infoslack / awesome-web-hacking

A list of web application security

penetration-testing web-hacking vulnerabilities scanner

65 commits **1** branch **0** releases **10** contributors

Branch: **master** New pull request Find file Clone or download

infoslack committed on Oct 25, 2017 Merge pull request #21 from WangYihang/patch-2 ··· Latest commit c64877a on Oct 25, 2017

README.md Merge pull request #21 from WangYihang/patch-2 7 months ago

README.md

awesome-web-hacking

This list is for anyone wishing to learn about web application security but do not have a starting point.

You can help by sending Pull Requests to add more information.

If you're not inclined to make PRs you can tweet me at `@infoslack`

Table of Contents

Books

- http://www.amazon.com/The-Web-Application-Hackers-Handbook/dp/8126533404/ The Web Application Hacker's Handbook: Finding and Exploiting Security Flaws
- http://www.amazon.com/Hacking-Web-Apps-Preventing-Application/dp/159749951X/ Hacking Web Apps: Detecting and Preventing Web Application Security Problems
- http://www.amazon.com/Hacking-Exposed-Web-Applications-Third/dp/0071740643/ Hacking Exposed Web Applications
- http://www.amazon.com/SQL-Injection-Attacks-Defense-Second/dp/1597499633/ SQL Injection Attacks and Defense
- http://www.amazon.com/Tangled-Web-Securing-Modern-Applications/dp/1593273886/ The Tangled WEB: A Guide to Securing Modern Web Applications
- http://www.amazon.com/Web-Application-Obfuscation-Evasion-Filters/dp/1597496049/ Web Application Obfuscation: '-/WAFs..Evasion..Filters//alert(/Obfuscation/)-'
- http://www.amazon.com/XSS-Attacks-Scripting-Exploits-Defense/dp/1597491543/ XSS Attacks: Cross Site Scripting Exploits and Defense
- http://www.amazon.com/Browser-Hackers-Handbook-Wade-Alcorn/dp/1118662091/ The Browser Hacker's Handbook
- http://www.amazon.com/Basics-Web-Hacking-Techniques-Attack/dp/0124166008/ The Basics of Web Hacking: Tools and Techniques to Attack the Web
- http://www.amazon.com/Web-Penetration-Testing-Kali-Linux/dp/1782163166/ Web Penetration Testing with Kali Linux
- http://www.amazon.com/Web-Application-Security-Beginners-Guide/dp/0071776168/ Web Application Security, A Beginner's Guide
- https://www.crypto101.io/ - Crypto 101 is an introductory course on cryptography
- http://www.offensive-security.com/metasploit-unleashed/ - Metasploit Unleashed
- http://www.cl.cam.ac.uk/~rja14/book.html - Security Engineering
- https://www.feistyduck.com/library/openssl-cookbook/ - OpenSSL Cookbook

Documentation

- https://www.owasp.org/ - Open Web Application Security Project
- http://www.pentest-standard.org/ - Penetration Testing Execution Standard
- http://www.binary-auditing.com/ - Dr. Thorsten Schneider's Binary Auditing

Tools

- http://www.metasploit.com/ - World's most used penetration testing software
- http://www.arachni-scanner.com/ - Web Application Security Scanner Framework
- https://github.com/sullo/nikto - Nikto web server scanner
- http://www.tenable.com/products/nessus-vulnerability-scanner - Nessus Vulnerability Scanner
- http://www.portswigger.net/burp/intruder.html - Burp Intruder is a tool for automating customized attacks against web apps.
- http://www.openvas.org/ - The world's most advanced Open Source vulnerability scanner and manager.
- https://github.com/iSECPartners/Scout2 - Security auditing tool for AWS environments
- https://www.owasp.org/index.php/Category:OWASP_DirBuster_Project - Is a multi threaded java application designed to brute force directories and files names on web/application servers.
- https://www.owasp.org/index.php/ZAP - The Zed Attack Proxy is an easy to use integrated penetration testing tool for finding vulnerabilities in web applications.
- https://github.com/tecknicaltom/dsniff - dsniff is a collection of tools for network auditing and penetration testing. * https://github.com/WangYihang/Webshell-Sniper - Manage your webshell via terminal. * https://github.com/DanMcInerney/dnsspoof - DNS spoofer. Drops DNS responses from the router and replaces it with the spoofed DNS response
- https://github.com/trustedsec/social-engineer-toolkit - The Social-Engineer Toolkit (SET) repository from TrustedSec

- https://github.com/sqlmapproject/sqlmap - Automatic SQL injection and database takeover tool
- https://github.com/beefproject/beef - The Browser Exploitation Framework Project
- http://w3af.org/ - w3af is a Web Application Attack and Audit Framework
- https://github.com/espreto/wpsploit - WPSploit, Exploiting Wordpress With Metasploit *
  https://github.com/WangYihang/Reverse-Shell-Manager - Reverse shell manager via terminal. *
  https://github.com/RUB-NDS/WS-Attacker - WS-Attacker is a modular framework for web services penetration testing
- https://github.com/wpscanteam/wpscan - WPScan is a black box WordPress vulnerability scanner
- http://sourceforge.net/projects/paros/ Paros proxy
- https://www.owasp.org/index.php/Category:OWASP_WebScarab_Project Web Scarab proxy
- https://code.google.com/p/skipfish/ Skipfish, an active web application security reconnaissance tool
- http://www.acunetix.com/vulnerability-scanner/ Acunetix Web Vulnerability Scanner
- http://www-03.ibm.com/software/products/en/appscan IBM Security AppScan
- https://www.netsparker.com/web-vulnerability-scanner/ Netsparker web vulnerability scanner
- http://www8.hp.com/us/en/software-solutions/webinspect-dynamic-analysis-dast/index.html HP Web Inspect
- https://github.com/sensepost/wikto Wikto - Nikto for Windows with some extra features
- http://samurai.inguardians.com Samurai Web Testing Framework
- https://code.google.com/p/ratproxy/ Ratproxy
- http://www.websecurify.com Websecurify
- http://sourceforge.net/projects/grendel/ Grendel-scan
- https://www.owasp.org/index.php/Category:OWASP_DirBuster_Project DirBuster
- http://www.edge-security.com/wfuzz.php Wfuzz
- http://wapiti.sourceforge.net wapiti
- https://github.com/neuroo/grabber Grabber
- https://subgraph.com/vega/ Vega

- http://websecuritytool.codeplex.com Watcher passive web scanner
- http://xss.codeplex.com x5s XSS and Unicode transformations security testing assistant
- http://www.beyondsecurity.com/avds AVDS Vulnerability Assessment and Management
- http://www.golismero.com Golismero
- http://www.ikare-monitoring.com IKare
- http://www.nstalker.com N-Stalker X
- https://www.rapid7.com/products/nexpose/index.jsp Nexpose
- http://www.rapid7.com/products/appspider/ App Spider
- http://www.milescan.com ParosPro
- https://www.qualys.com/enterprises/qualysguard/web-application-scanning/ Qualys Web Application Scanning
- http://www.beyondtrust.com/Products/RetinaNetworkSecurityScanner/ Retina
- https://www.owasp.org/index.php/OWASP_Xenotix_XSS_Exploit_Framework Xenotix XSS Exploit Framework
- https://github.com/future-architect/vuls Vulnerability scanner for Linux, agentless, written in golang.
- https://github.com/rastating/wordpress-exploit-framework A Ruby framework for developing and using modules which aid in the penetration testing of WordPress powered websites and systems.
- http://www.xss-payloads.com/ XSS Payloads to leverage XSS vulnerabilities, build custom payloads, practice penetration testing skills.
- https://github.com/joaomatosf/jexboss JBoss (and others Java Deserialization Vulnerabilities) verify and EXploitation Tool
- https://github.com/commixproject/commix Automated All-in-One OS command injection and exploitation tool
- https://github.com/pathetiq/BurpSmartBuster A Burp Suite content discovery plugin that add the smart into the Buster!
- https://github.com/GoSecure/csp-auditor Burp and ZAP plugin to analyze CSP headers
- https://github.com/ffleming/timing_attack Perform timing attacks against web applications
- https://github.com/lalithr95/fuzzapi Fuzzapi is a tool used for REST API pentesting
- https://github.com/owtf/owtf Offensive Web Testing Framework (OWTF)

- https://github.com/nccgroup/wssip Application for capturing, modifying and sending custom WebSocket data from client to server and vice versa.
- https://github.com/tijme/angularjs-csti-scanner Automated client-side template injection (sandbox escape/bypass) detection for AngularJS (ACSTIS).

Cheat Sheets

- http://n0p.net/penguicon/php_app_sec/mirror/xss.html - XSS cheatsheet
- https://highon.coffee/blog/lfi-cheat-sheet/ - LFI Cheat Sheet
- https://highon.coffee/blog/reverse-shell-cheat-sheet/ - Reverse Shell Cheat Sheet
- https://www.netsparker.com/blog/web-security/sql-injection-cheat-sheet/ - SQL Injection Cheat Sheet
- https://www.gracefulsecurity.com/path-traversal-cheat-sheet-windows/ - Path Traversal Cheat Sheet: Windows

Docker images for Penetration Testing

- `docker pull kalilinux/kali-linux-docker` official Kali Linux
- `docker pull owasp/zap2docker-stable` - official OWASP ZAP
- `docker pull wpscanteam/wpscan` - official WPScan
- `docker pull pandrew/metasploit` - docker-metasploit
- `docker pull citizenstig/dvwa` - Damn Vulnerable Web Application (DVWA)
- `docker pull wpscanteam/vulnerablewordpress` - Vulnerable WordPress Installation
- `docker pull hmlio/vaas-cve-2014-6271` - Vulnerability as a service: Shellshock
- `docker pull hmlio/vaas-cve-2014-0160` - Vulnerability as a service: Heartbleed
- `docker pull opendns/security-ninjas` - Security Ninjas
- `docker pull usertaken/archlinux-pentest-lxde` - Arch Linux Penetration Tester

- `docker pull diogomonica/docker-bench-security` - Docker Bench for Security
- `docker pull ismisepaul/securityshepherd` - OWASP Security Shepherd
- `docker pull danmx/docker-owasp-webgoat` - OWASP WebGoat Project docker image
- `docker pull citizenstig/nowasp` - OWASP Mutillidae II Web Pen-Test Practice Application

Vulnerabilities

- http://cve.mitre.org/ - Common Vulnerabilities and Exposures. The Standard for Information Security Vulnerability Names
- https://www.exploit-db.com/ - The Exploit Database – ultimate archive of Exploits, Shellcode, and Security Papers.
- http://0day.today/ - Inj3ct0r is the ultimate database of exploits and vulnerabilities and a great resource for vulnerability researchers and security professionals.
- http://osvdb.org/ - OSVDB's goal is to provide accurate, detailed, current, and unbiased technical security information.
- http://www.securityfocus.com/ - Since its inception in 1999, SecurityFocus has been a mainstay in the security community.
- http://packetstormsecurity.com/ - Global Security Resource
- https://wpvulndb.com/ - WPScan Vulnerability Database

Courses

- https://www.elearnsecurity.com/course/web_application_penetration_testing/ eLearnSecurity Web Application Penetration Testing
- https://www.elearnsecurity.com/course/web_application_penetration_testing_extreme/ eLearnSecurity Web Application Penetration Testing eXtreme
- https://www.offensive-security.com/information-security-training/advanced-web-attack-and-exploitation/ Offensive Security Advanced Web Attacks and Exploitation (live)

- https://www.sans.org/course/web-app-penetration-testing-ethical-hacking Sans SEC542: Web App Penetration Testing and Ethical Hacking
- https://www.sans.org/course/advanced-web-app-penetration-testing-ethical-hacking Sans SEC642: Advanced Web App Penetration Testing and Ethical Hacking * http://opensecuritytraining.info/ - Open Security Training
- http://securitytrainings.net/security-trainings/ - Security Exploded Training
- http://www.cs.fsu.edu/~redwood/OffensiveComputerSecurity/ - FSU - Offensive Computer Security
- http://www.cs.fsu.edu/~lawrence/OffNetSec/ - FSU - Offensive Network Security
- http://www.securitytube.net/ - World's largest Infosec and Hacking Portal.

Online Hacking Demonstration Sites

- http://testasp.vulnweb.com/ - Acunetix ASP test and demonstration site
- http://testaspnet.vulnweb.com/ - Acunetix ASP.Net test and demonstration site
- http://testphp.vulnweb.com/ - Acunetix PHP test and demonstration site
- http://crackme.cenzic.com/kelev/view/home.php - Crack Me Bank
- http://zero.webappsecurity.com/ - Zero Bank
- http://demo.testfire.net/ - Altoro Mutual

Labs

- http://www.cis.syr.edu/~wedu/seed/all_labs.html - Developing Instructional Laboratories for Computer SEcurity EDucation
- https://www.vulnhub.com/ - Virtual Machines for Localhost Penetration Testing.
- https://pentesterlab.com/ - PentesterLab is an easy and great way to learn penetration testing.

- https://github.com/jerryhoff/WebGoat.NET - This web application is a learning platform about common web security flaws.
- http://www.dvwa.co.uk/ - Damn Vulnerable Web Application (DVWA)
- http://sourceforge.net/projects/lampsecurity/ - LAMPSecurity Training
- https://github.com/Audi-1/sqli-labs - SQLI labs to test error based, Blind boolean based, Time based.
- https://github.com/paralax/lfi-labs - small set of PHP scripts to practice exploiting LFI, RFI and CMD injection vulns
- https://hack.me/ - Build, host and share vulnerable web apps in a sandboxed environment for free
- http://azcwr.org/az-cyber-warfare-ranges - Free live fire Capture the Flag, blue team, red team Cyber Warfare Range for beginners through advanced users. Must use a cell phone to send a text message requesting access to the range.
- https://github.com/adamdoupe/WackoPicko - WackoPicko is a vulnerable web application used to test web application vulnerability scanners.
- https://github.com/rapid7/hackazon - Hackazon is a free, vulnerable test site that is an online storefront built with the same technologies used in today's rich client and mobile applications.

SSL

- https://www.ssllabs.com/ssltest/index.html - This service performs a deep analysis of the configuration of any SSL web server on the public Internet.
- https://raymii.org/s/tutorials/Strong_SSL_Security_On_nginx.html - Strong SSL Security on nginx
- https://weakdh.org/ - Weak Diffie-Hellman and the Logjam Attack
- https://letsencrypt.org/ - Let's Encrypt is a new Certificate Authority: It's free, automated, and open.
- https://filippo.io/Heartbleed/ - A checker (site and tool) for CVE-2014-0160 (Heartbleed).

Security Ruby on Rails

- http://brakemanscanner.org/ - A static analysis security vulnerability scanner for Ruby on Rails applications.
- https://github.com/rubysec/ruby-advisory-db - A database of vulnerable Ruby Gems
- https://github.com/rubysec/bundler-audit - Patch-level verification for Bundler
- https://github.com/hakirisec/hakiri_toolbelt - Hakiri Toolbelt is a command line interface for the Hakiri platform.
- https://hakiri.io/facets - Scan Gemfile.lock for vulnerabilities.
- http://rails-sqli.org/ - This page lists many query methods and options in ActiveRecord which do not sanitize raw SQL arguments and are not intended to be called with unsafe user input.
- https://github.com/0xsauby/yasuo - A ruby script that scans for vulnerable & exploitable 3rd-party web applications on a network