

Recon Methodology

Finding Programs

```
inurl:"responsible disclosure policy"
inurl:"security.txt"
Public bug bounty list: https://www.bugcrowd.com/bug-bounty-list/
Awesome bug bounty: https://github.com/djadmin/awesome-bug-bounty
```

1. Check Initial Time To First Response
2. Check Program Triage Time
3. Check Report Resolve Time

[Tip: Go for larger scope targets initially]

Scope

1. Read and understand scope
2. Which Assets are in scope?
3. Automated tools are allowed?
4. What bugs are accepted by the program?
5. If in doubt send message to the support team.

Subdomain Discovery

Tools

1. Amass
2. Assetfinder
3. Subfinder
4. Finddomain
5. Subbrute
6. Crtsh-CLI / crt.sh [Web Interface]

Amass

amass enum -d target.com

Assetfinder

assetfinder --subs-only target

Subfinder

subfinder -d target.com

Finddomain

```
finddomain -t target.com
```

Crt.sh [Web Interface]

```
target.com
```

Subbrute

```
./subbrute.py target.com
```

Create a result.txt including all the tools outputs.

Eliminating The False Positives

Sort Subdomains in unique

```
cat results.txt | sort -u > resultsUnique.txt
```

Subdomain Live Testing

```
cat resultsUnique.txt | httpprobe -c 100 > resultsAlive.txt
```

Directory Bruteforcing

Tools

1. Dirb
2. Gobuster
3. Dirsearch
4. Ffuf

Wordlist

```
SecLists: https://github.com/danielmiessler/SecLists  
Assetnote:https://wordlists.assetnote.io/
```

Dirb

```
dirb target.com wordlist
```

Gobuster

```
gobuster dir -u target.com -w wordlist -x php,js,txt,bak,log
```

Dirsearch

```
dirsearch.py -u target.com -w wordlist -e php -b -t 200
```

Ffuf

```
ffuf -w wordlist -u target.com/FUZZ mc 200 -c -v
```

Bucket

Tools

```
Slurp
Bucket Flaws
S3 Scanner
AWS BucketDump
```

Slurp

slurp domain -t target.com

slurp keywords -t test

Shodan

Tutorials

```
Shodan Dorks:https://github.com/humblelad/Shodan-Dorks
Shodan Tutorial: https://danielmiessler.com/study/shodan/
https://pathakabhi24.medium.com/shodan-the-complete-guide-51c099cde0d3
```

Github

Tools

1. Gitrob
2. Trufflehog
3. Gityleaks

Tutorials

```
Github Dorks:https://github.com/H4CK3RT3CH/github-dorks
```

Google Dorks

Tutorials

```
Google Dorks Tutorials:https://www.exploit-db.com/google-hacking-database
```

Nmap

nmap -sS -p target.com/IP

nmap -sU -p target.com/IP

nmap -sV -p target.com/IP

Analyzing JS Files

Tools

```
Linkfinder
```

Linkfinder

```
python3 linkfinder -i target.com -o cli
```

Keywords to search in js file

1. api
2. http
3. https
4. api_key
5. apikey
6. token
7. secret
8. config
9. conf
10. cfg
11. ENV
12. env

Waybackurl

Tools

```
Waybackurls
```

Waybackurls

```
cat results.txt | waybackurls > urls
```