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 :)

You can also contribute with a beer IRL or with `buymeacoffee.com`

 (https://buymeacoff.ee/swissky)

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 (https://github.com/swisskyrepo/PayloadsAllTheThings/blob/master/Methodology%20and%20Resources/)
  - Active Directory Attack.md (https://github.com/swisskyrepo/PayloadsAllTheThings/blob/master/Methodology%20and%20Resources/Active%20Directory%20Attack.md)
  - Methodology_and_enumeration.md (https://github.com/swisskyrepo/PayloadsAllTheThings/blob/master/Methodology%20and%20Resources/Methodology_and_enumeration.md)
  - Network Pivoting Techniques.md (https://github.com/swisskyrepo/PayloadsAllTheThings/blob/master/Methodology%20and%20Resources/Network%20Pivoting%20Techniques.md)
  - Reverse Shell Cheatsheet.md (https://github.com/swisskyrepo/PayloadsAllTheThings/blob/master/Methodology%20and%20Resources/Reverse%20Shell%20Cheatsheet.md)
  - Windows - Download and Execute.md (https://github.com/swisskyrepo/PayloadsAllTheThings/blob/master/Methodology%20and%20Resources/Windows%20-%20Download%20and%20Execute.md)
  - Windows - Mimikatz.md (https://github.com/swisskyrepo/PayloadsAllTheThings/blob/master/Methodology%20and%20Resources/Windows%20-%20Mimikatz.md)
  - Windows - Persistence.md (https://github.com/swisskyrepo/PayloadsAllTheThings/blob/master/Methodology%20and%20Resources/Windows%20-%20Persistence.md)
  - Windows - Privilege Escalation.md (https://github.com/swisskyrepo/PayloadsAllTheThings/blob/master/Methodology%20and%20Resources/Windows%20-%20Privilege%20Escalation.md)
  - Windows - Using credentials.md (https://github.com/swisskyrepo/PayloadsAllTheThings/blob/master/Methodology%20and%20Resources/Windows%20-%20Using%20credentials.md)
- CVE Exploits (https://github.com/swisskyrepo/PayloadsAllTheThings/blob/master/CVE%20Exploits)
  - Apache Struts 2 CVE-2017-5638.py
  - Apache Struts 2 CVE-2017-9805.py
  - Drupalgeddon2 CVE-2018-7600.rb
  - Heartbleed CVE-2014-0160.py
  - Shellshock CVE-2014-6271.py
  - Tomcat CVE-2017-12617.py

Try Harder

Ever wonder where you can use your knowledge ? The following list will help you find "targets" to improve your skills.

- **Bug Bounty Platforms**
  - HackerOne (https://hackerone.com)
  - BugCrowd (https://bugcrowd.com)
  - Bounty Factory (https://bountyfactory.io)
  - Synack (https://www.synack.com/)
  - Intigriti (https://www.intigriti.com)
  - List of Bounty Program (https://bugcrowd.com/list-of-bug-bounty-programs/)
- **Online Platforms**
  - Hack The Box (hackthebox.eu/)
  - Penetration test lab "Test lab" | Pentestit (https://lab.pentestit.ru)
  - PentesterLab : Learn Web Penetration Testing: The Right Way (https://pentesterlab.com/)
  - Zenk-Security (https://www.zenk-security.com/epreuves.php)
  - Root-Me (https://www.root-me.org)
  - W3Challs (https://w3challs.com/)
  - NewbieContest (https://www.newbiecontest.org/)
  - Vulnhub (https://www.vulnhub.com/)
  - The Cryptopals Crypto Challenges (https://cryptopals.com/)
  - alert(1) to win (https://alf.nu/alert1)
  - Hacksplaining (https://www.hacksplaining.com/exercises)
  - HackThisSite (https://hackthissite.org)
  - Hackers.gg (hackers.gg)
  - Mind Map - Penetration Testing Practice Labs - Aman Hardikar (http://www.amanhardikar.com/mindmaps/Practice.html)

Book's list

Grab a book and relax, these ones are the best security books (in my opinion).

- Web Hacking 101 (https://leanpub.com/web-hacking-101)
- Breaking into Information Security: Learning the Ropes 101 - Andrew Gill (https://leanpub.com/ltr101-breaking-into-infosec)
- OWASP Testing Guide v4 (https://www.owasp.org/index.php/OWASP_Testing_Project)
- Penetration Testing: A Hands-On Introduction to Hacking (http://amzn.to/2dhHTSn)
- The Hacker Playbook 2: Practical Guide to Penetration Testing (http://amzn.to/2d9wYKa)
- The Hacker Playbook 3: Practical Guide to Penetration Testing - Red Team Edition (http://a.co/6MqC9bD)
- The Mobile Application Hacker's Handbook (http://amzn.to/2cVOIrE)
- Black Hat Python: Python Programming for Hackers and Pentesters (http://www.amazon.com/Black-Hat-Python-Programming-Pentesters/dp/1593275900)
- Metasploit: The Penetration Tester's Guide (https://www.nostarch.com/metasploit)
- The Database Hacker's Handbook, David Litchfield et al., 2005 (http://www.wiley.com/WileyCDA/WileyTitle/productCd-0764578014.html)
- The Shellcoders Handbook by Chris Anley et al., 2007 (http://www.wiley.com/WileyCDA/WileyTitle/productCd-047008023X.html)
- The Mac Hacker's Handbook by Charlie Miller & Dino Dai Zovi, 2009 (http://www.wiley.com/WileyCDA/WileyTitle/productCd-0470395362.html)
- The Web Application Hackers Handbook by D. Stuttard, M. Pinto, 2011 (http://www.wiley.com/WileyCDA/WileyTitle/productCd-1118026470.html)
- iOS Hackers Handbook by Charlie Miller et al., 2012 (http://www.wiley.com/WileyCDA/WileyTitle/productCd-1118204123.html)
- Android Hackers Handbook by Joshua J. Drake et al., 2014 (http://www.wiley.com/WileyCDA/WileyTitle/productCd-111860864X.html)
- The Browser Hackers Handbook by Wade Alcorn et al., 2014 (http://www.wiley.com/WileyCDA/WileyTitle/productCd-1118662091.html)
- The Mobile Application Hackers Handbook by Dominic Chell et al., 2015 (http://www.wiley.com/WileyCDA/WileyTitle/productCd-1118958500.html)
- Car Hacker's Handbook by Craig Smith, 2016 (https://www.nostarch.com/carhacking)

More resources

Blogs/Websites

- BUG BOUNTY FIELD MANUAL: THE DEFINITIVE GUIDE FOR PLANNING, LAUNCHING, AND OPERATING A SUCCESSFUL BUG BOUNTY PROGRAM (https://www.hackerone.com/blog/the-bug-bounty-field-manual)
- How to become a Bug Bounty Hunter - Sam Houston (https://forum.bugcrowd.com/t/researcher-resources-how-to-become-a-bug-bounty-hunter/1102)
- Tips from Top Hackers – Bug Hunting methodology and the importance of writing quality submissions - Sam Houston (https://www.bugcrowd.com/tips-from-top-hackers-bug-hunting-methodology-and-the-importance-of-writing-quality-submissions/)
- ARNE SWINNEN'S SECURITY BLOG JUST ANOTHER INFOSEC BLOG (https://www.arneswinnen.net)
- XSS Jigsaw - innerht.ml (https://blog.innerht.ml)
- ZeroSec Blog: Featuring Write-Ups, Projects & Adventures (https://blog.zsec.uk/tag/ltr101/)

Youtube

- Hunting for Top Bounties - Nicolas Grégoire (https://www.youtube.com/watch?v=mQjTgDuLsp4)
- BSidesSF 101 The Tales of a Bug Bounty Hunter - Arne Swinnen (https://www.youtube.com/watch?v=dsekKYNLBbc)
- Security Fest 2016 The Secret life of a Bug Bounty Hunter - Frans Rosén (https://www.youtube.com/watch?v=KDo68Laayh8)
- IppSec Channel - Hack The Box Writeups (https://www.youtube.com/channel/UCa6eh7gCkpPo5XXUDfygQQA)

Docker

Command	Link
`docker pull remnux/metasploit`	docker-metasploit (https://hub.docker.com/r/remnux/metasploit/)
`docker pull paoloo/sqlmap`	docker-sqlmap (https://hub.docker.com/r/paoloo/sqlmap/)
`docker pull kalilinux/kali-linux-docker`	official Kali Linux (https://hub.docker.com/r/kalilinux/kali-linux-docker/)
`docker pull owasp/zap2docker-stable`	official OWASP ZAP (https://github.com/zaproxy/zaproxy)
`docker pull wpscanteam/wpscan`	official WPScan (https://hub.docker.com/r/wpscanteam/wpscan/)
`docker pull infoslack/dvwa`	Damn Vulnerable Web Application (DVWA) (https://hub.docker.com/r/infoslack/dvwa/)
`docker pull danmx/docker-owasp-webgoat`	OWASP WebGoat Project docker image (https://hub.docker.com/r/danmx/docker-owasp-webgoat/)
`docker pull opendns/security-ninjas`	Security Ninjas (https://hub.docker.com/r/opendns/security-ninjas/)
`docker pull ismisepaul/securityshepherd`	OWASP Security Shepherd (https://hub.docker.com/r/ismisepaul/securityshepherd/)
`docker-compose build && docker-compose up`	OWASP NodeGoat (https://github.com/owasp/nodegoat#option-3---run-nodegoat-on-docker)
`docker pull citizenstig/nowasp`	OWASP Mutillidae II Web Pen-Test Practice Application (https://hub.docker.com/r/citizenstig/nowasp/)
`docker pull bkimminich/juice-shop`	OWASP Juice Shop (https://github.com/bkimminich/juice-shop#docker-container)