RICCARDO AGOSTINO
MONTI

S 6 L 2

LA FASE DI EXPLOIT: GLI ATTACCHI ALLE WEB APP

```
┌──(kali㉿kali)-[~]
└─$ ping 192.168.50.101
PING 192.168.50.101 (192.168.50.101) 56(84) bytes of data.
64 bytes from 192.168.50.101: icmp_seq=1 ttl=64 time=1.25 ms
64 bytes from 192.168.50.101: icmp_seq=2 ttl=64 time=0.862 ms
64 bytes from 192.168.50.101: icmp_seq=3 ttl=64 time=0.799 ms
64 bytes from 192.168.50.101: icmp_seq=4 ttl=64 time=0.900 ms
^C
--- 192.168.50.101 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3007ms
rtt min/avg/max/mdev = 0.799/0.951/1.246/0.173 ms
```

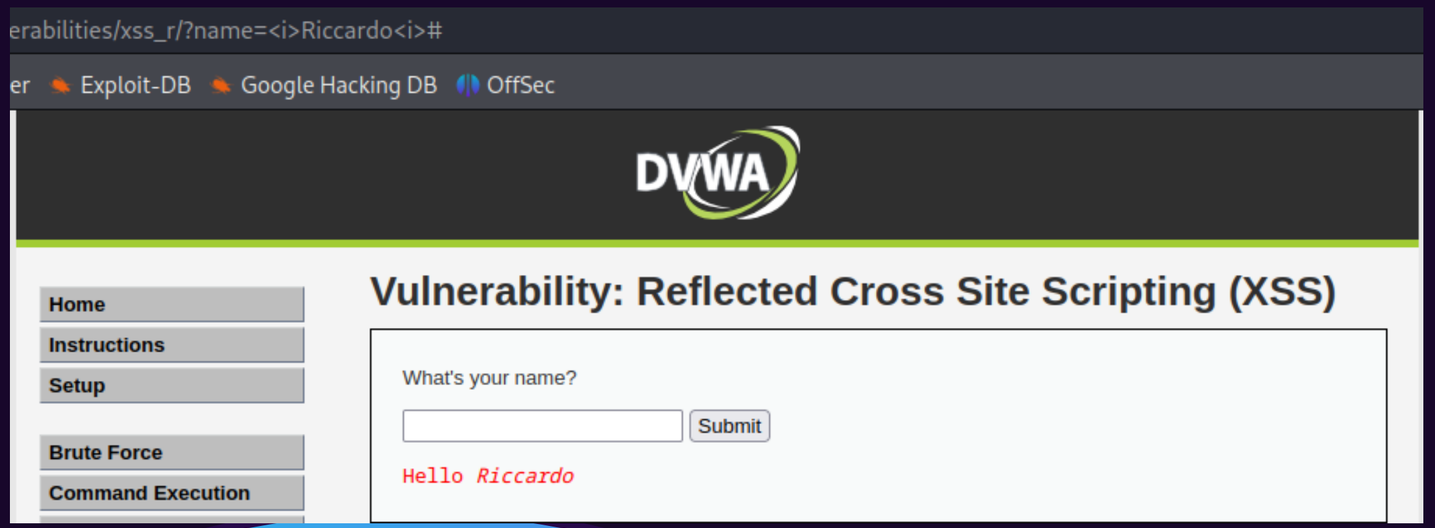
Setup Ambiente

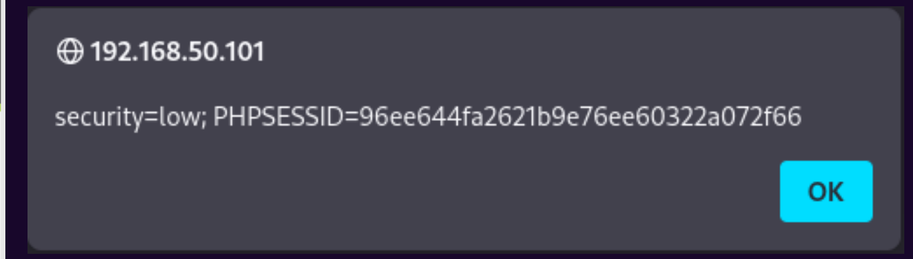
Verifichiamo che le macchine comunicano tra di loro.

RICCARDO AGOSTINO
MONTI

Inizia il test

Una volta controllato che le due macchine comunicano tra di loro, andiamo su DVWA di Meta, cliccando nella tendina XSS. Fatto ciò iniziamo a provare a scrivere qualcosa nella rifa di comando come nei seguenti screen:





Risultati

Come abbiamo visto siamo riusciti a utilizzare la casella “Name” per ottenere variazioni in url e ottenere le informazioni che desideravamo prelevare dal sito, in questo caso i cookie.

```
┌──(kali㉿kali)-[~]
└─$ ping 192.168.50.101
PING 192.168.50.101 (192.168.50.101) 56(84) bytes of data.
64 bytes from 192.168.50.101: icmp_seq=1 ttl=64 time=1.25 ms
64 bytes from 192.168.50.101: icmp_seq=2 ttl=64 time=0.862 ms
64 bytes from 192.168.50.101: icmp_seq=3 ttl=64 time=0.799 ms
64 bytes from 192.168.50.101: icmp_seq=4 ttl=64 time=0.900 ms
^C
--- 192.168.50.101 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3007ms
rtt min/avg/max/mdev = 0.799/0.951/1.246/0.173 ms
```

SQLi

Adesso proveremo ad utilizzare query per sfruttare le vulnerabilità di

Inizia il test

Abbiamo prima inserito nel campo ID
<< %' or 0=0 union select null, version() # >> per stampare tutti gli utenti e la versione del sistema operativo del server alla fine e successivamente
<< %' or 0=0 union select null, user() # >> per visualizzare l'utente del database che ha eseguito il codice PHP che alimenta il database.

RICCARDO AGOSTINO MONTI

Risultati

Questi sono i risultati: