

Report Esercizio 14/01/2025

Exploit DVWA - XSS e SQL Injection Leonardo Catalano

“La traccia di oggi ci chiede di sfruttare delle vulnerabilità XSS e SQL Injection sulla DVWA di Metasploit.

Le fasi da effettuare saranno le seguenti:

1. Configurazione delle macchine:

Le macchine dovranno essere configurate in rete interna e dovranno essere raggiungibili l'una con l'altra (devono poter comunicare) .

2. Impostazione della DVWA:

Accedere alla DVWA dalla macchina Kali Linux tramite il browser, e andare nella pagina di configurazione e settare il livello di sicurezza a LOW.

3. Sfruttamento delle Vulnerabilità:

Scegliere una vulnerabilità XSS reflected e una vulnerabilità SQL Injection (non blind).

Utilizzare le tecniche viste per sfruttare con successo entrambe le vulnerabilità.”

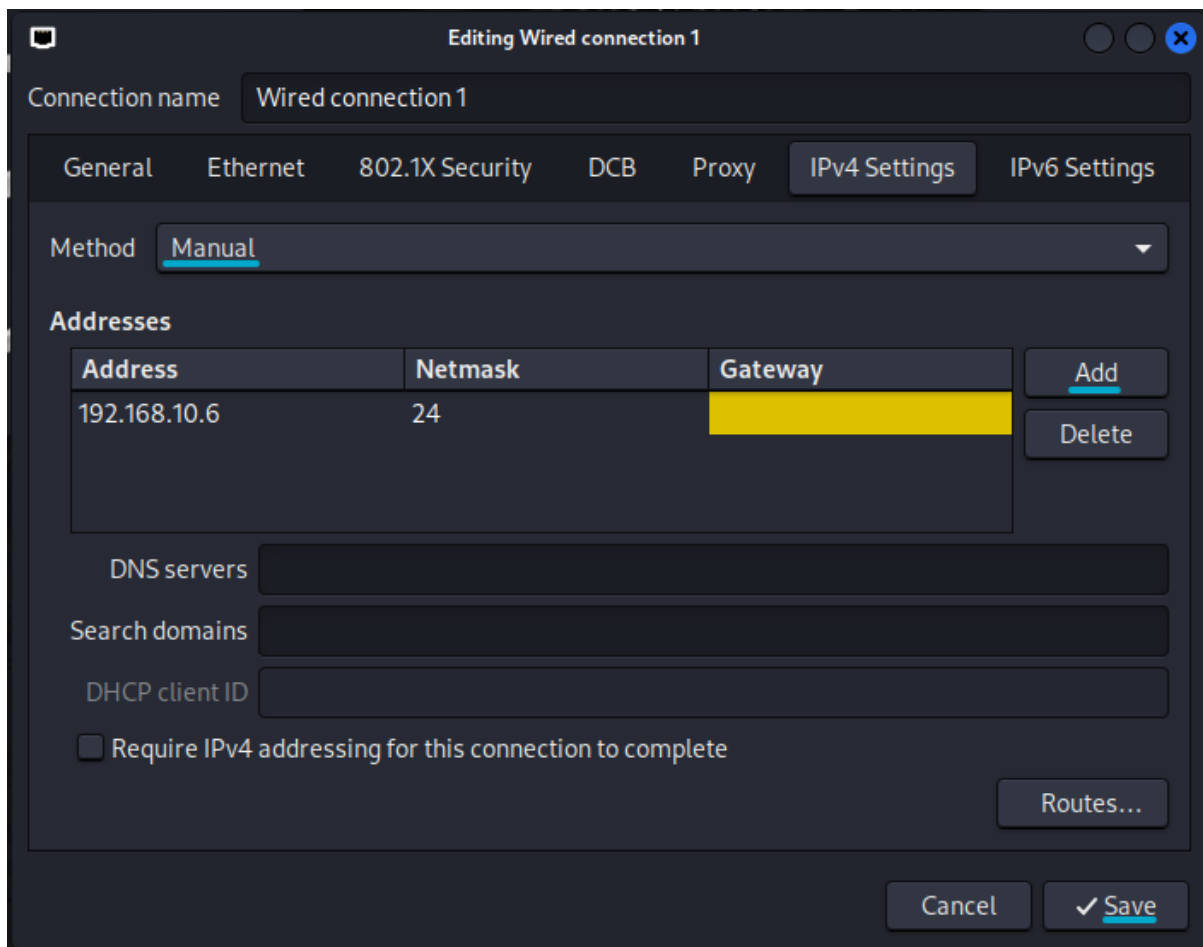
Preconfigurazione macchine virtuali:

Prima di tutto si configurano le VM per farle stare tutte nella stessa rete.

Come indirizzo di rete di riferimento uso il 192.168.10.0 /24.

-Macchina Kali Linux:

Per configurare l'indirizzo ipv4, si aprono le impostazioni della connessione, cliccando con il mouse destro sull'icona dell'ethernet, si va su IPv4 Settings, si cambia il metodo da DHCP a Manuale, si scrive l'indirizzo, si fa Add e si Salva.



Poi si disattiva la scheda di rete e la si riattiva e si va a verificare se l'indirizzo è stato assegnato correttamente aprendo la console e facendo il comando `ifconfig` o `ip a`.

```

kali@kali: ~
File Actions Edit View Help

(kali@kali)-[~]
└─$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
   link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
   inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
   inet6 ::1/128 scope host noprefixroute
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
   link/ether 08:00:27:ad:25:87 brd ff:ff:ff:ff:ff:ff
   inet 192.168.10.6/24 brd 192.168.10.255 scope global noprefixroute eth0
       valid_lft forever preferred_lft forever
   inet6 fe80::8638:cc35:20dd:4129/64 scope link noprefixroute
       valid_lft forever preferred_lft forever

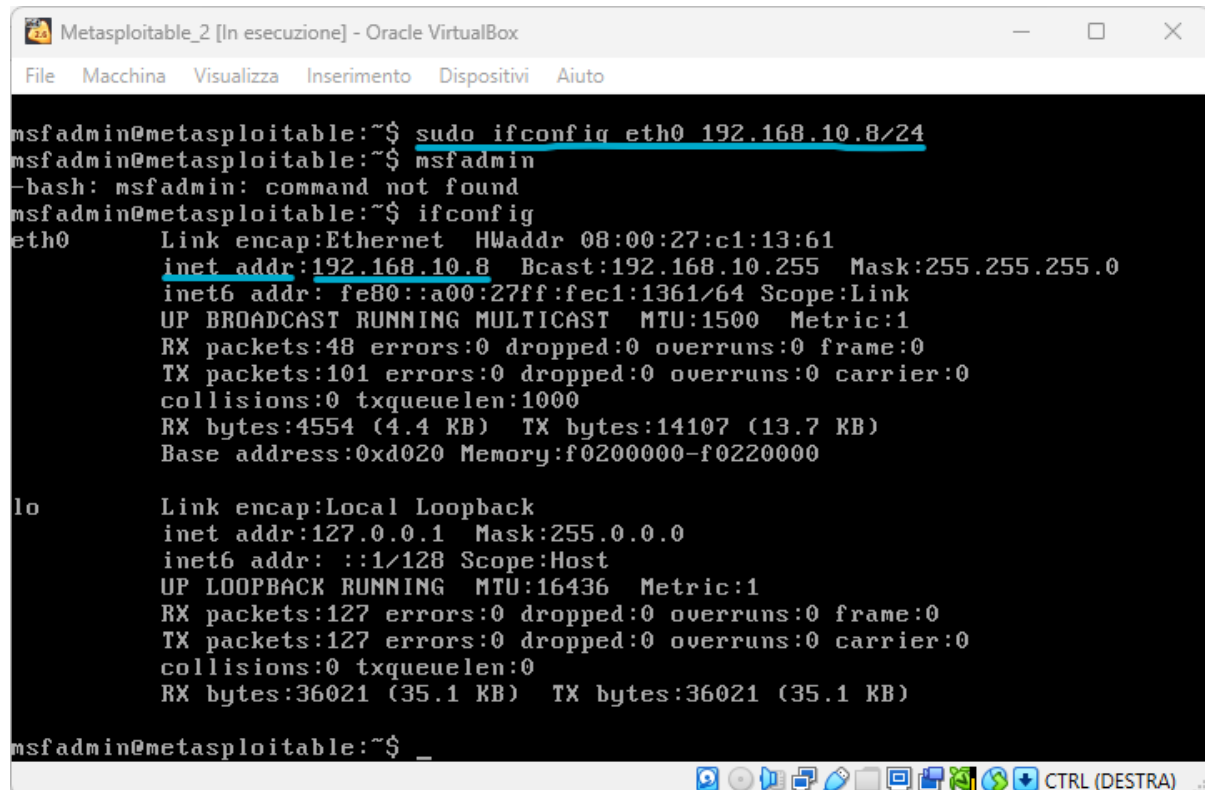
(kali@kali)-[~]
└─$ ifconfig

```

Come si può vedere l'indirizzo è stato configurato correttamente.

-Macchina Metasploitable:

Per configurare l'indirizzo ipv4 sulla macchina Metasploitable si utilizza il seguente comando: `sudo ifconfig eth0 192.168.10.8/24`



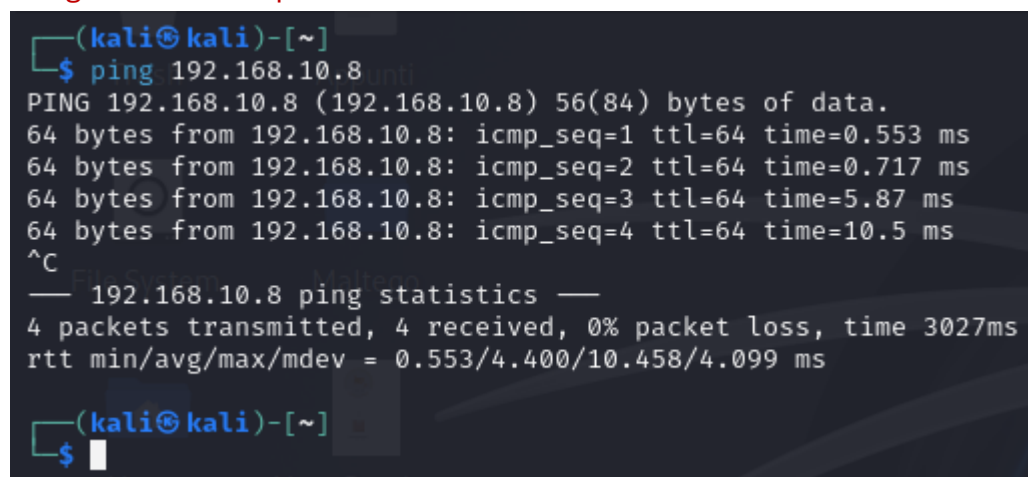
```
Metasploitable_2 [In esecuzione] - Oracle VirtualBox
File  Macchina  Visualizza  Inserimento  Dispositivi  Aiuto

msfadmin@metasploitable:~$ sudo ifconfig eth0 192.168.10.8/24
msfadmin@metasploitable:~$ msfadmin
-bash: msfadmin: command not found
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:c1:13:61
          inet addr:192.168.10.8  Bcast:192.168.10.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fec1:1361/64  Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:48 errors:0 dropped:0 overruns:0 frame:0
          TX packets:101 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:4554 (4.4 KB)  TX bytes:14107 (13.7 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:127 errors:0 dropped:0 overruns:0 frame:0
          TX packets:127 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:36021 (35.1 KB)  TX bytes:36021 (35.1 KB)

msfadmin@metasploitable:~$ _
```

-Ping Kali --> Metasploitable:

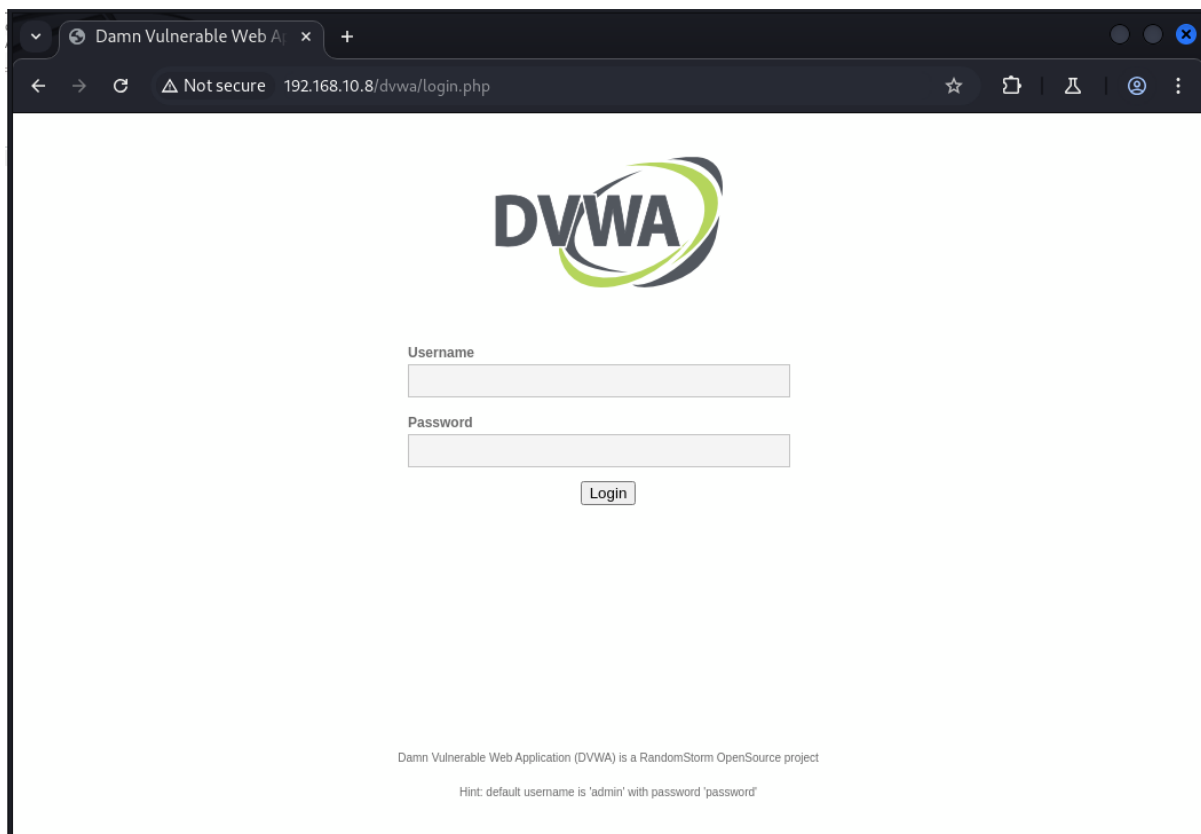


```
(kali@kali)-[~]
$ ping 192.168.10.8
PING 192.168.10.8 (192.168.10.8) 56(84) bytes of data.
64 bytes from 192.168.10.8: icmp_seq=1 ttl=64 time=0.553 ms
64 bytes from 192.168.10.8: icmp_seq=2 ttl=64 time=0.717 ms
64 bytes from 192.168.10.8: icmp_seq=3 ttl=64 time=5.87 ms
64 bytes from 192.168.10.8: icmp_seq=4 ttl=64 time=10.5 ms
^C
— 192.168.10.8 ping statistics —
4 packets transmitted, 4 received, 0% packet loss, time 3027ms
rtt min/avg/max/mdev = 0.553/4.400/10.458/4.099 ms

(kali@kali)-[~]
$
```

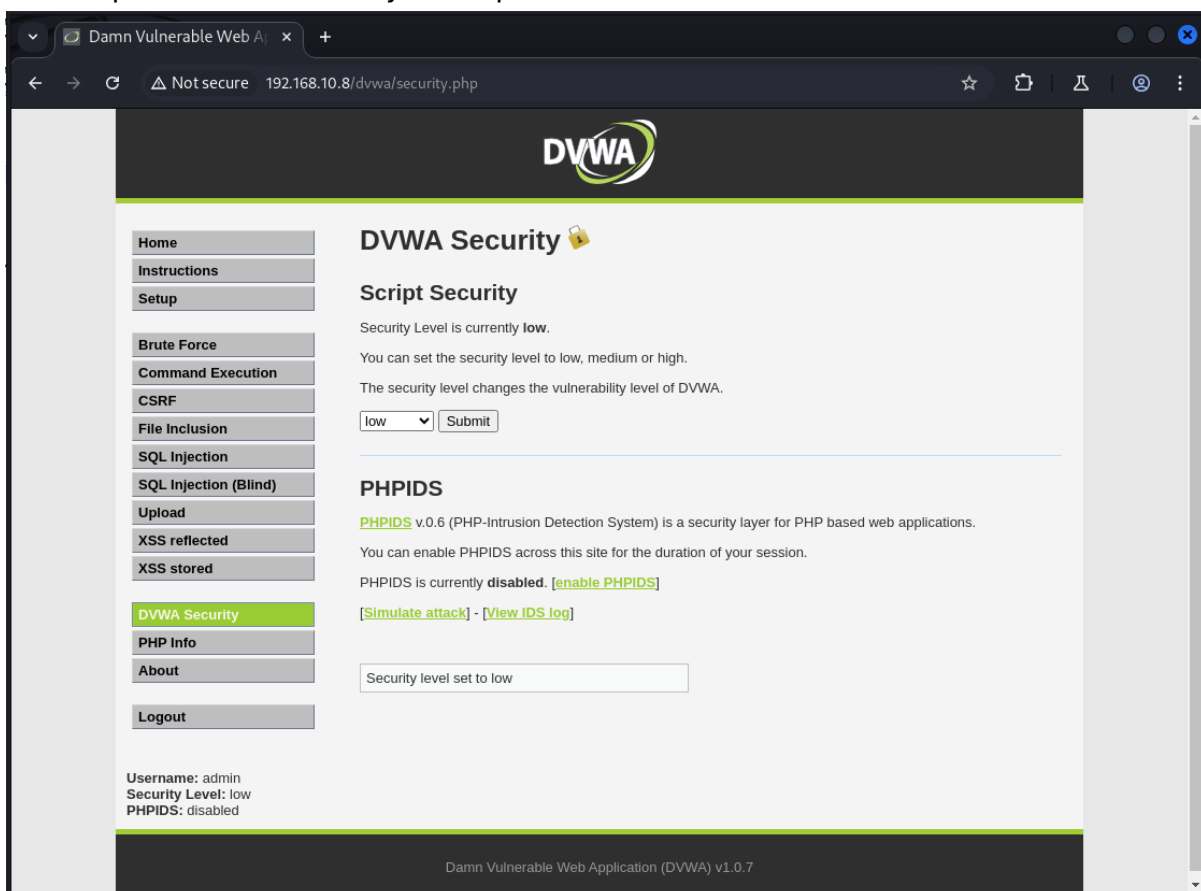
-Accesso Alla DVWA da Kali + BurpSuite:

Si accede alla DVWA tramite il browser da Kali, per intercettare e dopo modificare uso sin da subito il browser interno a BurpSuite:



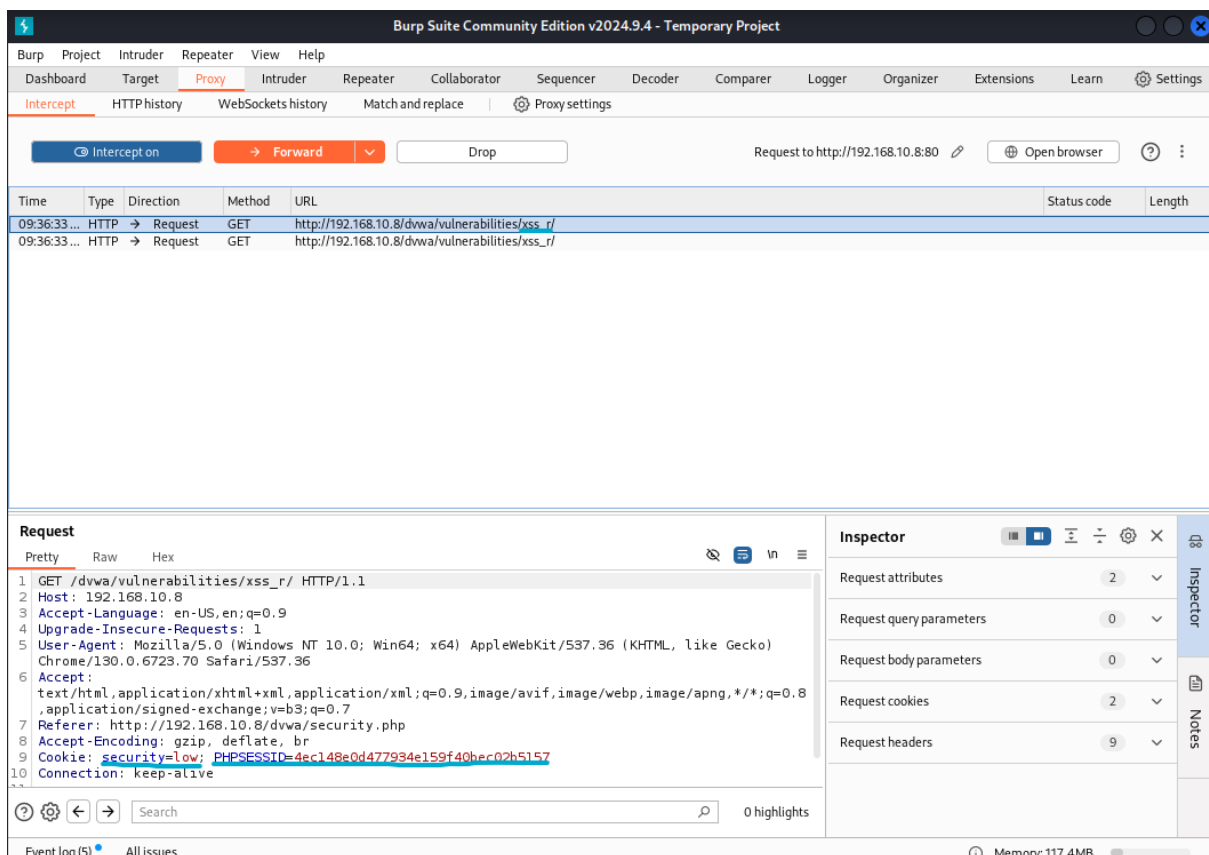
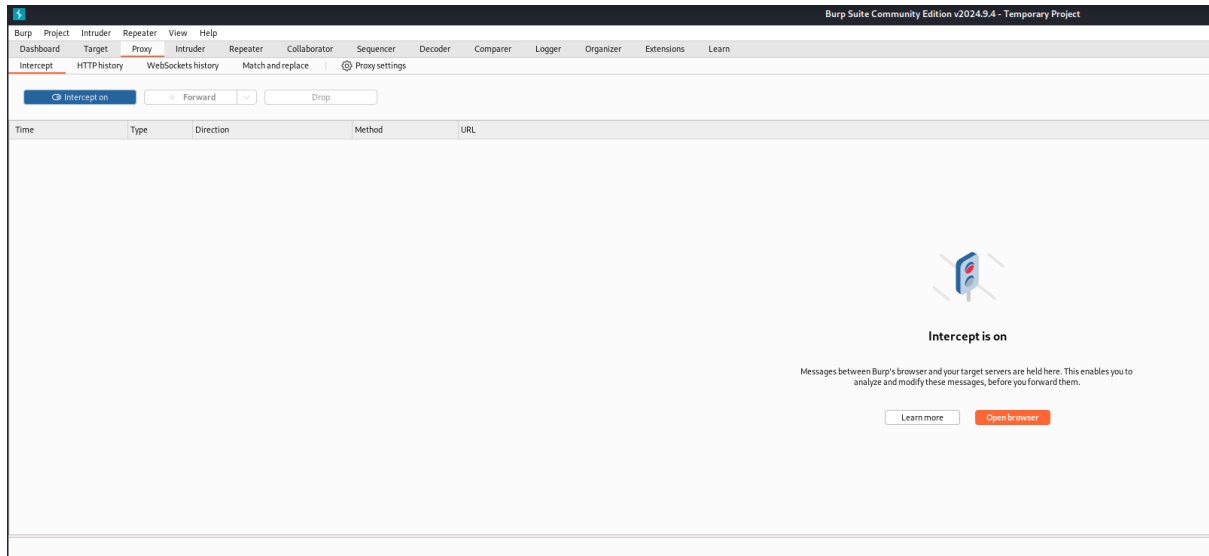
Si inseriscono i dati di accesso (admin password).

Si va dopo su DVWA Security e si imposta a low.

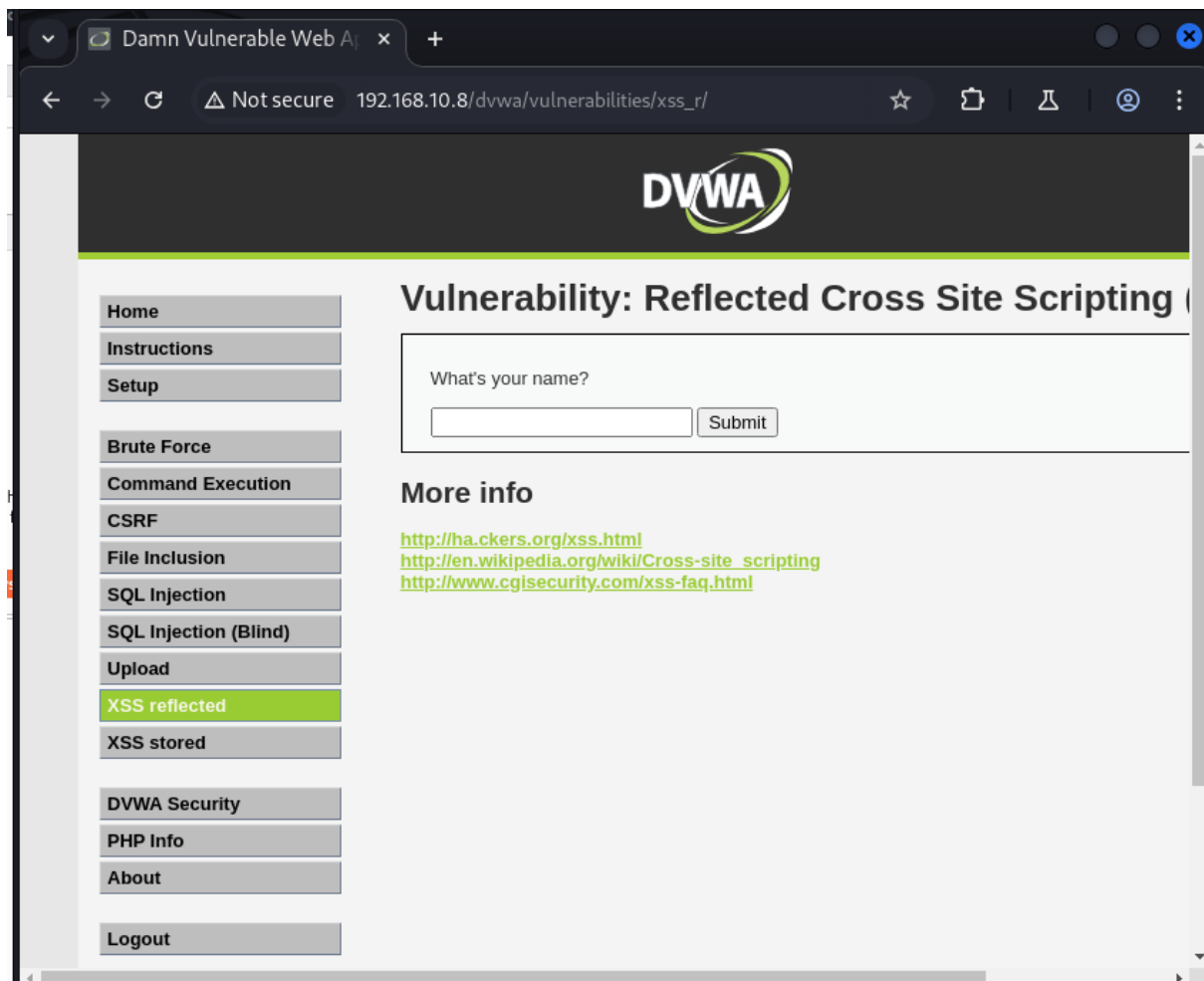


-XSS Reflected:

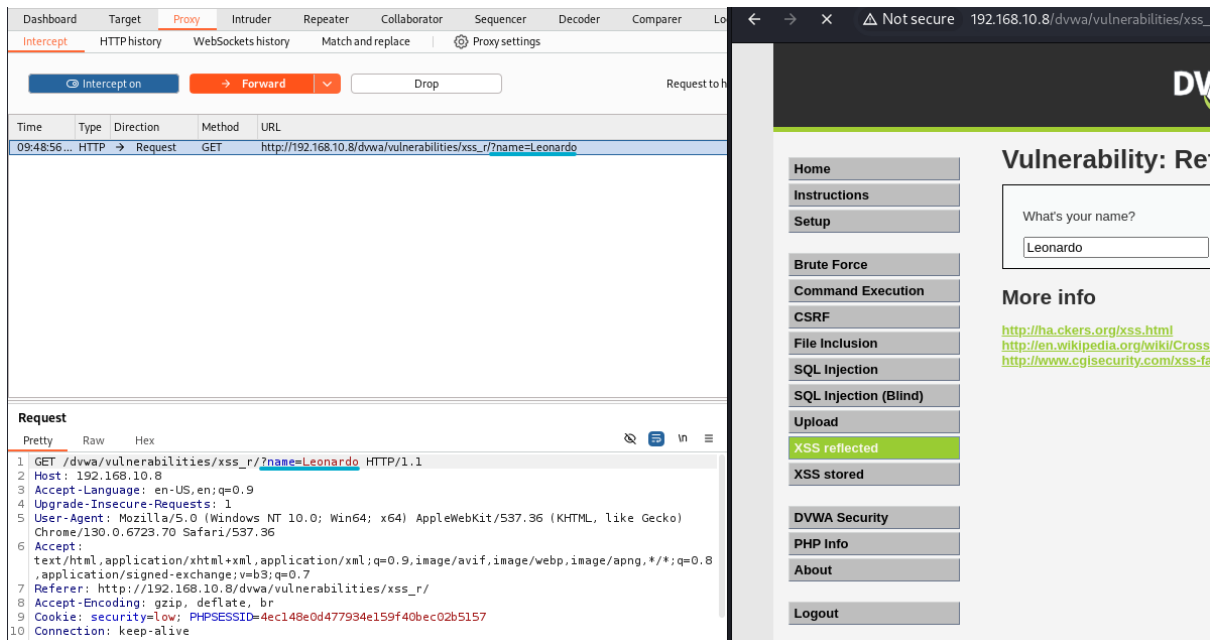
Successivamente si abilita l'intercept di Barp Suit a ON e si va sulla sezione XSS Reflected.



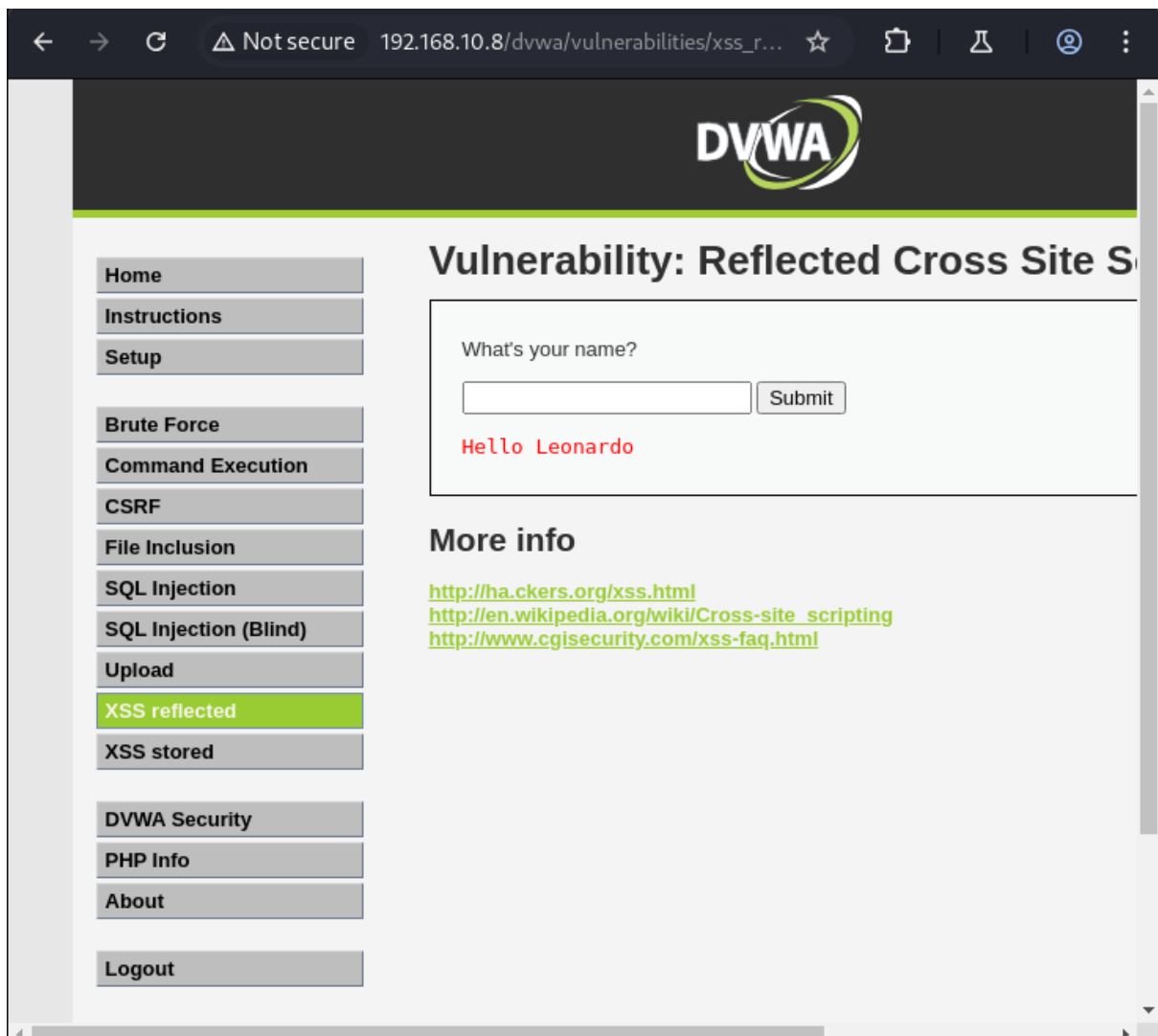
Burp Suite intercetta la richiesta e vediamo/modifichiamo la security a low e intercetta anche il PHPSession.



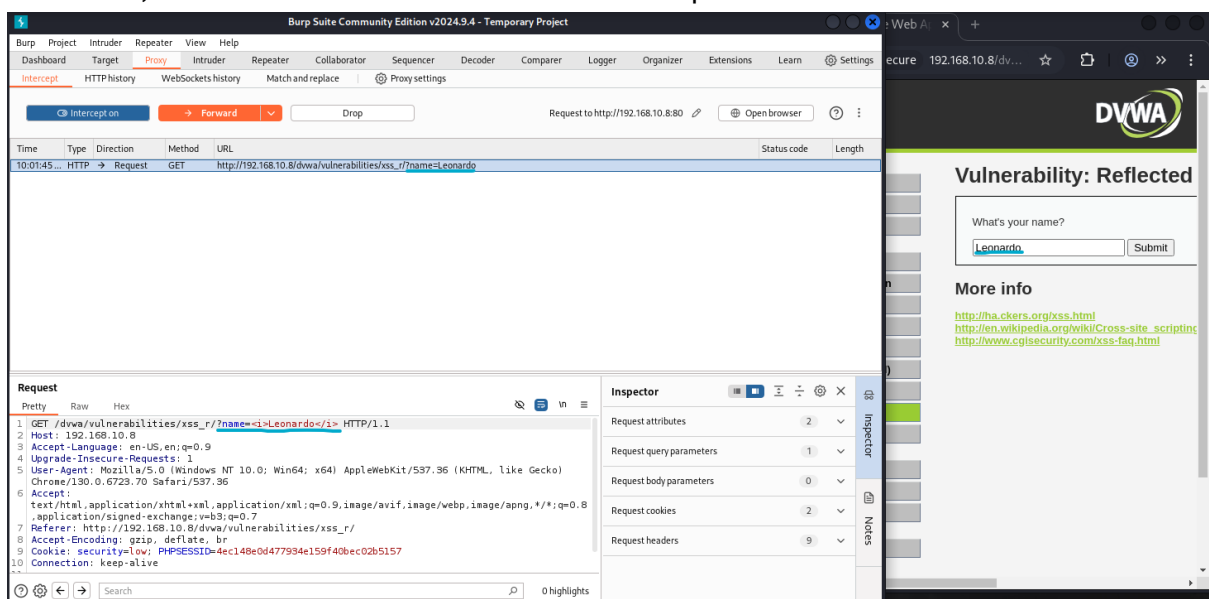
Se per Esempio scrivo Leonardo:



Non toccando nulla e facendo Forward avrò in output la risposta "Hello Leonardo"

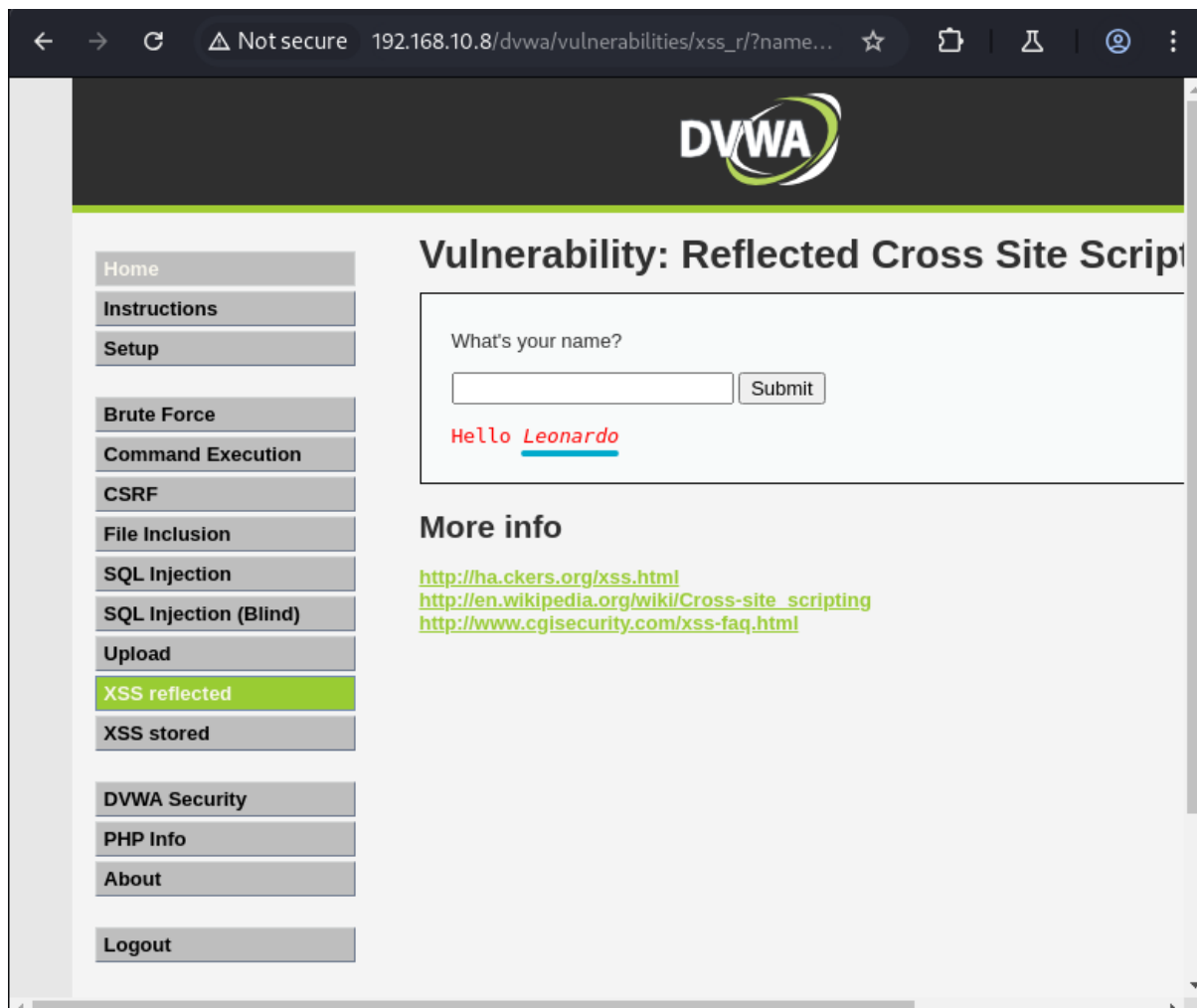


Volendo si può modificare l'header della richiesta e inserire uno script per fare un XSS Reflected, sia dall'interfaccia di DVWA che da Burp Suite:



In questa prova io utente ho scritto Leonardo sulla richiesta, intercettando la richiesta

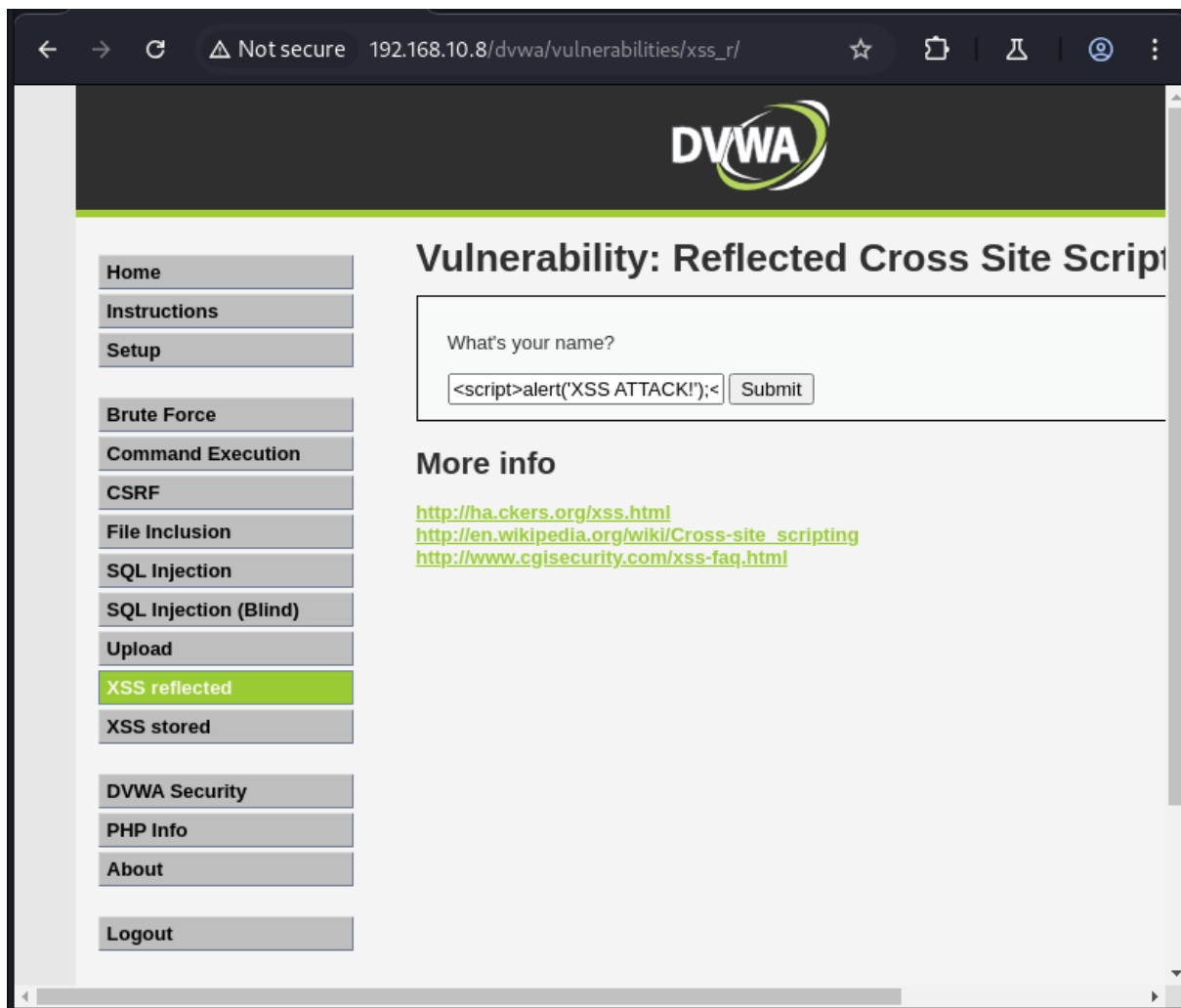
con BurpSuite sono andato a modificare l'header della richiesta inserendo un piccolo script `<i>Leonard </i>` (italic) che serve a far uscire l'output in corsivo.



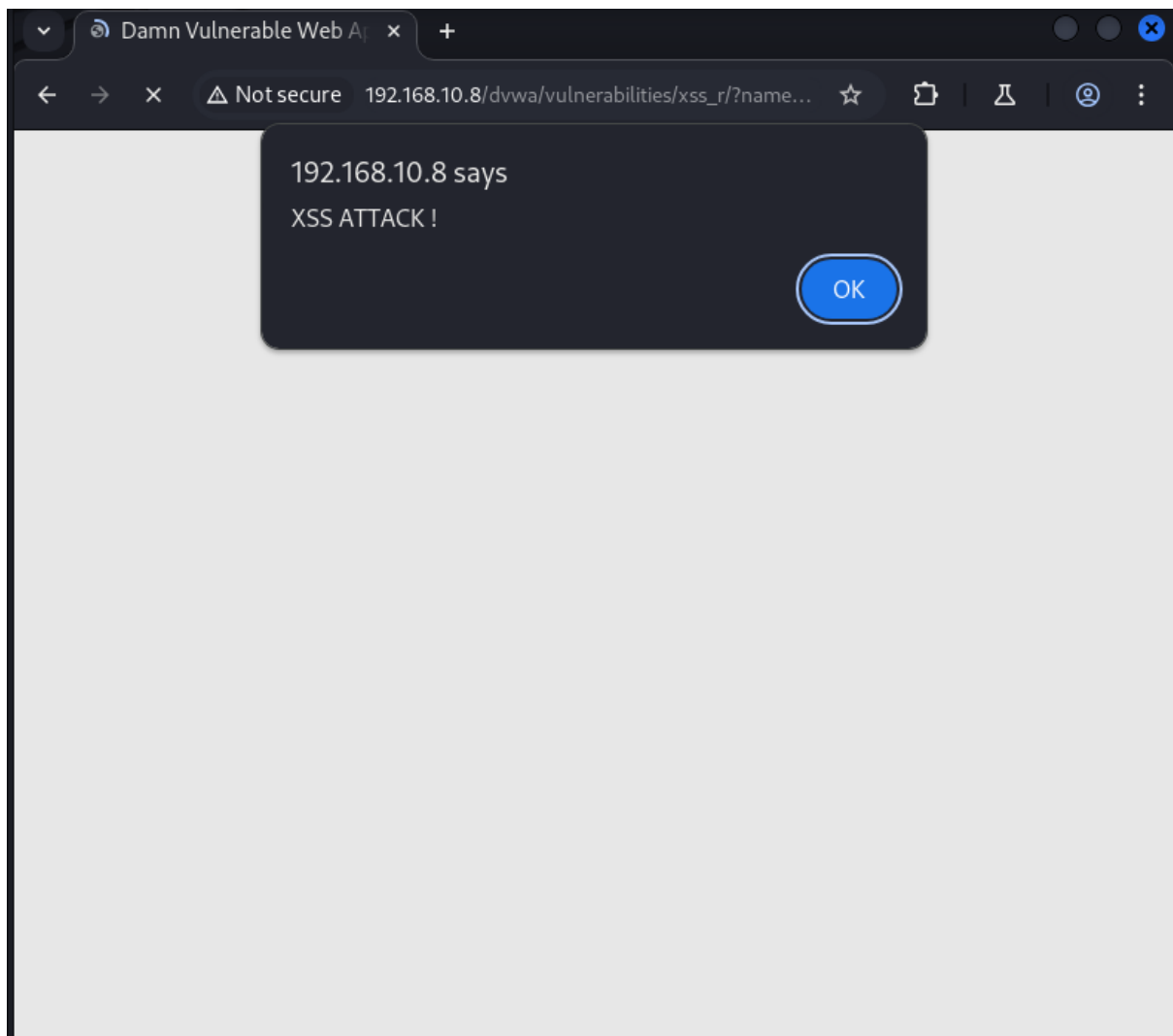
L'output è uscito in corsivo e l'utente dalla sua prospettiva non ha visto nulla.

Si può anche inserire uno script direttamente da questa richiesta, come esempio farò l>alert di un messaggio:

```
<script>alert('XSS ATTACK!');</script>
```

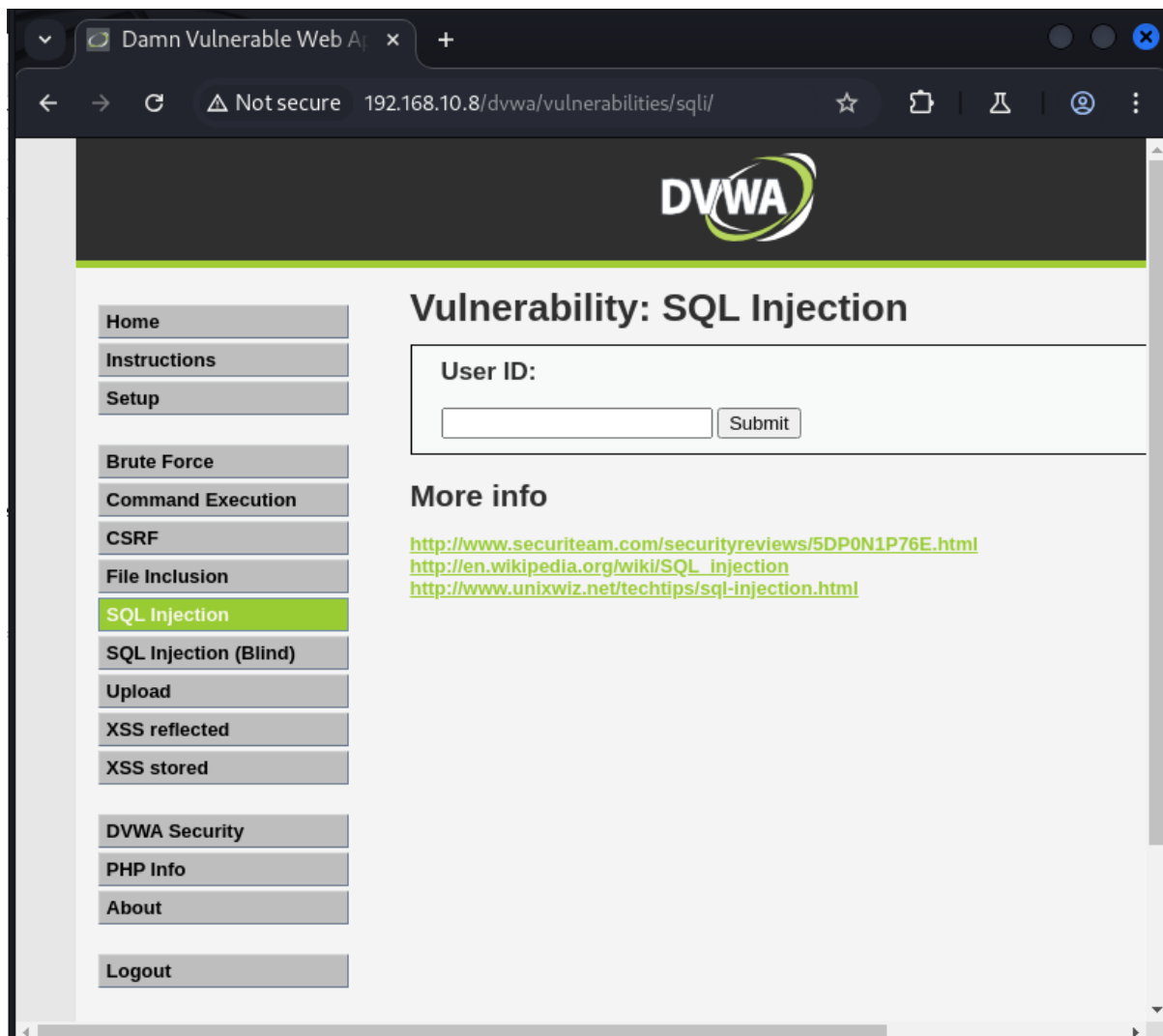
(Submit)



In output avremo l'alert e il messaggio inserito nello script.

-Sql Injection:

Ora si va nella sezione di SQL Injection di DVWA:

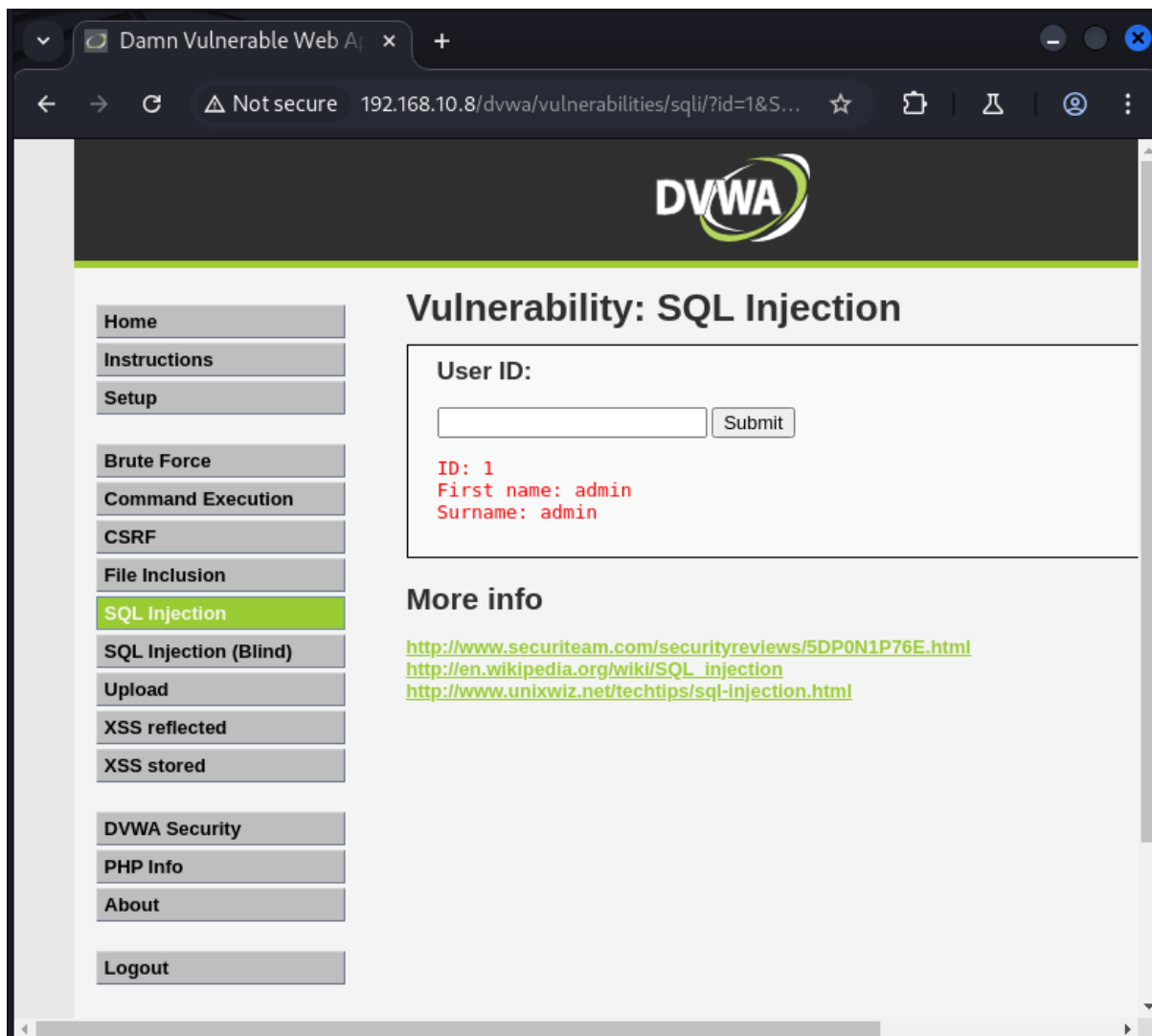


Facendo un test di inserimento di ID 1 noto che come output mi dà 2 campi:

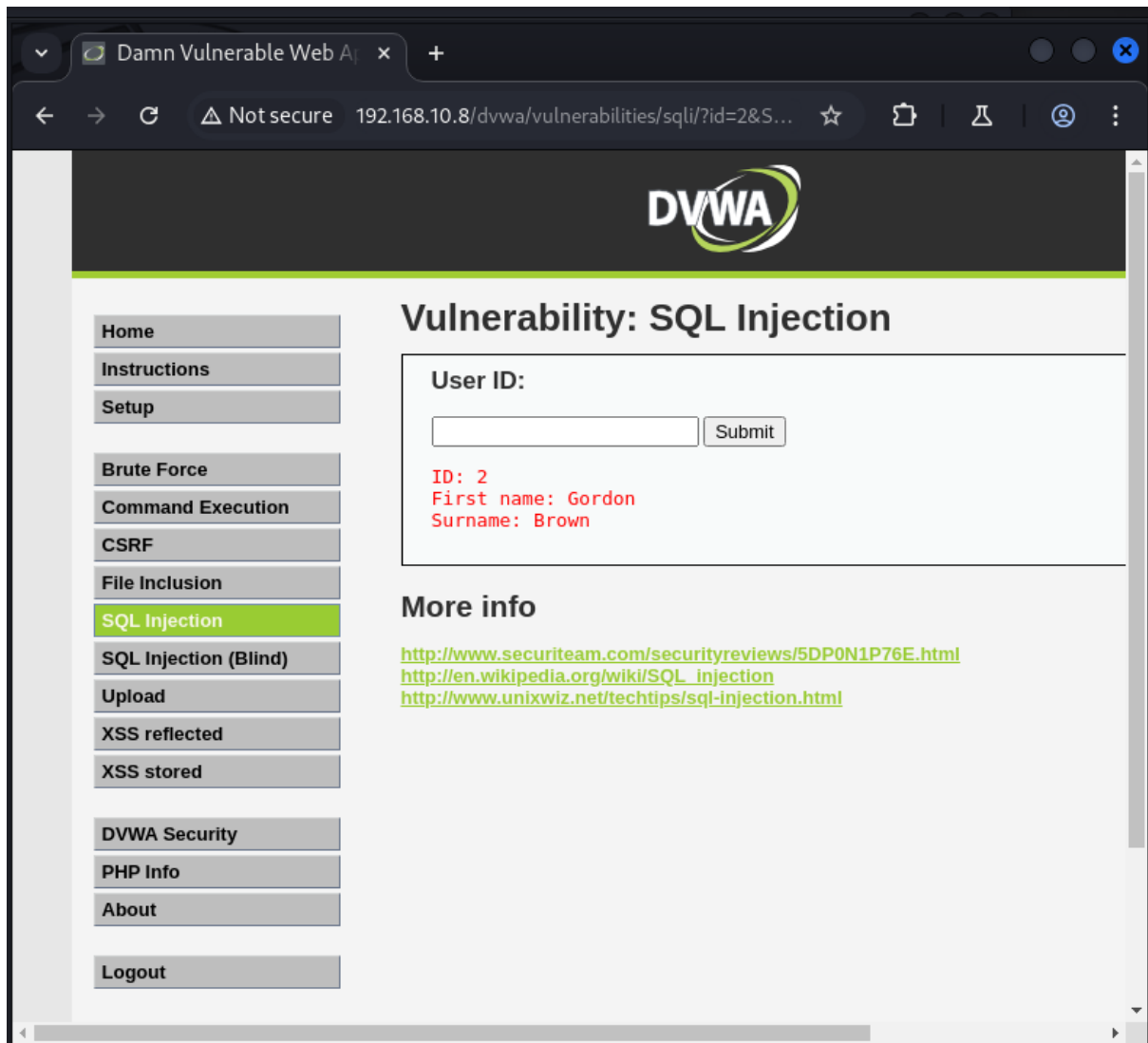
First name : admin e Surname : admin

Ciò mi fa pensare che ci sia una query di questo tipo:

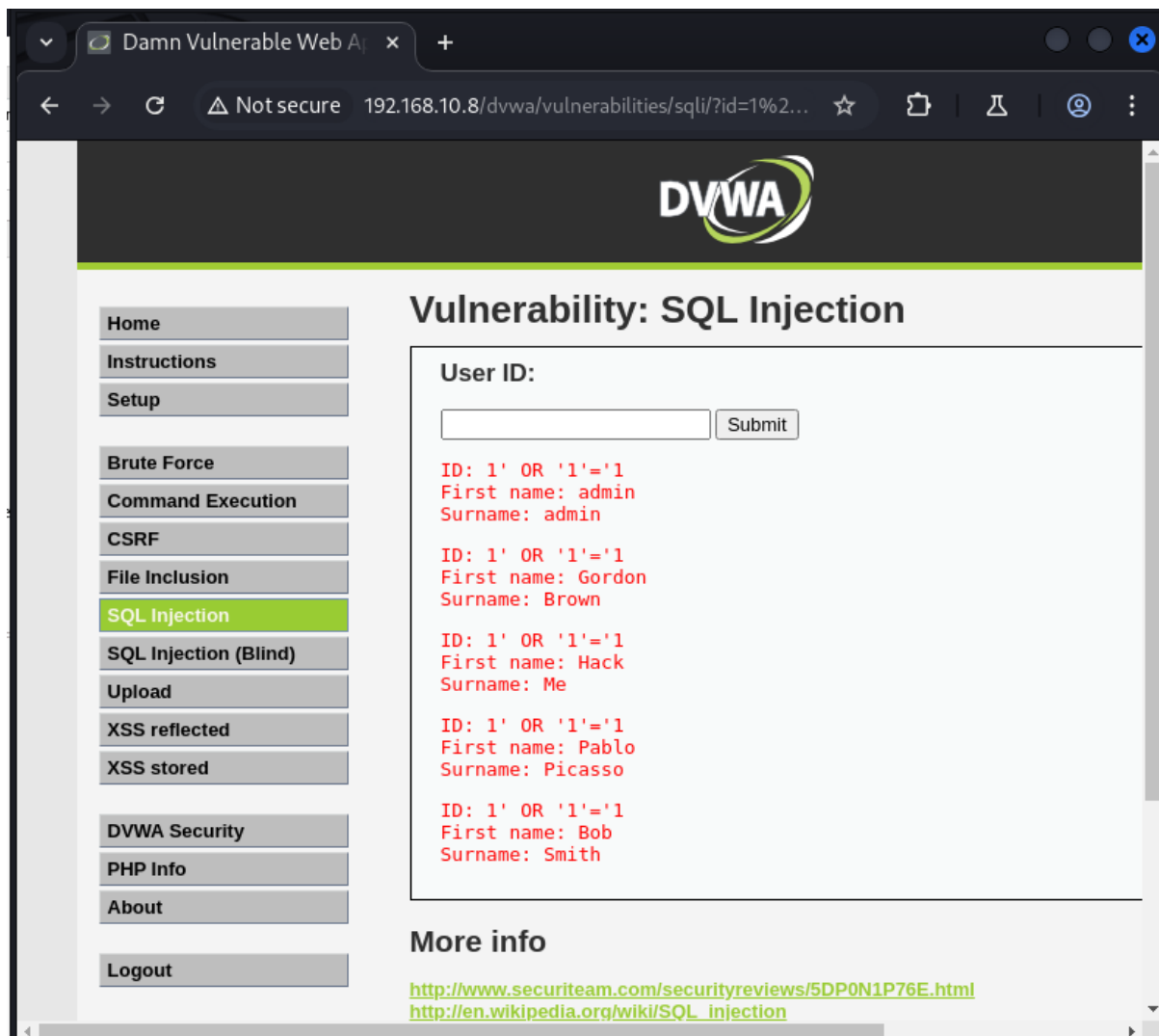
Select First name , Surname From Tabella Where id='numero'



Ho anche fatto un test con 2 e mi esce un'altro nome e cognome:



Allora ho provato ad inserire una query che come condizione è sempre Vera ovvero:
1' OR '1'='1



E l'output ha avuto successo e l'effetto corretto.

La query è sempre vera quindi il DB ci restituisce tutti i risultati presenti per il First name e Surname.

Generalmente se ci sono dei dati utenti ci saranno anche delle password.

Per provare a catturare le password bisogna fare una Union query, ricordando che per la Union dobbiamo sapere quanti parametri di output sono richiesti per la query originale (in questo caso sono 2: first name e surname).

Per far ciò si utilizza il comando:

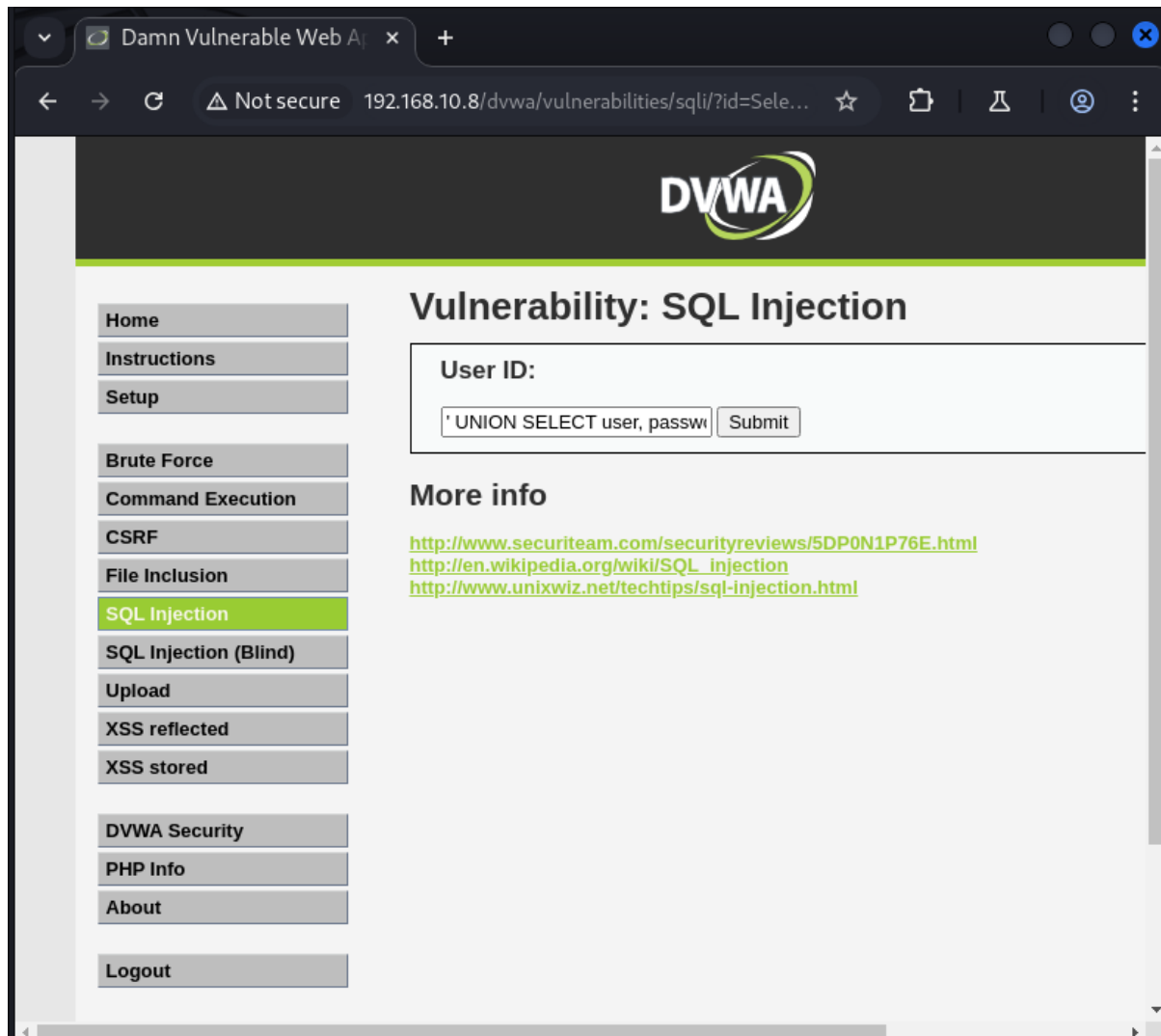
' UNION SELECT user, password FROM users# (il # serve come commento per terminare la richiesta).

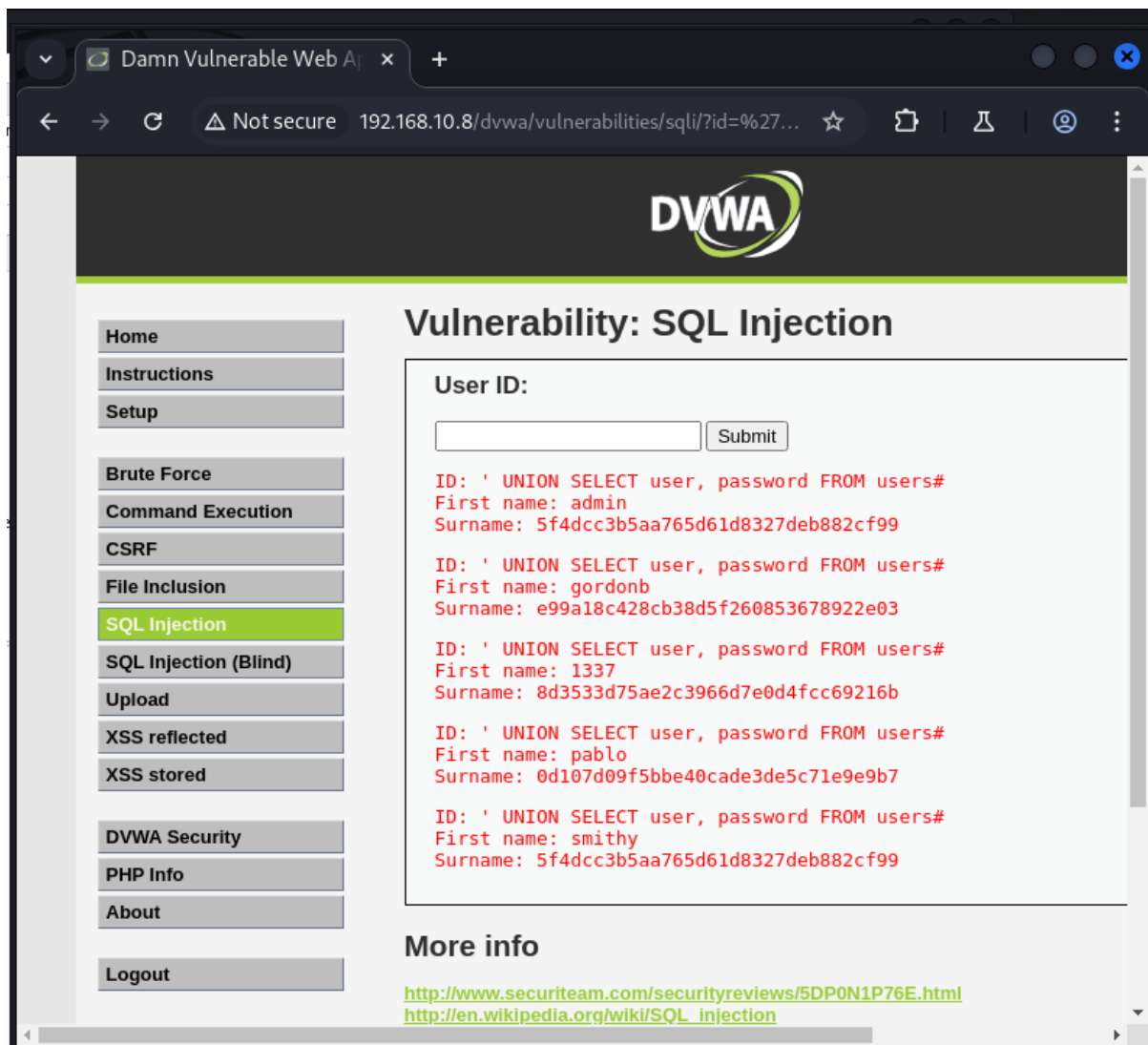
Quindi alla fine la query sarà questa SELECT First name, surname FROM users WHERE id = ''

UNION

SELECT user, password FROM users;

La clausola UNION permette di combinare i risultati di due query.
In questo caso, i dati verranno estrapolati dai campi user e password dalla tabella users.





La Query malevola di SQL Injection ha avuto successo, infatti ci escono le password degli utenti solo che sono criptate.