

Bug Bounty Methodology


▼ 1. Program Choose

▼ Beginners

▼ Fame

▼ Choose a Less Popular platform

- HackerOne

 [HackerOne | #1 Trusted Security Platfo...](#)

- BugCrowd

 [#1 Crowdsourced Cybersecurity Platfo...](#)

- Open Bug Bounty

 [Free Bug Bounty Program and Coordin...](#)

- Intigriti

 [Bug Bounty & Agile Pentesting Pl...](#)

- Yes We Hack

 [YesWeHack #1 Bug Bounty Platform in...](#)

- Safe Hats

 [safehats](#)

- CyberArmy

 [Bug Bounty Program | Cyber Army Ind...](#)

▼ VDPs

- FireBounty

 [FireBounty | The Ultimate Vulnerability...](#)

- Choose point only program
- Program should be big scoop
- Hunt it 1 month untill find a valid bug

▼ Money

- Use google dorking to find platfromless program

 [Bug Bounty Dorking - Google Docs](#)

- Program should be big scoop

- Hunt it 1 month until find a valid bug

▼ Avoid Program

▼ Read Writeup

- Pentester Land WriteUp

 [Writeups - Pentester Land](#)

- Vulnerability labs

 [VULNERABILITY LAB - SECURITY VULN...](#)

- Have a Bad Reputation and Review
- Delay in reply

▼ Advance

▼ Private Program

- Synack Red Team

 <https://www.synack.com/red-team/>

- Detectify

 [Detectify Crowdsource | Hack the planet](#)

- Cobalt

 [Cobalt: Offensive Security Services](#)

- Yogosha

 [Yogosha | Offensive Security Testing Pl...](#)

▼ Web v3

- HackenProof

 [HackenProof | Web3 Bug Bounty platf...](#)

- Immunefi

 [Immunefi](#)

▼ 2. Application Analysis

▼ Site Surfing

- Surfing site with burp proxy
- Surfing using VPN

▼ Purchase Paid Plan

- If program have a paid plan then purchase paid plan and create a free plan also

▼ Search Engine

- Change detection
- Company Job Post for Engineer
- Company Blog
- Employees blog
- Target newsletter
- Mail List Subscribe
- Affiliate program
- QNA Forum
- Conference talk
- Monitoring the domain for code change
- Github Issue
- Terms and Condition
- Privacy Policy text
- Copyright text
- Pastebin
- PasteHunter
 - [GitHub - kevthehermit/PasteHunter: S...](#)
- Google Calender
- Stackshare
- SlideShare
- BugBounty Writeup
- Stack Overflow
- Quora

▼ Make a Checklist

- You can make your own by site structure
- Owasp top 10 checklist
 - [GitHub - tanprathan/OWASP-Testing-...](#)

▼ Testing layers

- Open port and service

- Web hosting software
- App framwork
- App: Custom code or cots
- App library
- Integration

▼ Big Q

- #1 How does app pass data?
- ▼ #2 How/Where does app talk about users?
 - ▼ Users
 - ▼ Where
 - Cookies
 - API Call
 - ▼ How
 - UID
 - UUID
 - email
 - username
- ▼ #3 Does the site have multi-tenancy or user level?
 - ▼ Users
 - App is designed for multiple customers
 - App has multiple user level
- #4 Does the site have a unique threat model?
- #5 There been past security research and vulnerabilities?
- #6 How does app handle : XSS? , CSRF?, and more?

▼ Parameter Analysis

- Hunt
- XSSed
- Hackerone Public Disclosure
 - Tomnomnom's GF Tool
- SUS-Params

- BurpBounty
- BurpSuite

▼ Heat Mapping

- Note Down all heat mapping

▼ 3. Recon

▼ Root (Aquasition)

- Crunchbase

 [Crunchbase: Discover innovative comp...](#)

- Search Engine
- BugBounty Platfrom
- AI

▼ DNS Record

▼ Whois

- whois

Linux

Mac OS

Windows

▼ Reverse Whois

- ViewDnsInfo

 [Reverse Whois Lookup - ViewDNS.info](#)

▼ A Record (IPv4 addresses)

- nslookup -type=A DOMAIN_NAME / SERVER_IP

Linux

Mac OS

Windows

- dig SERVER_IP / DOMAIN_NAME A

Linux

Mac OS

Windows

▼ AAAA Record (IPv6 addresses)

- nslookup -type=AAAA DOMAIN_NAME / SERVER_IP

Linux

Mac OS

Windows

- dig SERVER_IP / DOMAIN_NAME AAAA

Linux

Mac OS

Windows

▼ CNAME Record

- nslookup -type=CNAME DOMAIN_NAME / SERVER_IP

Linux

Mac OS

Windows

- dig SERVER_IP / DOMAIN_NAME CNAME

Linux

Mac OS

Windows

▼ MX Record

- nslookup -type=MX DOMAIN_NAME / SERVER_IP

Linux

Mac OS

Windows

- dig SERVER_IP / DOMAIN_NAME MX

Linux

Mac OS

Windows

▼ TXT Record

- nslookup -type=TXT DOMAIN_NAME / SERVER_IP

Linux

Mac OS

Windows

- dig SERVER_IP / DOMAIN_NAME TXT

Linux

Mac OS

Windows

▼ SSL certificate

- Certificate Search


 <https://crt.sh/>

▼ Tools


- DNS Dumper

 [DNSDumpster.com - dns recon and re...](#)

- ViewDNS

 [ViewDNS.info - Your one source for D...](#)

- ARIN Whois

 [Whois-RWS](#)

- Hurricane Electric Internet Services

 [Hurricane Electric BGP Toolkit](#)

- MXToolBox

 <https://mxtoolbox.com/>

- MXToolBox Super Tools

 <https://mxtoolbox.com/SuperTool.aspx>

- Domain Tools

- Whois Lookup, Domain Availability & I...

- IP Address Guide

- Free IP address tools for IPv4 and IPv6...

- Whoxy

- WHOIS API | WHOIS Lookup API | Do...

- ▼ ASN to CIDR

- bgn.he.net

- <http://bgn.he.net>

- ASN Lookup

- <https://mxtoolbox.com/asn.aspx>

- Metabigor

- [GitHub - j3ssie/metabigor: OSINT tool...](#)

- Amass

- [GitHub - owasp-amass/amass: In-dept...](#)

- ▼ CIDR to IP

- MapCIDR

- [GitHub - projectdiscovery/mapcidr: Uti...](#)

- ▼ Networking

- ▼ Ping

- ping MACHINE_IP / HOSTNAME

- Linux

- Mac OS

- Windows

- IP Address Guide

- Free IP address tools for IPv4 and IPv6...

- ▼ Traceroute

- traceroute MACHINE_IP / HOSTNAME

- Linux

- Mac OS

- tracert MACHINE_IP / HOSTNAME

- Windows

- IP Address Guide

- Free IP address tools for IPv4 and IPv6 ...

- ▼ Technology and Services Footprinting

- ▼ Port Scan

- Rust Scan

- GitHub - RustScan/RustScan: 🐙 The ...

- Naabu

- GitHub - projectdiscovery/naabu: A fas...

- Nmap

- GitHub - nmap/nmap: Nmap - the Net...

- ▼ Service Footprinting

- Try Telnet and Netcat

- wafw00f

- GitHub - EnableSecurity/wafw00f: WAF...

- Brutesprey

- GitHub - x90skysn3k/brutespray: Brute...

- ▼ Tech Profiling

- Whatruns

- WhatRuns - Discover Website Technol...

- Wappalyzer

- Find out what websites are built with - ...

- WebAnalyzer

- webanalyzer free seo tool

- BuildWith

- quote-left

- StacksShare

- StackShare - Tech Stack Intelligence

- ▼ Cloud

- ▼ Cloud Recon

- GitHub - g0ldencybersec/CloudRecon

▼ Make a DB using this tool

▼ Parse out Subs

- `grep -F'.DOMAIN.com' 12_11_2023_DB.txt | awk -F'[.]' '{print $2}' | sed 's# #\n#g' | grep ".DOMAIN.com" | sort -fulcut -d','-f1| sort -u`

Linux

▼ Parse out all domains (potential apexes)

- `grep -F'.DOMAIN.com' 12_11_2023_DB.txt | awk -F'[.]' '{print $2}' | sed 's# #\n#g'| Sort -fu | cut -d','-f1|sort -u`

Linux

- Kaeferjaeger gay DB

 [Home • Directory Lister](#)

▼ IP to SubDomain

- dnsx

 [GitHub - projectdiscovery/dnsx: dnsx i...](#)

▼ SubDomain

▼ Linked and JS discovery

- Burp Suite Pro

 [Burp Suite Professional - PortSwigger](#)

- Gobuster

 [GitHub - OJ/gobuster: Directory/File,...](#)


- Hakrawler

 [GitHub - hakluke/hakrawler: Simple, fa...](#)

- SubDomainizer

 [GitHub - nsonaniya2010/SubDomainiz...](#)

- OneForAll

 [OneForAll/docs/en-us/README.md at ...](#)

▼ SubDomain Scrapping

- Amass



- Github Subdomains

 [GitHub - gwen001/github-subdomain...](#)

- Subfinder
 - [GitHub - projectdiscovery/subfinder: F...](#)

- Shosubgo
 - [GitHub - incogbyte/shosubgo: Small t...](#)

- Cloud Ranges
 - [GitHub - pry0cc/cloud-ranges: A list of...](#)

- OneForAll
 -

- ▼ Manually

- ▼ Search Engine source

- Yahoo
 - Google
 - Baidu
 - bing
 - Ask
 - Dogpile

- ▼ Infrastructure Source

- Censys
 - Robtex
 - Wayback Machine
 - Netcraft
 - DnsDB Search
 - Passive total
 - PTRarchive
 - DNSDumper

- ▼ Certificate Sources

- crt.sh
 - sslmate cert spotter
 - CertDB

- ▼ Security Source

- Hacker Target
- SecurityTrails
- VirusTotal
- F-security Riddler
- ThreadCrowd
- ThreatMiner

▼ SubDomain Bruteforcing

- Subfinder



- Amass



- FFUF



- Shuffledns



- OneForAll



▼ Peramutation

- AltDNS



- DNSGen



- OneForAll



▼ HTTP and Screenshots

▼ HTTP

- httpx



▼ Screenshots

- EyeWitness



▼ Directory

- Dirsearch

 [GitHub - maurosoria/dirsearch: Web p...](#)

▼ JS Analysis

▼ Recon

- GetJS

 [GitHub - 003random/getJS: A tool to f...](#)

- Katana



- Nuclei



- SubJS



▼ Analysis

- Secret Finder



- Mantra



- SubJS



▼ CVE

- Search Engine

- Nuclei



- Retier.js



- GoFingerprint



- Sn1per



- Intrigue core



- Vulners

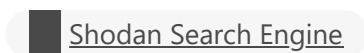


- Jaeles Scanner



▼ IOT Search Enging and Dorking

- ▼ Shodan



- Karma v2



▼ Third Party Hosting

- BUCKET.s3.amazonaws.com

- s3.amazonaws.com/BUCKET

- AWSCLI



- Lazys3



- S3Scanner



- GrayHat Warfare



▼ Github Recon and Code Analysis

- ▼ Github Recon

- Manually check Issue and Commit

- Manually Dorking

- TruffleHog



- Gitrob



- Gitgraber



- GitDorker



▼ Code Analysis

- KeyHacks



▼ Check Important things in code

- Variable

▼ Function

- authentication
- password reset
- private info read
- user input

- Configuration File

- Source2url



- APKleaks



▼ 4. Post Exploitation

▼ Vulnerability Chaining

- Always Try to Chain Small Vulnerability To RCE or Another Big Vulnerabilities

▼ Low Hanging Fruit

- If a low hanging fruit vulnerabilities in out of scope then always try to chain it. Or try to show a big impact
- Find low hanging fruit in web analysis area

▼ SubDomain TakeOver

▼ Recon

- Can I takeover xyz



- dig [server] [name] [type]

Linux

- ns lookup



▼ Hunt

- Subzy



- SubOver



- SubJack



- Nuclei



▼ Owasp Top Ten

- A01:2021-Broken Access Control
- A02:2021-Cryptographic Failures
- A03:2021-Injection
- A04:2021-Insecure Design
- A05:2021-Security Misconfiguration
- A06:2021-Vulnerable and Outdated Components
- A07:2021-Identification and Authentication Failures
- A08:2021-Software and Data Integrity Failures
- A09:2021-Security Logging and Monitoring Failures
- A10:2021-Server-Side Request Forgery

▼ Under-Rated Bug

▼ Prototype pollution

- Server-side parameter pollution
- HTTP Parameter Pollution

- Log4J
- HTTP request smuggling
- DOM-based vulnerabilities

▼ **Note Taking**

- Obsidian
- XMind

▼ **Reference**

- Jason Haddix Methodology
- Zseano's Methodology
<https://www.bugbountyhunter.com/m...>
- OWASP Web Security Testing Guide
[OWASP Web Security Testing Guide |...](#)
- OWASP Code Review Guide
[OWASP Code Review Guide | OWASP F...](#)

▼ **CTF**

- Hacker101
- TryHackMe
- HackTheBox
- PortSwigger Labs
- Proving Ground
- OWASP Juice Box
- HackThisSite
- CTFChallenge
- PenTesterLab
- XSSGame
- BugBountyHunter
- W3Challs
- Metasploitable 2
- BWAPP

- OVWA
- PicoCTF