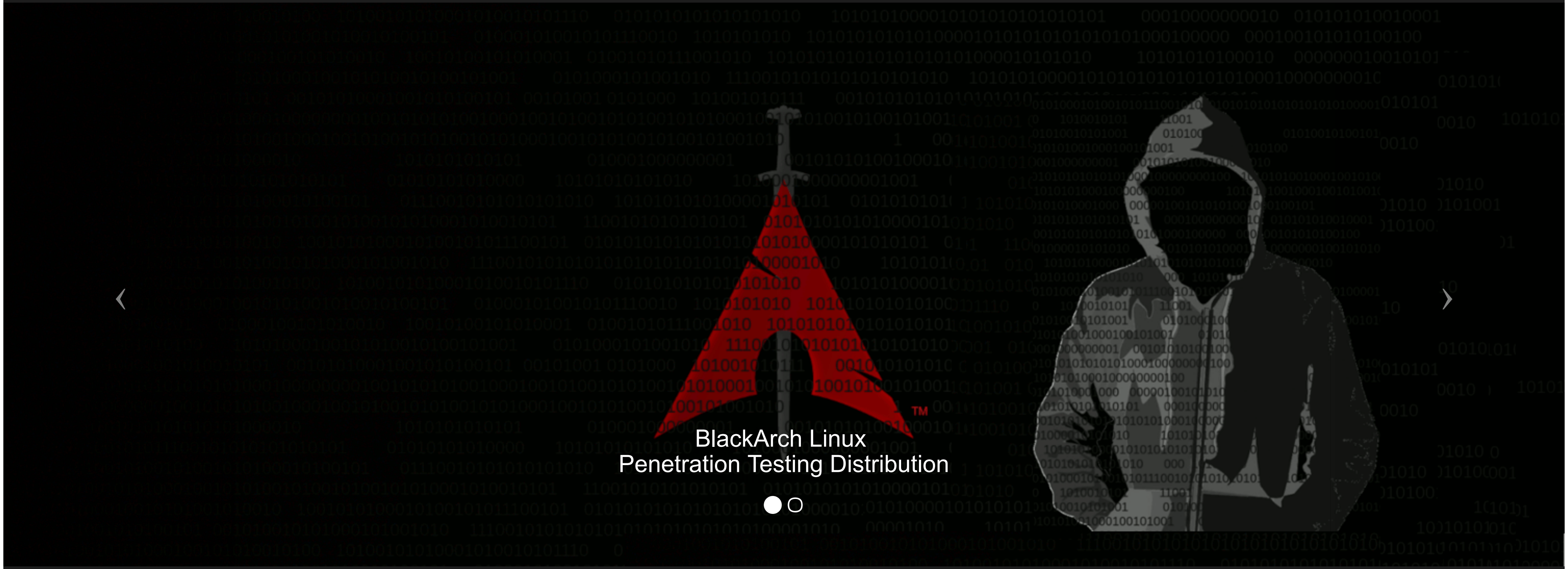

Webapp

The list

Home / tools / webapp

Packages that primarily attack social networking sites.

Tool count: 179

BlackArch webapp

Name	Version	Description	Homepage
0d1n	209.ce7c032	Web security tool to make fuzzing at HTTP inputs, made in C with libCurl.	↗
adfind	29.179602f	Simple admin panel finder for php,js,cgi,asp and aspx admin panels.	↗
adminpagefinder	0.1	This python script looks for a large amount of possible administrative interfaces on a given site.	↗
albatar	24.142f892	A SQLi exploitation framework in Python.	↗
anti-xss	166.2725dc9	A XSS vulnerability scanner.	↗
arachni	1.5.1	A feature-full, modular, high-performance Ruby framework aimed towards helping penetration testers and administrators evaluate the security of web applications.	↗
astra	486.394d538	Automated Security Testing For REST API's.	↗
bbqsql	261.b9859d2	SQL injection exploit tool.	↗
bbscan	39.57a2e33	A tiny Batch weB vulnerability Scanner.	↗
bing-lfi-rfi	0.1	Python script for searching Bing for sites that may have local and remote file inclusion vulnerabilities.	↗
blisqy	20.e9995fc	Exploit Time-based blind-SQL injection in HTTP-Headers (MySQL/MariaDB).	↗
brutexss	54.ba753df	Cross-Site Scripting Bruteforcer.	↗
bsqlbf	2.7	Blind SQL Injection Brute Forcer.	↗
bsqlinjector	13.027184f	Blind SQL injection exploitation tool written in ruby.	↗
c5scan	29.33a500c	Vulnerability scanner and information gatherer for the Concrete5 CMS.	↗
cansina	14.b42ff88	A python-based Web Content Discovery Tool.	↗
chankro	14.b560921	Tool that generates a PHP capable of run a custom binary (like a meterpreter) or a bash script (p.e. reverse shell) bypassing disable_functions & open_basedir).	↗
cjexploiter	6.72b08d8	Drag and Drop ClickJacking exploit development assistance tool.	↗

Name	Version	Description	Homepage
cloudget	53.807d08e	Python script to bypass cloudflare from command line. Built upon cfscrape module.	↗
cms-few	0.1	Joomla, Mambo, PHP-Nuke, and XOOPS CMS SQL injection vulnerability scanning tool written in Python.	↗
cmseek	265.e6be137	CMS (Content Management Systems) Detection and Exploitation suite.	↗
cmsfuzz	5.6be5a98	Fuzzer for wordpress, cold fusion, drupal, joomla, and phpnuke.	↗
comission	32.0ed0ba1	WhiteBox CMS analysis.	↗
commix	1290.b7acfb0	Automated All-in-One OS Command Injection and Exploitation Tool.	↗
crawlic	51.739fe2b	Web recon tool (find temporary files, parse robots.txt, search folders, google dorks and search domains hosted on same server).	↗
csrftester	1.0	The OWASP CSRFTester Project attempts to give developers the ability to test their applications for CSRF flaws.	↗
cybercrowl	108.39d9f0b	A Python Web path scanner tool.	↗
darkjumper	5.8	This tool will try to find every website that host at the same server at your target.	↗
davscan	28.13ae481	Fingerprints servers, finds exploits, scans WebDAV.	↗
dawnscanner	1.6.9	A static analysis security scanner for ruby written web applications.	↗
dff-scanner	1.1	Tool for finding path of predictable resource locations.	↗
dirbuster-ng	9.0c34920	C CLI implementation of the Java dirbuster tool.	↗
dirhunt	204.e369e98	Find web directories without bruteforce.	↗
dirsearch	281.181fbec	HTTP(S) directory/file brute forcer.	↗
domi-owned	41.583d0a5	A tool used for compromising IBM/Lotus Domino servers.	↗
doork	6.90c7260	Passive Vulnerability Auditor.	↗
dorknet	57.e4742cc	Selenium powered Python script to automate searching for vulnerable web apps.	↗

Name	Version	Description	Homepage
droopescan	1.41.2	A plugin-based scanner that aids security researchers in identifying issues with several CMSs, mainly Drupal & Silverstripe.	↗
drupal-module-enum	11.525543c	Enumerate on drupal modules.	↗
drupalscan	0.5.2	Simple non-intrusive Drupal scanner.	↗
drupwn	55.fce465f	Drupal enumeration & exploitation tool.	↗
dsfs	33.d3efef5	A fully functional File inclusion vulnerability scanner (supporting GET and POST parameters) written in under 100 lines of code.	↗
dsjs	24.711d6d1	A fully functional JavaScript library vulnerability scanner written in under 100 lines of code.	↗
dsss	117.3ba8faa	A fully functional SQL injection vulnerability scanner (supporting GET and POST parameters) written in under 100 lines of code.	↗
dsxs	122.bf39ef7	A fully functional Cross-site scripting vulnerability scanner (supporting GET and POST parameters) written in under 100 lines of code.	↗
epicwebhoneypot	2.0a	Tool which aims to lure attackers using various types of web vulnerability scanners by tricking them into believing that they have found a vulnerability on a host.	↗
eyewitness	758.902509a	Designed to take screenshots of websites, provide some server header info, and identify default credentials if possible.	↗
fbht	70.d75ae93	A Facebook Hacking Tool	↗
fhttp	1.3	This is a framework for HTTP related attacks. It is written in Perl with a GTK interface, has a proxy for debugging and manipulation, proxy chaining, evasion rules, and more.	↗
filebuster	55.e0aba68	An extremely fast and flexible web fuzzer.	↗
fuxploider	125.ca939e9	Tool that automates the process of detecting and exploiting file upload forms flaws.	↗
ghost-py	2.0.0	Webkit based webclient (relies on PyQT).	↗

Name	Version	Description	Homepage
gittools	46.37487f6	A repository with 3 tools for pwn'ing websites with .git repositories available'.	↗
gobuster	191.0e209e5	Directory/file & DNS busting tool written in Go.	↗
golismero	70.e8f274e	Opensource web security testing framework.	↗
gopherus	22.57d1d07	Tool generates gopher link for exploiting SSRF and gaining RCE in various servers.	↗
grabber	0.1	A web application scanner. Basically it detects some kind of vulnerabilities in your website.	↗
htcap	110.a0a04f6	A web application analysis tool for detecting communications between javascript and the server.	↗
httpforge	11.02.01	A set of shell tools that let you manipulate, send, receive, and analyze HTTP messages. These tools can be used to test, discover, and assert the security of Web servers, apps, and sites. An accompanying Python library is available for extensions.	↗
httppwnly	47.528a664	"Repeater" style XSS post-exploitation tool for mass browser control.	↗
jaidam	18.15e0fec	Penetration testing tool that would take as input a list of domain names, scan them, determine if wordpress or joomla platform was used and finally check them automatically, for web vulnerabilities using two well-known open source tools, WPScan and Joomscan.	↗
jexboss	86.338b531	Jboss verify and Exploitation Tool.	↗
jok3r	66.1f7e7b6	Network and Web Pentest Framework.	↗
jomplug	0.1	This php script fingerprints a given Joomla system and then uses Packet Storm's archive to check for bugs related to the installed components.	↗
jooforce	11.43c21ad	A Joomla password brute force tester.	↗
joomlascan	1.2	Joomla scanner scans for known vulnerable remote file inclusion paths and files.	↗
joomlavs	254.eea7500	A black box, Ruby powered, Joomla vulnerability scanner.	↗

Name	Version	Description	Homepage
joomscan	55.59ded07	Detects file inclusion, sql injection, command execution vulnerabilities of a target Joomla! web site.	↗
jshell	6.558906f	Get a JavaScript shell with XSS.	↗
jsql-injection	0.81	A Java application for automatic SQL database injection.	↗
jstillery	63.c6d8b87	Advanced JavaScript Deobfuscation via Partial Evaluation.	↗
kadimus	57.1d86f89	LFI Scan & Exploit Tool.	↗
kolkata	3.0	A web application fingerprinting engine written in Perl that combines cryptography with IDS evasion.	↗
lfi-exploiter	1.1	This perl script leverages /proc/self/environ to attempt getting code execution out of a local file inclusion vulnerability..	↗
lfi-fuzzploit	1.1	A simple tool to help in the fuzzing for, finding, and exploiting of local file inclusion vulnerabilities in Linux-based PHP applications.	↗
lfi-image-helper	0.8	A simple script to infect images with PHP Backdoors for local file inclusion attacks.	↗
lfi-sploiter	1.0	This tool helps you exploit LFI (Local File Inclusion) vulnerabilities. Post discovery, simply pass the affected URL and vulnerable parameter to this tool. You can also use this tool to scan a URL for LFI vulnerabilities.	↗
lfifreak	21.0c6adef	A unique automated LFi Exploiter with Bind/Reverse Shells.	↗
lfimap	6.0edee6d	This script is used to take the highest benefits of the local file include vulnerability in a webserver.	↗
liffy	65.8011cdd	A Local File Inclusion Exploitation tool.	↗
lightbulb	67.e0ddf00	Python framework for auditing web applications firewalls.	↗
list-urls	0.1	Extracts links from webpage.	↗
magescan	1.12.9	Scan a Magento site for information.	↗
mando.me	9.8b34f1a	Web Command Injection Tool.	↗
metoscan	05	Tool for scanning the HTTP methods supported by a webserver. It works by testing a URL and checking the responses for the different requests.	↗
mooscan	81.a0eff5f	A scanner for Moodle LMS.	↗

Name	Version	Description	Homepage
morxtraversal	1.0	Path Traversal checking tool.	↗
multiinjector	0.4	Automatic SQL injection utility using a lsit of URI addresses to test parameter manipulation.	↗
nosqlmap	238.ae0b461	Automated Mongo database and NoSQL web application exploitation tool	↗
novahot	23.69857bb	A webshell framework for penetration testers.	↗
opendoor	385.704cb08	OWASP WEB Directory Scanner.	↗
owasp-bywaf	26.e730d1b	A web application penetration testing framework (WAPTF).	↗
owtf	1017.0bbeea1	The Offensive (Web) Testing Framework.	↗
pappy-proxy	77.e1bb049	An intercepting proxy for web application testing.	↗
parameth	56.8da6f27	This tool can be used to brute discover GET and POST parameters.	↗
paros	3.2.13	Java-based HTTP/HTTPS proxy for assessing web app vulnerabilities. Supports editing/viewing HTTP messages on-the-fly, spiders, client certificates, proxy-chaining, intelligent scanning for XSS and SQLi, etc.	↗
payloadmask	16.ff38964	Web Payload list editor to use techniques to try bypass web application firewall.	↗
peepingtom	56.bc6f4d8	A tool to take screenshots of websites. Much like eyewitness.	↗
photon	307.c7326a6	Incredibly fast crawler which extracts urls, emails, files, website accounts and much more.	↗
php-findsock-shell	2.b8a984f	A Findsock Shell implementation in PHP + C.	↗
phpsploit	891.dfd9b16	Stealth post-exploitation framework.	↗
plecost	98.1a4a11b	Wordpress finger printer Tool.	↗
plown	13.ccf998c	A security scanner for Plone CMS.	↗
pown	91.d3457e4	Security testing and exploitation toolkit built on top of Node.js and NPM.	↗
proxenet	712.67fc6b5	THE REAL hacker friendly proxy for web application pentests.	↗

Name	Version	Description	Homepage
pyfiscan	2261.b6abeed	Free web-application vulnerability and version scanner.	↗
remot3d	35.788f2bb	An Simple Exploit for PHP Language.	↗
riwifshell	38.40075d5	Web backdoor - infector - explorer.	↗
ruler	271.882cc5f	A tool to abuse Exchange services.	↗
rww-attack	0.9.2	The Remote Web Workplace Attack tool will perform a dictionary attack against a live Microsoft Windows Small Business Server's 'Remote Web Workplace' portal. It currently supports both SBS 2003 and SBS 2008 and includes features to avoid account lock out.	↗
sawef	28.e65dc9f	Send Attack Web Forms.	↗
scrapy	1.6.0	A fast high-level scraping and web crawling framework.	↗
secscan	1.5	Web Apps Scanner and Much more utilities.	↗
shortfuzzy	0.1	A web fuzzing script written in perl.	↗
sitadel	59.7618dc7	Web Application Security Scanner.	↗
sitediff	3.1383935	Fingerprint a web app using local files as the fingerprint sources.	↗
smplshllctrlr	9.2baf390	PHP Command Injection exploitation tool.	↗
snallygaster	53.0e1fb70	Tool to scan for secret files on HTTP servers.	↗
snuck	6.76196b6	Automatic XSS filter bypass.	↗
spaf	11.671a976	Static Php Analysis and Fuzzer.	↗
sparty	0.1	An open source tool written in python to audit web applications using sharepoint and frontpage architecture.	↗
spiga	623.8bc1ddc	Configurable web resource scanner.	↗
spike-proxy	148	A Proxy for detecting vulnerabilities in web applications	↗
spipscan	69.4ad3235	SPIP (CMS) scanner for penetration testing purpose written in Python.	↗
sqid	0.3	A SQL injection digger.	↗
sqlmap	1.3.4	Automatic SQL injection and database takeover tool	↗
themole	0.3	Automatic SQL injection exploitation tool.	↗
tplmap	708.39c7c5b	Automatic Server-Side Template Injection Detection and Exploitation Tool.	↗

Name	Version	Description	Homepage
typo-enumerator	81.b01084b	Enumerate Typo3 version and extensions.	↗
uncaptcha2	7.473f33d	Defeating the latest version of ReCaptcha with 91% accuracy.	↗
uppwn	9.f69dec4	A script that automates detection of security flaws on websites' file upload systems'.	↗
urlcrazy	0.5	Generate and test domain typos and variations to detect and perform typo squatting, URL hijacking, phishing, and corporate espionage.	↗
urldigger	02c	A python tool to extract URL addresses from different HOT sources and/or detect SPAM and malicious code	↗
vanguard	0.1	A comprehensive web penetration testing tool written in Perl thatidentifies vulnerabilities in web applications.	↗
vbscan	37.f11f1f0	A black box vBulletin vulnerability scanner written in perl.	↗
vega	1.0	An open source platform to test the security of web applications.	↗
vsvbp	6.241a7ab	Black box tool for Vulnerability detection in web applications.	↗
vulnerabilities-spider	1.426e70f	A tool to scan for web vulnerabilities.	↗
wafninja	25.379cd98	A tool which contains two functions to attack Web Application Firewalls.	↗
wafp	0.01_26c3	An easy to use Web Application Finger Printing tool written in ruby using sqlite3 databases for storing the fingerprints.	↗
wafpass	44.624ac65	Analysing parameters with all payloads' bypass methods, aiming at benchmarking security solutions like WAF.	↗
wascan	26.59fe412	Web Application Scanner.	↗
waybackpack	49.36db906	Download the entire Wayback Machine archive for a given URL.	↗
web-soul	2	A plugin based scanner for attacking and data mining web sites written in Perl.	↗
webborer	162.be01969	A directory-enumeration tool written in Go.	↗
webhandler	344.a7490cf	A handler for PHP system functions & also an alternative 'netcat' handler.	↗

Name	Version	Description	Homepage
webslayer	5	A tool designed for brute forcing Web Applications.	↗
webxploiter	56.c03fe6b	An OWASP Top 10 Security scanner.	↗
weevely	829.8036a61	Weaponized web shell.	↗
whatsmyname	265.1f90346	Tool to perform user and username enumeration on various websites.	↗
whichcdn	22.5fc6ddd	Tool to detect if a given website is protected by a Content Delivery Network.	↗
wig	574.d5ddd91	WebApp Information Gatherer.	↗
witchxtool	1.1	A perl script that consists of a port scanner, LFI scanner, MD5 bruteforcer, dork SQL injection scanner, fresh proxy scanner, and a dork LFI scanner.	↗
wordpress-exploit-framework	902.4462106	A Ruby framework for developing and using modules which aid in the penetration testing of WordPress powered websites and systems.	↗
wpforce	87.31024e0	Wordpress Attack Suite.	↗
wpintel	6.741c0c9	Chrome extension designed for WordPress Vulnerability Scanning and information gathering.	↗
wpscan	3.4.4	Black box WordPress vulnerability scanner	↗
wpseku	34.bd45994	Simple Wordpress Security Scanner.	↗
ws-attacker	1.7	A modular framework for web services penetration testing.	↗
wssip	75.56d0d2c	Application for capturing, modifying and sending custom WebSocket data from client to server and vice versa.	↗
wuzz	209.4c6d320	Interactive cli tool for HTTP inspection.	↗
xattacker	88.0beb7a6	Website Vulnerability Scanner & Auto Exploiter.	↗
xsrfprobe	427.b5f2a32	The Prime Cross Site Request Forgery Audit and Exploitation Toolkit.	↗
xsscrapy	139.06ad0aa	XSS spider - 66/66 wavsep XSS detected.	↗
xsser	1.7	A penetration testing tool for detecting and exploiting XSS vulnerabilites.	↗
xssless	45.8e7ebe1	An automated XSS payload generator written in python.	↗
xsspy	56.d317b27	Web Application XSS Scanner.	↗

Name	Version	Description	Homepage
xsss	0.40b	A brute force cross site scripting scanner.	↗
xssscan	17.7f1ea90	Command line tool for detection of XSS attacks in URLs. Based on ModSecurity rules from OWASP CRS.	↗
xsssniper	79.02b59af	An automatic XSS discovery tool	↗
xsstrike	396.291f99a	An advanced XSS detection and exploitation suite.	↗
xssya	13.cd62817	A Cross Site Scripting Scanner & Vulnerability Confirmation.	↗
xwaf	153.8471a27	Automatic WAF bypass tool.	↗
yaaf	7.4d6273a	Yet Another Admin Finder.	↗
yasuo	121.994dcb1	A ruby script that scans for vulnerable & exploitable 3rd-party web applications on a network.	↗
yawast	607.6536cce	The YAWAST Antecedent Web Application Security Toolkit.	↗
ycrawler	0.1	A web crawler that is useful for grabbing all user supplied input related to a given website and will save the output. It has proxy and log file support.	↗
ysoserial	0.0.5	A proof-of-concept tool for generating payloads that exploit unsafe Java object deserialization.	↗
zaproxy	2.7.0	Integrated penetration testing tool for finding vulnerabilities in web applications	↗

BlackArch Linux 2013-2019