Web Application Security Assessment and Vulnerability Assessment

Enterprise IT Solutions (Hardware, Software, Services)
Shared Service and Outsourcing
Technology Products Distribution and Trading

Enterprise Solution
Professionals on Information and Network
Web Application Security Scanner

• Is your website hackable?
• 70% of the websites are at serious risk of being hacked
• Web applications attack accounts for up to 70% of all cyber attacks

Website security is possibly the most overlooked aspect of securing the enterprise and should be a priority in any organization. Hackers are concentrating their efforts on web applications such as shopping carts, login pages, forms, dynamic contents and etc.

Web applications are accessible 24 hours a day, 7 days a week and control valuable data since they often have direct access to the backend database such as customer database, credit card details and etc.

![Scan Results]

Firewalls, SSL and locked-down servers are futile against web application hacking
Any defense at network security level will provide no protection against web application attacks since they are launched on port 80 - which has to remain open. In addition, web applications are often tailor-made therefore tested less than off-the-shelf software and are more likely to have undiscovered vulnerabilities.
How Does Hacking Work?

1. A hacker finds a vulnerability in your custom web application and sends an attack via port 80/443 to the Web Server.
2. Web Server receives the malicious code and sends it to the Web Application Server.
3. Web Application Server receives malicious code from Web Server and sends it to the Database Server.
4. Database Server executes the malicious code on the Database. Database returns data from credit cards table.
5. Web Application Server dynamically generates a page with data including credit card details from database.
6. Web Server sends credit card details to Hacker.

Legend:
- Data exchanged between Hacker and Web Server over port 80/443 which also gets through the Web Application Server, Database Server and the Database itself.
- Credit card data is retrieved from Database.

Hacker Injects SQL Command to Database via Custom Web Application to Retrieve Credit Card Details.
To safeguard your enterprise’s web applications from hackers,

**E-Spin represented Acunetix Web Vulnerability Scanner is the solution you needed!**

E-Spin represented Acunetix Web Vulnerability Scanner (WVS) is an automated web application security testing tool that audits your web applications by checking for exploitable hacking vulnerabilities. Automated scans may be supplemented and cross-checked with the variety of manual tools to allow for comprehensive web site and web application penetration testing.

In short, this powerful tool allows you to scan and automatically checks your web applications for SQL Injection, Cross Site Scripting (XSS) & other web vulnerabilities.

**Acunetix History**

Acunetix has pioneered the web application security scanning technology: Its engineers have focused on web security as early as 1997 and developed an engineering lead in web site analysis and vulnerability detection.

**How Acunetix Works?**

Acunetix WVS has the ability to scan for vulnerability in web applications, provide fixing recommendations and reporting tool to ensure web applications are less hackable or exploitable from hackers. The software will perform typical work of a hacker by trying to scan and execute various hacking methods (non-destructive methods) to exploit the web applications. As a result, it will list down all the success attempts and in what scenario in order to enable developers to record which applications are exploitable and facilitate them to close the application vulnerability.

All in all, Acunetix WVS is a software that provides automatic or manual way to search for software vulnerability within web applications and reports it as well as recommend ways to fix the problem.
1. **AcuSensor Technology**
   - New technology that allows you to identify more vulnerabilities than a traditional black box scanner whilst generating less false positives.
   - Faster locating and fixing of vulnerabilities, whilst providing more information about each vulnerability. For instance, source code line number, stack trace and affected SQL query.
   - Check for web application configuration. Example misconfiguration of web.config or php.ini

2. **In depth checking for SQL Injection, XSS and Other Vulnerabilities**
   - Known Static Methods:
     - Specific Web Applications known exploits
     - Directory enumeration
     - Known web server exploits
     - Known web technology exploits (e.g. php)
     - Known network service exploits (e.g DNS, FTP)
   - Unknown Dynamic Methods:
     - SQL Injection
     - Cross Site Scripting (XSS)
     - Directory and Link Traversal
     - File Inclusion
     - Source Code Disclosure

3. **Port Scanner and Network Alerts**
   - Scan web server for open port
   - Also run network alert checks against network services running on open ports such as DNS cache poisoning, SNMP weak community strings, weak SSH ciphers, etc.

4. **Detailed Reports**
   - Able to generate different official and technical report (can customize report) to meet different users requirement: from executive summary, vulnerability report, compliance (HIPPA, PCI, OWASP, SOX, WASC) pre and post comparison report, statistical reports, etc.

5. **Advanced Penetration Tools**
   - Allow penetration testers to tune web application security checks
   - HTTP Editor: construct HTTP/HTTPS requests and analyze the web server response
   - HTTP Sniffer: intercept, log and modify all HTTP/HTTPS traffic and reveal all data sent by web application
   - HTTP Fuzzer: perform sophisticated testing for buffer overflows and input validation
   - Blind SQL Injector: automated database data extraction tool that is perfect for making manual test that allows further testing for SQL Injections.

6. **Scan Ajax and Web 2.0 Technologies**
   - The Client Script Analyzer (CSA) engine allows comprehensive scan of the latest and most complex Ajax/Web 2.0 for vulnerabilities

7. **Test Password Protected Areas and Web Forms**
   - With automatic HTML form filler, it enables to fill in web forms and authenticate against web logins. The form filling process is stored and the sequence will be used when scanning.

8. **Analyze Website against the Google Hacking Database**
   - Google Hacking Database (GHDB) is a database queries used by hackers to identify sensitive data on your website such as portal logon pages.
   - Acunetix launches GHDB onto your website and identify loopholes before the hackers do
Benefits to Organization

- **IT Security Greatly Enhanced.**
  - Acunetix’s unmatched automated and flexible manual scan capabilities provide comprehensive or selective area scan
  - Able to have truly secure web application in place which has been tested against various hacking attack to avoid unnecessary exploitation that will jeopardize the organization’s image

- **Time Saving**
  - By using automated scanning, it off loads the ongoing routine scanning tasks (if administrator allowed to do so based on company configuration), hence administrator can focus his time to perform value added service like interpret the report and communicate the report finding.
  - In addition, administrator will be flexible enough to conduct a manual specific scan (based on methods) in order to confirm whether the vulnerabilities have been fixed.

- **Reports**
  - With Acunetix capable of generating various reports, IT security staff is empowered to be proactive in managing security measures and ongoing compliance audit and monitoring
  - Based on the true and transparent report on all web applications vulnerabilities, IT security staff are able to communicate those findings to respective parties for fixing, reporting and compliance purposes

- **Compliance**
  - Able to meet various legal and regulatory compliance

**SYSTEM REQUIREMENTS:**
- Internet Explorer 6 or higher
- 250 MB of hard disk space
- 1GB of RAM
In Depth checking for SQL Injection

Acusensor Technology: Identifying more vulnerabilities
Port Scanner and Network Alert

Detailed Report
Advanced Penetration Tools

Analyze site against Google Hacking Database
About E-SPIN

E-SPIN is the leading technology solution and outsourcing vendor in providing enterprise solutions consulting, buying facilitation, network and system integration, software development and customisation, product training and certification testing, share service and outsourcing.

More information available at www.e-spincorp.com