The Acunetix Web Vulnerability Scanner

Website security is possibly today's most overlooked aspect of securing the 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, and other bespoke applications – to obtain access and to misuse control sensitive data such as customer details, credit card numbers and proprietary corporate data. Available 24 hours a day, 7 days a week such web applications often have direct access to backend data such as customer databases.

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. In addition, web applications are more open to uncovered vulnerabilities since these are generally custom-built and, therefore, pass through a lesser degree of testing than off-the-shelf software.

Auditing a website for vulnerabilities manually is impossible – scanning must be done automatically and regularly. On the other hand, automatic scanning must provide the peace of mind that all vulnerabilities are uncovered so as to completely protect sensitive data.

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

The Acunetix Web Vulnerability Scanner (WVS) is suitable for any small, medium sized and large organizations with intranets, extranets, and websites aimed at exchanging and/or delivering information with/to customers, vendors, employees and other stakeholders.

The Acunetix Web Vulnerability Scanner (WVS) broadens the scope of vulnerability scanning by introducing advanced and highly rigorous technologies to tackle the complexities of today's complex web-based environments. Besides automatically scanning for all vulnerabilities, WVS offers a strong and unique solution for analyzing web applications and websites that rely on JavaScript including AJAX applications.

It is these custom web applications that hackers always focus; the more the application is popular, the better. The solution is compatible with any technology that operates over HTTP/HTTPS. In general, WVS scans any website or web application that is accessible via a web browser and that respects HTTP/HTTPS rules.

The Acunetix WVS vulnerability database is not limited to known specific applications (e.g. off-the-shelf shopping carts) and/or module vulnerabilities (e.g. SQL injection in phpBB Login Form). If it were to do so, custom applications would remain untested for vulnerabilities. WVS "assumes" that all websites are uniquely structured and coded - WVS first crawls the entire website, analyzing in-depth each file it finds, and displaying the entire website structure. After this discovery stage, it performs an automatic audit for known security vulnerabilities by launching a

series of Web attacks. WVS checks for vulnerabilities on the web server and web application server and in website content itself.

Most important is the ability of WVS to analyze different Web technologies, such as HTML, PHP, ASP.NET, ASP, etc.. Put simply, WVS answers the questions: "which parts of a website we thought are secure are in fact open to hack attacks?" and "what data can we throw at an application to cause it to perform something it shouldn't do?".

WVS allows users to scan automatically for known vulnerabilities according to a regularly updated database while also ensuring other forms of intelligent vulnerability scans through manual intervention. In addition, WVS permits users to perform comprehensive automated hacking attacks that are not tied to particular applications. This allows the testing of custom applications irrespective of how and when they have been developed and who the developer is.

WVS 5: New Features Overview

WVS Version 5 contains a set of exciting new features including:

- **Microsoft Windows Vista Support**
- **Visual Improvements:** New graphics and visuals across the whole application.
- **Compliance Reporting:** This new versions offers detailed compliance reporting for OWASP, PCI, Sarbanes-Oxley, Web Application Security Consortium and HIPAA.
- **Subdomain Scanner:** The Subdomain scanner allows fast and easy identification of active Subdomains using various techniques and guessing of common subdomain names. The Subdomain Scanner can be configured to use the target's DNS server, or one specified by the user for flexibility.
- **Web Services Scanner:** The Web Services Scanner allows you to scan in an automated way for vulnerabilities in Web Services, and to generate a detailed security report from the results.
- **Web Services Editor:** The Web Services Editor allows you to import an online or local WSDL for custom editing and execution of various web service operations over different port types for an in depth analysis of WSDL requests and responses. The editor also features syntax highlighting for all languages to easily edit SOAP headers and customize your own manual attacks.
- **Site Structure File Selection:** This much requested feature allows the selection of individual files and folders from the Site Structure so that you will always be in control of what to scan.
- **Retain Settings on Upgrade:** WVS will now ask to keep your previous configuration and settings when upgrading from a previous build.
- **Scanning Mode Selection:** Each scan can now be executed in either one of three modes: Quick, Heuristic and Full. Each mode offers different approaches to test a website which compromise between detection rate and speed.
- **Reporter Application:** The reporting features of WVS have been revamped and integrated into a separate application which now supports reporting templates for: developers, executives, scan comparisons, statistics and also compliance reporting.

- **Password Protection:** WVS and all its supporting applications (like the Reporter, Scheduler, Vulnerability Editor and Command Line) can now be password protected to allow access only to authorized users.
- **Reduced Database Size:** Significantly reduced database size by 90% while keeping the same details and more! A new database structure had to be designed to achieve this which would require a database upgrade from older WVS version – for which a conversion tool is available.
- **Improved Scheduler:** The scheduler now support new ways to start a scan and different outputs such as a saved scan results file or a report. Support for Web Services scans scheduling is also included. Another requested new feature in the sending of mail notifications upon scan completion.
- **New / Improved Vulnerability Tests:**
  - Stores Cross-Site-Scripting (XSS) tests
  - Header Manipulation tests
  - Improved Blind SQL Injection tests
  - Improved Mod_Rewrite support
- **Improved Logic:**
  - Automatic detection of Directory Recursion Loops
  - Automatic detection of URL Rewrite website during a scan.
  - Grouping of test variants
  - Multi-Step Scanning
- **Other Improvements:**
  - Source View with syntax highlighting
  - Improved filtering (replacing the old search functionality)
  - Improved and more granular Logging options
  - Sitemap support

WVS Vulnerability Tests

WVS automatically crawls your website and all its related web applications to scan for the following classes of vulnerabilities:

- **Version Check**
  - Vulnerable Web Servers
  - Vulnerable Web Server Technologies
- **CGI Tester**
  - Checks for Web Servers Problems
  - Verify Web Server Technologies
  - Get Web Server Information
- **Authentication**
  - Input Validation
  - Authentication Attacks
- **Parameter Manipulation**
  - Cross-Site Scripting (XSS)
  - SQL Injection
  - Code Execution
  - Directory Traversal

    - File Inclusion
    - Script Source Code Disclosure
    - CRLF Injection / HTTP Response Splitting
    - Cross Frame Scripting (XFS)
    - PHP Code Injection
    - XPath Injection
    - Full Path Disclosure
    - LDAP Injection
    - Cookie Manipulation
    - URL Redirection
    - Application Error Messages
- **MultiRequest Parameter Manipulation**
    - Blind SQL/XPath Injection
- **File Checks**
    - Checks for Backup Files or Directories
    - Cross Site Scripting in URI
    - Checks for Script Errors
- **Directory Checks**
    - Looks for Common Files (such as logs, traces, CVS)
    - Discover Sensitive Files/Directories
    - Discovers Directories with Weak Permissions
    - Cross Site Scripting in Path and PHPSESSID Session Fixation.
- **Web Applications** – Large database of known vulnerabilities for specific web applications such as Forums, Web Portals, Collaboration Platforms, CMS Systems, E-Commerce Applications and PHP Libraries.
- **Text Search**
    - Directory Listings
    - Source Code Disclosure
    - Check for Common Files
    - Check for Server Side Includes (SSI) Directives
    - Check for Email Addresses
    - Microsoft Office Possible Sensitive Information
    - Local Path Disclosure
    - Error Messages
- **Web Services – Parameter Manipulation**
    - SQL Injection / Blind SQL Injection
    - Directory Traversal
    - Code Execution
    - XPath Injection
    - Application Error Messages
- **GHDB Google Hacking Database**
    - Over 1400 GHDB Search Entries in the Database

Other vulnerability tests may also be performed using the manual tools provided, including:

- Input Validation
- Authentication attacks
- Buffer overflows

Through the Scanning Profile configuration, users may set WVS to scan for all (default) or a selection of these vulnerability classes.

Advanced Tools

The Acunetix WVS broadens the scope of vulnerability scanning by introducing advanced and highly rigorous technologies to tackle the complexities of today's complex web-based environments. WVS allows users to scan automatically for known vulnerabilities according to a regularly updated database while also allowing for other forms of intelligent vulnerability scans through manual intervention. In addition, WVS allows the user to perform comprehensive automated hacking attacks that are not tied to particular applications. This allows the testing of custom applications irrespective of how and when they have been developed and who the developer is.

The following is a list of the more advanced WVS tools:

- **Target Finder**: The Target Finder is a port scanner that may be used to locate a web site within a given range of IP addresses.
- **Authentication Tester**: Audit password protected pages by launching a dictionary attack with the powerful Authentication Tester tool.
- **Subdomain Scanner:** The Subdomain scanner allows fast and easy identification of active Subdomains using various techniques and guessing of common subdomain names. The Subdomain Scanner can be configured to use the target's DNS server, or one specified by the user for flexibility.
- **HTTP Editor**: Construct HTTP/HTTPS requests and analyze the resulting web server responses with the HTTP Editor tool. In addition, you may perform custom SQL Injection and Cross Site Scripting attacks.
- **HTTP Sniffer**: Log, intercept and modify all HTTP/HTTPS traffic with the HTTP Sniffer to develop a deep insight into what data your web application/s is/are sending.
- **HTTP Fuzzer**: With this tool you can perform sophisticated testing for buffer overflows and input validation. It allows you to modify HTTP/HTTPS requests to include any type of generator and send multiple queries in an automated manner, saving a lot of time compared to manual testing.
- **Web Services Scanner**: The Web Services Scanner allows you to scan in an automated way for vulnerabilities in Web Services, and to generate a detailed security report from the results.
- **Web Services Editor**: The Web Services Editor allows you to import an online or local WSDL for custom editing and execution of various web service operations over different port types for an in depth analysis of WSDL requests and responses. The editor also features syntax highlighting for all languages to easily edit SOAP headers and customize your own manual attacks.
- **Reporter**: The Reporter application allows you to quickly create reports which specify all the vulnerabilities detected classifying them according to risk levels. Each vulnerability is presented with detailed recommendations on the action you need to take to correct it and prevent your site/application from being hacked. Furthermore, all scan sessions can be saved to a MS SQL Server or Access database for you to satisfy your custom reporting requirements. In WVS v5 the reporting features of WVS have been revamped and integrated into a separate application which now supports reporting templates for: developers, executives, scan comparisons, statistics and also compliance reporting.
- **Compare Results Tool**: The compare results tool allows you to analyze the differences between two scans performed at different dates.

- **Scheduler**: Schedule such tasks as automated web crawling and scanning at a time that is most convenient to you. Tasks may be run daily, weekly, monthly, at certain times and/or continuously within a queue.
- **Command Line Support**: This can be used to launch the application via the command line with various parameters.

Other Features

WVS contains a host of other features including:

- Scan Wizard – to simplify the scanning process.
- User agent definition – You can customise how Acunetix WVS identify itself to the server.
- Custom HTTP Tuning to control how fast the application sends requests to a web server.
- Online Updates from within the application for product updates and for new vulnerabilities.
- By default WVS ignores multimedia files which would slow down the scan. (e.g. BMP, AVI, etc..)
- Site Crawler configuration with File / Directory Filters, URL Rewrite and Custom Cookies.
- MS Access and MS SQL Server support to store the scan results.
- Support for HTTP and SOCKS Proxy servers.
- SSL Client Certificates support.
- Custom Scanning Profiles.
- Scanner list of allowed hosts.
- Login sequence recorder for all types of logins.
- HTML Forms custom submission inputs.
- Support for Custom 404 Error Pages
- Custom GHDB Database filters.
- Application logging for troubleshooting purposes.