qazbnm456 / **awesome-web-security**

A curated list of Web Security materials and resources. https://awesomelists.top/#/repos/qazb…

awesome-list awesome list web security websecurity penetration-testing

206 commits **1** branch **0** releases **9** contributors

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

qazbnm456 Merge pull request #15 from Metnew/master ··· Latest commit 0848478 6 days ago

.vscode	lint	3 months ago

.gitignore	Update README.md	a year ago
CONTRIBUTING.md	Fixed broken link	2 months ago
README-jp.md	feat(readme-jp): add uxss-db	6 days ago
README-zh.md	feat(readme-zh): add uxss-db	6 days ago
README.md	feat(readme): add uxss-db	7 days ago
code-of-conduct.md	add code-of-conduct.md & README.md and revise CONTRIBUTING.md	10 months ago

README.md

Awesome Web Security 

> 🐱 Curated list of Web Security materials and resources.

Needless to say, most websites suffer from various types of bugs which may eventually lead to vulnerabilities. Why would this happen so often? There can be many factors involved including misconfiguration, shortage of engineers' security skills, etc. To combat this, here is a curated list of Web Security materials and resources for learning cutting edge penetrating techniques.

Please read the contribution guidelines before contributing.

🌈 **Want to strengthen your penetration skills?**
I would recommend playing some awesome-ctfs.

If you enjoy this awesome list and would like to support it, check out my Patreon page :)
Also, don't forget to check out my repos 🐾 or say *hi* on my Twitter!

Contents

    - Crypto
    - Web Shell
    - OSINT
    - Books
- Evasions
    - CSP
    - WAF
    - JSMVC
    - Authentication
- Tricks
    - CSRF
    - Remote Code Execution
    - XSS
    - SQL Injection
    - NoSQL Injection
    - FTP Injection
    - XXE
    - SSRF
    - Header Injection
    - URL
    - Others
- Browser Exploitation
- PoCs
    - JavaScript

- Tools
  - Auditing
  - Reconnaissance
    - OSINT
    - Sub Domain Enumeration
  - Code Generating
  - Fuzzing
  - Penetrating
  - Leaking
  - Offensive
    - XSS
    - SQL Injection
    - Template Injection
  - Detecting
  - Preventing
  - Proxy
  - Webshell
  - Disassembler
  - Decompiler
  - Others
- Social Engineering Database
- Blogs
- Twitter Users
- Practices

    - Application
    - AWS
    - XSS
    - ModSecurity / OWASP ModSecurity Core Rule Set
- Community
- Miscellaneous

Forums

- Phrack Magazine - Ezine written by and for hackers.
- The Hacker News - Security in a serious way.
- Security Weekly - The security podcast network.
- The Register - Biting the hand that feeds IT.
- Dark Reading - Connecting The Information Security Community.
- HackDig - Dig high-quality web security articles for hacker.

Resources

Tips

- Hacker101 - Written by hackerone.
- The Daily Swig - Web security digest - Written by PortSwigger.
- Web Application Security Zone by Netsparker - Written by Netsparker.
- Infosec Newbie - Written by Mark Robinson.
- The Magic of Learning - Written by @bitvijays.

- CTF Field Guide - Written by Trail of Bits.

XSS - Cross-Site Scripting

- Cross-Site Scripting – Application Security – Google - Introduction to XSS by Google.
- H5SC - HTML5 Security Cheatsheet - Collection of HTML5 related XSS attack vectors by @cure53.
- XSS.png - XSS mind map by @jackmasa.
- C.XSS Guide - Comprehensive tutorial on cross-site scripting by @JakobKallin and Irene Lobo Valbuena.

CSV Injection

- CSV Injection -> Meterpreter on Pornhub - Written by Andy.
- The Absurdly Underestimated Dangers of CSV Injection - Written by George Mauer.

SQL Injection

- SQL Injection Cheat Sheet - Written by @netsparker.
- SQL Injection Wiki - Written by NETSPI.
- SQL Injection Pocket Reference - Written by @LightOS.

Command Injection

- Potential command injection in resolv.rb - Written by @drigg3r.

ORM Injection

- HQL for pentesters - Written by @h3xstream.

- HQL : Hyperinsane Query Language (or how to access the whole SQL API within a HQL injection ?) - Written by @_m0bius.
- ORM2Pwn: Exploiting injections in Hibernate ORM - Written by Mikhail Egorov.
- ORM Injection - Written by Simone Onofri.

FTP Injection

- Advisory: Java/Python FTP Injections Allow for Firewall Bypass - Written by Timothy Morgan.
- SMTP over XXE − how to send emails using Java's XML parser - Written by Alexander Klink.

XXE - XML eXternal Entity

- XXE - Written by @phonexicum.

CSRF - Cross-Site Request Forgery

- Wiping Out CSRF - Written by @jrozner.

SSRF - Server-Side Request Forgery

- SSRF bible. Cheatsheet - Written by @Wallarm.

Rails

- Rails Security - First part - Written by @qazbnm456.

AngularJS

- XSS without HTML: Client-Side Template Injection with AngularJS - Written by Gareth Heyes.

- DOM based Angular sandbox escapes - Written by @garethheyes

SSL/TLS

- SSL & TLS Penetration Testing - Written by APTIVE.

Webmail

NFS

- NFS | PENETRATION TESTING ACADEMY - Written by PENETRATION ACADEMY.

AWS

- PENETRATION TESTING AWS STORAGE: KICKING THE S3 BUCKET - Written by Dwight Hohnstein from Rhino Security Labs.
- AWS PENETRATION TESTING PART 1. S3 BUCKETS - Written by @VirtueSecurity.
- AWS PENETRATION TESTING PART 2. S3, IAM, EC2 - Written by @VirtueSecurity.

Fingerprint

Sub Domain Enumeration

- A penetration tester's guide to sub-domain enumeration - Written by Bharath.
- The Art of Subdomain Enumeration - Written by Patrik Hudak.

Crypto

- Applied Crypto Hardening - Written by The bettercrypto.org Team.

Web Shell

- Hunting for Web Shells - Written by Jacob Baines.
- Hacking with JSP Shells - Written by @_nullbind.

OSINT

- Hacking Cryptocurrency Miners with OSINT Techniques - Written by @s3yfullah.
- OSINT x UCCU Workshop on Open Source Intelligence - Written by Philippe Lin.
- 102 Deep Dive in the Dark Web OSINT Style Kirby Plessas - Presented by @kirbstr.

Books

- XSS Cheat Sheet - 2018 Edition - Written by @brutelogic.

Evasions

CSP

- CSP: bypassing form-action with reflected XSS - Written by Detectify Labs.
- TWITTER XSS + CSP BYPASS - Written by Paulos Yibelo.

WAF

- Web Application Firewall (WAF) Evasion Techniques - Written by @secjuice.
- Web Application Firewall (WAF) Evasion Techniques #2 - Written by @secjuice.
- Airbnb – When Bypassing JSON Encoding, XSS Filter, WAF, CSP, and Auditor turns into Eight Vulnerabilities - Written by @Brett Buerhaus.

- How to bypass libinjection in many WAF/NGWAF - Written by @d0znpp.

JSMVC

- JavaScript MVC and Templating Frameworks - Written by Mario Heiderich.

Authentication

- Trend Micro Threat Discovery Appliance - Session Generation Authentication Bypass (CVE-2016-8584) - Written by @malerisch and @steventseeley.
- Yahoo Bug Bounty: Chaining 3 Minor Issues To Takeover Flickr Accounts - Written by Mishre.

Tricks

CSRF

- Neat tricks to bypass CSRF-protection - Written by Twosecurity.
- Exploiting CSRF on JSON endpoints with Flash and redirects - Written by @riyazwalikar.
- Stealing CSRF tokens with CSS injection (without iFrames) - Written by @dxa4481.

Remote Code Execution

- Exploiting Node.js deserialization bug for Remote Code Execution - Written by OpSecX.
- DRUPAL 7.X SERVICES MODULE UNSERIALIZE() TO RCE - Written by Ambionics Security.
- How we exploited a remote code execution vulnerability in math.js - Written by @capacitorset.
- GitHub Enterprise Remote Code Execution - Written by @iblue.
- How I Chained 4 vulnerabilities on GitHub Enterprise, From SSRF Execution Chain to RCE! - Written by Orange.

- How i Hacked into a PayPal's Server - Unrestricted File Upload to Remote Code Execution - Written by Vikas Anil Sharma.

XSS

- Query parameter reordering causes redirect page to render unsafe URL - Written by kenziy.
- ECMAScript 6 from an Attacker's Perspective - Breaking Frameworks, Sandboxes, and everything else - Written by Mario Heiderich.
- How I found a $5,000 Google Maps XSS (by fiddling with Protobuf) - Written by @marin_m.
- DON'T TRUST THE DOM: BYPASSING XSS MITIGATIONS VIA SCRIPT GADGETS - Written by Sebastian Lekies, Krzysztof Kotowicz, and Eduardo Vela.
- Uber XSS via Cookie - Written by zhchbin.
- DOM XSS – auth.uber.com - Written by StamOne_.
- Stored XSS on Facebook - Written by Enguerran Gillier.

SQL Injection

- MySQL Error Based SQL Injection Using EXP - Written by @osandamalith.
- SQL injection in an UPDATE query - a bug bounty story! - Written by Zombiehelp54.
- GitHub Enterprise SQL Injection - Written by Orange.

NoSQL Injection

- GraphQL NoSQL Injection Through JSON Types - Written by @east5th.

FTP Injection

- XML Out-Of-Band Data Retrieval - Written by @a66at and Alexey Osipov.

- XXE OOB exploitation at Java 1.7+ - Written by Ivan Novikov.

XXE

- Evil XML with two encodings - Written by Arseniy Sharoglazov.

SSRF

- PHP SSRF Techniques - Written by @themiddleblue.
- SSRF in https://imgur.com/vidgif/url - Written by aesteral.
- A New Era of SSRF - Exploiting URL Parser in Trending Programming Languages! - Written by Orange.
- SSRF Tips - Written by xl7dev.

Header Injection

- Java/Python FTP Injections Allow for Firewall Bypass - Written by Timothy Morgan.

URL

- Some Problems Of URLs - Written by Chris Palmer.
- Phishing with Unicode Domains - Written by Xudong Zheng.
- Unicode Domains are bad and you should feel bad for supporting them - Written by VRGSEC.
- [dev.twitter.com] XSS - Written by Sergey Bobrov.

Others

- How I hacked Google's bug tracking system itself for $15,600 in bounties - Written by @alex.birsan.
- Some Tricks From My Secret Group - Written by PHITHON.

- Uber Bug Bounty: Gaining Access To An Internal Chat System - Written by MISHRE.
- Inducing DNS Leaks in Onion Web Services - Written by @epidemics-scepticism.
- Stored XSS, and SSRF in Google using the Dataset Publishing Language - Written by @signalchaos.

Browser Exploitation

Frontend (like CSP bypass, URL spoofing, and something like that)

- JSON hijacking for the modern web - Written by portswigger.
- IE11 Information disclosure - local file detection - Written by James Lee.
- SOP bypass / UXSS – Stealing Credentials Pretty Fast (Edge) - Written by Manuel.
- Особенности Safari в client-side атаках - Written by Bo0oM.

Backend (core of Browser implementation, and often refers to C or C++ part)

- Attacking JavaScript Engines - A case study of JavaScriptCore and CVE-2016-4622 - Written by phrack@saelo.net.
- Three roads lead to Rome - Written by Luke Viruswalker.
- Exploiting a V8 OOB write. - Written by @halbecaf.
- FROM CRASH TO EXPLOIT: CVE-2015-6086 – OUT OF BOUND READ/ASLR BYPASS - Written by payatu.
- SSD Advisory – Chrome Turbofan Remote Code Execution - Written by SecuriTeam Secure Disclosure (SSD).
- Look Mom, I don't use Shellcode - Browser Exploitation Case Study for Internet Explorer 11 - Written by @moritzj.

PoCs

JavaScript

- js-vuln-db - Collection of JavaScript engine CVEs with PoCs by @tunz.
- awesome-cve-poc - Curated list of CVE PoCs by @qazbnm456.
- Some-PoC-oR-ExP - 各种漏洞poc、Exp的收集或编写 by @coffeehb.
- uxss-db - Collection of UXSS CVEs with PoCs by @Metnew.

Tools

Auditing

- prowler - Tool for AWS security assessment, auditing and hardening by @Alfresco.
- A2SV - Auto Scanning to SSL Vulnerability by @hahwul.

Reconnaissance

OSINT - Open-Source Intelligence

- Shodan - Shodan is the world's first search engine for Internet-connected devices by @shodanhq.
- Censys - Censys is a search engine that allows computer scientists to ask questions about the devices and networks that compose the Internet by University of Michigan.
- urlscan.io - Service which analyses websites and the resources they request by @heipei.
- ZoomEye - Cyberspace Search Engine by @zoomeye_team.
- FOFA - Cyberspace Search Engine by BAIMAOHUI.
- NSFOCUS - THREAT INTELLIGENCE PORTAL by NSFOCUS GLOBAL.
- FOCA - FOCA (Fingerprinting Organizations with Collected Archives) is a tool used mainly to find metadata and hidden information in the documents its scans by ElevenPaths.
- SpiderFoot - Open source footprinting and intelligence-gathering tool by @binarypool.

- xray - XRay is a tool for recon, mapping and OSINT gathering from public networks by @evilsocket.
- gitrob - Reconnaissance tool for GitHub organizations by @michenriksen.
- GSIL - Github Sensitive Information Leakage（Github敏感信息泄露）by @FeeiCN.
- raven - raven is a Linkedin information gathering tool that can be used by pentesters to gather information about an organization employees using Linkedin by @0x09AL.
- ReconDog - Recon Dog is an all in one tool for all your basic information gathering needs by @UltimateHackers.
- Databases - start.me - Various databases which you can use for your OSINT research by @technisette.
- peoplefindThor - the easy way to find people on Facebook by [postkassen](mailto:postkassen@oejvind.dk?subject=peoplefindthor.dk comments).
- tinfoleak - The most complete open-source tool for Twitter intelligence analysis by @vaguileradiaz.
- OSINT TOOLKIT - OSINT TOOLKIT by the OSINT Toolkit Admin Team.

Sub Domain Enumeration

- EyeWitness - EyeWitness is designed to take screenshots of websites, provide some server header info, and identify default credentials if possible by @ChrisTruncer.
- subDomainsBrute - A simple and fast sub domain brute tool for pentesters by @lijiejie.
- AQUATONE - Tool for Domain Flyovers by @michenriksen.
- domain_analyzer - Analyze the security of any domain by finding all the information possible by @eldraco.
- VirusTotal domain information - Searching for domain information by VirusTotal.
- Certificate Transparency - Google's Certificate Transparency project fixes several structural flaws in the SSL certificate system by @google.
- Certificate Search - Enter an Identity (Domain Name, Organization Name, etc), a Certificate Fingerprint (SHA-1 or SHA-256) or a crt.sh ID to search certificate(s) by @crtsh.
- GSDF - Domain searcher named GoogleSSLdomainFinder by @We5ter.

Code Generating

- VWGen - Vulnerable Web applications Generator by @qazbnm456.

Fuzzing

- wfuzz - Web application bruteforcer by @xmendez.
- charsetinspect - Script that inspects multi-byte character sets looking for characters with specific user-defined properties by @hack-all-the-things.
- IPObfuscator - Simple tool to convert the IP to a DWORD IP by @OsandaMalith.
- wpscan - WPScan is a black box WordPress vulnerability scanner by @wpscanteam.
- JoomlaScan - Free software to find the components installed in Joomla CMS, built out of the ashes of Joomscan by @drego85.
- domato - DOM fuzzer by @google.

Penetrating

- Burp Suite - Burp Suite is an integrated platform for performing security testing of web applications by portswigger.
- TIDoS-Framework - Web-penetration testing toolkit, presently suited for reconnaissance purposes by @the-Infected-Drake.
- Astra - Automated Security Testing For REST API's by @flipkart-incubator.
- aws_pwn - A collection of AWS penetration testing junk by @dagrz.

Offensive

XSS - Cross-Site Scripting

- XSStrike - XSStrike is a program which can fuzz and bruteforce parameters for XSS. It can also detect and bypass WAFs by @UltimateHackers.
- xssor2 - XSS'OR - Hack with JavaScript by @evilcos.

SQL Injection

- sqlmap - Automatic SQL injection and database takeover tool.

Template Injection

- tqlmap - Code and Server-Side Template Injection Detection and Exploitation Tool by @epinna.

Leaking

- HTTPLeaks - All possible ways, a website can leak HTTP requests by @cure53.
- dvcs-ripper - Rip web accessible (distributed) version control systems: SVN/GIT/HG... by @kost.
- DVCS-Pillage - Pillage web accessible GIT, HG and BZR repositories by @evilpacket.
- GitMiner - Tool for advanced mining for content on Github by @UnkL4b.
- gitleaks - Searches full repo history for secrets and keys by @zricethezav.
- CSS-Keylogging - Chrome extension and Express server that exploits keylogging abilities of CSS by @maxchehab.
- pwngitmanager - Git manager for pentesters by @allyshka.
- snallygaster - Tool to scan for secret files on HTTP servers by @hannob.

Detecting

- sqlchop - SQL injection detection engine by chaitin.
- xsschop - XSS detection engine by chaitin.
- retire.js - Scanner detecting the use of JavaScript libraries with known vulnerabilities by @RetireJS.

- malware-jail - Sandbox for semi-automatic Javascript malware analysis, deobfuscation and payload extraction by @HynekPetrak.
- repo-supervisor - Scan your code for security misconfiguration, search for passwords and secrets.
- bXSS - bXSS is a simple Blind XSS application adapted from cure53.de/m by @LewisArdern.

Preventing

- js-xss - Sanitize untrusted HTML (to prevent XSS) with a configuration specified by a Whitelist by @leizongmin.

Proxy

- Charles - HTTP proxy / HTTP monitor / Reverse Proxy that enables a developer to view all of the HTTP and SSL / HTTPS traffic between their machine and the Internet.
- mitmproxy - Interactive TLS-capable intercepting HTTP proxy for penetration testers and software developers by @mitmproxy.

Webshell

- webshell - This is a webshell open source project by @tennc.
- Weevely - Weaponized web shell by @epinna.
- Webshell-Sniper - Manage your website via terminal by @WangYihang.
- Reverse-Shell-Manager - Reverse Shell Manager via Terminal @WangYihang.
- reverse-shell - Reverse Shell as a Service by @lukechilds.

Disassembler

- plasma - Plasma is an interactive disassembler for x86/ARM/MIPS by @plasma-disassembler.
- radare2 - Unix-like reverse engineering framework and commandline tools by @radare.

- Iaitō - Qt and C++ GUI for radare2 reverse engineering framework by @hteso.

Decompiler

- CFR - Another java decompiler by @LeeAtBenf.

Others

- Dnslogger - DNS Logger by @iagox86.
- CyberChef - The Cyber Swiss Army Knife - a web app for encryption, encoding, compression and data analysis - by @GCHQ.

Social Engineering Database

use at your own risk

- haveibeenpwned - Check if you have an account that has been compromised in a data breach by Troy Hunt.
- databases.today - The biggest free-to-download collection of publicly available website databases for security researchers and journalists by @publicdbhost.
- mysql-password - Database of MySQL hashes.

Blogs

- Orange - Taiwan's talented web penetrator.
- leavesongs - China's talented web penetrator.
- James Kettle - Head of Research at PortSwigger Web Security.
- Broken Browser - Fun with Browser Vulnerabilities.

- Scrutiny - Internet Security through Web Browsers by Dhiraj Mishra.
- Blog of Osanda - Security Researching and Reverse Engineering.
- BRETT BUERHAUS - Vulnerability disclosures and rambles on application security.
- n0tr00t - ~# n0tr00t Security Team.
- OpnSec - Open Mind Security!
- LoRexxar - 带着对技术的敬畏之心成长，不安于一隅...
- Wfox - 技术宅，热衷各种方面。

Twitter Users

- @HackwithGitHub - Initiative to showcase open source hacking tools for hackers and pentesters
- @filedescriptor - Active penetrator often tweets and writes useful articles
- @cure53berlin - Cure53 is a German cybersecurity firm.
- @XssPayloads - The wonderland of JavaScript unexpected usages, and more.
- @kinugawamasato - Japanese web penetrator.
- @h3xstream - Security Researcher, interested in web security, crypto, pentest, static analysis but most of all, samy is my hero.
- @garethheyes - English web penetrator.
- @hasegawayosuke - Japanese javascript security researcher.

Practices

Application

- BadLibrary - vulnerable web application for training - Written by @SecureSkyTechnology.

- Hackxor - realistic web application hacking game - Written by @albinowax.
- SELinux Game - Learn SELinux by doing. Solve Puzzles, show skillz - Written by @selinuxgame.

AWS

- FLAWS - Amazon AWS CTF challenge - Written by @0xdabbad00.

XSS

- XSS Thousand Knocks - XSS Thousand Knocks - Written by @yagihashoo.
- XSS game - Google XSS Challenge - Written by Google.
- prompt(1) to win - Complex 16-Level XSS Challenge held in summer 2014 (+4 Hidden Levels) - Written by @cure53.
- alert(1) to win - Series of XSS challenges - Written by @steike.
- XSS Challenges - Series of XSS challenges - Written by yamagata21.

ModSecurity / OWASP ModSecurity Core Rule Set

- ModSecurity / OWASP ModSecurity Core Rule Set - Series of tutorials to install, configure and tune ModSecurity and the Core Rule Set - Written by @ChrFolini.

Community

- Reddit
- Stack Overflow

Miscellaneous

- awesome-bug-bounty - Comprehensive curated list of available Bug Bounty & Disclosure Programs and write-ups by @djadmin.
- bug-bounty-reference - List of bug bounty write-up that is categorized by the bug nature by @ngalongc.
- Google VRP and Unicorns - Written by Daniel Stelter-Gliese.
- Brute Forcing Your Facebook Email and Phone Number - Written by PwnDizzle.
- GITLEAKS - Search engine for exposed secrets on lots of places.
- Pentest + Exploit dev Cheatsheet wallpaper - Penetration Testing and Exploit Dev CheatSheet.
- The Definitive Security Data Science and Machine Learning Guide - Written by JASON TROS.
- EQGRP - Decrypted content of eqgrp-auction-file.tar.xz by @x0rz.
- Browser Extension and Login-Leak Experiment - Browser Extension and Login-Leak Experiment.
- notes - Some public notes by @ChALkeR.
- A glimpse into GitHub's Bug Bounty workflow - Written by @gregose.
- Cybersecurity Campaign Playbook - Written by Belfer Center for Science and International Affairs.
- Infosec_Reference - Information Security Reference That Doesn't Suck by @rmusser01.
- Internet of Things Scanner - Check if your internet-connected devices at home are public on Shodan by BullGuard.
- The Bug Hunters Methodology v2.1 - Written by @jhaddix.
- $7.5k Google services mix-up - Written by Ezequiel Pereira.
- How I exploited ACME TLS-SNI-01 issuing Let's Encrypt SSL-certs for any domain using shared hosting - Written by @fransrosen.
- TL:DR: VPN leaks users' IPs via WebRTC. I've tested seventy VPN providers and 16 of them leaks users' IPs via WebRTC (23%) - Written by voidsec.
- Escape and Evasion Egressing Restricted Networks - Written by Chris Patten, Tom Steele.
- Be careful what you copy: Invisibly inserting usernames into text with Zero-Width Characters - Written by @umpox.
- Domato Fuzzer's Generation Engine Internals - Written by sigpwn.

Code of Conduct

Please note that this project is released with a Contributor Code of Conduct. By participating in this project you agree to abide by its terms.

License

To the extent possible under law, @qazbnm456 has waived all copyright and related or neighboring rights to this work.