



---

# HACKING ÉTICO

---

Unidad 2. Actividad 29



15 DE FEBRERO DE 2024  
CARLOS DÍAZ MONTES  
ESPECIALIZACIÓN DE CIBERSEGURIDAD

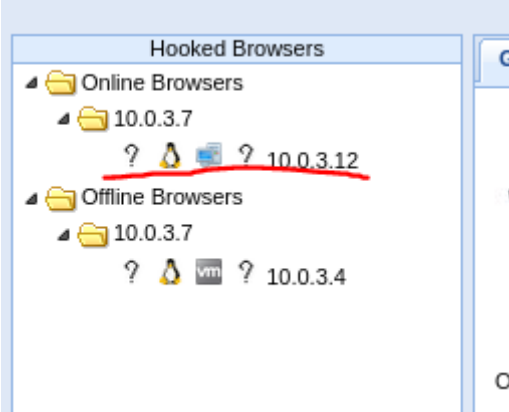
## Índice

XSS – Beef.....	2
-----------------	---

## XSS – Beef

### Ejercicio 1: Hazlo tu mismo

En mi caso he usado un opensuse. Vemos como podemos interceptarlo:



```
pps@localhost:~> 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: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 08:00:27:46:6c:08 brd ff:ff:ff:ff:ff:ff
    altname enp0s3
    inet 10.0.3.12/24 brd 10.0.3.255 scope global dynamic noprefixroute eth0
        valid_lft 496sec preferred_lft 496sec
    inet6 fe80::bee6:7029:dd7f:68c2/64 scope link noprefixroute
        valid_lft forever preferred_lft forever
3: br-139074c21a93: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc noqueue state DOWN group default
    link/ether 02:42:4b:a4:d4:10 brd ff:ff:ff:ff:ff:ff
    inet 192.168.49.1/24 brd 192.168.49.255 scope global br-139074c21a93
        valid_lft forever preferred_lft forever
4: br-5b5f9e71a038: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc noqueue state DOWN group default
    link/ether 02:42:c0:6a:c0:0b brd ff:ff:ff:ff:ff:ff
    inet 172.18.0.1/16 brd 172.18.255.255 scope global br-5b5f9e71a038
        valid_lft forever preferred_lft forever
5: br-a4b3fba82315: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc noqueue state DOWN group default
    link/ether 02:42:4b:2c:14:c5 brd ff:ff:ff:ff:ff:ff
    inet 172.20.0.1/16 brd 172.20.255.255 scope global br-a4b3fba82315
        valid_lft forever preferred_lft forever
6: docker0: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc noqueue state DOWN group default
    link/ether 02:42:63:fb:0b:0e brd ff:ff:ff:ff:ff:ff
    inet 172.17.0.1/16 brd 172.17.255.255 scope global docker0
        valid_lft forever preferred_lft forever
pps@localhost:~> Soy Carlos Diaz
```

## Ejercicio 2: Capabilities

[illegible]

### Ejercicio 3: Capturar tu nombre

24	278.353s - [User Typed] Monte
23	277.343s - [User Typed] iaz
22	276.335s - [User Typed] s D
21	275.320s - [User Typed] rlo
20	274.309s - [User Typed] Ca

### Ejercicio 4: Alert box

Creamos la alerta:

Getting Started
Logs
Zombies
**Current Browser**

---

Details
Logs
**Commands**
Proxy
XSSReays
Network

### Module Tree

- create alert dialogue
  - Browser (2)
    - Create Alert Dialog
    - Create Prompt Dialog
  - Exploits (1)
    - NtfsCommonCreate DoS
  - Misc (1)
    - Create Invisible IFrame
  - Persistence (3)
    - Create Foreground iFrame
    - Create Pop Under
    - Create Pop Under (IE)
  - Phonegap (1)
    - Alert User

### Module Results History

id	date	label
0	2024-03-05 06:08	command 1
1	2024-03-05 06:08	command 2
2	2024-03-05 06:09	command 3
3	2024-03-05 06:09	command 4
4	2024-03-05 06:10	command 5

### Create Alert Dialog

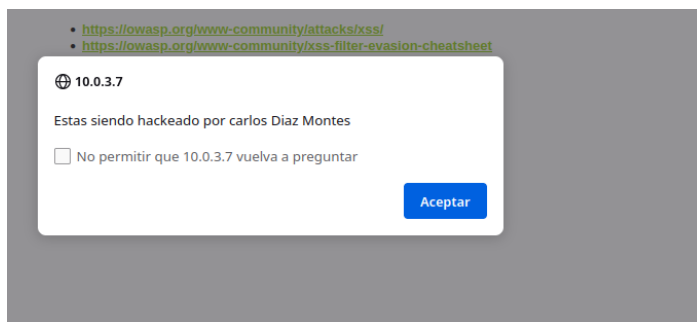
Description: Sends an alert dialog to the hooked browser.

Id: 290

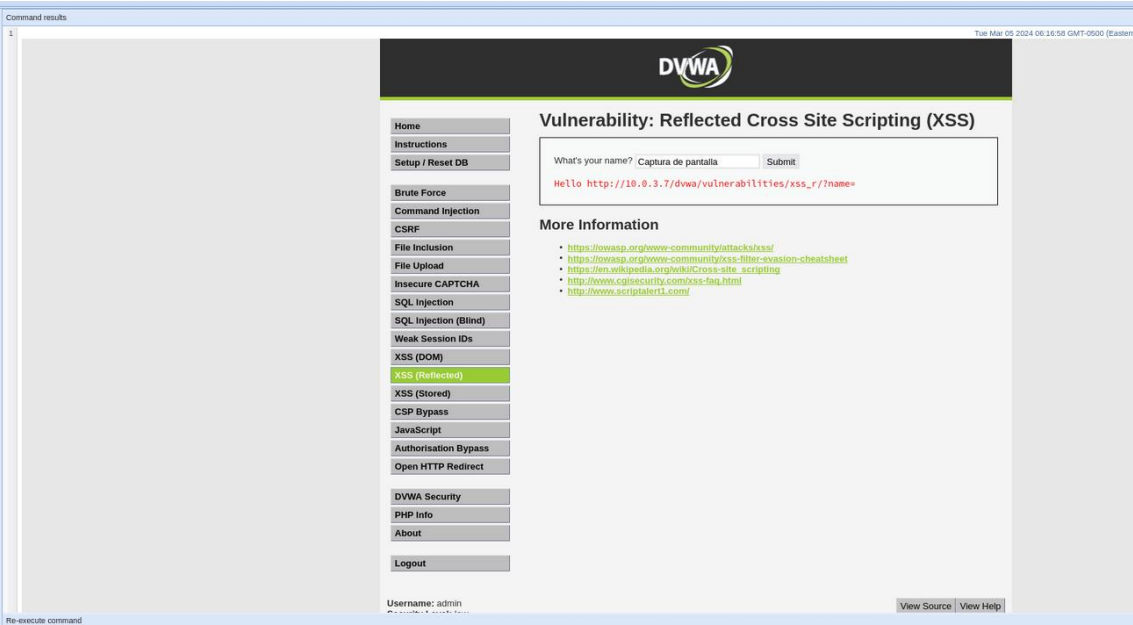
Alert text:

```
Estat sendo backdoor por Carlos Diaz Moron
```

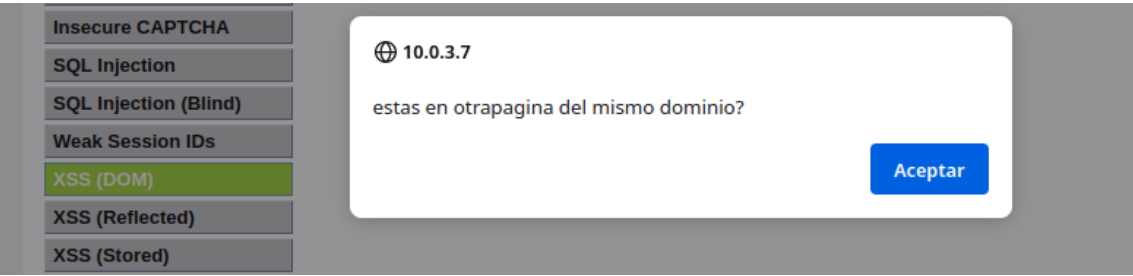
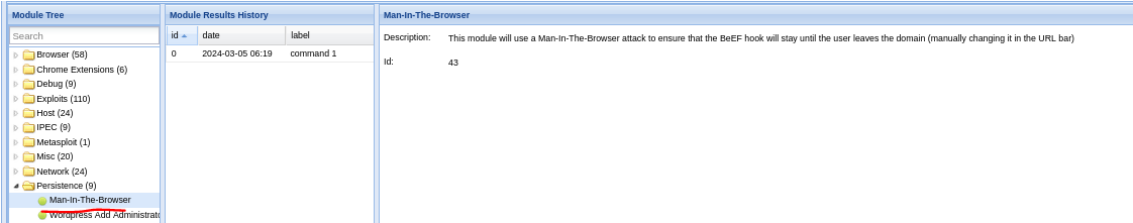
Vemos como se nos ve:



Ejercicio 5: Captura de pantalla



Ejercicio 6: Persistencia



Ejercicio 7: Investiga

He encontrado uno que coge el html de la página:

