



List of Scanner Features (3 of 3)



Scanner	Advanced Features		Additional Information	
	Ajax Support	WAF Evasion	Other Features	Overview
Acunetix WVS (Commercial Edition)	Yes		JS/Ajax analysis & crawling, URI Coverage for XSS & SQLi, Web Services Scanning Features, GHDB, Network Scanning Features, Subdomain Scanner, Authentication tester, Sniffer, AcuSensor Whitebox Analysis.	
Acunetix WVS Free Edition	Yes	Yes	Detection of XSS in URI, Analyze javascript and Ajax, Custom 404 support.	Pretty impressive amount of XSS payloads; probably useful for bypassing filters and web application firewalls.
aidSQL			Exploitation Features.	
Andiparos			Removes "Accept-Encoding: gzip,deflate" headers as a workaround for compression support.	An actively developed fork of the Paros project. Supports an XSS attack vector with the whole URL path as an input origin.
arachni			Highlighted command line output, Internal proxy plugin.	The gzip/deflate support was not verified.
Burp Suite Professional			AMF String Vales Attack Vector, Parameter Name Attack Vector, Rest-style Parameters Attack Vector, External Plugins Implementing Java Serialized Objects and WCF Binary Manual Testing Support.	
Cenzic Hailstorm Professional	Yes		OTP/Captch Support, Credential Enumeration, Source Code Analysis, Web Service Scanning (with WS Security Support).	
crawfish				
Damn Small SQLi Scanner (DSSS)			Crawler limited to depth 1.	A proof of concept tool designed to prove that the accuracy of commercial vendors can be beaten with less than 200 lines of python code... definitely a challenge.
Gamja				SSL and HTTP Compression support derive from the use of WGET.
Grabber	Yes		Simple AJAX support (parse every JavaScript to get URLs, and try to get the parameters).	The tool vulnerability tests generally work, but the tool does not seem to handle malformed HTML pretty well, has several configuration / crawling issues and is not really fitted for scanning .net applications (false positives).
Grendel Scan			POST coverage does not work due to a bug.	Crashes every once in a while.
IBM Rational AppScan	Yes		Custom HTTP Location Attack Vector, Restful Param Support, Manual Configuration for AntiCSRF Token Support*, Indirect login CAPTCHA support through, the "prompt login" feature, JS / Flash Parsing & Execution, Kerberos authentication support	Flash AMF Scanning, Web Services Scanning, Runtime Analysis (GlassBox), Javascript Security Analysis (JSA), Credential Enumeration, Multiphase operation support (manual & automatic), External Integration for exploitation tools, Web Malware Analysis & Detection (Pattern & Behavioral Analysis), Certain WAF create rules automatically from AppScan reports
iScan				

	Advanced Features		Additional Information	
Scanner	Ajax Support	WAF Evasion	Other Features	Overview
JSky (Commercial Edition)	Yes		Partial Form Authentication Support, Urls detection using Java Class Parsing (Unique!) & Flash parsing, Parameter Name & URI Coverage (XSS), MD5 Cracker, Subdomain Scanner, GHDB, Exploitation Features, Web Malware Discovery.	The following database are supported in the injection/exploitation tests: Oracle, MSSQL, Mysql, Informix, DB2, Access, Sqlite, Sybase, PostgreSQL.
JSky Free Edition			Custom 404 page definition, Claims the ability to extract URLs from Javascript, flash and java applets.	The tool only scans GET parameters (all scans were performed through a proxy), and does not seem to submit forms or scan POST parameters. As a result, it will be difficult to rely on it in an actual penetration test.
LoverBoy		Yes	Exploitation Features.	
Mini MySqlatOr				
Nessus			Parameter Name Attack Vector, Network scanning features with thousands of plugins.	Nessus is a network vulnerability assessment tool that also has web application scanning features. It's not a pure - hardcore web application vulnerability scanner.
Netsparker (Commercial Edition)	Yes		URL & Extra Params XSS support, Parses Javascript & Text, MSSQL, MySQL, Oracle, Postgresql, DB2 & MsAccess Support, Anti-CSRF token support, Credential Enumeration, SQLi & LFI Exploitation Features.	
Netsparker Community Edition	Yes		Parses Javascript & Text.	Many features are reserved for the commercial version, but in the overall, the tool is VERY user friendly and simple to use, and the tester can still benefit a lot from running it, in spite of the missing features. There is however a potential problem: the usage of the tool may result in privacy violation: in the installation process, the license agreement presented to the user includes a section that permits the software to gather information from the various scans performed with it. Even though the official claim is that the purpose of this information is to improve the product (a legitimate and worthy demand in its own right), this behavior may still cause sensitive and private customer information to be disclosed to entities that did not sign an NDA agreement with the customer, and whom the customer may not trust.
N-Stalker 2009 Free Edition		Yes	Spider is limited to 100 URLs in the free edition, Manual crawl support via Web Macro scripts, Flash/CSS/Javascript parsing features and Javascript execution features (coverage).	The free edition specialization seems to be web server security, and the XSS scanning feature is thrown in as a "bonus". The spider is limited to 100 URLs, thus reducing the benefit from exceptional coverage features (Flash/CSS/JS parsing), and with mediocre accuracy in XSS detection the free edition of the tool will be an insufficient and unreliable choice for most applications.
N-Stalker 2012 Free Edition		Yes	Flash/CSS/Javascript parsing features and Javascript execution features (coverage).	
NTOSpider	Yes		URL attack vector, Ajax & SOAP Scan, External manual crawling (via burp/paros log), Crawling & verification via multiple browser engines (IE, Firefox), Advanced form submitting engine, Report-integrated exposure verification applet, WAF rule generation.	The tool creates an application map, as a tool for the customer to inspect the test scope. The next major upcoming release of NTO (v6.x) is supposed to include AMF Support and Improved AJAX crawling. Future plans for Chrome crawling / exposure verification. The tool currently does not provide VBs exploitation payloads for XSS.

Scanner	Advanced Features		Additional Information	
	Ajax Support	WAF Evasion	Other Features	Overview
Oedipus			manual crawling is supported due to the burp log parsing feature and URL file parsing feature (including POST support).	A wide variety of features, relatively easy execution (once you figured out how to do it), a high detection rate and a low false positive rate make this tool a must have in any hacking arsenal. The tool uses blind & union SQL injection exploits to verify vulnerabilities, a very advanced feature for a scanner that old, not to mention the fact that this tool was the only one that found the obvious internal SQL injection (!) in the dot net banking application. The tool has some faults (such as the inability to handle non standard ports in windows, due to the character ":" which has a unique significance when writing files), but those limitations can eventually be bypassed (replacing the string in the log, using port forwarding, etc).
openAcunetix			No crawler.	
Paros Proxy			Removes "Accept-Encoding: gzip,deflate" headers as a workaround for compression support.	Slows down (and sometimes crashes) when dealing with large applications, or with heavy content (video/audio).
ParosPro	Yes		JS Parsing, Port Scanner.	
PowerFuzzer				
Priamos				
ProxyStrike			Append constant parameters to URLs.	Basic authentication is supported only through browser features or through adding HTTP headers. Form authentication and URL exclusion are possible simply by manually accessing pages without using the spider.
safe3wvs	Yes			
Sandcat Free Edition	Yes	Yes	Source code analysis (white-box mode), Customize 404 page.	Free edition limitation for some of the versions out there: every few minutes the scanner delays the scan for a short amount of time. The tool is freeware for non commercial use.
Sandcat Pro	Yes	Yes	Source Code Analysis (white-box mode), Customize 404 page, Partial Cookie Coverage (Cookie Manipulations Plugin), Java & Flash parsing, Handle Malformed HTML.	
SandcatCS	Yes	Yes	Source Code Analysis Features	
Scrawler				The tool does not submit forms, does not perform checks on POST parameters, does not parse JS / flash and does not implement any intelligent coverage method. Furthermore, the scan is limited to 1500 pages; due to all those reasons, it is hard to see the benefit of executing it, when so many tools with greater coverage, equivalent simplicity and similar efficiency are freely available.
ScreamingCSS				

	Advanced Features		Additional Information	
Scanner	Ajax Support	WAF Evasion	Other Features	Overview
Secubat				The tool is pretty difficult to install (requires installation of MSSQL, manual execution of a database creation script and initially loading the plug-ins through the GUI). It seems to succeed in the crawling process (the database is populated with information and the data is available for future usage in the GUI), but did not detect exposures in a consistent manner, regardless of the scan execution method (scan alongside the crawling process, immediately after crawling or in a separate time and instance) and the scan plug-ins selected (but depending on the application tested). The crawler does not seem to handle malformed HTML very well, and gets stuck or stops the crawling process when referred to pages that contain it (Probably related to the fact the tool is in early beta). The tool detects multiple locations of the same instance of XSS exposures, and also assigns unclear description to the SQL injections detected.
SkipFish			URL XSS, Detailed configuration options for various scan aspects.	
SQID (SQL Injection Digger)			Manual crawling supported due to the URL file parsing feature.	
SQLiX			Manual crawl supported due to URL file feature. Exploitation Features. An undocumented partially implemented proxy support.	
sqlmap			Manual crawling is possible thanks to the proxy log parsing feature (The URL file parsing feature expects a single request). The tool specializes in exploitation of predefined URLs.	
Uber Web Security Scanner				
Vega			Manual Testing Support due to Interception Proxy Features.	
VulnDetector				
W3AF	Yes	Yes	Fuzzing Features, Exploitation, Credential Enumeration. Scans HTTP headers as well. Suppose to support Web Service/Ajax scanning, but I did not test this feature, and the official documentation claims that developers should still develop plug-ins for it.	The current version of W3AF is very easy to install, and the automatic SVN updates are an excellent feature that will help both the users and the authors resolve problems quickly; that being said, I still had my share of problems when I updated my v1.0 stable version to the latest SVN version, and I have no one to blame but myself, for obsessively pressing the update button. As it always is with W3AF, the tester needs to learn how to configure it for each type of scan. and needs to learn how avoid being greedy... Simply put, avoid using plenty of plug-ins altogether (especially grep plug-ins).
Wapiti				
Watobo			Supports Anti-CSRF-Tokens / Detect One-Time-Token.	Custom cookies could be set by intercepting responses and adding set-cookie headers.
Web Injection Scanner (WIS)				

Scanner	Advanced Features		Additional Information	
	Ajax Support	WAF Evasion	Other Features	Overview
WebCruiser Enterprise Edition		Yes	Built in Web Browser (NOT adding any crawled URLs to the scan), Exploitation features.	
WebCruiser Free Edition		Yes	Built in Web Browser (NOT adding any crawled URLs to the scan), Exploitation features.	The tool did not have any features that enable it to distinguish between case sensitive technologies and case insensitive technologies, resulting in false positives and identical exposures.
WebInspect	Yes		URL Attack Vector Coverage, Web Service Scanning, Flash Scanning (SWFScan), Source Code Scanning, Credential Enumeration, Fuzzer, JS/VBs/Flash/Silverlight Analysis.	
WebScarab				
WebSecurify				Authentication support as a part of the built in browser features.
WSTool				The GUI is implemented as a web application. The web version is supposed to support authentication and cookie customization, but I had problems activating a scan within it.
Xcobra				
XSSer		Yes	Exploitation features, Rough manual crawling support due to the URL file parsing feature (No FORM submission), GET/POST coverage (rough POST coverage for single URL scans).	The tool implements some useful and even rare features (DOM XSS, etc), but is very difficult to execute it in an effective manner on a large scale application, and naturally, as an alpha product, its prone to various bugs.
XSSploit				
XSSS			partial POST coverage. Manual crawling is roughly supported by providing the tool a file with a list of URLs.	
ZAP			Brute force, Fuzzing, Beanshell integration, port scanner, break points.	An actively developed fork of the Paros project.