# Bug Bounty Career – WEB HACKING

Joas Antonio

# Details

- The objective is to help Information Security professionals, enthusiasts and even the youngest, to enter the Bug Bounty area;
- Knowing the skills necessary to work in the area of Bug Bounty;
- Of course, this is not a guide that will make you a professional, but I hope it helps;

My LinkedIn: https://www.linkedin.com/in/joas-antonio-dos-santos/

# Bug Bounty Platforms

1. HackerOne
2. Bugcrowd
3. Intigriti
4. Bug Hunt
5. Hackaflag
6. Yogosha
7. Zeroday initiative
8. Open Bug Bounty
9. YesWeHack
10. Cobalt.io
11. Synack Red Team

# Skills Bug Bounty Hunter

- Knowledge in Programming Logic;
- Knowledge in Web Attack Vectors;
- Knowledge in Reverse Engineering;
- Skills in Web Development;
- Programming Logic exercised;
- Computational basis;
- CTF Player;
- Knowledge in Network Computer;
- Knowledge in System Administrator (Linux and Windows);
- Knowledge in Cloud Computer (AWS, GOOGLE and AZURE);
- Skills in Infrastructure Exploitation;

# Web Vulnerabilities – TOP 17

1. Open Redirect;
2. HTTP Parameter Pollution;
3. Cross-Site Request Forgery;
4. HTML Injection and Content Spoofing;
5. Carriage Return Line Feed Injection;
6. Cross Site Scripting;
7. Template Injection;
8. SQL Injection;
9. Server Side Request Forgery;
10. XML External Entity;
11. Remote Code Execution;
12. Memory Vulnerabilities;
13. Subdomain Takeover;
14. Race Conditions;
15. Insecure Direct Object References;
16. Oauth Vulnerabilities;
17. Application Logic and Configuration Vulnerabilities;

# Web Vulnerabilities - List

Arbitrary file access
Binary planting
Blind SQL Injection
Blind XPath Injection
Brute force attack
Buffer overflow attack
Cache Poisoning
Cash Overflow
Clickjacking
Command injection attacks
Comment Injection Attack
Content Security Policy
Content Spoofing
Credential stuffing
Cross Frame Scripting
Cross Site History Manipulation (XSHM)
Cross Site Tracing
Cross-Site Request Forgery (CSRF)
Cross Site Port Attack (XSPA)
Cross-Site Scripting (XSS)
Cross-User Defacement
Custom Special Character Injection
Denial of Service
Direct Dynamic Code Evaluation ('Eval Injection')
Execution After Redirect (EAR)
Exploitation of CORS
Forced browsing
Form action hijacking
Format string attack
Full Path Disclosure
Function Injection
Host Header injection
HTTP Response Splitting
HTTP verb tampering
HTML injection
LDAP injection
Log Injection
Man-in-the-browser attack
Man-in-the-middle attack
Mobile code: invoking untrusted mobile code
Mobile code: non-final public field
Mobile code: object hijack
One-Click Attack
Parameter Delimiter
Page takeover
Path Traversal
Reflected DOM Injection
Regular expression Denial of Service – ReDoS
Repudiation Attack
Resource Injection

# Web Vulnerabilities - List

Server-Side Includes (SSI) Injection
Session fixation
Session hijacking attack
Session Prediction
Setting Manipulation
Special Element Injection
SMTP injection
SQL Injection
SSI injection
Traffic flood
Web Parameter Tampering
XPATH Injection
XSRF or SSRF

https://owasp.org/www-community/vulnerabilities/

# Vulnerabilities – HackerOne Rank

| | Weakness Type | Bounties Total Financial Rewards Amount | YOY % Chage |
|---|---|---|---|
| 1 | XSS | $4,211,006 | 26% |
| 2 | Improper Access Control - Generic | $4,013,316 | 134% |
| 3 | Information Disclosure | $3,520,801 | 63% |
| 4 | Server-Side Request Forgery (SSRF) | $2,995,755 | 103% |
| 5 | Insecure Direct Object Reference (IDOR) | $2,264,833 | 70% |
| 6 | Privilege Escalation | $2,017,592 | 48% |
| 7 | SQL Injection | $1,437,341 | 40% |
| 8 | Improper Authentication - Generic | $1,371,863 | 36% |
| 9 | Code Injection | $982,247 | -7% |
| 10 | Cross-Site Request Forgery (CSRF) | $662,751 | -34% |

https://www.hackerone.com/top-ten-vulnerabilities

# Resources Study

- https://chawdamrunal.medium.com/pro-tips-for-bug-bounty-f9982a5fc5e9
- https://medium.com/bugbountywriteup/bug-bounty-hunting-methodology-toolkit-tips-tricks-blogs-ef6542301c65
- https://www.bugcrowd.com/resources/webinars/5-tips-and-tricks-to-run-successful-bug-bounty-programs/
- https://www.youtube.com/watch?v=CU9Iafc-Igs&ab_channel=ST%C3%96K
- https://github.com/EdOverflow/bugbounty-cheatsheet https://chawdamrunal.medium.com/pro-tips-for-bug-bounty-f9982a5fc5e9
- https://medium.com/bugbountywriteup/bug-bounty-hunting-methodology-toolkit-tips-tricks-blogs-ef6542301c65
- https://www.bugcrowd.com/resources/webinars/5-tips-and-tricks-to-run-successful-bug-bounty-programs/

# Resources Study

- https://www.youtube.com/watch?v=CU9Iafc-Igs&ab_channel=ST%C3%96K
- https://github.com/EdOverflow/bugbounty-cheatsheet
- https://github.com/djadmin/awesome-bug-bounty
- https://github.com/devanshbatham/Awesome-Bugbounty-Writeups
- https://github.com/Muhammd/awesome-bug-bounty
- https://github.com/ajdumanhug/awesome-bug-bounty-tips
- https://medium.com/bugbountyhunting/bug-bounty-toolkit-aa36f4365f3f
- https://github.com/nahamsec/Resources-for-Beginner-Bug-Bounty-Hunters
- https://github.com/bobby-lin/bug-bounty-guide

# Writeups Bug Bounty

- https://pentester.land/list-of-bug-bounty-writeups.html
- https://medium.com/bugbountywriteup
- https://github.com/yaworsk/bugbounty/blob/master/writeups.md
- https://www.youtube.com/channel/UCNRM4GH-SD85WCSqeSb4xUA
- https://paper.seebug.org/802/

# Skills Development – YouTube Channels

- STÖK (Fredrik Alexandersson)

https://lnkd.in/djwu5A6

- Red Team Village DC Red Team Village

https://lnkd.in/dDhcEa5

- InsiderPhD Katie Paxton-Fear

https://lnkd.in/duDph87

- Nahamsec Ben Sadeghipour

https://lnkd.in/drBQim3

- HackerOne

https://lnkd.in/d7QNQE8

- BugCrowd

https://lnkd.in/dAqbA84

- The Cyber Mentor Heath Adams

https://lnkd.in/dbYCM5Q

- John Hammond John H.

https://lnkd.in/dAp3xJM

# Skills Development – Youtube Channels

- Codingo Michael S.

https://lnkd.in/dpEsrEk

- HackerSploit HackerSploit

https://lnkd.in/dGXwDkX

- LiveOverflow

https://lnkd.in/dTWHXSD

- IPPSec

https://lnkd.in/deCU5YZ

- S4vitar Marcelo Vázquez (Spanish Content)

https://lnkd.in/dMjbPft

- Zigoo Ebrahim Hegazy (Arabic )

https://lnkd.in/dgQTeuG

# Skills Development – Youtube Channels

- ACADI-TI

https://www.youtube.com/channel/UCi8P9S-PW7AF71g8Pi0W6Jw

- Michael LaSalvia

https://www.youtube.com/user/genxweb

- Wraiith

https://www.youtube.com/user/Wraiith75

- Bsides

https://www.youtube.com/channel/UCVImyGhRATNFGPmJfxaq1dw

- Vinicius Vieira

https://www.youtube.com/channel/UCySphP8k4rv7Jf-7v3baWIA

# Skills Development – Youtube Channels

- Kindred

https://www.youtube.com/channel/UCwTH3RkRCIE35RJ16Nh8V8Q

- Bug Bounty Public Disclosure

https://www.youtube.com/channel/UCNRM4GH-SD85WCSqeSb4xUA

- https://www.youtube.com/channel/UCxHzA-Z97sjfK3OISjkbMCQ (RoadSec)
- https://www.youtube.com/channel/UC2QgCedRNj_tLDrGWSM3GsQ (Mindthesec)
- https://www.youtube.com/channel/UCz1PsqIhim7PUqQfuXmD-Bw (Hackaflag)
- https://www.youtube.com/user/BlackHatOfficialYT (Blackhat)

# Skills Development – Youtube Channels

- https://www.youtube.com/channel/UCqGONXW1ORgz5Y4qK-0JdkQ (Joe Grand)
- https://www.youtube.com/user/DEFCONConference (Defcon)
- https://www.youtube.com/channel/UC4dxXZQq-ofAadUWbqhoceQ (DeviantOllam)
- https://www.youtube.com/channel/UC3s0BtrBJpwNDaflRSoiieQ (Hak5)
- https://www.youtube.com/channel/UCimS6P854cQ23j6c_xst7EQ (Hacker Warehouse)
- https://www.youtube.com/channel/UCe8j61ABYDuPTdtjItD2veA (OWASP)
- https://www.youtube.com/channel/UC42VsoDtra5hMiXZSsD6eGg/featured (The Modern Rogue)
- https://www.youtube.com/channel/UC3S8vxwRfqLBdIhgRlDRVzw (Stack Mashing)

# Skills Development – Youtube Channels

- https://www.youtube.com/channel/UCW6MNdOsqv2E9AjQkv9we7A (PwnFunction)
- https://www.youtube.com/channel/UCUB9vOGEUpw7IKJRoR4PK-A (Murmus CTF)
- https://www.youtube.com/channel/UCND1KVdVt8A580SjdaS4cZg (Colin Hardy)
- https://www.youtube.com/user/GynvaelEN (GynvaelEN)
- https://www.youtube.com/channel/UCBcljXmuXPok9kT_VGA3adg (Robert Baruch)
- https://www.youtube.com/channel/UCGISJ8ZHkmIv1CaoHovK-Xw (/DEV/NULL)
- https://www.youtube.com/channel/UCDbNNYUME_pgocqarSjfNGw (Kacper)
- https://www.youtube.com/channel/UCdNLW93OyL4lTav1pbKbyaQ (Mentorable)

# Skills Development – Youtube Channels

- https://www.youtube.com/channel/UCMACXuWd2w6_IEGog744UaA (Derek Rook)
- https://www.youtube.com/channel/UCFvueUEWRfQ9qT9UmHCw_og (Prof. Joas Antonio)
- https://www.youtube.com/user/ricardolongatto (Ricardo Longatto)
- https://www.youtube.com/user/daybsonbruno (XTREME Security)
- https://www.youtube.com/user/eduardoamaral07 (Facil Tech)
- https://www.youtube.com/channel/UC70YG2WHVxlOJRng4v-CIFQ (Gabriel Pato)
- https://www.youtube.com/user/Diolinux (Diolinux)
- https://www.youtube.com/user/greatscottlab (Great Scott!)
- https://www.youtube.com/user/esecuritytv (eSecurity)
- https://www.youtube.com/channel/UCzWPaANpPISEE_xvJm8lqHA (Cybrary)
- https://www.youtube.com/user/DanielDonda (Daniel Donda)
- https://www.youtube.com/user/ZetaTwo (Calle Svensson)
- https://www.youtube.com/channel/UCNKUSu4TPk979JzMeKDXiwQ (Georgia Wedman)
- https://www.youtube.com/channel/UCqDLY9WFoJWqrhycW8cbv1Q (Manoel T)

# Tools - Bug Bounty

- https://github.com/KingOfBugbounty/KingOfBugBountyTips
- https://medium.com/@hackbotone/10-recon-tools-for-bug-bounty-bafa8a5961bd
- https://portswigger.net/solutions/bug-bounty-hunting/best-bug-bounty-tools
- https://github.com/nahamsec/Resources-for-Beginner-Bug-Bounty-Hunters/blob/master/assets/tools.md
- https://www.hackerone.com/blog/100-hacking-tools-and-resources