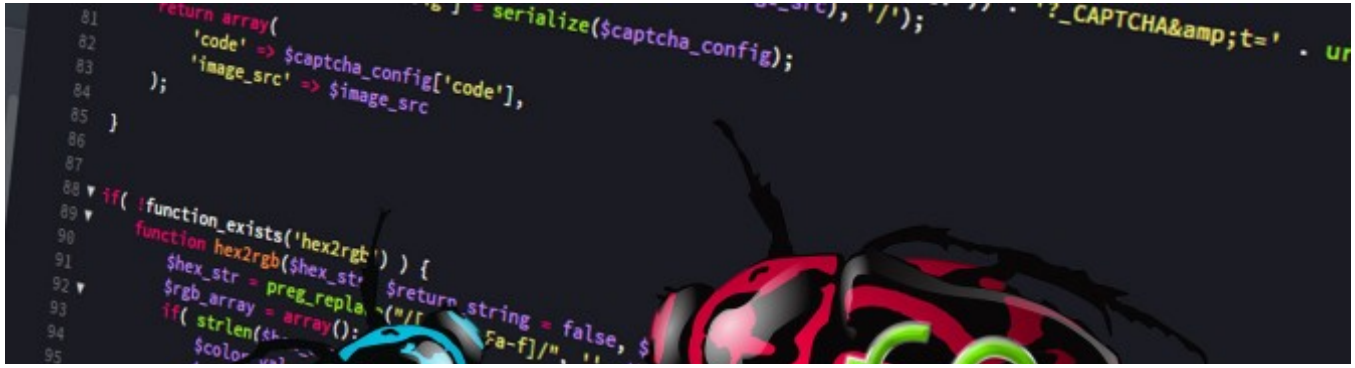
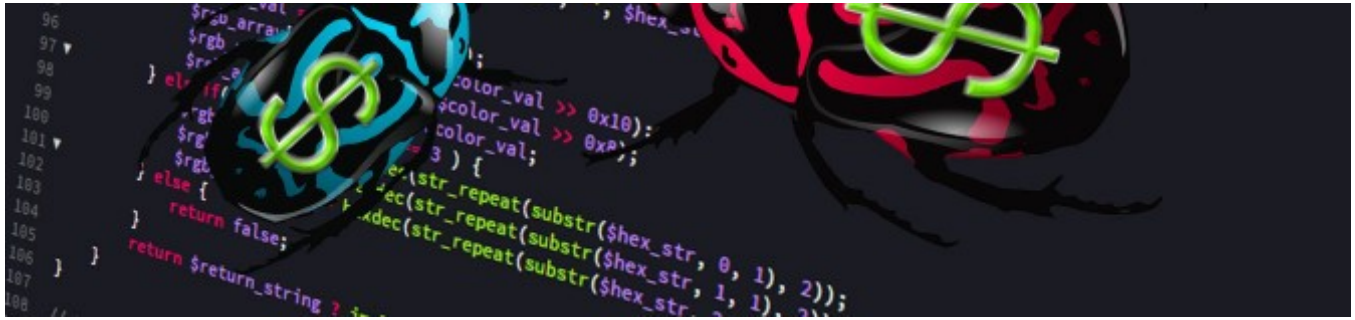
# Bug Bounty Guide

Thuvarakan Nakarajah Follow
Aug 21, 2018 · 5 min read

Bug bounty hunting is the finding security vulnerabilities in a site and responsibly disclosing it to that company's security team. but the particular site should have the bug bounty program. otherwise, it will become an illegal activity. Nowadays Bug bounty program is most important to major sites. Most of the major sites provide the bug bounty programs. They reward acknowledgment as "white hat" hackers(HOF), Swag and bounties.





If anyone discovers any security vulnerability in the web or software, they may try to exploit them, or selling them on underground markets. but if that site or software has bounty program they should report.

> “If I had 8 hours to chop down a tree, I would spend 6 of those hours sharpening my axe”

Definitely bug bounty achievement is not the one day program, Bug Hunting is a way of thinking and Matter of Skills. We never **give up,** because some bugs are already reported. You May end up getting depressed by duplicates, would suggest to at least choose any program Spend a week

on it. We never expect anything after reported, just go away and find other bugs, otherwise, it will make sad.

## My Tips and Tricks

**Always read the source code**
*https://github.com/UnkL4b/GitMiner*

**Try to find the Subdomains (eg touch.facebook.com)**

**Use Google Dorks (**inurl:index.php?id=)

**Record video When you test**

**Check each request and response**

**Target their mobile apps**

**Use encoding methods**

If you find any BUG, first ask this question yourself: **what's the security impact on the application? ,** Because in the bug bounty, that bug should have the security impact. Here first we can see the bug bounty platform list, below sites, provide bounty programs.

***Bugcrowd***

*https://www.bugcrowd.com/*

***Hackerone***

*https://www.hackerone.com/*

***Synack***

*https://www.synack.com/*

***Japan Bug Bounty Program***

*https://bugbounty.jp/*

***Cobalt***

*https://cobalt.io/*

***Zerocopter***

*https://zerocopter.com/*

***Hackerproof***

*https://hackenproof.com/*

***BountyFactory***

*https://bountyfactory.io*

I have listed Guides for Web application penetration testing methodology and hunting the web.You can learn the basics and essentials of penetration testing and bug hunting.

***Facebook Accepted Vulnerability Summary Note***

## Video Tutorials

*(playlist)*

*How To Shot Web — Jason Haddix, 2015*

*Bug Bounty Hunting Methodology v2 — Jason Haddix, 2017*

*Hunting for Top Bounties — Nicolas Grégoire, 2014*

*The Secret life of a Bug Bounty Hunter — Frans Rosén, 2016*

*Finding Bugs with Burp Plugins & Bug Bounty 101 — Bugcrowd, 2014*

*How to hack all the bug bounty things automagically reap the rewards profit — Mike Baker, 2016*

*JackkTutorials on YouTube*

*DEFCON Conference videos on YouTube*

*Hak5 on YouTube*

*How To Shot Web — Jason Haddix, 2015*

*Bug Bounty Hunting Methodology v2 — Jason Haddix, 2017*

*Hunting for Top Bounties — Nicolas Grégoire, 2014*

*The Secret life of a Bug Bounty Hunter — Frans Rosén, 2016*

*Finding Bugs with Burp Plugins & Bug Bounty 101 — Bugcrowd, 2014*

*How to hack all the bug bounty things automagically reap the rewards profit — Mike Baker, 2016*

## Common vulnerability guides

***OWASP Top 10***

*OWASP Top 10, 2017 RC2 [PDF]*

***SSRF Bible Cheatsheet***

*https://docs.google.com/document/d/1v1TkWZtrhzRLy0bYXBcdLUedXGb9njTNIJXa3u9akHM/edit*

***File upload Stored XSS***

*https://brutelogic.com.br/blog/file-upload-xss/*

*SANS TOP 25*

*SSRF Bible Cheat Sheet*

*OWASP Web Application Security Testing Cheat Sheet*

## E-Books

*The Web Application Hacker's Handbook*

*OWASP Testing Guide*
*Highly suggested by Bugcrowd Jason Haddix*

*Penetration Testing*

*The Hacker Playbook 2: Practical Guide to Penetration Testing*

*The Tangled Web: A Guide to Securing Web Applications*

*Jhaddix Bug Hunting Methodology*

*The Hacker Playbook-3*

*Ethical Hacking and Penetration Guide*

*Web Penetration Testing with Kali Linux*

## Hacker's blog spot

- *Detectify Blog*
- *Security Shizzle — Inti De Ceukelaire*
- *fin1te: Bug Bounty Participant*
- *maKthePla.net*
- *Security & Code Blog*
- *VYSEC*
- *PWNHACK*
- *Philippe Harewood*
- *ARNE SWINNEN'S SECURITY BLOG*

- *Hacks4Pancakes*
- *NahamSec.com*
- *Daniel LeCheminant*
- *We Hack People*
- *IT-Securityguard Blog*
- *The misunderstood X-XSS-Protection*
- *Bug Bounty Findings by Meals*
- *Respect XSS*
- *Graceful Security!*
- *Fooling the Interpreter*
- *Klikki Oy*

Here I have listed some **Vulnerable applications** for practicing to test your skills in simulated environments. Here you can get an idea of what you'll run up against in the real world.

*BWAPP*

*Webgoat*

*Rootme*

*OWASP Juicy Shop*

*Hacker101*

*Hacksplaining*

*Penetration Testing Practice Labs*

*Damn Vulnerable iOS App (DVIA)*

*Mutillidae*

*Trytohack*

*HackTheBox*

*SQL Injection Practice*

## Web Vulnerability Scanners

*Netsparker Application Security Scanner — Application security scanner to automatically find security flaws.*

*Nikto — Noisy but fast black box web server and web application vulnerability scanner.*

*Arachni — Scriptable framework for evaluating the security of web applications.*

*w3af — Web application attack and audit framework.*

*Wapiti — Black box web application vulnerability scanner with built-in fuzzer.*

*SecApps — In-browser web application security testing suite.*

*WebReaver — Commercial, graphical web application vulnerability scanner designed for macOS.*

*WPScan — Black box WordPress vulnerability scanner.*

*Zoom — Powerful wordpress username enumerator with infinite scanning.*

*cms-explorer — Reveal the specific modules, plugins, components and themes that various websites powered by content management systems are running.*

*joomscan — Joomla vulnerability scanner.*

*ACSTIS — Automated client-side template injection (sandbox escape/bypass) detection for AngularJS.*

*SQLmate — A friend of sqlmap that identifies sqli vulnerabilities based on a given dork and website (optional).*

## InfoSec CheatSheet

1. *Pentest Bookmarks*
2. *Awesome OSINT Cheat-sheet*
3. *Awesome Pentest Cheat-sheet*
4. *Bug Bounty Cheat-sheet*
5. *Awesome Hacking Cheat-sheet*
6. *Awesome-Infosec Cheat-Sheet*
7. *SQL Injection Cheat-Sheet*
8. *XSS Cheat-Sheet*
9. *XXE Payload*

## Tools & OS :

*Bug Bounty Forum Tool list*

*Bug crowd Tool list*

*Nmap*

*Burp Suite*

*Wp-scan*

*Kali Linux*

Sqlmap

*Browser (Water fox , Epic)*

## Payloads

**SecLists**

https://github.com/danielmiessler/SecLists

Payloads All The Things

XSS Payloads

XSS Payloads -2

SQL Injection Payloads

Google-Dorks Payloads

Google-Dorks-2 Payloads

***fuzzdb*** — *https://github.com/fuzzdb-project/fuzzdb*

***SecLists*** — *https://github.com/danielmiessler/SecLists*

***NickSanzotta*** — *https://github.com/NickSanzotta/BurpIntruder*

***shadsidd*** — *https://github.com/shadsidd*

***shikari1337*** — *https://www.shikari1337.com/list-of-xss-payloads-for-cross-site-scripting/*

***7ioSecurity*** — *https://github.com/7ioSecurity/XSS-Payloads*

***xmendez*** — *https://github.com/xmendez/wfuzz*

***minimaxir*** — *https://github.com/minimaxir/big-list-of-naughty-strings*

***xsscx*** — *https://github.com/xsscx/Commodity-Injection-Signatures*

***TheRook*** — *https://github.com/TheRook/subbrute*

**ALL.txt**
https://gist.github.com/jhaddix/86a06c5dc309d08580a018c66354a056

## Browser Plugin's

- ***Chrome*** : http://resources.infosecinstitute.com/19-extensions-to-turn-google-chrome-into-penetration-testing-tool/
- ***Firefox*** : http://resources.infosecinstitute.com/use-firefox-browser-as-a-penetration-testing-tool-with-these-add-ons/

**Finally when you found a vulnerability, then You have to make a good report to submit.**

http://www.hackeone.info/2017/12/how-to-write-great-vulnerability-report.html

https://blog.cobalt.io/how-to-write-a-great-vulnerability-report-ab8654c6290c

## Happy Hunting

Security Bug Bounty Bug Hunting Secure

18 claps

WRITTEN BY

**Thuvarakan Nakarajah**

White hat hacker

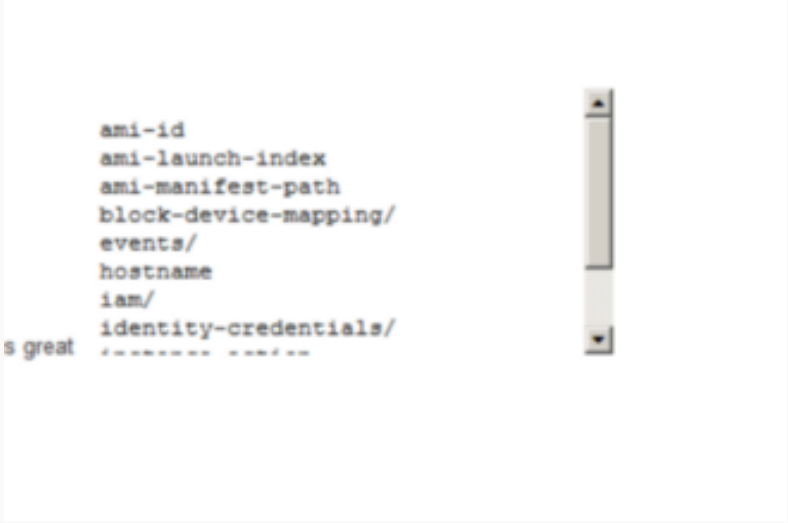
Follow

Write the first response

## More From Medium

Related reads

### The Bugs Are Out There, Hiding in Plain Sight




A Bug'z Life in A Bug'z Life
Jul 15 · 6 min read ★

240

Related reads

### What to Do if Your WordPress Website Was Hacked

HostPapa
Oct 16, 2018 · 11 min read

46

Related reads

# From Microsoft “Build the Shield” to Microsoft “Hall of Fame”

Sai Krishna Kothapalli

May 18, 2018 · 7 min read

1.6K