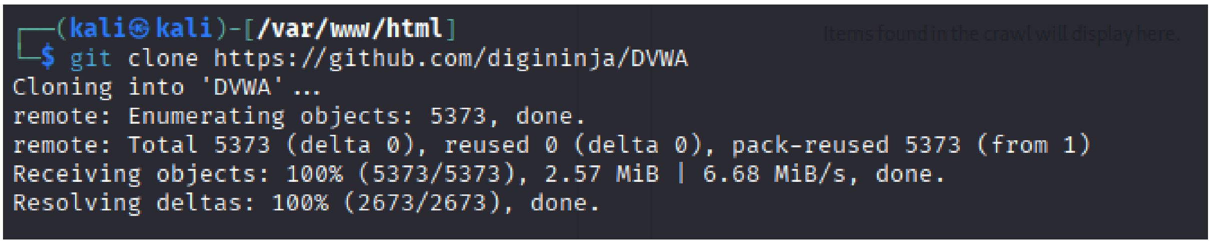
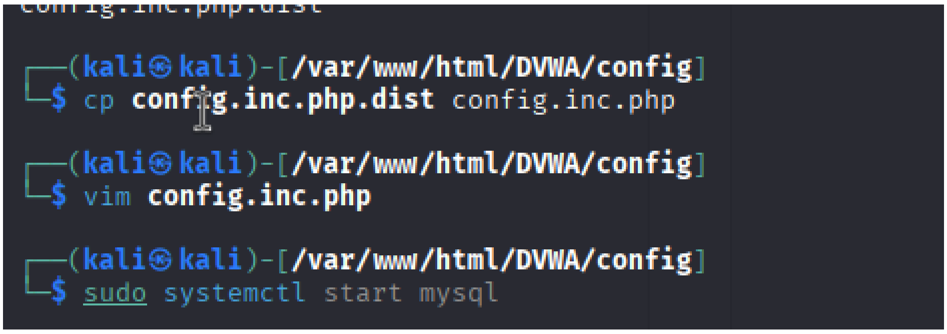
Traccia: In questa lezione pratica vedremo come configurare una DVWA – ovvero damn vulnerable web application in Kali Linux. La DVWA ci sarà molto utile per i nostri test, in cui vedremo da vicino le tecniche per sfruttare le vulnerabilità nella fase di exploit.

1) installiamo DVWA nella nostra Kali Linux.



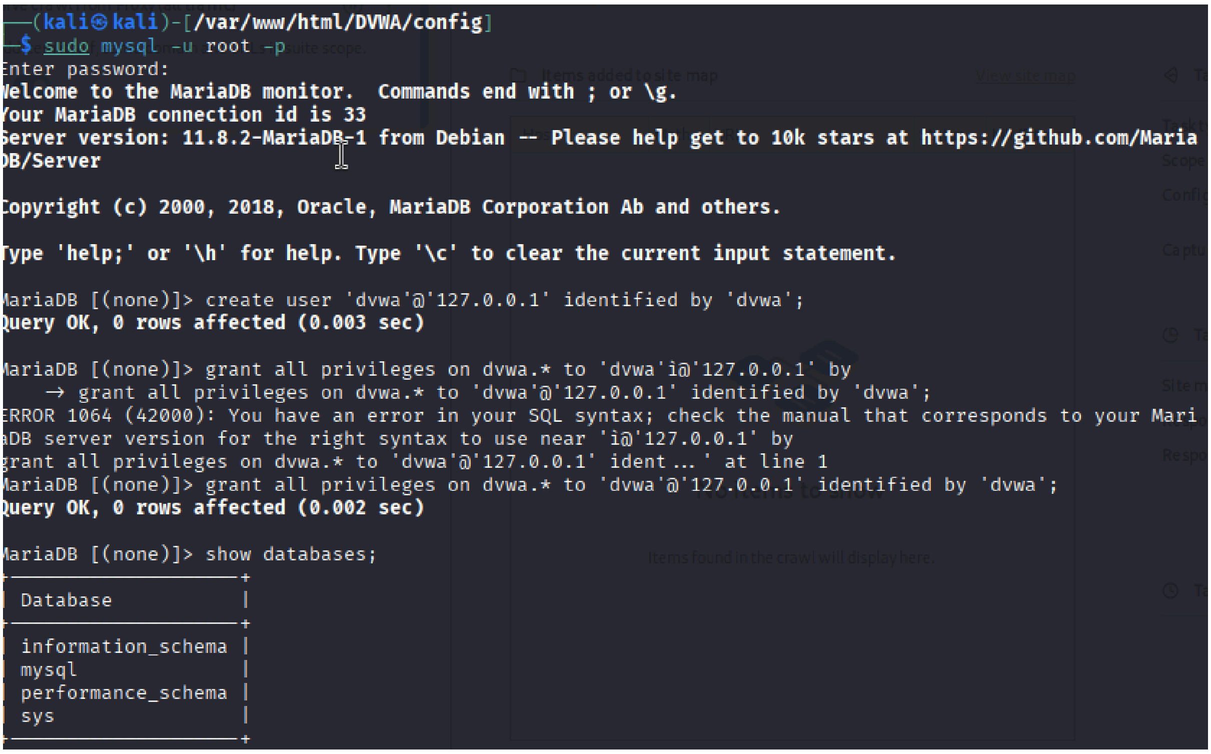
```
┌──(kali㉿kali)-[/var/www/html]
└─$ git clone https://github.com/digininja/DVWA
Cloning into 'DVWA' ...
remote: Enumerating objects: 5373, done.
remote: Total 5373 (delta 0), reused 0 (delta 0), pack-reused 5373 (from 1)
Receiving objects: 100% (5373/5373), 2.57 MiB | 6.68 MiB/s, done.
Resolving deltas: 100% (2673/2673), done.
```

2) configuriamo le credenziali dvwa user e dvwa come password



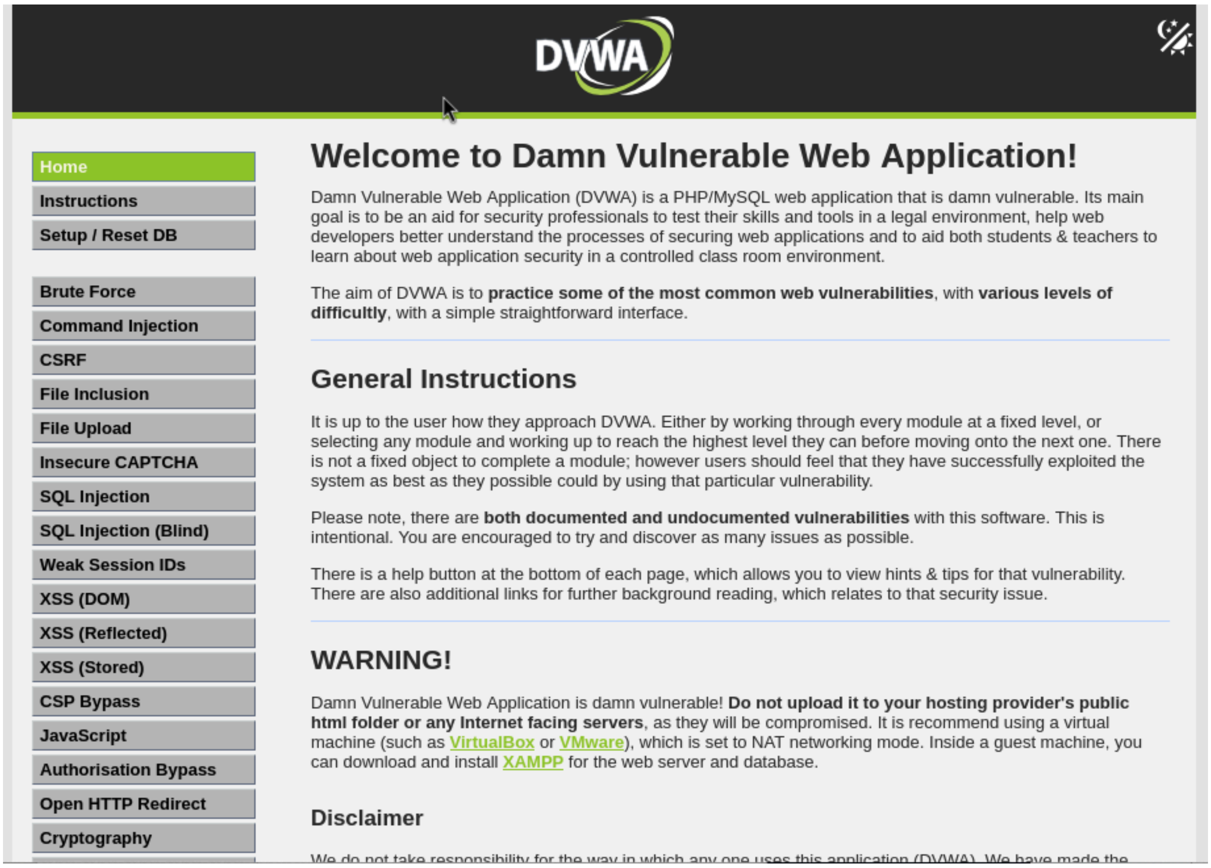
```
config.inc.php.dist

┌──(kali㉿kali)-[/var/www/html/DVWA/config]
└─$ cp config.inc.php.dist config.inc.php

┌──(kali㉿kali)-[/var/www/html/DVWA/config]
└─$ vim config.inc.php

┌──(kali㉿kali)-[/var/www/html/DVWA/config]
└─$ sudo systemctl start mysql
```

3) avviamo mysql service nativo in Kali



```
──(kali㉿kali)-[/var/www/html/DVWA/config]
─$ sudo mysql -u root -p
Enter password:
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 33
Server version: 11.8.2-MariaDB-1 from Debian -- Please help get to 10k stars at https://github.com/Maria
DB/Server

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MariaDB [(none)]> create user 'dvwa'@'127.0.0.1' identified by 'dvwa';
Query OK, 0 rows affected (0.003 sec)

MariaDB [(none)]> grant all privileges on dvwa.* to 'dvwa'i@'127.0.0.1' by
    → grant all privileges on dvwa.* to 'dvwa'@'127.0.0.1' identified by 'dvwa';
ERROR 1064 (42000): You have an error in your SQL syntax; check the manual that corresponds to your Mari
aDB server version for the right syntax to use near 'i@'127.0.0.1' by
grant all privileges on dvwa.* to 'dvwa'@'127.0.0.1' ident...' at line 1
MariaDB [(none)]> grant all privileges on dvwa.* to 'dvwa'@'127.0.0.1' identified by 'dvwa';
Query OK, 0 rows affected (0.002 sec)

MariaDB [(none)]> show databases;
+--------------------+
| Database           |
+--------------------+
| information_schema |
| mysql              |
| performance_schema |
| sys                |
+--------------------+
```

4) startiamo anche apache2



Welcome to Damn Vulnerable Web Application!

Damn Vulnerable Web Application (DVWA) is a PHP/MySQL web application that is damn vulnerable. Its main goal is to be an aid for security professionals to test their skills and tools in a legal environment, help web developers better understand the processes of securing web applications and to aid both students & teachers to learn about web application security in a controlled class room environment.

The aim of DVWA is to **practice some of the most common web vulnerabilities**, with **various levels of difficultly**, with a simple straightforward interface.

General Instructions

It is up to the user how they approach DVWA. Either by working through every module at a fixed level, or selecting any module and working up to reach the highest level they can before moving onto the next one. There is not a fixed object to complete a module; however users should feel that they have successfully exploited the system as best as they possible could by using that particular vulnerability.

Please note, there are **both documented and undocumented vulnerabilities** with this software. This is intentional. You are encouraged to try and discover as many issues as possible.

There is a help button at the bottom of each page, which allows you to view hints & tips for that vulnerability. There are also additional links for further background reading, which relates to that security issue.

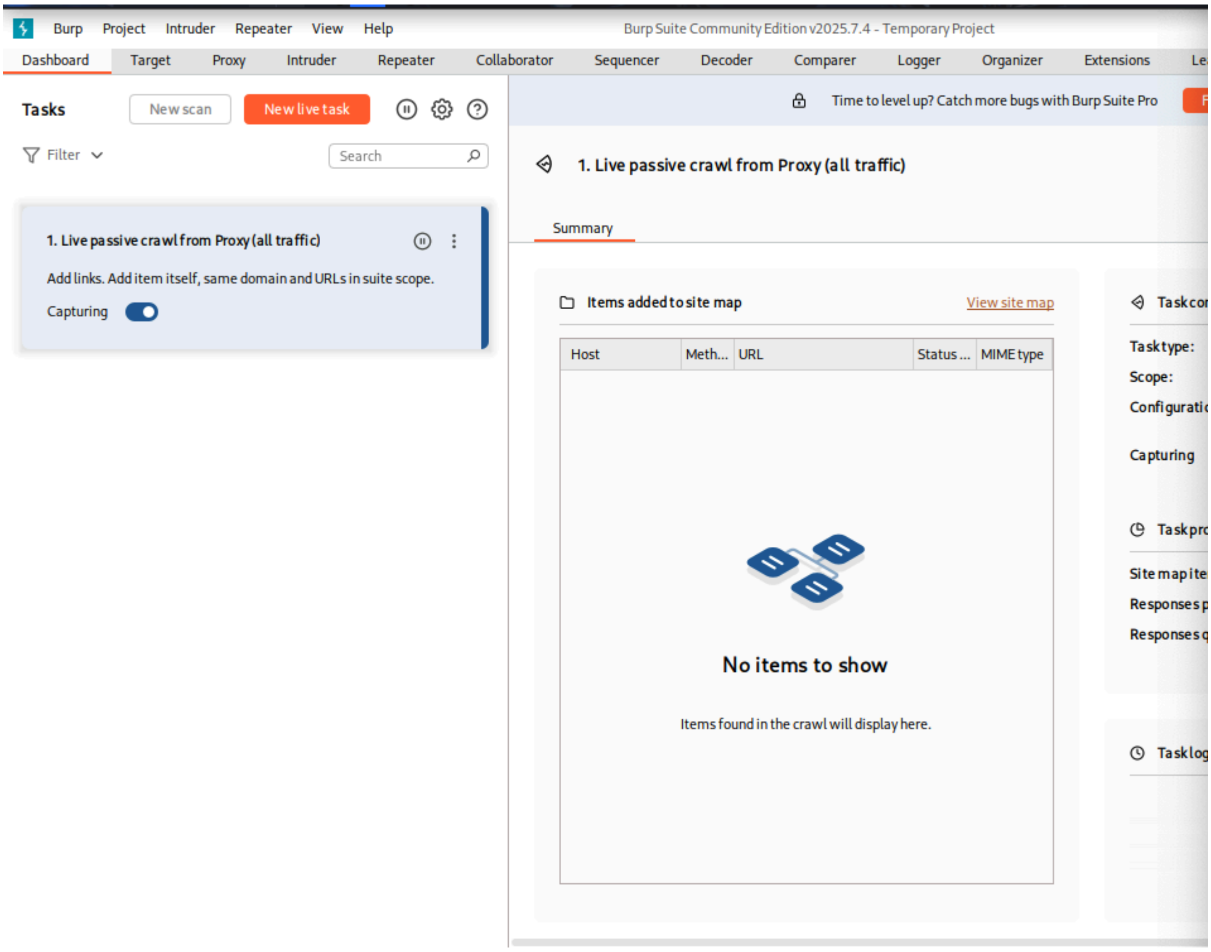
WARNING!

Damn Vulnerable Web Application is damn vulnerable! **Do not upload it to your hosting provider's public html folder or any Internet facing servers**, as they will be compromised. It is recommend using a virtual machine (such as VirtualBox or VMware), which is set to NAT networking mode. Inside a guest machine, you can download and install XAMPP for the web server and database.

Disclaimer

We do not take responsibility for the way in which any one uses this application (DVWA). We have made the

5) fatto anche il login ci spostiamo in Burp Suite



Burp Suite Community Edition v2025.7.4 - Temporary Project

Time to level up? Catch more bugs with Burp Suite Pro

1. Live passive crawl from Proxy (all traffic)

Add links. Add item itself, same domain and URLs in suite scope.

Capturing

1. Live passive crawl from Proxy (all traffic)

Items added to site map

Host	Meth...	URL	Status ...	MIME type

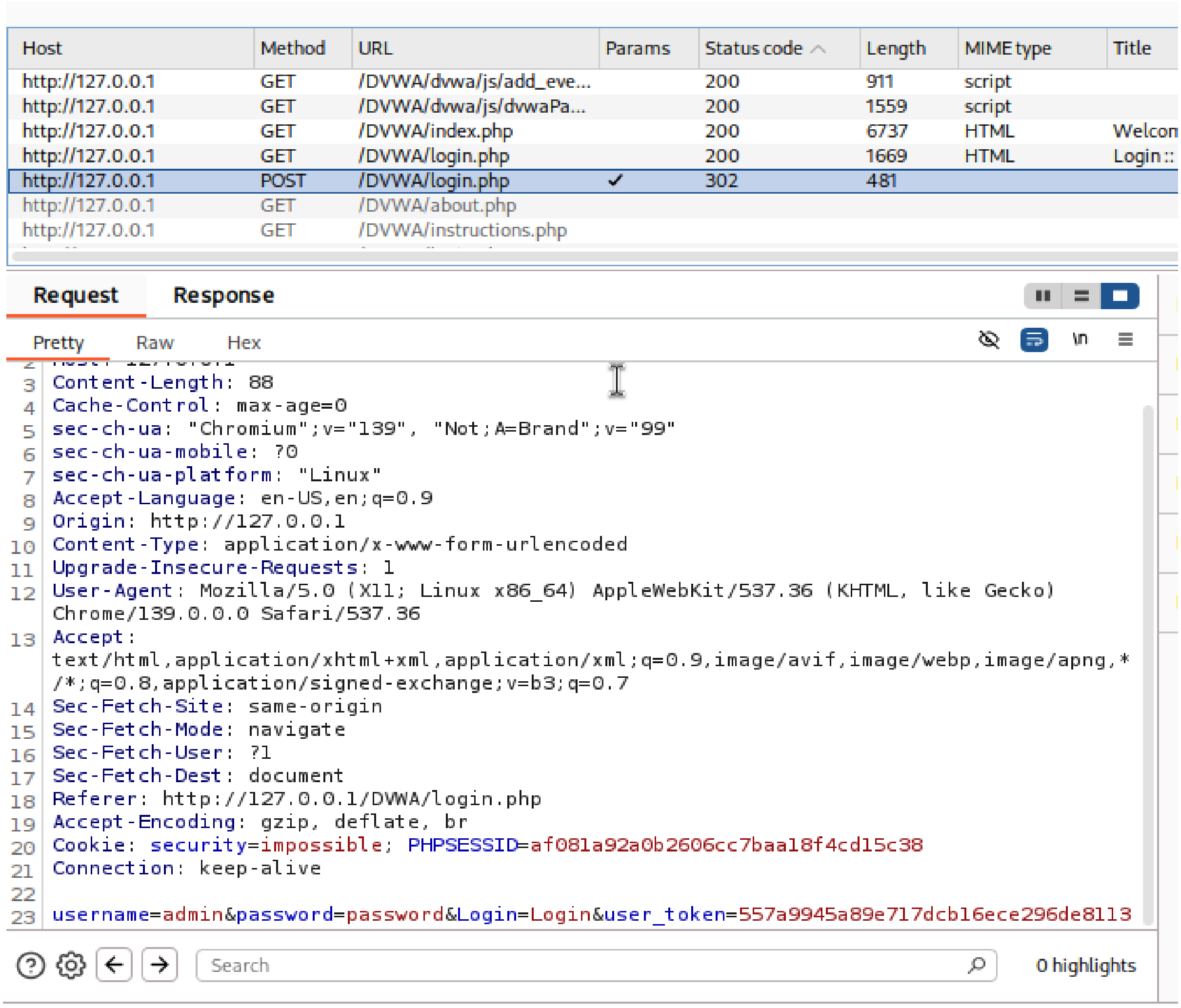
No items to show

Items found in the crawl will display here.

Task type:
Scope:
Configurati
Capturing

Site map ite
Responses p
Responses q

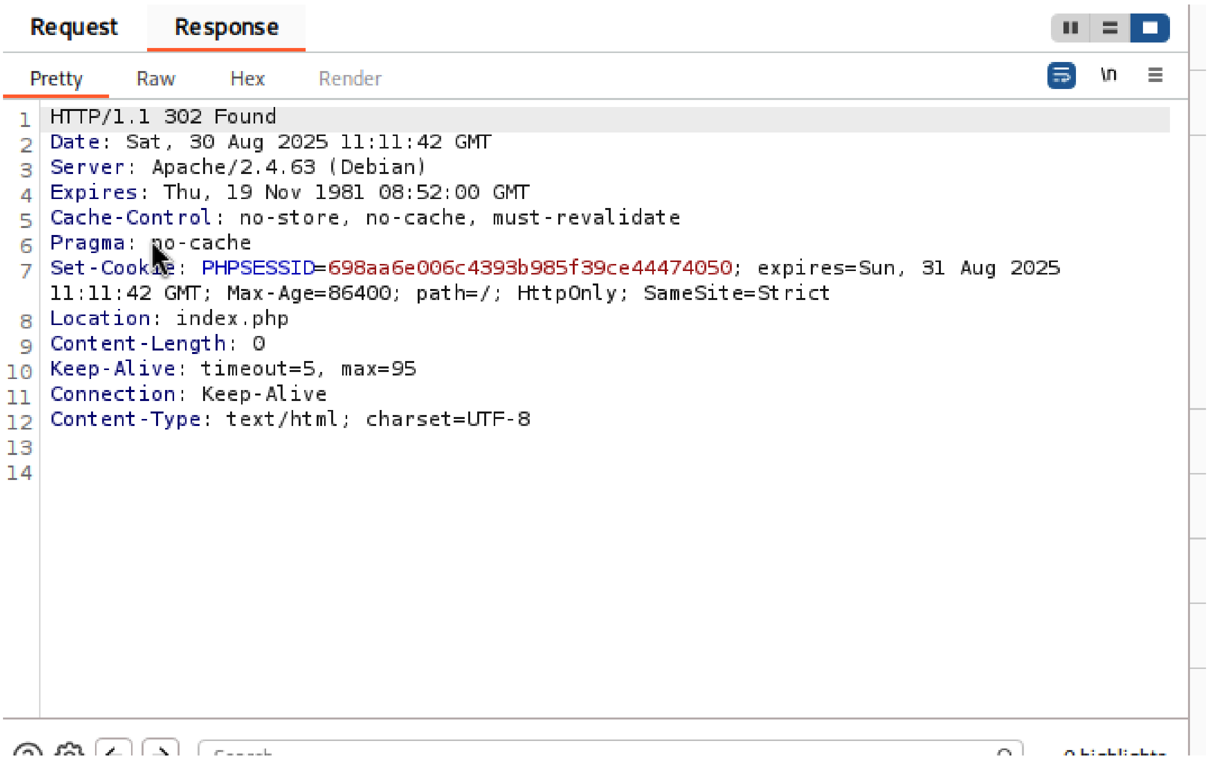
6) faccio il login e visualizzo la post di accesso



Host	Method	URL	Params	Status code	Length	MIME type	Title
http://127.0.0.1	GET	/DVWA/dvwa/js/add_eve...		200	911	script	
http://127.0.0.1	GET	/DVWA/dvwa/js/dvwaPa...		200	1559	script	
http://127.0.0.1	GET	/DVWA/index.php		200	6737	HTML	Welcom
http://127.0.0.1	GET	/DVWA/login.php		200	1669	HTML	Login ::
http://127.0.0.1	POST	/DVWA/login.php	✓	302	481		
http://127.0.0.1	GET	/DVWA/about.php					
http://127.0.0.1	GET	/DVWA/instructions.php					

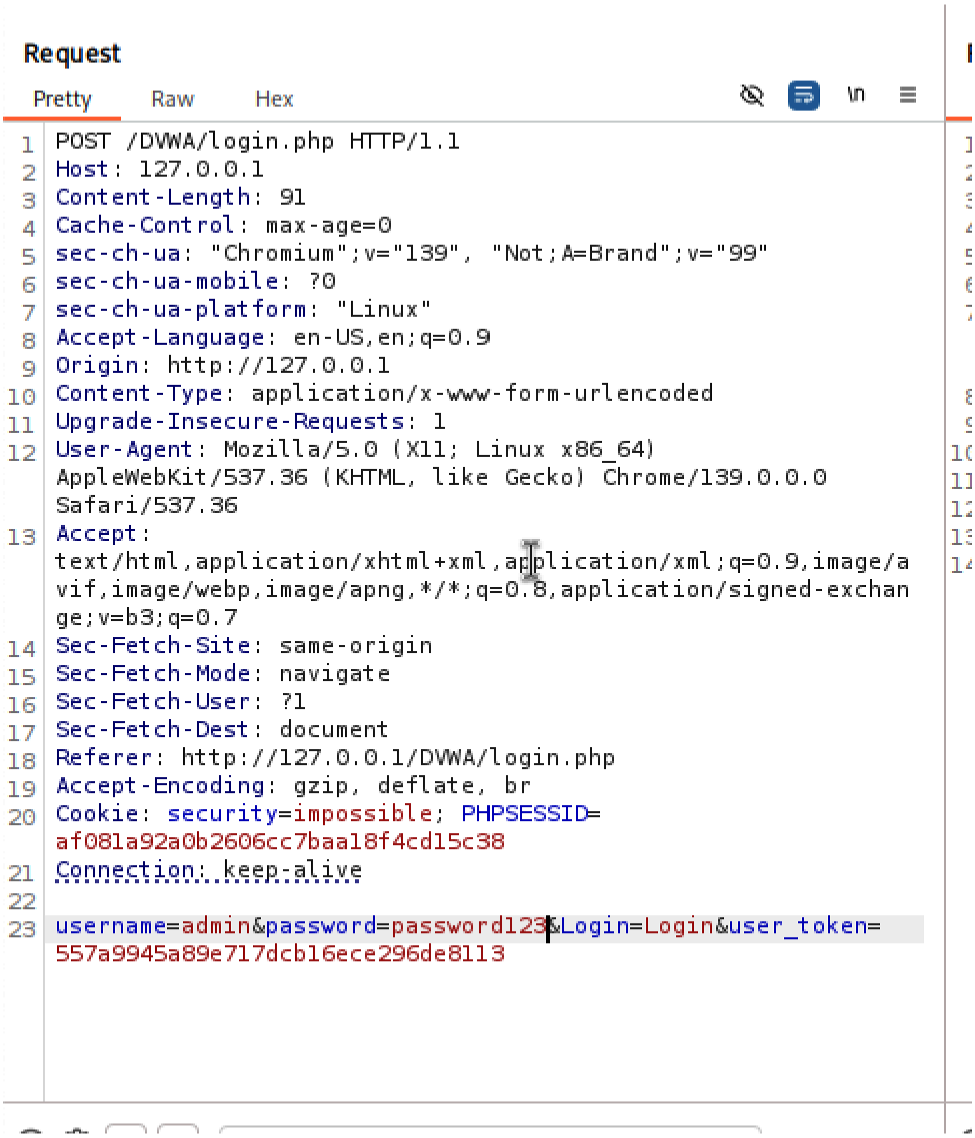
```
Content-Length: 88
Cache-Control: max-age=0
sec-ch-ua: "Chromium";v="139", "Not;A=Brand";v="99"
sec-ch-ua-mobile: ?0
sec-ch-ua-platform: "Linux"
Accept-Language: en-US,en;q=0.9
Origin: http://127.0.0.1
Content-Type: application/x-www-form-urlencoded
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/139.0.0.0 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
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: http://127.0.0.1/DVWA/login.php
Accept-Encoding: gzip, deflate, br
Cookie: security=impossible; PHPSESSID=af081a92a0b2606cc7baa18f4cd15c38
Connection: keep-alive

username=admin&password=password&Login=Login&user_token=557a9945a89e717dcb16ece296de8113
```

7) la risposta è



```
HTTP/1.1 302 Found
Date: Sat, 30 Aug 2025 11:11:42 GMT
Server: Apache/2.4.63 (Debian)
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Set-Cookie: PHPSESSID=698aa6e006c4393b985f39ce44474050; expires=Sun, 31 Aug 2025 11:11:42 GMT; Max-Age=86400; path=/; HttpOnly; SameSite=Strict
Location: index.php
Content-Length: 0
Keep-Alive: timeout=5, max=95
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8
```

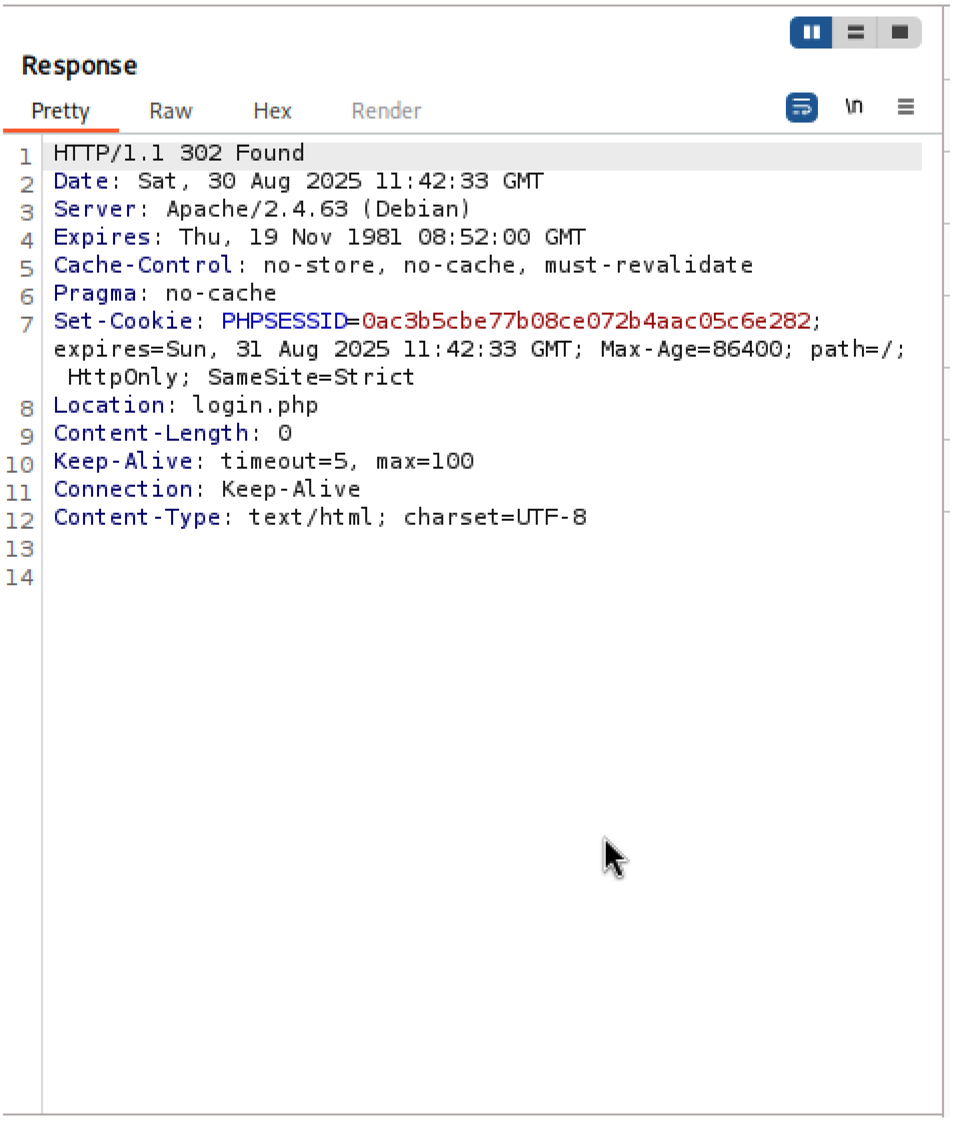
8) proviamo con il Repater la password sbagliata



```
POST /DVWA/login.php HTTP/1.1
Host: 127.0.0.1
Content-Length: 91
Cache-Control: max-age=0
sec-ch-ua: "Chromium";v="139", "Not;A=Brand";v="99"
sec-ch-ua-mobile: ?0
sec-ch-ua-platform: "Linux"
Accept-Language: en-US,en;q=0.9
Origin: http://127.0.0.1
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/139.0.0.0 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
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: http://127.0.0.1/DVWA/login.php
Accept-Encoding: gzip, deflate, br
Cookie: security=impossible; PHPSESSID=af081a92a0b2606cc7baa18f4cd15c38
Connection: keep-alive

username=admin&password=password123&Login=Login&user_token=557a9945a89e717dcb16ece296de8113
```

9)

10) vediamo che siamo in login.php e non index come prima



```
HTTP/1.1 302 Found
Date: Sat, 30 Aug 2025 11:42:33 GMT
Server: Apache/2.4.63 (Debian)
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Set-Cookie: PHPSESSID=0ac3b5cbe77b08ce072b4aac05c6e282;
expires=Sun, 31 Aug 2025 11:42:33 GMT; Max-Age=86400; path=/;
 HttpOnly; SameSite=Strict
Location: login.php
Content-Length: 0
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8
```