

# IWCon W2022

Orwa GodFather



# IWCON

- Basic Recon
- Tools
- IWCon 2022 Tips ==> To Find Easy High/Critical Bugs



# ABOUT ME

- Orwa Atyat From Jordan
- Full Time Bug Hunter
- BugCrowd Full Rank : Top 100  
BugCrowd P1 Warrior Rank: Top 10
- Completing Nearly **190 P1** Report On BugCrowd
- **CVE-2022-21500 | CVE-2022-21567**





# BASIC RECON & TOOLS

- Subdomain Enumerations

<https://crt.sh/?q=%25.target.com>

[https://securitytrails.com/list/apex\\_domain/target.com](https://securitytrails.com/list/apex_domain/target.com)

<https://www.shodan.io/search?query=Ssl.cert.subject.CN%3A%22target.com%22>

Single Domain:

```
amass enum -passive -norecursive -noalts -d domain .com -o  
sub-list.txt
```

Domains List:

```
amass enum -passive -norecursive -noalts -df domains.txt -o  
subs-list.txt
```



# SUBDOMAIN ENUMERATIONS TOOLS

GitHub - iamthefrogy/frogy

[GitHub - Cyber-Guy1/domainCollector](#)

<https://gitlab.com/prawps/ohdns>

After collecting everything remove the duplicate subs

```
cat full-subdomain-list.txt | sort -u > sub-list.txt
```



# BUGCROWD

Filter the subs with httpx

```
cat sub-list.txt | httpx -o live-subs.txt
```

Scan port top 1000 port or – Full ports with nabbu

```
naabu -list sub-list.txt -top-ports 1000 -exclude-ports 80,443,21,22,25 -o ports.txt
```

```
naabu -list sub-list.txt -p - -exclude-ports 80,443,21,22,25 -o ports.txt
```



# COLLECTING URLS ENDPOINTS

<https://urlscan.io/search/#target.com>

[https://web.archive.org/cdx/search/cdx?url=\\*.target.com&fl=original&collapse=urlkey](https://web.archive.org/cdx/search/cdx?url=*.target.com&fl=original&collapse=urlkey)

Google dorking

site:target.com

Bing dorking

site:target.com



# SEARCH FOR SOURCES/BACKUP FILES

- Tip:
- orwa.iwcon.com
- orwa.iwcon.com/orwa.zip - iwcon.zip – admin.zip – backup.zip
- orwa.iwcon.com/orwa/orwa.zip - wicon.zip – admin.zip – backup.zip
- orwa.iwcon.com/iwcon/orwa.zip - iwcon.zip – admin.zip – backup.zip
- orwa.iwcon.com/admin/orwa.zip - iwcon.zip – admin.zip – backup.zip
- <https://github.com/musana/fuzzuli>

for fuzzing on backups



# ALL IN ONE

- <https://offsec.tools/>

The screenshot displays the homepage of **offsec.tools**, a platform for discovering security tools. The interface is dark-themed with a sidebar on the left containing a list of tool categories and their counts. The main content area features a search bar, sorting options, and a grid of tool cards. Each card includes the tool's name, a brief description, and GitHub statistics (Contributors, Issues, Stars, Forks). The tools shown are:

- 4-ZERO-3** by Dheerajmadhukar/ (403/401 Bypass Methods + Bash Automation + Your Support:))
- altdns** by infosec-au/ (Generates permutations, alterations and mutations of subdomains and then resolves them)
- Amass** by OWASP/ (In-depth Attack Surface Mapping and Asset Discovery)
- aquatone** by michenriksen/ (A Tool for Domain Flyovers)
- Arjun** (HTTP parameter discovery suite)
- ASNmap** (Quickly maps organization network ranges using ASN information)
- assetfinder** by tomnomnom/ (Find domains and subdomains related to a given domain)
- BFAC** (Check for backup artifacts that may disclose the web-application's source code)

**Categories and Counts (from sidebar):**

- # all: 143
- # allinone: 8
- # cloud: 9
- # cms: 5
- # crawler: 4
- # cves: 6
- # directories: 9
- # dns: 12
- # endpoints: 25
- # fuzzing: 14
- # git: 2
- # ips: 10
- # network: 11
- # osint: 6
- # passwords: 8
- # probing: 3
- # proxy: 3
- # scanner: 23
- # secrets: 8
- # subdomains: 37
- # vulnerabilities: 14



# TIPS/TRICKS

- Github.....

Try Searching For Leakes On

- [gist.github.com](https://gist.github.com)
- [Gitlab.com](https://gitlab.com)

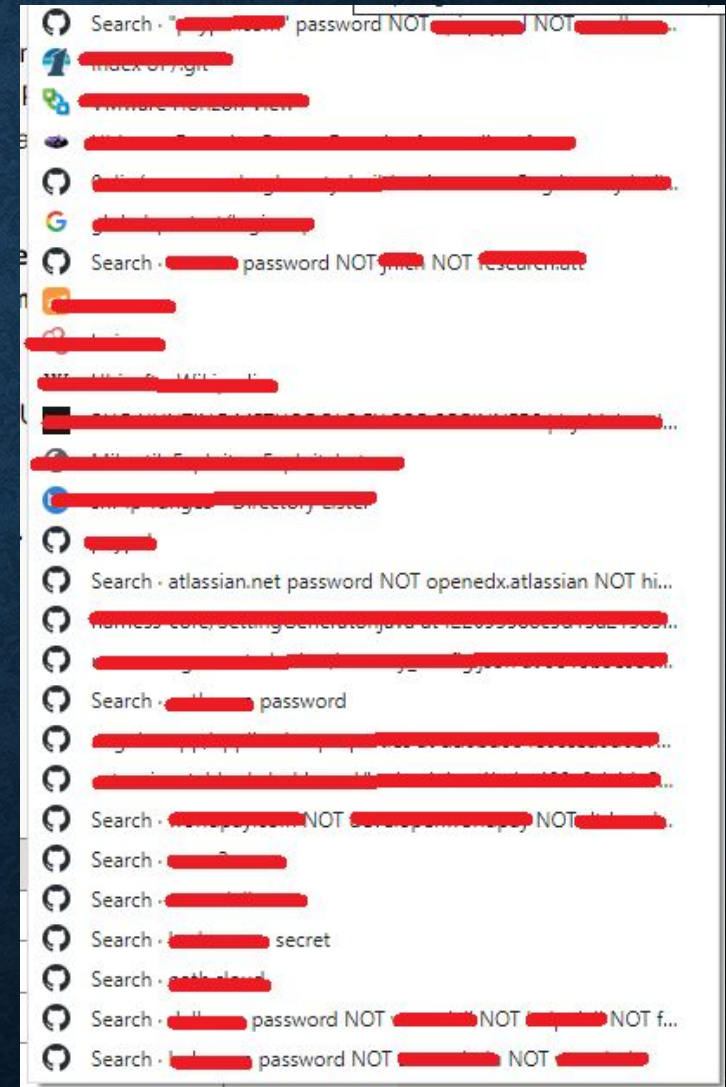
Tip for finds more leaks and before anyone

Check your target 2 times per day

To do that

Target.com password ☐ **Recently indexed** ☐ **Bookmark this tap**

[CTRL + D]





# TIPS/TRICKS

- Search For **PII** (Personal Identifiable Information) On Google
- Leaked Credentials On Google

In Google Sheets/Groups

*site:docs.google.com/spreadsheets "company name"*

*site:groups.google.com "company name"*



# TIPS/TRICKS

- Create a Nuclui Template

any bug you found create a template by that and test it on all programs scopes

- Find Some Ends For Dead Host And Tested On The Same Live IP

Example

[176.001.X.XX] = live

its in ssl recorded to [orwa.iwcon.com] = dead host

Collect endpoints for [orwa.iwcon.com] and test that endpoints on [176.001.X.XX]



# TIPS/TRICKS

## UNAUTHORIZED ACCESS

This example for critical bug I found it in FACEBOOK via Response Manipulation

I Found In FaceBook (Instagram Employee Panel) So I Tried Normal Login It Was `302` redirect to login page But Content-Length of redirect response so big

Some Playing With Burp **Match And Replace** I Was Able To Bypass Authentication And Taking Actions.

Tip Here:

If Response 302 With Very Big Content-Length

Try To Bypassed

- Normal Response Was
- HTTP/1.1 302 Found
- Location: ../login/?redirect=//location/?5

Replaced To

- HTTP/1.1 200 OK
- And Deleted Header Location: ../login/?redirect=//location/?5
- **Match And Replace**  
type: response header  
match : HTTP/1.1 302 Found  
replace: HTTP/1.1 200 ok
- **Match And Replace**  
type: response header  
match : Location: ../login/?redirect=//location/?5  
replace:



# THANKS ALL

## IWCON

- <https://twitter.com/GodfatherOrwa>
- <https://bugcrowd.com/OrwaGodfather>
- <https://hackerone.com/mr-hakhak>
- <https://medium.com/@orwaatyat>