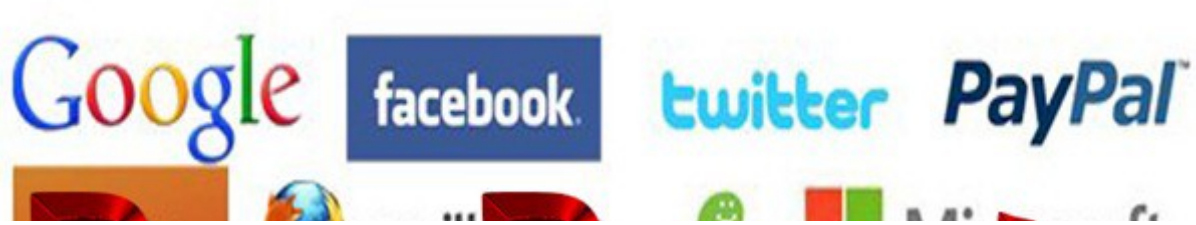
BUG BOUNTY HUNTING (METHODOLOGY , TOOLKIT , TIPS & TRICKS , Blogs)

Sanyam Chawla Follow
Mar 18, 2018 · 8 min read

A **bug bounty** program is a deal offered by many websites and software developers by which individuals can receive recognition and compensation for reporting **bugs**, especially those pertaining to exploits and vulnerabilities.

> ***A reward offered to a perform who identifies an error or vulnerability in a computer program or system.***
> ***'The company boosts security by offering a bug bounty'***



Bug Bounty—Image Source Google

Bug Bounty Platforms

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/

Hackenproof

https://hackenproof.com/

BountyFactory

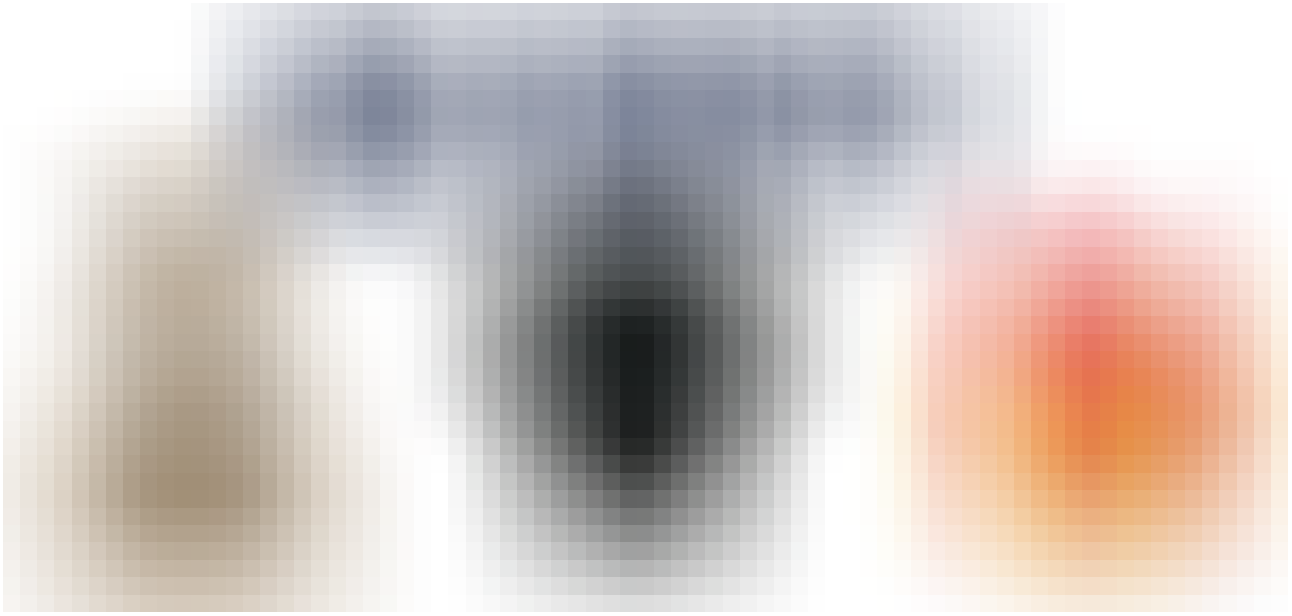
https://bountyfactory.io

Bug Bounty Programs List

https://www.bugcrowd.com/bug-bounty-list/

AntiHack

https://www.antihack.me/



Bug Bounty—Image Source Google

Some Books for reading about Bug Hunting

There are some books for Web application penetration testing methodology and hunting the web. Through this you learn the basics and essentials of

penetration testing and bug hunting. Since bug bounties often include website targets, we'll focus on getting you started with Web Hacking and later we'll branch out.

> ***The Web Application Hacker's Handbook***
>
> ***OWASP Testing Guide***
> ***Highly suggested by Bugcrowd's 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***

And for our Mobile hacking friends:

> ***The Mobile Application Hacker's Handbook***
>
> ***iOS Application Security***
>
> ***Owasp Mobile AppSec***

Practice makes Perfect!

While you're learning it's important to make sure that you're also understanding and retaining what you learn. Practicing on vulnerable applications and systems is a great way to test your skills in simulated

environments. These will give you 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

Read tech Vulnerabilities POCs (Proof of Concepts) and write-ups from other hackers

Now that you've got a baseline understanding of how to find and exploit security vulnerabilities, it's time to start checking out what other hackers are finding in the wild. Luckily the security community is quite generous with sharing knowledge and we've collected a list of write-ups & tutorials:

Bug Bounty write-ups and POC

Awesome Bug Bounty

SecurityBreached-BugBounty POC

Facebook Hunting POC

Bug Hunting Tutorials

PentesterLand Bug Bounty Writeups

Hackerone POC Reports

Bug Bounty POC

Netsec on Reddit

Bug Bounty World

Watch tutorials (Bug Hunting) on YouTube!

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

SecurityIdiots

> ***BlackHat***
>
> ***Injector PCA***
>
> ***DevilKiller***
>
> ***SulemanMalik***
>
> ***Penetration Testing in linux***

Bugcrowd Approach for Bug Hunting

Okay, now you're at the point where it's almost time to start hunting for bounties. But first, let's learn how bug bounties work and how to get started, just to make sure we maximize our chances of success.

How to approach a target

Advice from other bug hunters that will help you find more success when

approaching a bug bounty.

How to write a Great Vulnerability Report

This will walk you through how to write a great vulnerability report. The better your report, the higher chance you will get a bounty!

How to write a Proof of Concept

Proof of Concepts show the customer how your bug is exploited and that it works. This is crucial to being rewarded successfully.

How to Report a Bug

Our walkthrough for reporting a bug via the Bugcrowd platform.

Vulnerability guides

> ***OWASP Top 10 2017***
>
> ***SANS TOP 25***

> ***SSRF Bible Cheetsheet***
>
> ***File upload Stored XSS***
>
> ***OWASP Web Application Security Testing Cheat Sheet***

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

Pen Testing Methodologies

1. ***Penetration Testing Framework***
2. ***The Penetration Testing Execution Standard***
3. ***The WASC Threat Classification***
4. ***OWASP Top Ten Project***
5. ***The Social Engineering Framework***

My Tips & Tricks

> **Bug Bounty Hunting Tip #1- Always read the Source Code**
>
> **Bug Bounty Hunting Tip #2- Try to Hunt Subdomains**
>
> **Bug Bounty Hunting Tip #3- Always check the Back-end CMS & backend language (builtwith)**

> **Bug Bounty Hunting Tip #4- Google Dorks is very helpful**
>
> **Bug Bounty Hunting Tip #5- Check each request and response**
>
> **Bug Bounty Hunting Tip #6- Active Mind - Out of Box Thinking :)**

My Methodology for Bug Hunting

> ***First review the scope***
>
> ***Perform reconnaissance to find valid targets***
>
> ***Find sub-domains through various tools Sublist3, virus-total etc.***
>
> ***Select one target then scan against discovered targets to gather additional information (Check CMS, Server and all other information which i need)***
>
> ***Use google dorks for information gathering of a particular taget.***

> *Review all of the services, ports and applications.*
>
> *Fuzz for errors and to expose vulnerabilities*
>
> *Attack vulnerabilities to build proof-of-concepts*

For Bug bounty programs, First I'm going to review the scope of the target. There's a huge difference between a scope such as *.facebook.com versus a small company's single application test environment.

If scope is big than they accepts submissions for any of their servers, I'm going to start doing reconnaissance using search engines such as Google, Shodan, Censys, ARIN, etc. to discover subdomains, endpoints, and server IP addresses. This is a mix of Google dorking, scanning IP ranges owned by companies, servers ports scanning etc. Anything that gives me information on servers that may be owned by that company.

When I have a list of servers, I start to perform nmap port and banner scanning to see what type of servers are running. You may get some quick finds such as open SSH ports that allow password-based authentication. At

this point I tend to stay away from reporting those smaller issues. I opt to spend more time looking for critical applications running on non-standard web ports such as Jenkins that may have weak default configuration or no authentication in front of them.

Before I hunt into the websites too deeply, I first do a quick run through the web servers looking for common applications such as WordPress ,Drupal , joomla etc . This is a mix of just browsing the sites manually or directory hunting by using wordlist, looking for sitemaps, looking at robots.txt, etc. Some open source plugins are typically poorly made and with some source review can lead to critical findings.

Then dig in to website, check each request and response and analysis that, I'm trying to understand their infrastructure such as how they're handling sessions/authentication, what type of CSRF protection they have (if any).

Sometimes I use negative testing to through the error, this Error information is very helpful for me to finding internal paths of the website. I spend most of my time trying to understand the flow of the application to get a better idea of what type of vulnerabilities to look for.

Once I've done all of that, depending on the rules of the program, I'll start to dig into using scripts for wordlist bruteforcing endpoints. This can help with finding new directories or folders that you may not have been able to find just using the website. This tends to be private admin panels, source repositories they forgot to remove such as /.git/ folders, or test/debug scripts. After that check each form of the website then try to push client side attacks. Use multiple payloads to bypass client side filters. Best tools for all over the Bug Bounty hunting is "BURP SUITE" :)

This is just the methodology for Bug bounty hunting and Penetration testing that seems to work for me :)

TOOLS , Wordlists , Patterns, Payloads , Blogs

Tools & OS :

> **Bug Bounty Forum Tool list**
>
> **Bug crowd Tool list**

> **Nmap**
>
> **Burp Suite**
>
> **Wp-scan**
>
> **Kali Linux**
>
> **Browser :)**

Wordlist :

> **SecLists (Discovery, Fuzzing, Shell, Directory Hunting, CMS)**
>
> **Directory wordlist**
>
> **Portable Wordlist**

FUZZ-DB

Mix-Wordlist

Popular Google Dorks Use(finding Bug Bounty Websites)

1. **site:.eu responsible disclosure**
2. **inurl:index.php?id=**
3. **site:.nl bug bounty**
4. **“index of” inurl:wp-content/ (Identify Wordpress Website)**
5. **inurl:”q=user/password” (for finding drupal cms)**

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/

Passive Reconnaissance

> ***Shodan***
>
> ***BuiltWith***
>
> ***Censys***
>
> ***Whois***
>
> ***OSINT Framework***

Payloads for Hunting

Payloads All The Things

XSS Payloads

XSS Payloads -2

SQL Injection Payloads

Google-Dorks Payloads

Google-Dorks-2 Payloads

Information Security / Bug Hunting Blogs

"My daily inspiration are those who breaks their own limits and get success.
"

- *fin1te: Bug Bounty Participant*
- *Security & Code Blog*

- *Bug Crowd Forum*
- *ARNE SWINNEN'S SECURITY BLOG*
- *Hacks4Pancakes*
- *Daniel LeCheminant*
- *We Hack People*
- *IT-Securityguard Blog*
- *The misunderstood X-XSS-Protection*
- *Bug Bounty Findings by Meals*
- *VYSEC*
- *PWNHACK*
- *Philippe Harewood*
- *ARNE SWINNEN'S SECURITY BLOG*
- *Hacks4Pancakes*
- *NahamSec.com*

- *Daniel LeCheminant*
- *The misunderstood X-XSS-Protection*
- *Bug Bounty Findings by Meals*
- *Respect XSS*
- *Graceful Security!*
- *Fooling the Interpreter*
- *Klikki Oy*

> *Hope you like it , If you have any queries ... Feel free to connect me through linkedin or Twitter :) If I missed something, kindly comment below so i will add to the Bug Bounty- Infosec List- If you like this blog- do clap and share with your friends :)*

Whoami:- https://infosecsanyam.wixsite.com/infosecsanyam

Blog :- https://infosecsanyam.blogspot.in/

Linkedin : https://www.linkedin.com/in/infosecsanyam/

“My daily inspiration are those who breaks their own limits and get success. “

Security | Bug Bounty | Bugs | Vulnerability Research | Security Vulnerabilities

Sanyam Chawla

Information Security Specialist || Penetration Tester || Ethical Hacker || Security Researcher || Bug Bounty Hunter

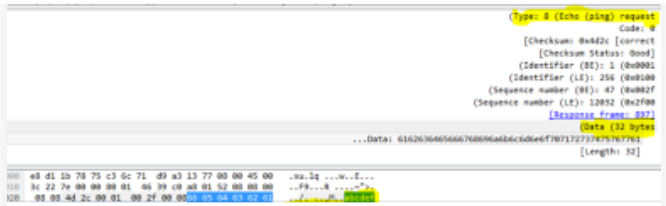
InfoSec Write-ups

A collection of write-ups from the best hackers in the world on topics ranging from bug bounties and CTFs to vulnhub machines, hardware challenges and real life encounters. In a nutshell, we are the largest InfoSec publication on Medium. #sharingiscaring

More from InfoSec Write-ups

Writing a Password Protected Bind Shell (Linux/x64)

0x0FFB347
Mar 8 · 5 min read
249



More from InfoSec Write-ups

Ping Power—ICMP Tunnel

Nir Chako
Dec 17, 2018 · 8 min read
488

More from InfoSec Write-ups

How to Make a Captive Portal of Death

Trevor Phillips
Dec 18, 2018 · 6 min read
280

Responses

Write a response...

Show all responses