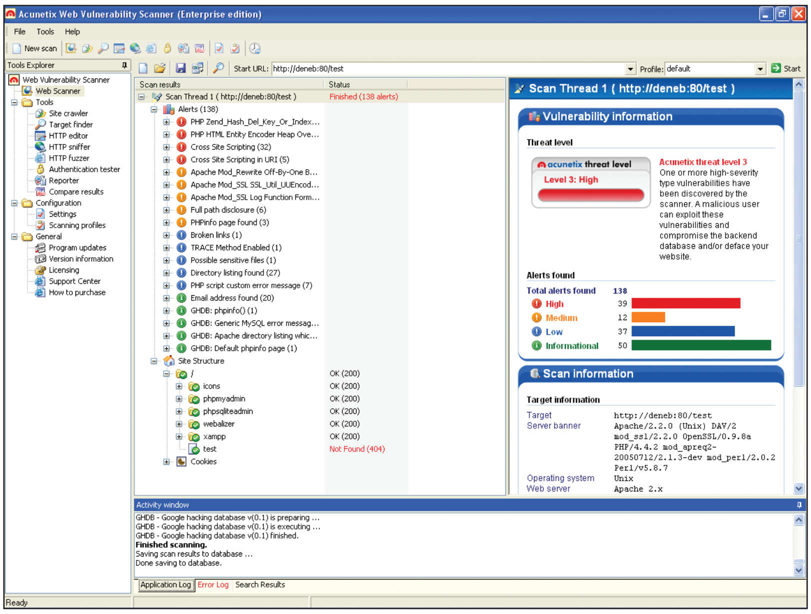
Acunetix Web Vulnerability Scanner

A comprehensive set of security tools in one package, with a convenient and easy-to-use interface

An organisation's web presence can be a source of problems as well as revenue. Some problems such as site defacement are obvious and easily dealt with, but others may not even be noticed, and these can do far more damage. A successful SQL injection attack will leave few traces, but it can hand the contents of your company's database over to the attacker. New vulnerabilities come to light almost every day, and keeping on top of them can be difficult. The Acunetix Web Vulnerability Scanner software runs security scans against a website, testing for known vulnerabilities. Operating in much the same way as a hacker, it can mount attacks based on what it finds.



```
Scan results                                      Status
Scan Thread 1 ( http://deneb:80/test )            Finished (138 alerts)
  Alerts (138)
    PHP Zend_Hash_Del_Key_Or_Index...
    PHP HTML Entity Encoder Heap Ove...
    Cross Site Scripting (32)
    Cross Site Scripting in URI (5)
    Apache Mod_Rewrite Off-By-One B...
    Apache Mod_SSL SSL_Util_UUEncod...
    Apache Mod_SSL Log Function Form...
    Full path disclosure (6)
    PHPinfo page found (3)
    Broken links (1)
    TRACE Method Enabled (1)
    Possible sensitive files (1)
    Directory listing found (27)
    PHP script custom error message (7)
    Email address found (20)
    GHDB: phpinfo() (1)
    GHDB: Generic MySQL error messag...
    GHDB: Apache directory listing whic...
    GHDB: Default phpinfo page (1)
  Site Structure
    /                                             OK (200)
      icons                                       OK (200)
      phpmyadmin                                  OK (200)
      phpsqliteadmin                              OK (200)
      webalizer                                   OK (200)
      xampp                                       OK (200)
      test                                        Not Found (404)
    Cookies
```

Scan Thread 1 (http://deneb:80/test)

Vulnerability information

Threat level

acunetix threat level: Level 3: High

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 found

Total alerts found	138
High	39
Medium	12
Low	37
Informational	50

Scan information

Target information

```
Target             http://deneb:80/test
Server banner      Apache/2.2.0 (Unix) DAV/2
                   mod_ssl/2.2.0 OpenSSL/0.9.8a
                   PHP/4.4.2 mod_apreq2-
                   20050712/2.1.3-dev mod_perl/2.0.2
                   Perl/v5.8.7
Operating system   Unix
Web server         Apache 2.x
```

Activity window

```
GHDB - Google hacking database v(0.1) is preparing ...
GHDB - Google hacking database v(0.1) is executing ...
GHDB - Google hacking database v(0.1) finished.
Finished scanning.
Saving scan results to database ...
Done saving to database.
```

ACUNETIX DISPLAYS TOOLS AND RESULTS IN A CLEAR AND CONCISE WAY, WITH DETAILED INFORMATION AND REPORTS AVAILABLE ON DEMAND.

We tested the scanner on some websites that were under active development but not yet live. The results were surprising, and at first sight depressing, with one site returning no less than 138 alerts, of which 39 were classified as "high". However, not all alerts are equal, and several were potential rather than actual problems. As with all security scans, the results need to be interpreted, and the software went to great lengths to explain what the risks might be. Even more information and suggested remedies were provided in the reports generated by the system, backed up by links to useful reference sources on the web.

The software can scan for a wide range of known security flaws, ranging from simple version checks and parameter manipulation exploits, such as HTTP splitting, to cross-site scripting and SQL injection vulnerabilities. It also checks the site structure, looking for broken links, weak directory permissions and other potential security gaps. AJAX applications aren't ignored, and the site crawler will analyse and execute JavaScript files as it builds up the site profile. Acunetix also makes use of the hacking database maintained at **http://johnny.ihackstuff.com**, which contains lists of search queries that can return data useful to hackers.

Scanning is controlled by profiles that can be used to restrict it to relevant operations. The default profile will scan for everything, while other options will concentrate on specific areas such as version checks or SQL injection. Automated scanning will detect most problems, but Acunetix has provided tools to help construct more specific tests. The HTTP editor can be used to build SQL injection or cross-site scripting attacks. The HTTP sniffer can record web traffic for use in more complex attacks. The HTTP fuzzer checks for buffer overflows and flaws in input validation scripts, while the authentication tester tool can access the strength of any passwords used to validate users through HTML Forms or HTTP Authentication.

Evaluating website security is never easy, and Acunetix has provided a range of tools to help. Hackers almost certainly can and will run similar scans against your website at some time, and they won't share the results with you. With this software you can know what they know and act accordingly.

IAN PARSONS

WEBSITE SECURITY

PRICE
Single website, €1,705 exc VAT, includes first-year premium maintenance

UPGRADE
Included in licence

SUPPLIER
Acunetix Ltd
0845 612 6712

INTERNET
www.acunetix.com

REQUIREMENTS
Windows 2000/2003/XP • Internet Explorer 5.1 or later • MS SQL Server or Access for database facility • 200MB hard disk space

EASE OF USE
★★★★★☆

FEATURES
★★★★★☆

VALUE FOR MONEY
★★★★★☆

OVERALL
★★★★★☆