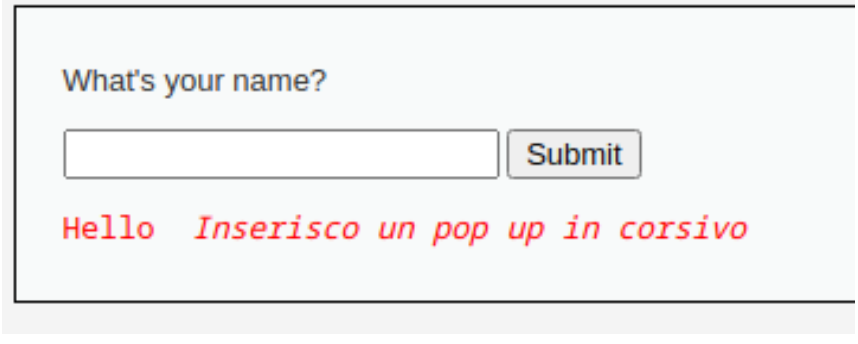
Exploit DVWA - XSS e SQL Injection

Per questo tipo di operazioni si puo lanciare il tool Sqlmap che lavora automaticamente, come segue in figura:

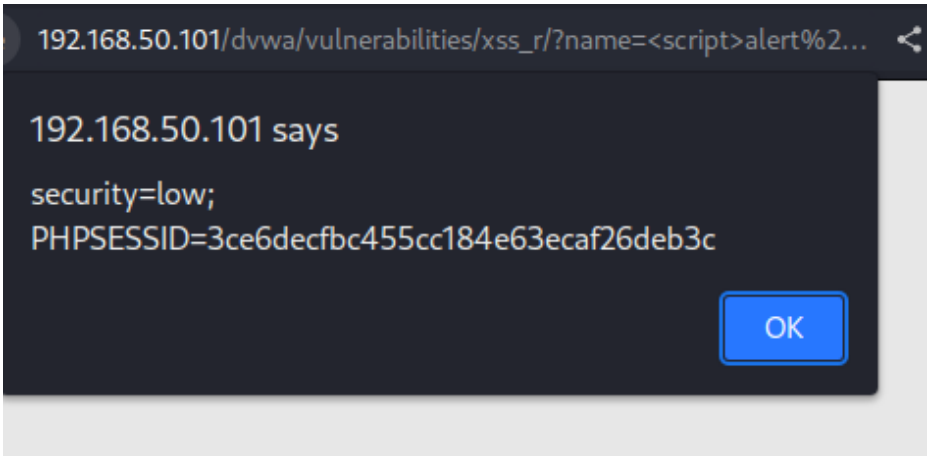
Oppure, in alternativa operare manualmente, come ci è richiesto di fare nell'esercizio di oggi, andando sul DVWA di Metasploitable, sul browser di Kali.
Dopo aver settato il livello di security su Low fornisco degli esempi rispettivamente di:
- XSS:

1. alert di javascript: andiamo ad aprire una finestra pop-up che printa il contenuto tra gli apici della stringa inserita con il seguente script in html:
<script>alert('inserisco un pop up')</script>

2. corsivo di html: interpreta il codice <i> Inserisco un pop up in corsivo

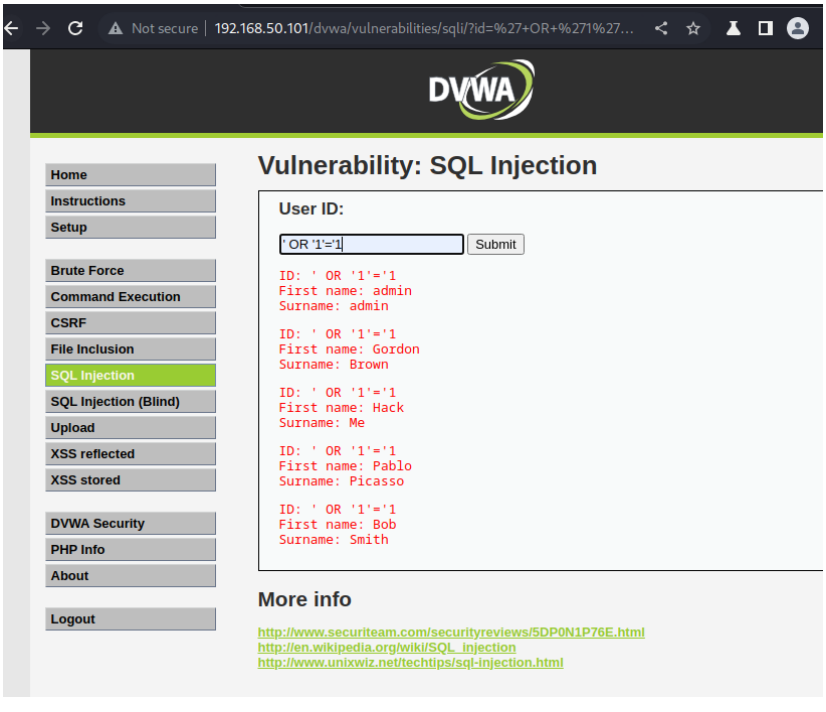


3. recupero cookie: inseriamo il codice <script>alert(document.cookie)</script>, che mostri i cookie dell'utente attuale



- SQL

Inserisco il codice ' OR '1'='1 che sfrutta il fatto che l'istruzione '1'='1' è sempre vera, e quindi la clausola OR restituisce sempre tutti i risultati nella query. L'obiettivo del codice è quello di sfruttare una vulnerabilità nel sito web che potrebbe consentire di eseguire comandi SQL malevoli



Di seguito invece inserisco 2 codici, che sono esempi di un attacco SQL injection di tipo "UNION SELECT" che può essere utilizzato per estrarre informazioni dal database del sito web. I codici sono:

"%' and 1=0 union select null, concat(first_name,0x0a,last_name,0x0a,user,0x0a,password) from

users #%' and 1=0 union select null, concat(first_name,0x0a,last_name,0x0a,user,0x0a,password) from users"

e

1' OR 1=1 UNION SELECT user, password FROM users