

BSidesOdisha

Godfather Of Recon

Godfather Of Recon

- Build your setup for hunting
Tools , Extensions , Etc...
- Quick Orwa Methodology 2023
- SQL Injection
- #BugBountyTips

—\$ whoami

Orwa Atiyat (OrwaGodfather) from
Jordan

Full time bug hunter
(Starting bug bounty 2020)

Bugcrowd P1 Warrior Rank: Top 3
550+ critical/high bug submitted
HOF: Meta / Google / Microsoft /

Hack Cup Winner 2022/2023
LevelUpX Champion 2022/2023

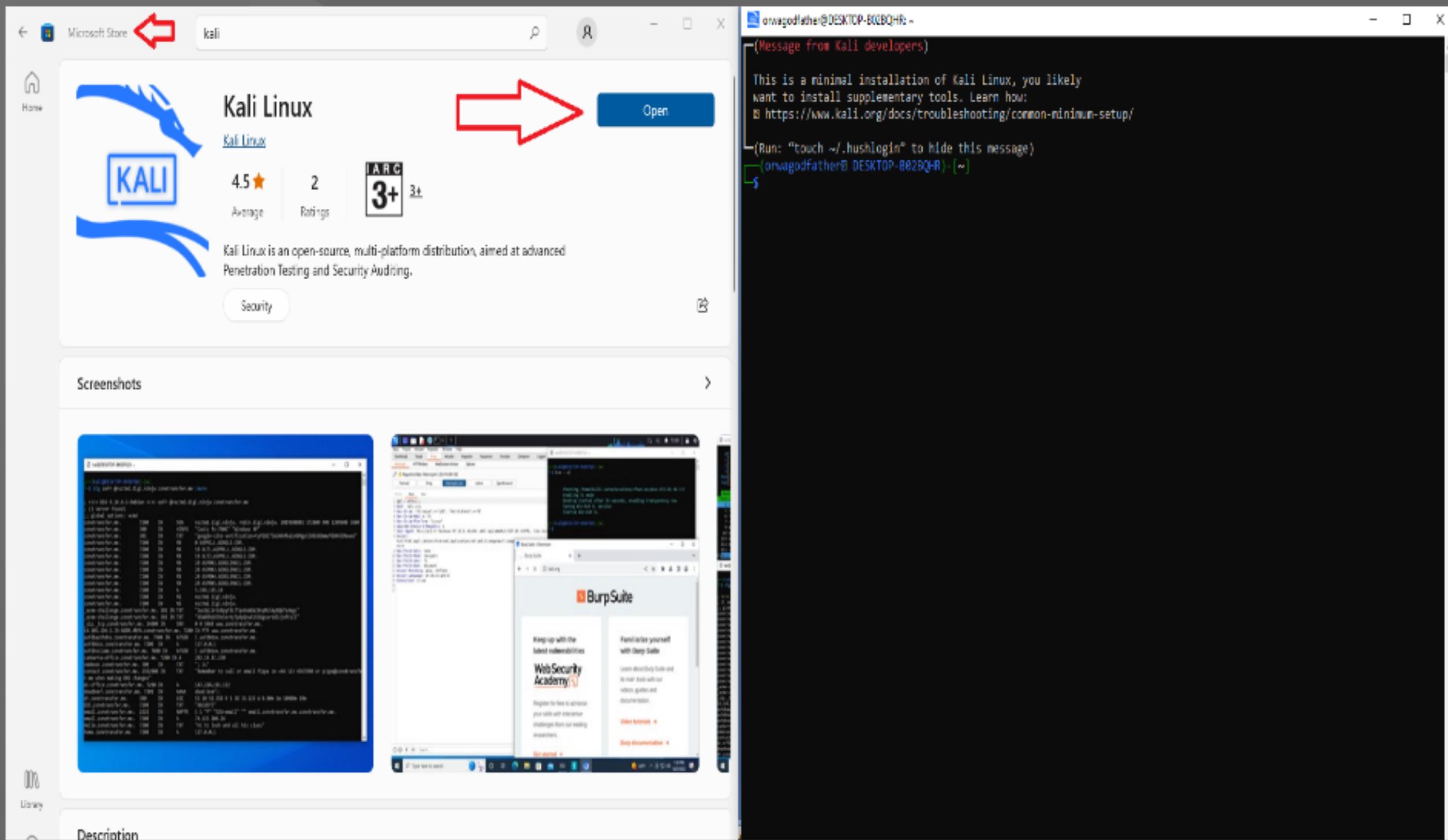
10+ 0Days/CVEs



**Why all the time Orwa talked about
Recon , Recon , Recon**



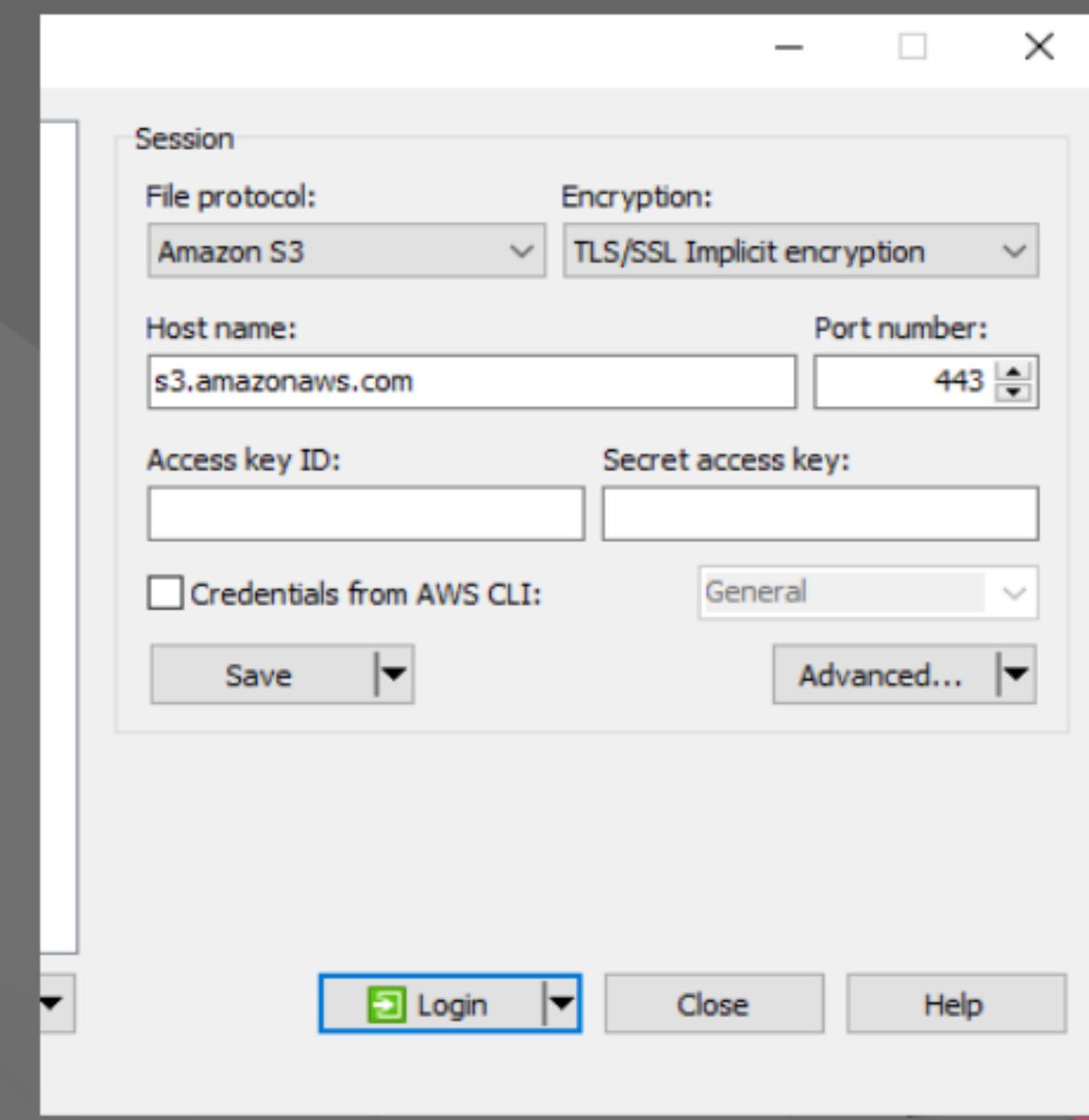
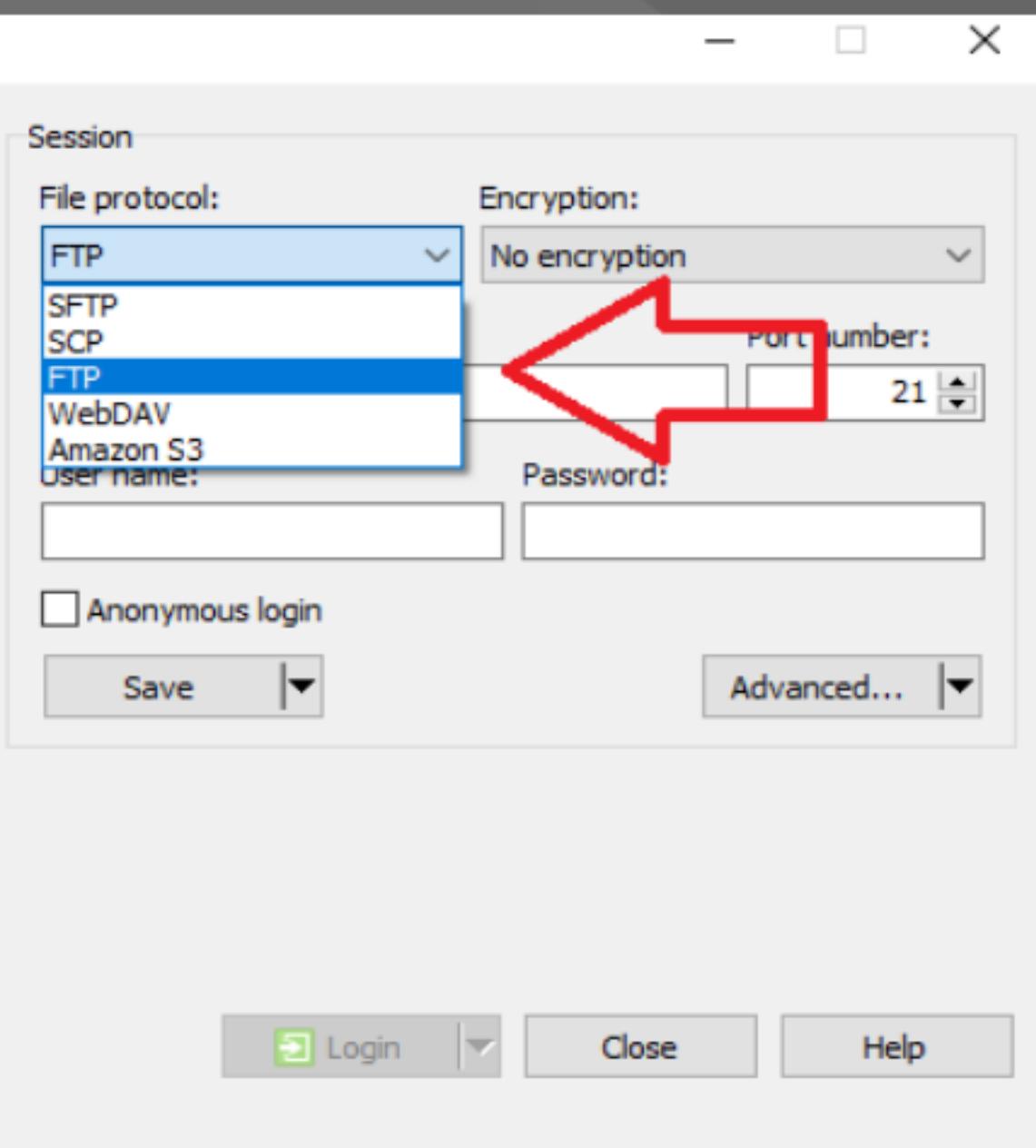
Build your setup for hunting System (Windows OS + Linux)



Build your setup for hunting

Windows Software's/Tools

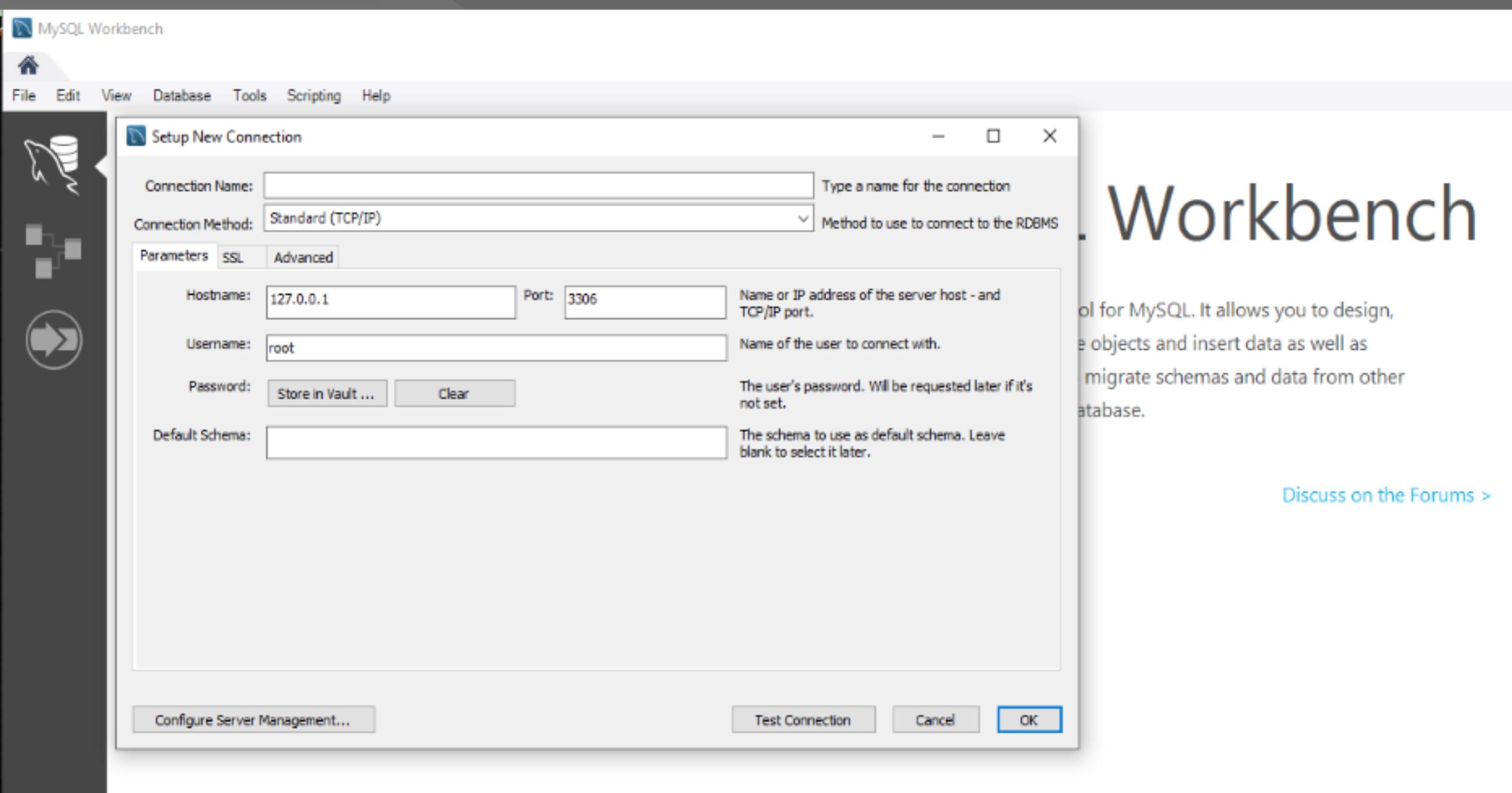
1 WinSCP



Build your setup for hunting

Windows Software's/Tools

2 MySQL Workbench



The screenshot shows the MySQL Workbench interface. On the left is a vertical toolbar with icons for Home, File, Edit, View, Database, Tools, Scripting, Help, and Server Management. The main window title is "MySQL Workbench". A central dialog box titled "Setup New Connection" is open. It has fields for "Connection Name" (empty), "Connection Method" set to "Standard (TCP/IP)", and tabs for "Parameters", "SSL", and "Advanced". Under "Parameters", the "Hostname" is "127.0.0.1", "Port" is "3306", "Username" is "root", and "Default Schema" is empty. Descriptions for these fields are provided. At the bottom of the dialog are buttons for "Configure Server Management...", "Test Connection", "Cancel", and "OK". The "OK" button is highlighted with a blue border.

Workbench

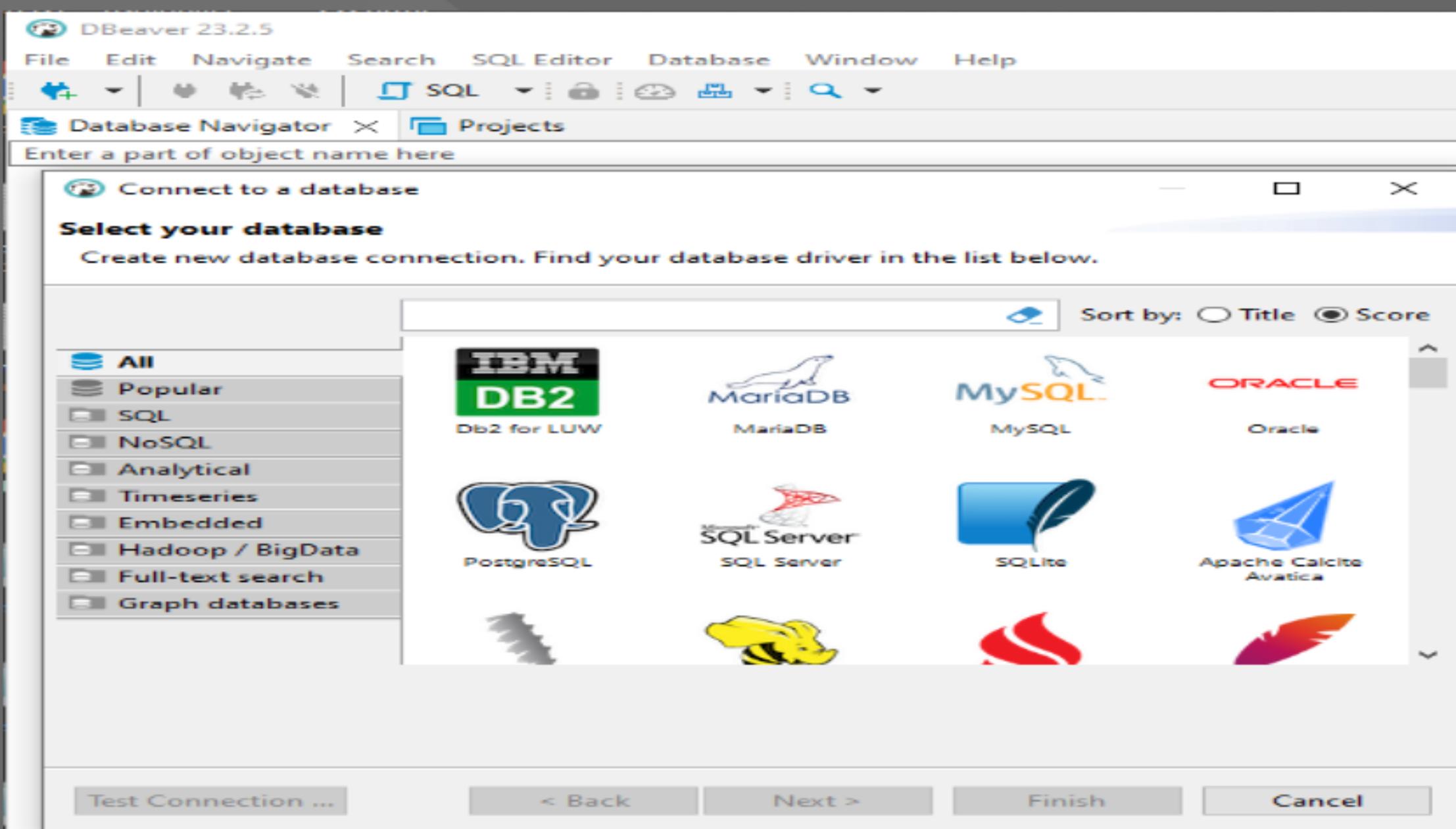
ol for MySQL. It allows you to design, e objects and insert data as well as migrate schemas and data from other database.

Discuss on the Forums >

Build your setup for hunting

Windows Software's/Tools

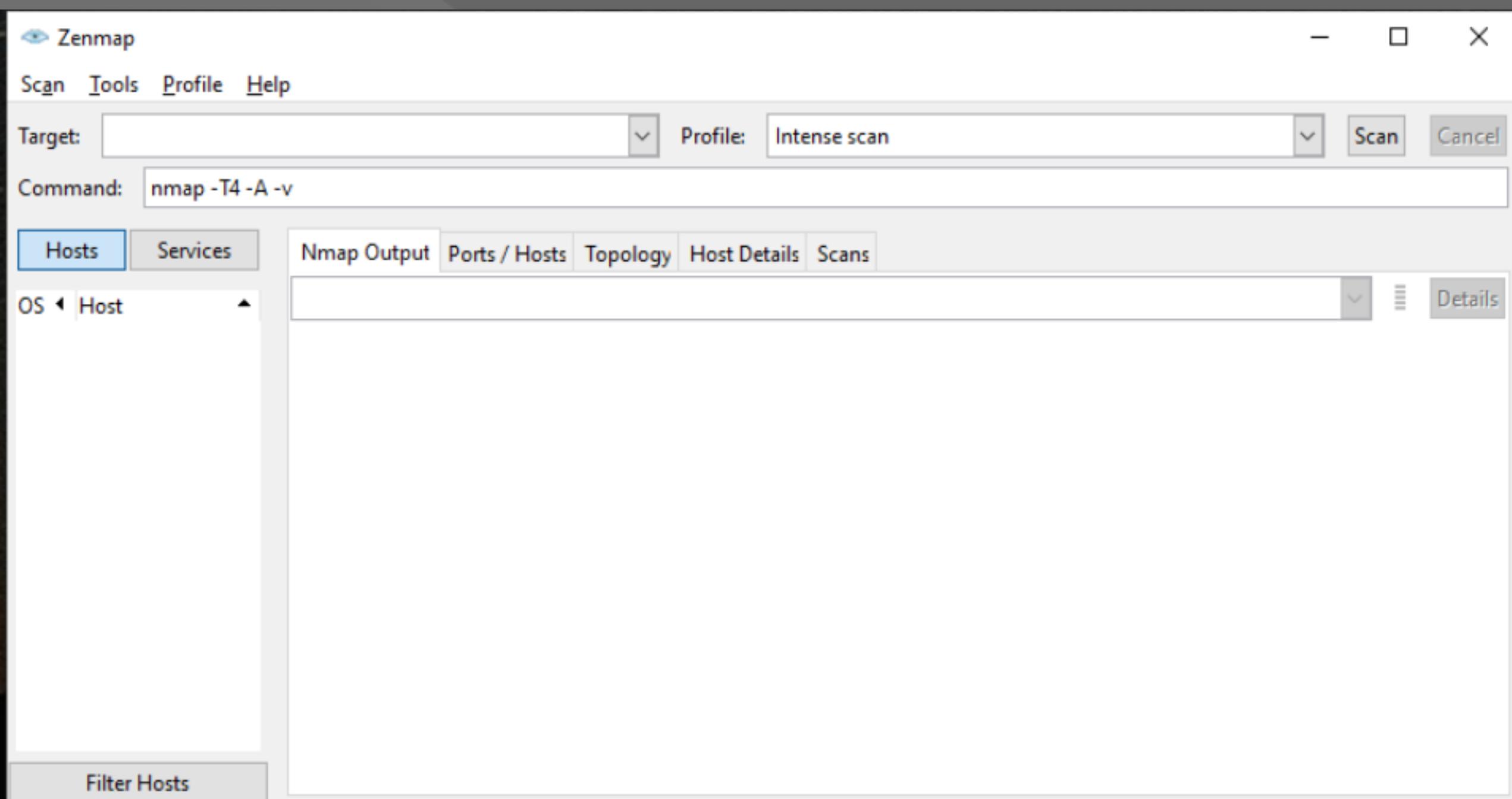
3 DBeaver



Build your setup for hunting

Windows Software's/Tools

4 Nmap – Zenmap GUI



Build your setup for hunting

Windows Software's/Tools

5 Notepad++

6 Visual Studio Code

7 JetBrains dotPeek

8 virustotal

9 Burp Suite (with following extensions)

*(403 Bypasser , 5GC API Parser , Active Scan++ ,
Backslash Powered Scanner , CO2 , IP Rotate ,
J2EEScan , JS Link Finder , JS Miner , Logger++ , Log
Viewer , GAP , Distribute Damage , IIS Tilde , Look Over
There , Param Miner , Software Vulnerability Scanner ,
SAML Raider , Authorize , Encode IP , Asset Discovery)*

Build your setup for hunting

MobSF & Free Docker

```
~ docker pull opensecurity/mobile-security-framework-mobsf  
~ docker run -it -rm -p 8000:8000 opensecurity/mobile-security-framework-mobsf:latest
```

<https://labs.play-with-docker.com/>

The screenshot shows a web-based interface for managing Docker instances. On the left, there's a sidebar with a clock showing 03:59:43, a 'CLOSE SESSION' button, and tabs for 'Instances' and '+ ADD NEW INSTANCE'. Below these are buttons for 'DELETE' and 'EDITOR'. The main area displays a session for the IP 192.168.0.13. The session details include the IP address, an 'OPEN PORT' button, and tabs for 'Memory' and 'CPU'. Under the 'Memory' tab, there's an SSH connection information: 'ssh ip172-18-0-98-clj3tpcsnmng009b78i0@direct.labs.play-' followed by a copy icon. At the bottom of the session area, there's a terminal window showing a root shell on the host node1.

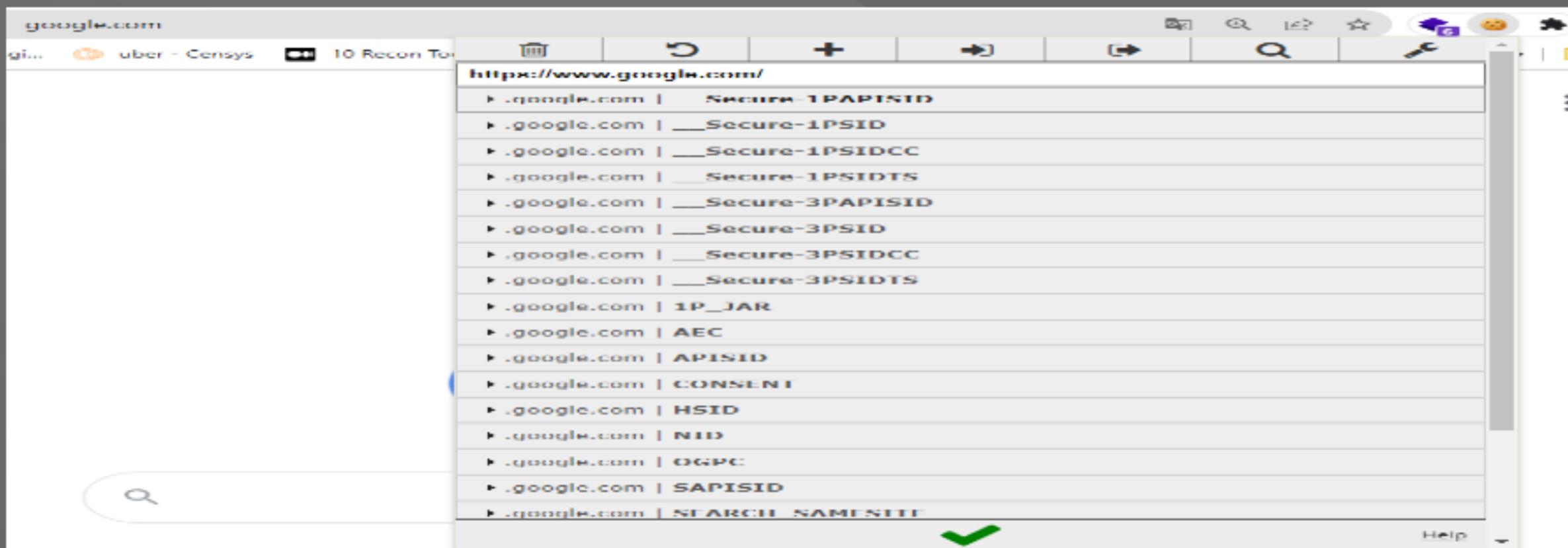
```
03:59:43  
CLOSE SESSION  
Instances + ADD NEW INSTANCE  
192.168.0.13 node1  
DELETE EDITOR  
clj3tpcs_clj3tsksnmng009b78ig  
IP 192.168.0.13 OPEN PORT  
Memory CPU  
SSH ssh ip172-18-0-98-clj3tpcsnmng009b78i0@direct.labs.play-   
#####  
# WARNING!!!!  
# This is a sandbox environment. Using personal credentials  
# is HIGHLY! discouraged. Any consequences of doing so are  
# completely the user's responsibilities.  
#  
# The PWD team.  
#####  
[node1] (local) root@192.168.0.13 ~  
$
```

Build your setup for hunting

Browser Extensions

1 Wappalyzer (checking webapp technologies)

2 EditThisCookie



Build your setup for hunting

Example from shodan

 SSL Certificate	HTTP/1.1 200 OK
Issued By:	Set-Cookie: [REDACTED]; JSESSIONID=[REDACTED]; tptaap16;
- Common Name:	X-XSS-Protection: 1; mode=block
 Organization	X-Frame-Options: SAMEORIGIN
Validation:	Content-Security-Policy: default-src 'self'; script-src 'self' 'unsafe-inline' 'u
- Organization:	[REDACTED]
 Organization	[REDACTED]
Issued To:	
- Common Name:	

Build your setup for hunting

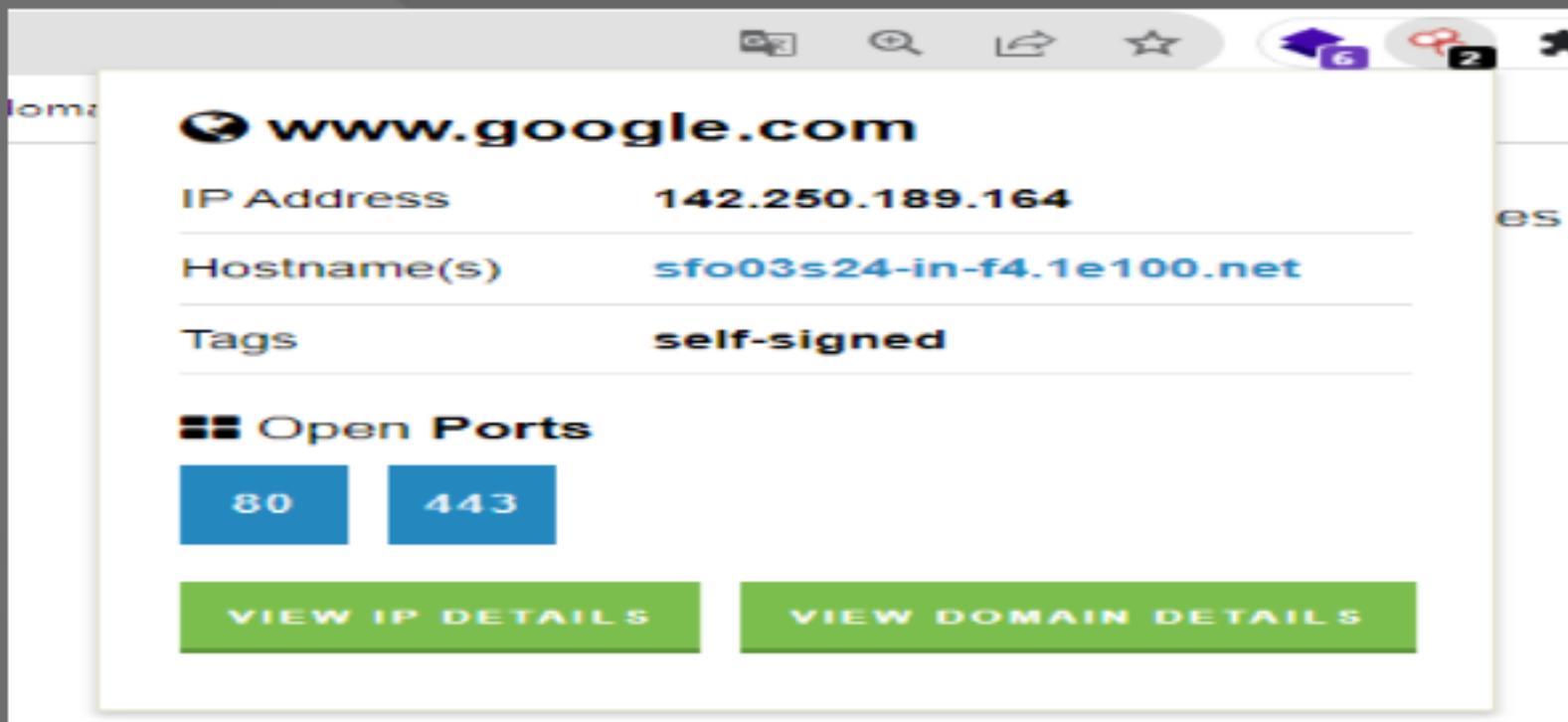
3 DotGit (orwa.com/.git/config)

The image shows a dual-screen setup. On the left, a window titled "DotGit" displays a list of 10 vulnerabilities found in ".git/config" files. The list includes URLs like "https://[REDACTED].git/config" and "https://[REDACTED].git/config" with download and delete icons. On the right, a GitHub search results page for "[REDACTED] Due To Accessible .git Repository" is shown, listing several issues with titles such as "Accessible [.git Repository]", "due to accessible .git Repository", and "due to accessible .git Repository". Each issue includes a price (e.g., \$1,500, \$2,500, \$750, \$3,000, \$150), points (e.g., 20 points, 10 points), and comment counts (e.g., 6 comments, 7 comments, 10 comments).

Vulnerability Description	Price	Points	Comments
[REDACTED] Due To Accessible .git Repository	\$1,500	20 points	6
to accessible .git Repository	\$2,500	20 points	7
Accessible [.git Repository]	\$750	10 points	6
.git Repository	\$3,000	10 points	10
due to accessible .git Repository	\$150	10 points	2

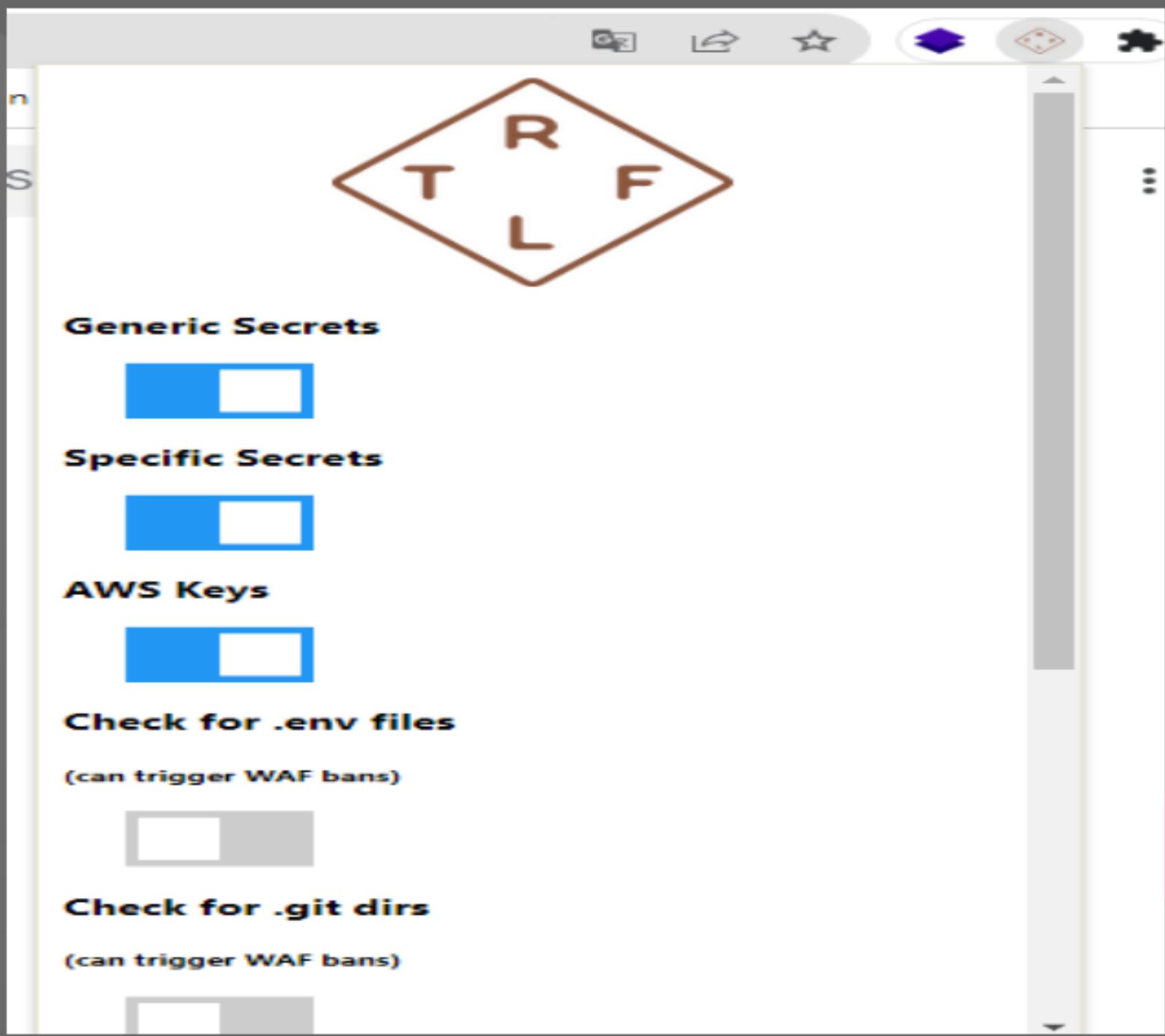
Build your setup for hunting

4 Shodan



Build your setup for hunting

5 Trufflehog



Build your setup for hunting

Kali Tools

ReconFTW (Cover lot of tools and fix missing in kali)

Amass & Httpx & Naabu

FFUF & Waymore & Arjun

SqlMap & Shodan Cli & GitTools

Metasploit & TplMap & Aem-Hacker

Setup Is Ready To Hunt

*Don't ask how I will go to the recon , Ask how
the recon will came to me....*



Orwa Methodology 2023

Program (A)

Scope

dev.orwa.com

sso.orwa.com/admin/login

Program (B)

Scope

*.orwa.com

Program (C)

Scope

Anything Owned By Orwa Inc. In Scope

Orwa Methodology 2023

Program (A)

Scope

dev.orwa.com

sso.orwa.com/admin/login

(1) scan full port 1 time per day

(2) collect all endpoints for *.orwa.com and create a wordlist by all of this endpoints and tested on program scope

Orwa Methodology 2023

(3) Check program scope endpoint on ...

Ex

- <https://urlscan.io/search/#dev.orwa.com>
- https://web.archive.org/cdx/search/cdx?url=*.dev.orwa.com&fl=original&collapse=urlkey
- https://otx.alienvault.com/api/v1/indicators/domain/orwa.com/url_list?limit=100&page=1 **private tip**
- Bing & Google Dorking: [site:dev.orwa.com]
- Github checking: dev.orwa.com

Orwa Methodology 2023

(4) Search for dev-uat-prod-test apps

Ex

sso-dev.orwa.com

ssouat.orwa.com

prod-sso.orwa.com

(5) Search for leaked creds for orwa.com and tested on sso.orwa.com (moving from out of scope to in scope)

(6) FuZZ webapp (fuzz in bugbountytips part)

Orwa Methodology 2023

Remember , burp all the time on and proxy is connected

When you done from everything back and check your burp and start looking for interesting stuff

Orwa Methodology 2023

Program (B)

Scope

*.orwa.com

(1) Collect sub domain

- reconFTW

- Amass

~amass enum -passive -norecursive -noalts -d orwa.com -o sub-list.txt

- CrtSH <https://crt.sh/?q=%25.orwa.com>

- Securitytrails https://securitytrails.com/list/apex_domain/orwa.com

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

Orwa Methodology 2023

There's a lot of other resources such as (github , fofa urlscan , etc...) , use everything add everything to one list , remove duplicate by

```
~cat everything.txt | sort -u > sub-list.txt
```

(2)

Send *sub-list.txt* to httpx & naabu

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

Top 1000 port

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

Full Port

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

Orwa Methodology 2023

(3) shodan checking for IPs & Origin IPs

Ssl.cert.subject.CN:"orwa.com"

Origin IP and Waf bypass via
(match and replace in burp)
Explained in BsidesAhmedabad Slides

(4) Start with Program(A) Method

Orwa Methodology 2023

Program (C)

Scope

Anything Owned By Orwa Inc. In Scope

(1) Collect domains

On crt.sh Orwa Inc.

On Shodan "ssl:Orwa Inc."

Threes lot of other recourses to get domains

Send all domains from all recourses to 1.txt file

Remove duplicate

```
~cat 1.txt | sort -u > domains.txt
```

Orwa Methodology 2023

Extract sub domains via amass by use -df (domains file)

```
~amass enum -passive -norecursive -noalts -df domin.txt -o subs-1.txt
```

Get more sub domains from subs-1.txt

```
~amass enum -passive -norecursive -noalts -df subs-1.txt -o all-sub.txt
```

Send all-subs.txt to httpx & naabu

(2) Search for Creds/PII/Endpoints from
Google Sheets&Groups

site:docs.google.com/spreadsheets "Orwa Inc."

*site:groups.google.com "Orwa Inc" **Amazing Tip***

Orwa Methodology 2023

(3) Check my Method about discovering more domains & 3rd party's & Endpoints

In BsidesAhmedabad Slides

(4) Start with Program(B) Method

(5) Start with Program(A) Method

Orwa Methodology 2023

Don't forget, burp all the time on and proxy is connected

BE CAREFUL



SQL Injection

Error Based & Blind

POST /wp-adminX/admin-ajax.phpX HTTP/1.1

Accept: */*

Referer: https://orwa.com/

Cookie: wp-wpml_current_language=enX;
cmplz_consent同意_services=X; cmplz_policy_id=14X;
cmplz_functional=allowX

Accept-Encoding: gzip,deflate,br

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/117.0.0.0 Safari/537.36X

Host: orwa.com

Connection: Keep-alive

Content-Type: application/x-www-form-urlencoded

Content-Length: 70

action=loadMorePostsX¬_show=xxxxX&posts_page=6X&search_argument=xxxxxxX

SQL Injection

Target Positions Payloads Options

Payload Positions

Configure the positions where payloads will be inserted into the base request. The attack type determines the way in which payloads are assigned to payload positions - see help for full details.

Start attack

Attack type: Sniper

```
POST /wp-admin$$_admin-ajax.php$$_ HTTP/1.1
Accept: */*
Referer: https://orwa.com/
Cookie: wp-wpml_current_language=$en$; cmplz_consent同意_services=$$; cmplz_policy_id=$14$;
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/117.0.0.0 Safari/537.36$$
Host: orwa.com
Connection: Keep-alive
Content-Type: application/x-www-form-urlencoded
Content-length: 70

action=$loadMorePosts$&not_show=$xxxx$&posts_page=$6$&search_argument=$xxxxxx$
```

Add §

Clear §

Auto §

Refresh

? < + > Type a search term

0 matches

Clear

SQL Injection

```
POST /wp-admin/admin-ajax.php HTTP/1.1
Accept: /*
Referer: https://orwa.com/
Cookie: wp-wpml_current_language=en; cplz_consentedservices=; cplz_policy_id=14
Accept-Encoding: gzip, deflate, br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/117.0.0.0 Safari/537.36
Host: orwa.com
Connection: Keep-alive
Content-Type: application/x-www-form-urlencoded
Content-Length: 70

action=loadMorePosts&not_show=xxxx&posts_page=6&search_argument=xxxxxx$|
```

SQL Injection

Change body encoding

Go Cancel < | > | ▾

Request

Raw Params Headers Hex

```
POST /wp-admin/admin-ajax.php HTTP/1.1
Accept: */*
Referer: https://orwa.com/
Cookie: wp-wpml_current_language=en; cmplz_consentedservices=; cmplz_policy_id=1
cmplz_preferences=deny; cmplz_banner-status=dismissed
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
Host: orwa.com
Connection: Keep-alive
Content-Type: application/x-www-form-urlencoded
Content-Length: 70

action=loadMorePosts&not_show=xxxx&posts_page=6&search_argument=xxxxxx
```

Send to Spider
Do an active scan
Send to Intruder Ctrl+I
Send to Repeater Ctrl+R
Send to Sequencer
Send to Comparer
Send to Decoder
Request in browser ►

ng=deny; cmplz_statist 36

Send request to Autorize
Send Cookie header to Autorize
Send Authorization header to Autorize
Send to Backup Finder
Send to SQLMapper
Send to Laudanum
Send to Upload Scanner
Guess params ►
Param Miner ►
Run JS Auto-Mine (check everything)
Run all passive scans
Config ►
Scans ►
Log ►
Engagement tools ►
Change request method
Change body encoding ►
Copy URL
Copy as curl command
Copy to file

SQL Injection

Change body encoding

Request

Raw Params Headers Hex

```
POST /wp-admin/admin-ajax.php HTTP/1.1
Accept: */*
Referer: https://orwa.com/
Cookie: wp-wpml_current_language=en; cmplz_consentedservices=; cmplz_policy_id=14; cmplz_functional=allow; cmplz_marketing=deny; cmplz_statistics=deny;
cmplz_preferences=deny; cmplz_banner-status=dismissed
Accept-Encoding: gzip, deflate, br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/117.0.0.0 Safari/537.36
Host: orwa.com
Connection: Keep-alive
Content-Type: multipart/form-data; boundary=-----50442952
Content-Length: 345

-----50442952
Content-Disposition: form-data; name="action"

loadMorePosts
-----50442952
Content-Disposition: form-data; name="not_show"

xxxx
-----50442952
Content-Disposition: form-data; name="posts_page"

6
-----50442952
Content-Disposition: form-data; name="search_argument"

xxxxxx
-----50442952--
```

SQL Injection

Change body encoding

Attack type: Sniper

```
cmplz_banner-status=dismissed
Accept-Encoding: gzip, deflate, br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/117.0.0.0 Safari/537.36
Host: orwa.com
Connection: Keep-alive
Content-Type: multipart/form-data; boundary=-----50442952
Content-Length: 345

-----50442952
Content-Disposition: form-data; name="action"

loadMorePosts$$
-----50442952
Content-Disposition: form-data; name="not_show"

xxxx$$
-----50442952
Content-Disposition: form-data; name="posts_page"

6$$
-----50442952
Content-Disposition: form-data; name="search_argument"

xxxxxx$$
-----50442952--
```

SQL Injection

Quick check for SQL Error

Id=1' Id=1" Id=1"" Id=1''' symbol

Wordlist for intruder checking

<https://github.com/orwagodfather/SQL-Wordlist>

In SQL wordlist replace
xxx.burpcollaborator.net with your burp/server

SQL Injection

Add * in the request to when you try inject that location via sqlmap

Ex

POST /wp-admin*/admin-ajax.php HTTP/1.1

Referer: https://orwa.com/

Cookie: wp-wpml_current_language=en; cmplz_consentedservices=; cmplz_policy_id=14

Accept-Encoding: gzip,deflate,br

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)

Chrome/117.0.0.0 Safari/537.36

Host: orwa.com

Connection: Keep-alive

Content-Type: application/x-www-form-urlencoded

Content-Length: 70

action=loadMorePosts¬_show=xxxx&posts_page=6&search_argument=xxxxx

Don't forget clear */* from Accept

Bug Bounty Tips & Resources

1) all the time on all requests check
PUT & DELETE Methods

With **PUT** Method You can create files on server such as (stored XSS Files , Shell to RCE)

With **DELETE** Method you can delete any file on directory and that led sometimes to take down the full app

Bug Bounty Tips & Resources

- 2) All the time try to add for your request
X-Forwarded-For Header & Referer Header
And try inject that with (**SQL injection** payload or
Blind XSS payload)
- 3) Use this extension to create a wordlist from burp site map

<https://github.com/lvcvanderpoel/Burp-Wordlist-Generator>

Bug Bounty Tips & Resources

Ffuf

Normal and best command

ffuf -w /wordlist -u app/FUZZ

Matcher: Response status: 200-299,301,302,307,401,403,405,500



[Status: 403, Size: 312, Words: 17, Lines: 7, Duration: 86ms]

Don't use -mc xxx or -fc xxx

Remove the duplicates by other -f filters

EX...

Size use -fs 312 / Words use -fw 17 / Lines use -fl 7

Bug Bounty Tips & Resources

Amazing Books I read when i start bug bounty
And still read it till today

[https://drive.google.com/file/d/
1ZPK5ln4lULal0nwSdQTWA3ccUttayAj1/view?usp=sharing](https://drive.google.com/file/d/1ZPK5ln4lULal0nwSdQTWA3ccUttayAj1/view?usp=sharing)

[https://drive.google.com/file/d/
1UVJJpfYZ4X8vKEKM3QpCdFe2bcskYbta/view?usp=sharing](https://drive.google.com/file/d/1UVJJpfYZ4X8vKEKM3QpCdFe2bcskYbta/view?usp=sharing)

[https://drive.google.com/file/d/
1Oh8AxcHir8AC4UefIvgc5LI5IDjRfnXV/view?usp=sharing](https://drive.google.com/file/d/1Oh8AxcHir8AC4UefIvgc5LI5IDjRfnXV/view?usp=sharing)

[https://drive.google.com/file/d/
1xwoG5N8UmWUdcMBfqeZ2HZsA3dz1la5w/view?
usp=sharing](https://drive.google.com/file/d/1xwoG5N8UmWUdcMBfqeZ2HZsA3dz1la5w/view?
usp=sharing)

Orwa Resources

BsidesAhmedabad Talk slides

https://docs.google.com/presentation/d/1AA0gX2-SI_9ErTkBhtW0b-5BH70-1B1X/edit#slide=id.p1

The Power Of Shodan

https://youtu.be/WgMGLjpznao?si=MNHIABqzEvb_gt4o

IWCON Talk about Recon skills

https://youtu.be/z1r0MrCOGA0?si=_mKVIWviplZBzzR9

How to write excellent reports, techniques

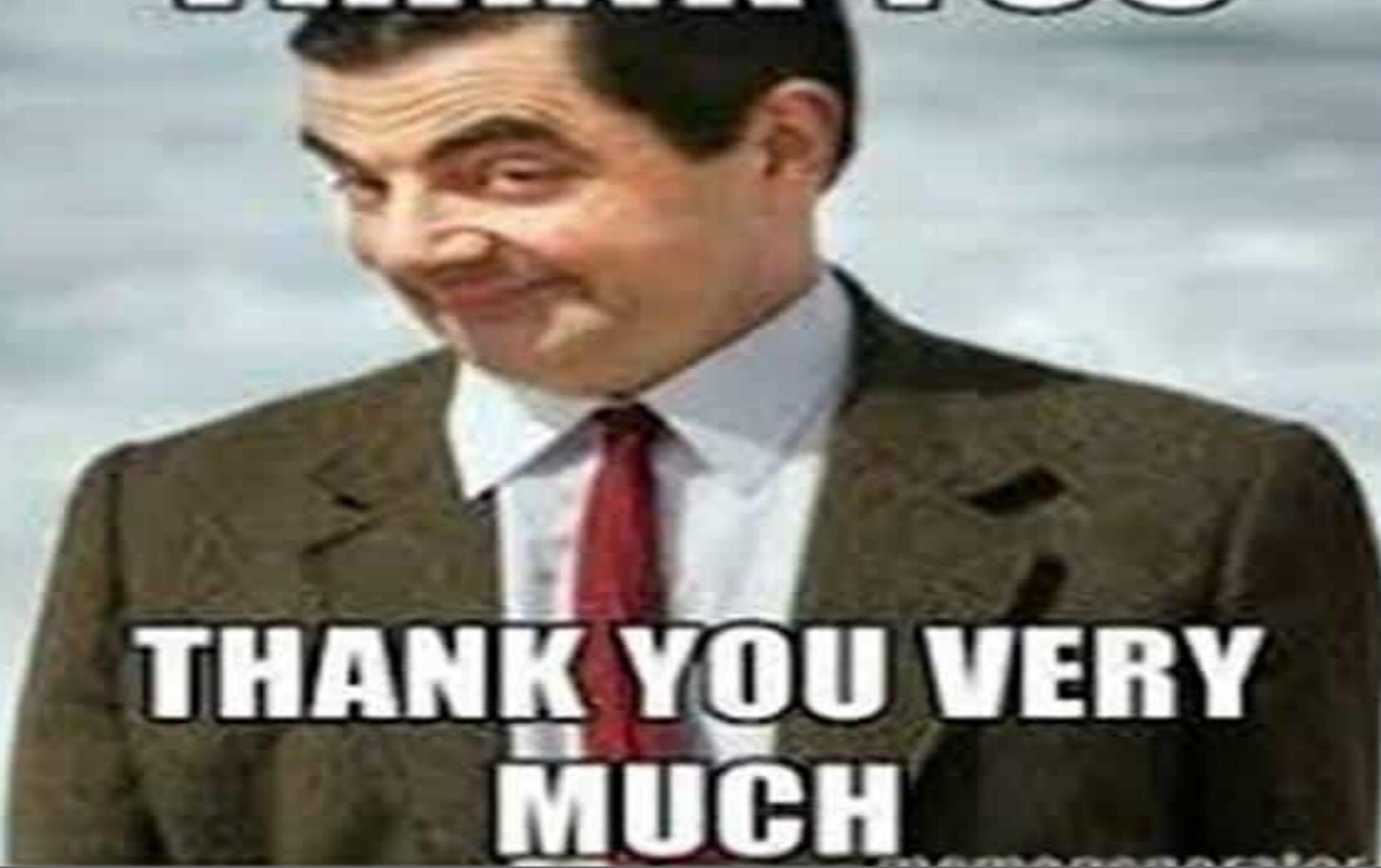
<https://www.bugcrowd.com/resources/levelup/how-to-write-excellent-reports-techniques-that-save-triagers-time-and-mistakes-that-should-be-avoided-in-reports/>

Medium Writes

<https://orwaatyat.medium.com>

End Of Topic

THANK YOU



**THANK YOU VERY
MUCH**