# A COMPREHENSIVE STUDY INTO BUG BOUNTY TOOLS

**By Harsh Tandel to Cyber frat, Mumbai**

# WHO AM I

- Cyber Security Consultant
- Part time Bug Hunter
- Block chain Security Researcher
- P1 Warrior Bug crowd
- Integrity Global top 1000
- Public Speaker and Blog Writer
- LinkedIn
- Twitter

# Burp Suite

➢ Fine-tune Proxy Traffic

1. TLS Pass Through
2. Scope based Proxy interception rule

➢ Fine-tune History

1. Miscellaneous Proxy setting
2. Filter settings, Color Highlight

❑ Project Settings

➢ Intruder

1. Playing with Intruder
2. Grep

➢ Extender

1. Turbo intruder
2. Bapp store

➢ Upstream Proxy

Network>User setting > Upstream Proxy

# SQL MAP

## ➢Defining File and Parameter

1. Storing request in file and define vulnerable parameter with “ ***** ”.
2. Defining file to get request with “**-r** ”.

## ➢Fine tuning exploitation

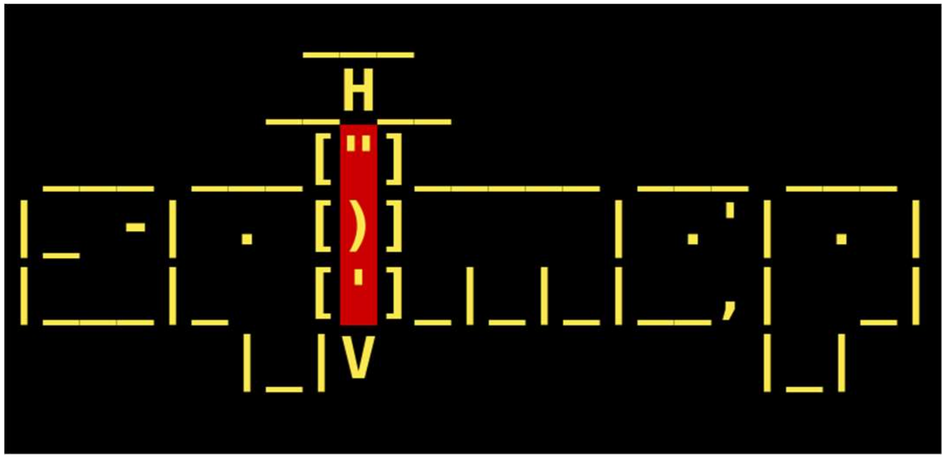
1. Defining database with “—dbms”
2. Defining Exploitation technique with “ –-technique”

   B: Boolean-based blind    E: Error-based

   U: Union query-based    S: Stacked queries

   T: Time-based blind    Q: Inline queries

- --batch command is used for non-interactive sessions.



```
        ___
       __H__
 ___ ___["]_____ ___ ___
|_ -| . [)]     | .'| . |
|___|_  [']_|_|_|__,|  _|
      |_|V          |_|
```

## ➢WAF bypass

1. --random-agent , sqlmap will randomly select a User-Agent from the ./txt/user-agents.
2. — level and — risk options are used to control the intensity and aggressiveness of the SQL injection testing process.
3. --tempare allows you to modify the SQL query sent to the website in a way that can bypass the sanitation or even the WAF on the website

# SHODAN

- Shodan is a search engine that lets users search for various types of servers connected to the internet.

1.Misconfigured Jenkins Instances: "http.title:Dashboard" "jenkins country:YOUR_COUNTRY_CODE"

2.Open Elasticsearch Instances: port:9200 country:"YOUR_COUNTRY_CODE"

3. Exposed MongoDB Databases: port:27017 country:"YOUR_COUNTRY_CODE"

4. Unsecured VNC: "RFB 003.003" port:5900 country:"YOUR_COUNTRY_CODE“

5. Exposed Redis Instances:port:6379 country:"YOUR_COUNTRY_CODE"

6.SSL/TLS Certificates :`ssl.cert.issuer.cn:Microsoft ssl.cert.subject.cn:Microsoft`

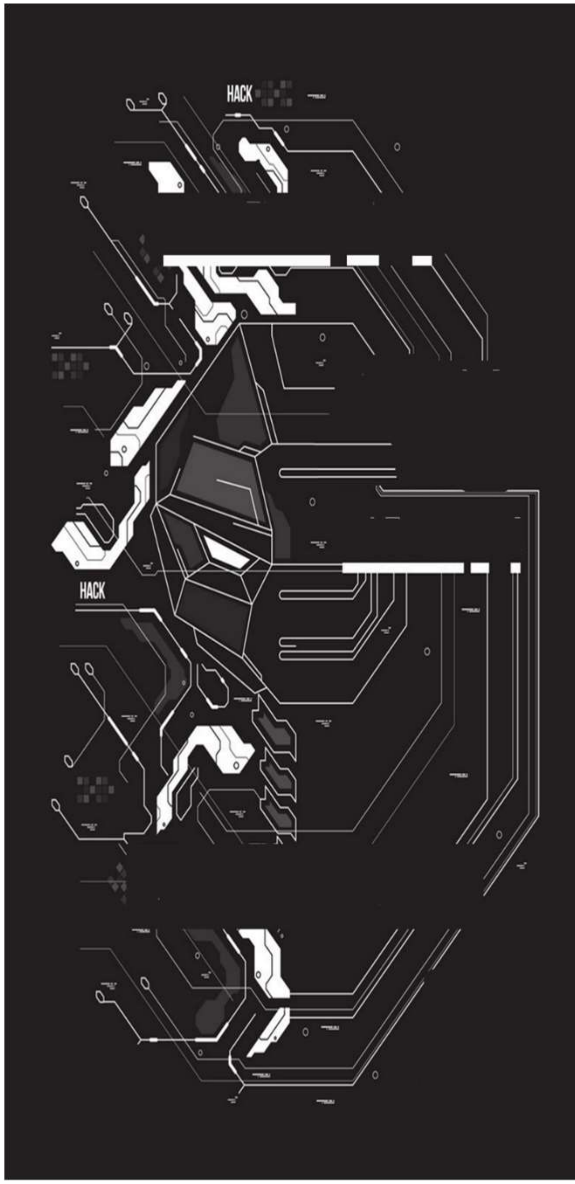
❑ “port:80 country:US org:Microsoft”

# Recon Tools

- Attack surface finding tools
- Knockpy
- Subfinder
- Httpx
- subfinder -d target.com | httpx | tee target.txt
- Subbrute for second and third level subdomain enumeration.
- Waybackurl
- cat target.txt | waybackurls | tee wayback.txt
- Eyewitness /gowitness

# Miscellaneous

1. Certificate Search : Search record based on org ssl certificate
2. Censys : Same Like a Shodan help to find host and port
3. Web Archive : Find Archive web pages
4. Subdomainfinder : Online Subdomain Finder
5. URLScan : Search for domains, IPs, filenames, hashes, ASNs
6. Lopseg : OSINT Website useful for BugBounty
7. WSL - explorer.exe



## Postman

- Proxy with burp suite
- Authentication
- Graphql module

## Mobsf

- Static Scan

# Thank You for Attention and providing platform