

[Features](#)[Business](#)[Explore](#)[Marketplace](#)[Pricing](#)[This repository](#)[Sign in](#) or [Sign up](#)[swisskyrepo](#) / **PayloadsAllTheThings**[Watch](#)

268

[★ Star](#)

2,478

[Fork](#)

831

[Code](#)[Issues](#) 2[Pull requests](#) 0[Projects](#) 0[Insights](#)

Join GitHub today

GitHub is home to over 20 million developers working together to host and review code, manage projects, and build software together.








[Sign up](#)[Dismiss](#)

A list of useful payloads and bypass for Web Application Security and Pentest/CTF

[python](#)[pentest](#)[payload](#)[bypass](#)[web-application](#)[hacking](#)[xss-vulnerability](#)[sqli-vulnerability-scanner](#)[vulnerability](#)[useful-payloads](#)[useful](#)[140 commits](#)[1 branch](#)[0 releases](#)[8 contributors](#)Branch: **master** ▾[New pull request](#)[Find file](#)[Clone or download ▾](#)**swisskyrepo** AD - Ropnop Tricks

Latest commit 81eebea a day ago

📁 AWS Amazon Bucket S3	Update README.md	9 months ago
📁 CRLF injection	SQLmap tips + Active Directory attacks + SQLite injections	2 months ago
📁 CSV injection	Fix in juggling type + CSV injection	2 years ago
📁 CVE Exploits	Drupalgeddon2 update + Payment API in Methodology	16 days ago
📁 File Inclusion - Path Traversal	SVG XSS + SSRF enclosed alphanumerics	6 months ago
📁 Insecured source code management	Multiple update - LFI/RCE via phpinfo, Struts2 v2	8 months ago
📁 Java Deserialization	Refactoring XSS 0/?	2 months ago
📁 LDAP injection	Refactoring XSS 0/?	2 months ago
📁 Methodology and Resources	AD - Ropnop Tricks	a day ago
📁 NoSQL injection	Traversal Dir + NoSQL major updates + small addons	3 months ago
📁 OAuth	Add CSRF to OAuth2	7 months ago
📁 Open redirect	AD Attack - Golden Ticket + SQL/OpenRed/SSRF	27 days ago
📁 PHP juggling type	Fix in juggling type + CSV injection	2 years ago
📁 PHP serialization	Payloads - Quick fix	3 months ago
📁 Remote commands execution	SQLmap tips + Active Directory attacks + SQLite injections	2 months ago
📁 SQL injection	Oracle SQL + SQL injection updates (MS SQL/MYSQL/ GENERAL)	12 days ago
📁 SSRF injection	AD Attack - Golden Ticket + SQL/OpenRed/SSRF	27 days ago
📁 Server Side Template injections	SQLmap tips + Active Directory attacks + SQLite injections	2 months ago
📁 Tar commands execution	Clean project - Renamed and added PHP juggling type	2 years ago
📁 Traversal directory	Traversal Dir + NoSQL major updates + small addons	3 months ago

 Upload insecure files	Payloads - Quick fix	3 months ago
 Web cache deception	Typo fix in Web cache	a year ago
 XPATH injection	LDAP & XPATH injection + Small fixes and payloads	10 months ago
 XSS injection	Fix README broken links	2 months ago
 XXE injections	Payloads - Quick fix	3 months ago
 .gitignore	AD refactoring part1	4 days ago
 README.md	AD refactoring part1	4 days ago

README.md

Payloads All The Things

A list of useful payloads and bypasses for Web Application Security. Feel free to improve with your payloads and techniques !
I <3 pull requests :)

Every section contains:

- README.md - vulnerability description and how to exploit it
- Intruders - a set of files to give to Burp Intruder
- Some exploits

You might also like :

- [Methodology and Resources](#)
- [CVE Exploits](#)

- Shellshock
- HeartBleed
- Apache Struts 2

Tools

- [Kali Linux](#)
- [Web Developer](#)
- [Hackbar](#) - Not compatible with Firefox Quantum
- [Burp Proxy](#)
- [Fiddler](#)
- [DirBuster](#)
- [GoBuster](#)
- [Knockpy](#)
- [SQLmap](#)
- [Nikto](#)
- [Nessus](#)
- [Recon-ng](#)
- [Wappalyzer](#)
- [Metasploit](#)
- [OpenVAS](#)

Online Challenges

- [Hack The Box](#)

- [Root-Me](#)
- [Zenk-Security](#)
- [W3Challs](#)
- [NewbieContest](#)
- [Vulnhub](#)
- [The Cryptopals Crypto Challenges](#)
- [Penetration Testing Practice Labs](#)
- [alert\(1\) to win](#)
- [Hacksplaining](#)
- [HackThisSite](#)
- [PentesterLab : Learn Web Penetration Testing: The Right Way](#)
- [Hackers.gg](#)

Bug Bounty

- [HackerOne](#)
- [BugCrowd](#)
- [Bounty Factory](#)
- [List of Bounty Program](#)

Docker

Command	Link
<code>docker pull remnux/metasploit</code>	docker-metasploit

Command	Link
<code>docker pull paoloo/sqlmap</code>	docker-sqlmap
<code>docker pull kalilinux/kali-linux-docker</code>	official Kali Linux
<code>docker pull owasp/zap2docker-stable</code>	official OWASP ZAP
<code>docker pull wpscanteam/wpscan</code>	official WPScan
<code>docker pull infoslack/dvwa</code>	Damn Vulnerable Web Application (DVWA)
<code>docker pull danmx/docker-owasp-webgoat</code>	OWASP WebGoat Project docker image
<code>docker pull opendns/security-ninjas</code>	Security Ninjas
<code>docker pull ismisepaul/securityshepherd</code>	OWASP Security Shepherd
<code>docker-compose build && docker-compose up</code>	OWASP NodeGoat
<code>docker pull citizenstig/nowasp</code>	OWASP Mutillidae II Web Pen-Test Practice Application
<code>docker pull bkimminich/juice-shop</code>	OWASP Juice Shop

More resources

Book's list:

- [Web Hacking 101](#)
- [OWASP Testing Guide v4](#)
- [Penetration Testing: A Hands-On Introduction to Hacking](#)

- [The Hacker Playbook 2: Practical Guide to Penetration Testing](#)
- [The Mobile Application Hacker's Handbook](#)
- [Black Hat Python: Python Programming for Hackers and Pentesters](#)
- [Metasploit: The Penetration Tester's Guide](#)
- [The Database Hacker's Handbook](#), David Litchfield et al., 2005
- [The Shellcoders Handbook](#) by Chris Anley et al., 2007
- [The Mac Hacker's Handbook](#) by Charlie Miller & Dino Dai Zovi, 2009
- [The Web Application Hackers Handbook](#) by D. Stuttard, M. Pinto, 2011
- [iOS Hackers Handbook](#) by Charlie Miller et al., 2012
- [Android Hackers Handbook](#) by Joshua J. Drake et al., 2014
- [The Browser Hackers Handbook](#) by Wade Alcorn et al., 2014
- [The Mobile Application Hackers Handbook](#) by Dominic Chell et al., 2015
- [Car Hacker's Handbook](#) by Craig Smith, 2016

Blogs/Websites

- <http://blog.zsec.uk/101-web-testing-tooling/>
- <https://blog.innerht.ml>
- <https://blog.zsec.uk>
- <https://www.exploit-db.com/google-hacking-database>
- <https://www.arneswinnen.net>
- <https://forum.bugcrowd.com/t/researcher-resources-how-to-become-a-bug-bounty-hunter/1102>

Youtube

- [Hunting for Top Bounties - Nicolas Grégoire](#)

- [BSidesSF 101 The Tales of a Bug Bounty Hunter - Arne Swinnen](#)
- [Security Fest 2016 The Secret life of a Bug Bounty Hunter - Frans Rosén](#)
- [IppSec Channel - Hack The Box Writeups](#)

