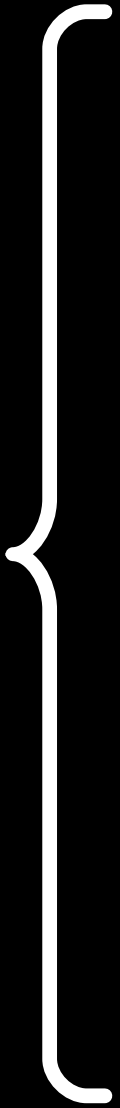


# Bug Bounty Methodology

Presented with **xmind**

# **Bug Bounty Methodology**

- 
1. Program Choose
  2. Application Analysis
  3. Recon
  4. Post Exploitation

# 1. Program Choose

**1. Program  
Choose** { **Beginners**  
**Advance**

# Beginners

- Fame
- Money
- Avoid Program

# Fame

- Choose a Less Popular platform
- VDPs
- Choose point only program
- Program should be big scoop
- Hunt it 1 month until find a valid bug

# Fame

• CHOOSE a LESS popular platform

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

# Choose a Less Popular platform

- HackerOne [↗](#)
- BugCrowd [↗](#)
- Open Bug Bounty [↗](#)
- Intigriti [↗](#)
- Yes We Hack [↗](#)



# Choose a Less Popular platform

• Open Bug Bounty [↗](#)

• Intigriti [↗](#)

• Yes We Hack [↗](#)

• Safe Hats [↗](#)

• CyberArmy [↗](#)

# VDPs

---

FireBounty [↗](#)

# Money

- Use google dorking to find platformless program [↗](#)
- Program should be big scoop
- Hunt it 1 month until find a valid bug

# Avoid Program

- Read Writeup
- Have a Bad Reputation and Review
- Delay in reply

# Read Writeup

- Pentester Land WriteUp [↗](#)
- Vulnerability labs [↗](#)

# Advance

- Private Program
- Web v3

# Private Program

- Synack Red Team [↗](#)
- Detectify [↗](#)
- Cobalt [↗](#)
- Yogosha [↗](#)

# Web v3

- HackenProof [↗](#)
- Immunefi [↗](#)



# 2. Application Analysis

## 2. **Application Analysis**

Site Surfing

Purchase Paid Plan

Search Engine

Make a Checklist

Testing layers

## 2. **Application Analysis**

Make a Checklist

Testing layers

Big Q

Parameter Analysis

Heat Mapping

# 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

# Search Engine

- Target newsletter
- Mail List Subscribe
- Affiliate program
- QNA Forum
- Conference talk

# Search Engine

- Monitoring the domain for code change
- Github Issue
- Terms and Condition
- Privacy Policy text
- Copyright text



# Search Engine

- Copyright text
- Pastebin
- PasteHunter [↗](#)
- Google Calender
- Stackshare

# Search Engine

• StackShare

• SlideShare

• BugBounty Writeup

• Stack Overflow

• Quora

# Search Engine

- SlideShare
- BugBounty Writeup
- Stack Overflow
- Quora

# Make a Checklist

- ★ You can make your own by site structure
- Owasp top 10 checklist [↗](#)

# Testing layers

- Open port and service
- Web hosting software
- App framework
- App: Custom code or cots
- App library

# Testing layers

• web testing software

- App framework
- App: Custom code or cots
- App library
- Integration

# Big Q

- ? #1 How does app pass data?
- ? #2 How/Where does app talk about users?
- ? #3 Does the site have multi-tenancy or user level?
- ? #4 Does the site have a unique threat model?
- ? #5 There been past security research and

# Big Q

- ? #3 Does the site have multi-tenancy or 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?



# #2 How/Where does app talk about users?

---

Users

# Users

- Where
- How

# Where

- Cookies
- API Call

# How

- UID
- UUID
- email
- username

 #3 Does the site  
have multi-tenancy ...


---

Users


# Users

- App is designed for multiple customers
- App has multiple user level

# Parameter Analysis

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

# Parameter Analysis

-  Tomnomnom's GF Tool
- SUS-Params
- BurpBounty
- BurpSuite



# Heat Mapping

---

Note Down all heat mapping

# 3. Recon

# 3. Recon

- Root (Aquasition)
- DNS Record
- ASN to CIDR
- CIDR to IP
- Networking

# 3. Recon

- Networking
- Cloud
- IP to SubDomain
- SubDomain
- HTTP and Screenshots

# 3. Recon

- Directory
- JS Analysis
- CVE
- IOT Search Enging and Dorking
- Third Party Hosting

# 3. Recon

Reconnaissance

- CVE
- IOT Search Enging and Dorking
- Third Party Hosting
- Github Recon and Code Analysis

# Root (Aquasition)

- Crunchbase [↗](#)
- Search Engine
- BugBounty Platfrom
- AI

# DNS Record

- Whois
- Reverse Whois
- A Record (IPv4 addresses)
- AAAA Record (IPv6 addresses)
- CNAME Record



# DNS Record

- CNAME Record
- MX Record
- TXT Record
- SSL certificate
- Tools

# DNS Record

OR/WIRE RECORD

- MX Record
- TXT Record
- SSL certificate
- Tools

# Whois

---

whois

# whois

Linux

Mac OS

Windows

# Reverse Whois

---

ViewDnsInfo 

# A Record (IPv4 addresses)

- `nslookup -type=A DOMAIN_NAME / SERVER_IP`
- `dig SERVER_IP / DOMAIN_NAME A`

**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`
- `dig SERVER_IP / DOMAIN_NAME AAAA`

**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`
- `dig SERVER_IP / DOMAIN_NAME CNAME`

**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`
- `dig SERVER_IP / DOMAIN_NAME MX`

**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`
- `dig SERVER_IP / DOMAIN_NAME TXT`

**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 [↗](#)

# Tools





- DNS Dumper [↗](#)
- ViewDNS [↗](#)
- ARIN Whois [↗](#)
- Hurricane Electric Internet Services [↗](#)
- MXToolBox [↗](#)

# Tools

- MXToolBox [↗](#)
- MXToolBox Super Tools [↗](#)
- Domain Tools [↗](#)
- IP Address Guide [↗](#)
- Whoxy [↗](#)

# Tools

MXTOOLBOX 

- MXToolBox Super Tools 
- Domain Tools 
- IP Address Guide 
- Whoxy 



# ASN to CIDR

- [bgn.he.net](#) ↗
- [ASN Lookup](#) ↗
- [Metabigor](#) ↗
- [Amass](#) ↗

# CIDR to IP

---

MapCIDR [!\[\]\(3dfb8d66e81160ad61421a3452093d1b\_img.jpg\)](#)

# Networking

- Ping
- Traceroute
- Technology and Services Footprinting

# Ping

- ping MACHINE\_IP / HOSTNAME
- IP Address Guide [↗](#)

# ping MACHINE\_IP / HOSTNAME

Linux

Mac OS

Windows

# Traceroute

- `tracert MACHINE_IP / HOSTNAME`
- `tracert MACHINE_IP / HOSTNAME`
- IP Address Guide [↗](#)

**traceroute MACHINE\_IP / HOSTNAME**

Linux

Mac OS

**tracert MACHINE\_IP / HOSTNAME**

Windows



# Technology and Services F...

- Port Scan
- Service Footprinting
- Tech Profiling

# Port Scan

- Rust Scan [↗](#)
- Naabu [↗](#)
- Nmap [↗](#)

# Service Footprinting

- Try Telnet and Netcat
- wafw00f [↗](#)
- Brutesprey [↗](#)

# Tech Profiling

- Whatruns [↗](#)
- Wappalyzer [↗](#)
- WebAnalyzer [↗](#)
- BuildWith [↗](#)
- StacksShare [↗](#)

# Tech Profiling

• [Wappalizer](#) 

- Wappalyzer 

- WebAnalyzer 

- BuildWith 

- StacksShare 

# Cloud

- Cloud Recon [↗](#)
- Kaeferjaeger gay DB [↗](#)

# Cloud Recon

---

Make a DB using this tool

# Make a DB using this tool

- Parse out Subs
- Parse out all domains (potential apexes)



# 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
```

```
grep -F'.DOMAIN.com' 12_11_2023_DB.txt | awk -  
F[I]' '{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
```

```
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

# IP to SubDomain

---

dnsx 

# SubDomain

- Linked and JS discovery
- SubDomain Scrapping
- SubDomain Bruteforcing
- Peramutation

# Linked and JS discovery

- Burp Suite Pro [↗](#)
- Gobuster [↗](#)
- Hakrawler [↗](#)
- SubDomainizer [↗](#)
- OneForAll [↗](#)

# Linked and JS discovery

• Burp Suite [↗](#)

• Gobuster [↗](#)

• Hakrawler [↗](#)

• SubDomainizer [↗](#)


• OneForAll [↗](#)



# SubDomain Scrapping

- Amass [↗](#)
- Github Subdomains [↗](#)
- Subfinder [↗](#)
- Shosubgo [↗](#)
- Cloud Ranges [↗](#)

# SubDomain Scrapping

- Shosubgo [↗](#)
- Cloud Ranges [↗](#)
- OneForAll [↗](#)
-  Manually

# ! Manually

- Search Engine source
- Infrastructure Source
- Certificate Sources
- Security Source

# Search Engine source

- Yahoo
- Google
- Baidu
- bing
- Ask

# Search Engine source

• Google

- Baidu
- Bing
- Ask
- Dogpile

# Infrastructure Source

- Censys
- Robtex
- Wayback Machine
- Netcraft
- DnsDB Search

# Infrastructure Source

Infrastructure

- DnsDB Search
- Passive total
- PTRarchive
- DNSDumper

# Certificate Sources

- crt.sh
- sslmate cert spotter
- CertDB



# Security Source

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

# Security Source

- VirusTotal
- F-security Riddler
- ThreadCrowd
- ThreatMiner

# SubDomain Bruteforcing

- Subfinder [↗](#)
- Amass [↗](#)
- FFUF [↗](#)
- Shuffledns [↗](#)
- OneForAll [↗](#)

# SubDomain Bruteforcing

• Subfinder [↗](#)

- Amass [↗](#)

- FFUF [↗](#)

- Shuffledns [↗](#)

- OneForAll [↗](#)

# Peramutation

- AltDNS [↗](#)
- DNSGen [↗](#)
- OneForAll [↗](#)

# HTTP and Screenshots

- HTTP
- Screenshots

# HTTP

---

httpx 

# Screenshots

---

EyeWitness 



# Directory

---

Dirsearch [!\[\]\(919a2cb85b99741a73c0c31a427236a8\_img.jpg\)](#)

# JS Analysis

- Recon
- Analysis




# Recon

- GetJS [↗](#)
- Katana [↗](#)
- Nuclei [↗](#)
- SubJS [↗](#)

# Analysis

- Secret Finder [↗](#)
- Mantra [↗](#)
- SubJS [↗](#)

# CVE

-  Search Engine
-  Nuclei [↗](#)
-  Retier.js [↗](#)
- GoFingerprint [↗](#)
- Sn1per [↗](#)

# CVE

cc fingerprint ↗

- Sn1per ↗
- Intrigue core ↗
- Vulners ↗
- Jaeles Scanner ↗

# IOT Search Enging and Dorking

---

 Shodan 






 **Shodan** 

---

**Karma v2** 



# Third Party Hosting

-  BUCKET.s3.amazonaws.com
-  s3.amazonaws.com/BUCKET
- AWSCLI 
- Lazys3 
- S3Scanner 

# Third Party Hosting

- AWSCLI [↗](#)
- Lazys3 [↗](#)
- S3Scanner [↗](#)
- GrayHat Warfare [↗](#)

# Github Recon and Code Analysis


- Github Recon
- Code Analysis

# Github Recon



- ★ Manually check Issue and Commit
- ★ Manually Dorking
- ★ TruffleHog [↗](#)
- Gitrob [↗](#)
- Gitgraber [↗](#)

# Github Recon

 Mandatory Dorking

-  TruffleHog [↗](#)
- Gitrob [↗](#)
- Gitgraber [↗](#)
- GitDorker [↗](#)

# Code Analysis

-  KeyHacks [↗](#)
-  Check Important things in code
- Source2url [↗](#)
- APKleaks [↗](#)

# Check Important things in code

- Variable
- Function
- Configuration File

# Function

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



# 4. Post Exploitation

## **4. Post Exploitation**

Vulnerability Chaining

Low Hanging Fruit

SubDomain TakeOver

Owasp Top Ten

Under-Rated Bug

# 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
- Hunt

# Recon

- Can I takeover xyz [↗](#)
- dig [server] [name] [type]
- ns lookup [↗](#)

# dig [server] [name] [type]

Linux

# 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

# Owasp Top Ten

- 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

# Owasp Top Ten

A07:2021-Identification and Authentication Failures

- 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
- Log4J
- HTTP request smuggling
- DOM-based vulnerabilities

# Prototype pollution

- Server-side parameter pollution
- HTTP Parameter Pollution

# Note Taking






# Note Taking

- Obsidian
- XMind

# Reference



# Reference

-  Jason Haddix Methodology
-  Zseano's Methodology 
- OWASP Web Security Testing Guide 
- OWASP Code Review Guide 

# CTF

# CTF

- Hacker101
- TryHackMe
- HackTheBox
- PortSwigger Labs
- Proving Ground

# CTF

- Proving Ground
- OWASP Juice Box
- HackThisSite
- CTFChallenge
- PenTesterLab

# CTF

- XSSGame
- BugBountyHunter
- W3Challs
- Metasploitable 2
- BWAPP

# CTF

- Metasploitable 2
- BWAPP
- OVWA
- PicoCTF

# Thank you