



Additional Scan Features (3 of 3)



Scanner	Web Server Hardening	CGI Scanning	File / Dir Enumeration	Passive Scanning	Notes and Other Features
IBM Rational AppScan	Y	Y	Y	Y	Null Byte, Parameter Tampering (eShopLifting, Debug Mode, Boolean Parameters), Range Restriction Bypass, HTML5 Attacks (HTML5 SQLi, Client Command Execution, Client Side Open Redirect), Flash Specific Attacks (XSF, XSS via Flash, Flash Permissions, Phishing via Flash), XML Specific Attacks (XML Entity, SOAP Array Overflow), Account Lockout, Floating Point DoS, Code Injection (Perl, Partial PHP)
WebInspect	Y	Y	Y	Y	Partial LDAP Injection & Xpath Injection support, Parameter Manipulations, JSON Hijacking, Flash Attacks (XSS via Flash, Flash Analysis, Information Disclosure), Web Service Attacks (Unknown), Numerous Product Specific Plugins, Traversal(LFI).
W3AF	Y	Y	Y	Y	phishingVector, generic flaws, Partial DOM-XSS detection, RegEx DoS, Technology specific vulnerabilities and a TON of discovery plugins, fingerprinting, brute-force, enumeration and analysis features,PHP vul.
Cenzic Hailstorm Professional	Y	Y	Y	Y	Code Injection (PHP/Perl), Weak Password, Flash Permissions, Cross Frame Scripting, HTTP Parameter Pollution, Ineffective Session Termination, No User Lockout, Clickjacking,, and more.
Nessus	Y	Y	Y	Y	Generic Injection, RFI & LFI & Traversal (All)
Acunetix WVS (Commercial Edition)	Y	Y		Y	Fuzzer, Code Injection (PHP), File Tampering, Server-Specific audit policies, a large number of CGI detection modules, Numerous general & tech-specific passive analysis features, Network scanning features.
SkipFish	Y	Y	Y	Y	Client SQL Execution, Code Injection (PHP), Many Passive Analysis Features.
SandcatCS	Y	Y	Y	Y	Parameter Tampering, Code Injection (PHP) and various other checks and features.
Sandcat Pro	Y	Y	Y	Y	Code Injection (PHP)
arachni	Y	Y	Y	Y	Code Injection (PHP, Ruby, Python, JSP, ASP.Net), XSS in both path & URI.
Sandcat Free Edition	Y	Y	Y	Y	Code Injection (PHP)
JSky (Commercial Edition)	Y	Y	Y	Y	Captcha Cracker (Unique!).
NTOSpider				Y	Parameter Analysis, Basic flash/java analysis, Malicious frame/script analysis, Java Grinder, Credential Dictionary Attacks, Reverse Proxy.
Netsparker (Commercial Edition)	Y	Y		Y	Blind Command Injection, Remote Code Evaluation, Source Code Disclosure (PHP).
Burp Suite Professional	Y			Y	Header Manipulation.
Vega	Y			Y	Several Passive Analysis Modules.
Wapiti					Htaccess bypass, Resource consumption, Potentially dangerous file detection.
Grendel Scan	Y	Y	Y	Y	Fuzzing

Scanner	Web Server Hardening	CGI Scanning	File / Dir Enumeration	Passive Scanning	Notes and Other Features
ZAP	Y		Y	Y	Parameter Tampering.
ParosPro	Y	Y		Y	Parameter Tampering.
Oedipus	Y	Y		Y	Simple fuzzing (error detection).
Andiparos	Y			Y	Parameter Tampering, XSS in path.
Watobo	Y			Y	Fuzzer, various SAP & JBoss tests (unique feature!), Lotus domino DB enumeration, Unencrypted password transmissions.
JSKY Free Edition	Y		Y	Y	
Paros Proxy	Y			Y	Parameter Tampering
Netsparker Community Edition	Y			Y	In the free edition, the blind SQL injection feature is really limited to boolean (binary) SQL injection.
PowerFuzzer					Detect exceptions.
Uber Web Security Scanner					claims to fuzz for XML/SOAP injection, Code Injection (PHP, Perl), Detailed RFI. Supports detailed SQL Injection configuration.
iScan	Y	Y			GET/POST coverage. Port scanner. Many known vulnerabilities in web server default application.
WebSecurify	Y			Y	
Grabber					A few QA features.
WebCruiser Enterprise Edition		Y			Injection features support MSSQL, MySQL, Oracle, DB2 and MS Access..
N-Stalker 2012 Free Edition	Y	Y	Y	Y	
WebCruiser Free Edition		Y			
WSTool		Y		Y	SQL injection is limited to MSSQL, CGI scanning is limited to administrative pages. Attempts to locate 5xx and 4xx errors.
N-Stalker 2009 Free Edition	Y	Y		Y	
WebScarab					Fuzzing
Acunetix WVS Free Edition					It is unclear whether or not the free version actually performs persistent XSS tests.
ProxyStrike					
safe3wvs					The commercial version also supports the detection of admin applications, file upload vulnerabilities, directory listing and additional vulnerabilities.
Priamos					SQL exploitation module.
XSSploit					Exploit code generation, XSRF generation.
sqlmap					Full support for MySQL, Oracle, PostgreSQL, Microsoft SQL Server, Microsoft Access, SQLite, Firebird, Sybase and SAP MaxDB.
Xcobra					
Gamja					Validation error detection.

Scanner	Web Server Hardening	CGI Scanning	File / Dir Enumeration	Passive Scanning	Notes and Other Features
Mini MySqlatOr					SQL Exploitation Framework.
XSSer					Plenty of different XSS flavors.
Secubat					
Scrawler					Scans ONLY GET parameters, 1500 Max Crawled URLs.
openAcunetix					
SQLiX					
Web Injection Scanner (WIS)		Y			
VulnDetector					
Damn Small SQLi Scanner (DSSS)					
ScreamingCSS					
LoverBoy					
XSSS					
SQID (SQL Injection Digger)					
aidSQL					
crawlfish					