



Web Site Security Audit

WSSA (Web Site Security Audit) is a hosted website vulnerability scanner that examines website pages, applications and web servers to find and report on security weaknesses and vulnerabilities that give hackers an opportunity to do damage.

WSSA identifies web site security risks by looking for weaknesses in web site code, errors in web server settings and by detecting the indicators of viruses, Trojans or worms. WSSA does this by scanning the target web site from the outside to find system and application vulnerabilities and then re-tests routinely to ensure new weaknesses are quickly identified.

Comprehensive Security Assessment

WSSA employs an extensive library of known security issues to comprehensively detect and monitor vulnerabilities caused by web site weaknesses, including the following:

Vulnerability	Examples
Application Code	This includes poorly coded web pages, database connections that allow access to private data, SQL injection, XSS (cross-site scripting), CSRF (cross-site request forgery) and other web-based attacks
Viruses, Trojans and Worms	The WSSA test database contains 'fingerprints' to identify many known viruses, Trojans and worms
System Misconfiguration	Examples are common services with default user name or passwords left unchanged or vital security updates and patches not installed

Key Features

- No software or hardware to install or maintain
- Scans servers, routers, firewalls, switches, operating systems—anything with an Internet-facing IP address
- Flexible scan frequency: weekly, daily or on-demand
- Fast Reporting—Get detailed reports within one hour
- OEM white label re-branding available
- 24/7 unlimited phone support with access to the Beyond Security network of security experts

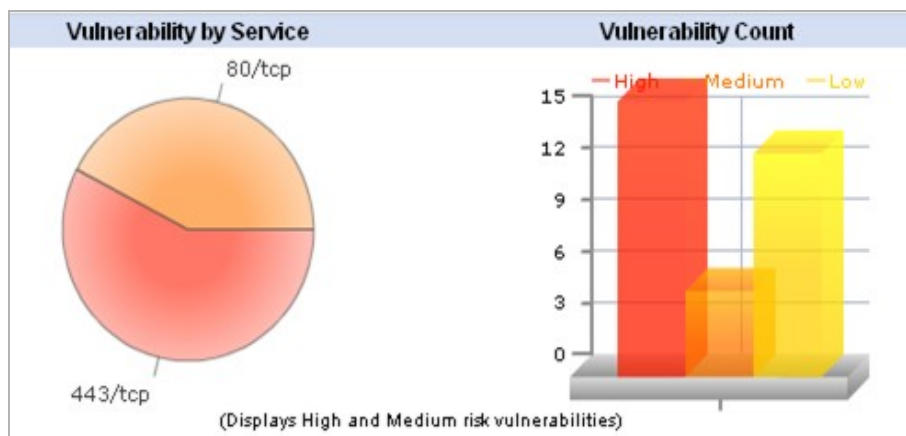
Managed Service Providers

Offer your customers a valuable service and generate new revenue, with no upfront costs. Simple turnkey setup available.

“Data Action is in the position, as are many companies, where associated service costs are passed directly on to the customer.”

“We found the service supplied to us by Beyond Security to be a very valuable best-cost strategy for us to supply to our customers.”
 –David Stork.
 Data Action

Audit Results



- Results available quickly, typically within one hour or less
- Vulnerabilities ranked by risk level: High, Medium and Low
- Available in multiple formats: XML/HTML, PDF and CSV
- Expert risk solution recommendations to assist webmasters and IT staff

Beyond Security Seal



The Beyond Security seal provides visual confirmation to all visitors that the site is secure. Retail site owners typically find that adding a Beyond Security Seal increases visitor confidence and pays for itself with increased sales.

“70% of Internet users only use Internet shopping sites that display a security protection seal” –IBM study¹

Internal Network Audits?

WSSA is a hosted scanning solution for web sites, web servers and all Internet-facing IP addresses. For internal scanning of networks consisting of any number of servers, ports or IP addresses, use our appliance-based solution: AVDS.

Contact Us

For more information, visit www.beyondsecurity.com

For pricing details, contact us at sales@beyondsecurity.com

+1 800 801 2821

“I am extremely satisfied with your service, which seems to have uncovered significant issues with the security of the server we rent space on.”
–Tom Andrews



Scanning Features

- Thorough scanning of web site, firewall and servers – Tests for over 10,000 vulnerabilities, depending upon open ports and available services
- Tests the site code, firewall and servers beyond the level required for Payment Card Industry (PCI) compliance
- Flexible scan frequency: weekly, daily or on-demand
- False positive prevention
- Risk solution recommendations – Specific recommendations include code revision, settings changes, software updates or operating system patches
- Complete, actionable reports – Online, interactive reports include an overview for executives and links to equipment vendor sites for updates and patches
- Vulnerability database supplied by SecuriTeam Portal (www.securiteam.com), a industry respected security clearinghouse with over 2 million visits annually and 8,500 online articles
- 24/7 unlimited phone support with access to Beyond Security experts

Service Levels

	Basic	Standard	Advanced
15-day free trial	✓	✓	✓
60-day satisfaction guarantee	✓	✓	✓
Domains	1	2	10
Scan and report frequency	Once a week	Daily	Unlimited on-demand custom schedule
Daily vulnerability updates	✓	✓	✓
Vulnerability solution recommendations	✓	✓	✓
Beyond Security Seal		✓	✓
Security risk alerts by email		✓	✓

Vulnerability Checks

Scans	Sample Checks
Web Applications	Apache, Microsoft IIS®, Oracle WebLogic®, IBM WebSphere®, Adobe ColdFusion®, FTP, SSH, TELNET, shopping carts
Databases	Oracle®, MySQL, Microsoft SQL Server®, Lotus Notes®, DB2®
Network Systems	Routers, Firewalls, IPSec, PPTP, DHCP, DNS, LDAP, SNMP, VPNs
Operating Systems	Microsoft Windows NT, 2000, Server 2003 and 2008, XP, Vista®, Windows 7®, Solaris®, AIX®, HP-UX®, SCO Unixware®, BSD (OpenBSD, NetBSD), Linux, AS/400®, VMS®
Languages	SQL, ASP, PHP, CGI, JavaScript, PERL, Ruby, .NET

System Requirements

The WSSA service requires only the address of the domain to be scanned and the email address where to deliver the scan report. To view the interactive online scan report, use one of the following recommended browsers:

- IE 6.0 or later
- Mozilla Firefox 1.5 or later

¹ <http://www-03.ibm.com/press/us/en/pressrelease/19154.wss> – 25 Jan 2006