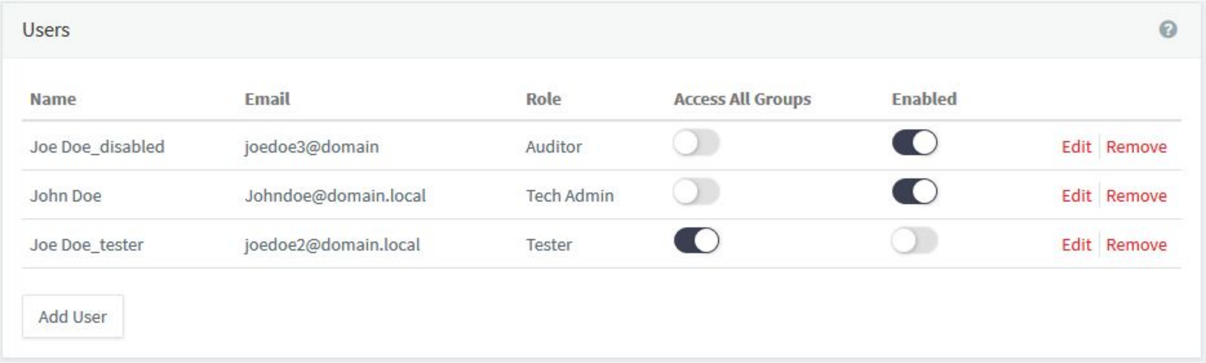
□ Access All Groups

3. Insert the email address, name, surname and password for the new user.
4. Select the Role for the new user. User Roles are explained above.
5. Select if to give the user account access to all Target Groups configured in Acunetix. If this is not selected, you will have to assign permissions to specific Target Groups after the user is created.
6. Click Add User when done
7. After you create the user, you will need to permissions to specific Target Groups. You can also choose to give access to all Targets Groups on your account (keeping in mind the Role selected for the user)
8. Click Update after configuring access to the Scan Targets.

Notes

- When a user is given access to a Scan Target Group, the user will retain access to the Scan Targets that are added to the Scan Target Group thereafter. Similarly, the user will lose access to the Scan Targets that are removed from the Scan Target Group.
- Tech Admins can create new Scan Targets and they can decide to add them to Scan Target Groups on which they have privileges.

Managing User Accounts



Users

Name	Email	Role	Access All Groups	Enabled	
Joe Doe_disabled	joedoe3@domain	Auditor	○	●	Edit | Remove
John Doe	Johndoe@domain.local	Tech Admin	○	●	Edit | Remove
Joe Doe_tester	joedoe2@domain.local	Tester	●	○	Edit | Remove

You can manage all your User Accounts from the Users section within the General Settings page. From here, you can instantly review the roles given to each user. You can also give access to all Targets to individual users, Disable users and Remove users from your account.

Troubleshooting and Support

User Manual

The most common queries can be answered by consulting this user manual.

Frequently Asked Questions

Our support team maintains a list of frequently asked questions at http://www.acunetix.com/support/faq/.

Acunetix Blog

We highly recommend that you follow our security blog by browsing to: http://www.acunetix.com/blog/.

Request Support

If you encounter persistent problems that you cannot resolve, we encourage you to contact the Acunetix Support team via email at support@acunetix.com. Please include any information you think is useful to help us diagnose your issue, such as information on the web technologies being used, screenshots showing the problem etc. Please include also the license key information in the support email.
We will do our best to answer your query within 24 hours or less, depending on your time zone.

Knowledge base / Support page

You can also explore the Acunetix knowledge base and other support options by browsing to: http://www.acunetix.com/support/.

Acunetix Facebook page

Join us on Facebook for the latest product and industry updates: http://www.facebook.com/Acunetix.