

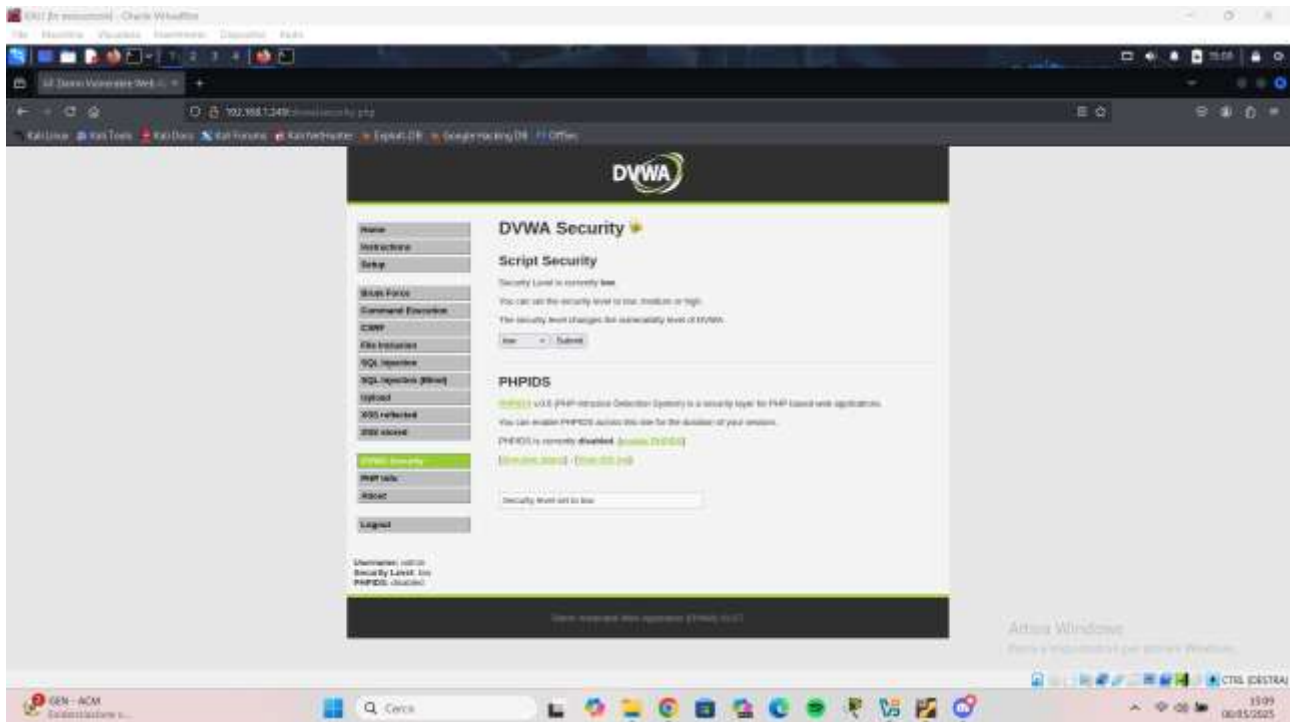
S6L2:ESERCIZIO

- Configurazione del Laboratorio: ○ Configurate il vostro ambiente virtuale in modo che la macchina DVWA sia raggiungibile dalla macchina Kali Linux (l'attaccante). ○ Verificate la comunicazione tra le due macchine utilizzando il comando ping.

```
(kali@kali)-[~]
$ ping 192.168.1.249
PING 192.168.1.249 (192.168.1.249) 56(84) bytes of data.
64 bytes from 192.168.1.249: icmp_seq=1 ttl=64 time=6.22 ms
64 bytes from 192.168.1.249: icmp_seq=2 ttl=64 time=3.55 ms
64 bytes from 192.168.1.249: icmp_seq=3 ttl=64 time=3.85 ms
64 bytes from 192.168.1.249: icmp_seq=4 ttl=64 time=0.979 ms
64 bytes from 192.168.1.249: icmp_seq=5 ttl=64 time=4.92 ms
^C
— 192.168.1.249 ping statistics —
5 packets transmitted, 5 received, 0% packet loss, time 4422ms
rtt min/avg/max/mdev = 0.979/3.903/6.221/1.736 ms
(kali@kali)-[~]
$
```

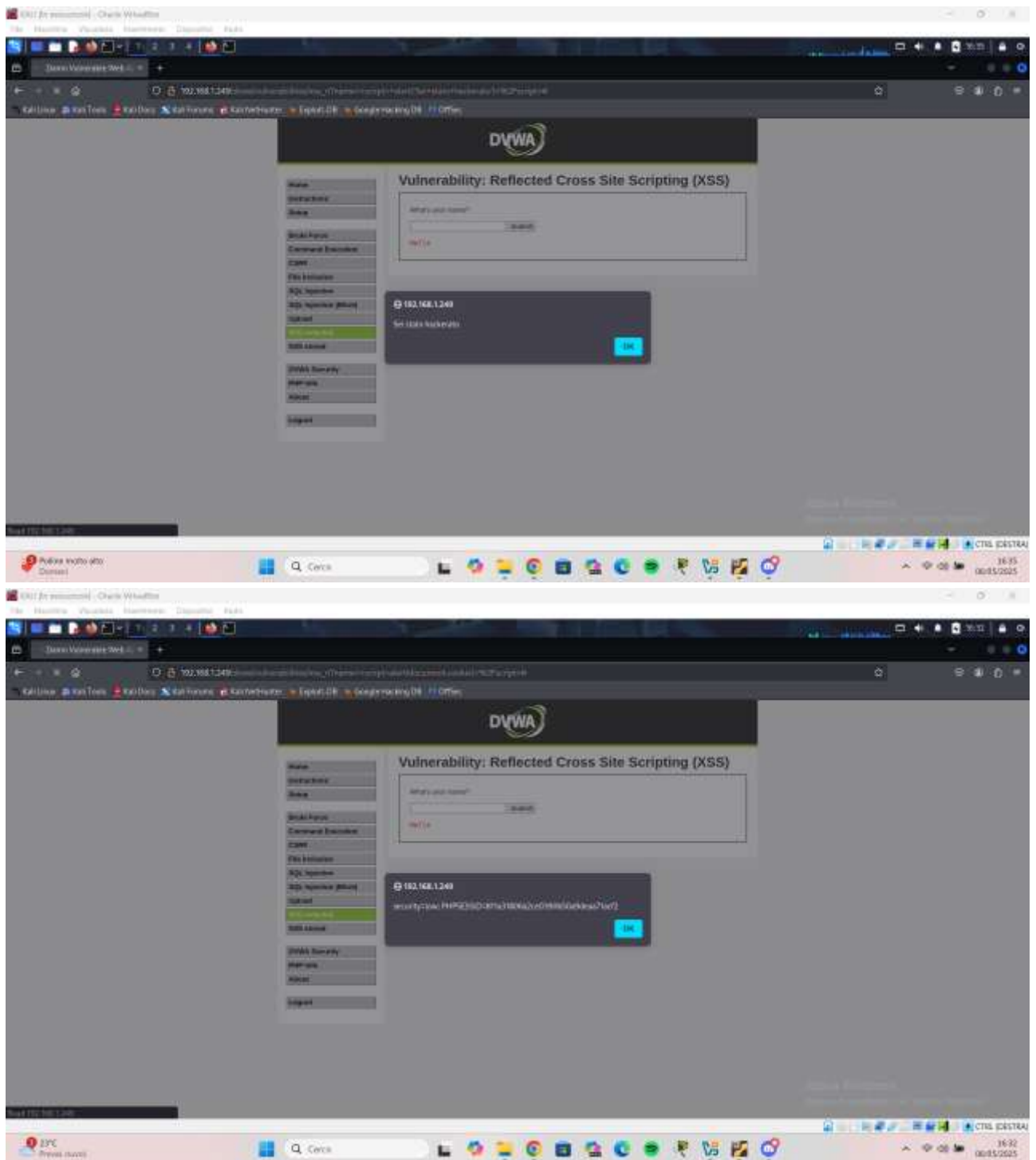
```
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:2f:5c:8d
          inet addr:192.168.1.249  Bcast:192.168.1.255  Mask:255.255.255.0
```

- Impostazione della DVWA ◀ ○ Accedete alla DVWA dalla macchina Kali Linux tramite il browser. ○ Navigate fino alla pagina di configurazione e settate il livello di sicurezza a LOW.

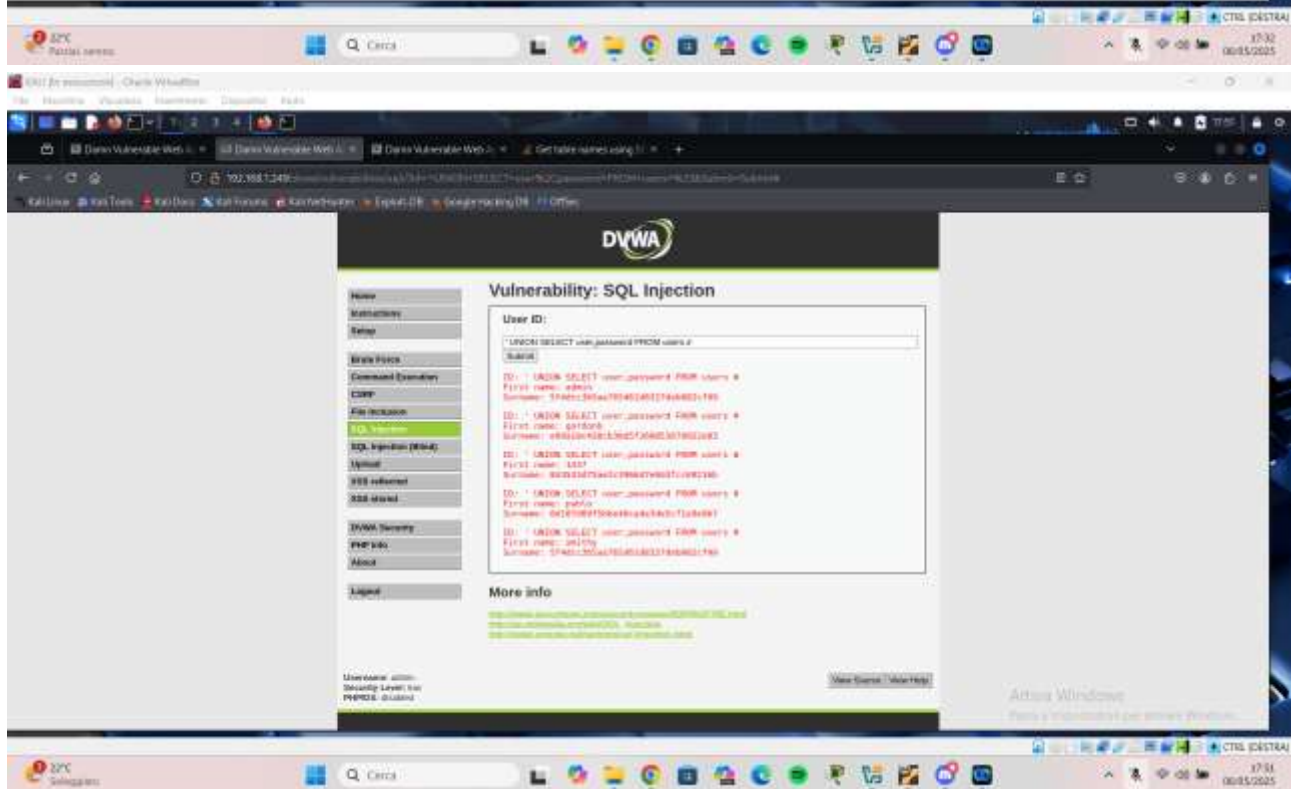
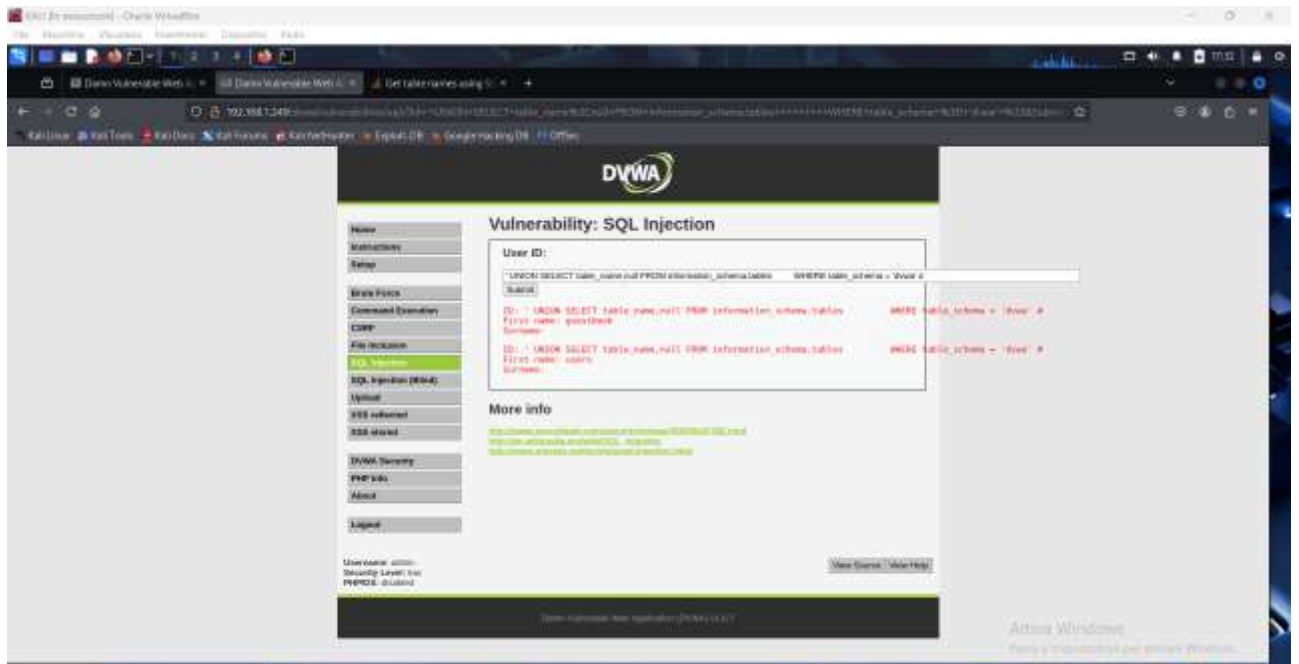


- Sfruttamento delle Vulnerabilità: ○ Scegliete una vulnerabilità XSS reflected e una vulnerabilità SQL Injection (non blind). Sfruttamento delle Vulnerabilità: ○ Scegliete una vulnerabilità XSS reflected e una vulnerabilità SQL Injection (non blind).

XSS REFLECTED:



SQL INJECTION:





- 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
- Logout

Vulnerability: SQL Injection

User ID:

ID: 2
First name: Gordon
Surname: Brown

More info

<http://www.securiteam.com/securityreviews/5DP0N1P76E.html>
http://en.wikipedia.org/wiki/SQL_injection
<http://www.unixwiz.net/techtips/sql-injection.html>

Jusername: admin
Security Level: low
PHPIDS: disabled

[View Source](#) [View Help](#)