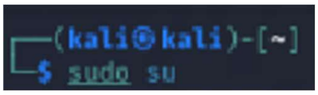
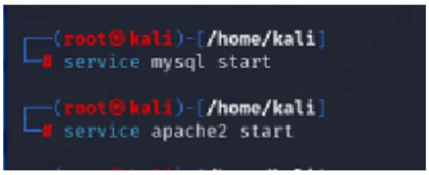
Traccia: Nella lezione pratica di oggi vedremo come configurare una DVWA – ovvero damn vulnerable web application in Kali Linux. La DVWA ci sarà molto utile per i nostri test.

Seguo le istruzioni nella guida del docente per installare DVWA, in particolare impostando come account in mysql su localhost (127.0.0.1 indirizzo di loopback) l'account kali e fornendogli i permessi necessari per poterci operare

Dopo aver configurato correttamente mysql e impostato i permessi, avvio mysql e apache2 con i seguenti comandi:



```
┌──(kali㉿kali)-[~]
└─$ sudo su
```

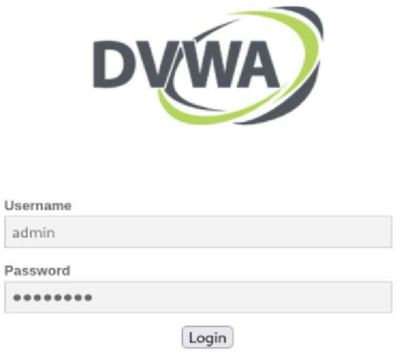


```
┌──(root㉿kali)-[/home/kali]
└─# service mysql start

┌──(root㉿kali)-[/home/kali]
└─# service apache2 start
```

Vado sulla pagina di login e testo il login con le credenziali "admin", "password"

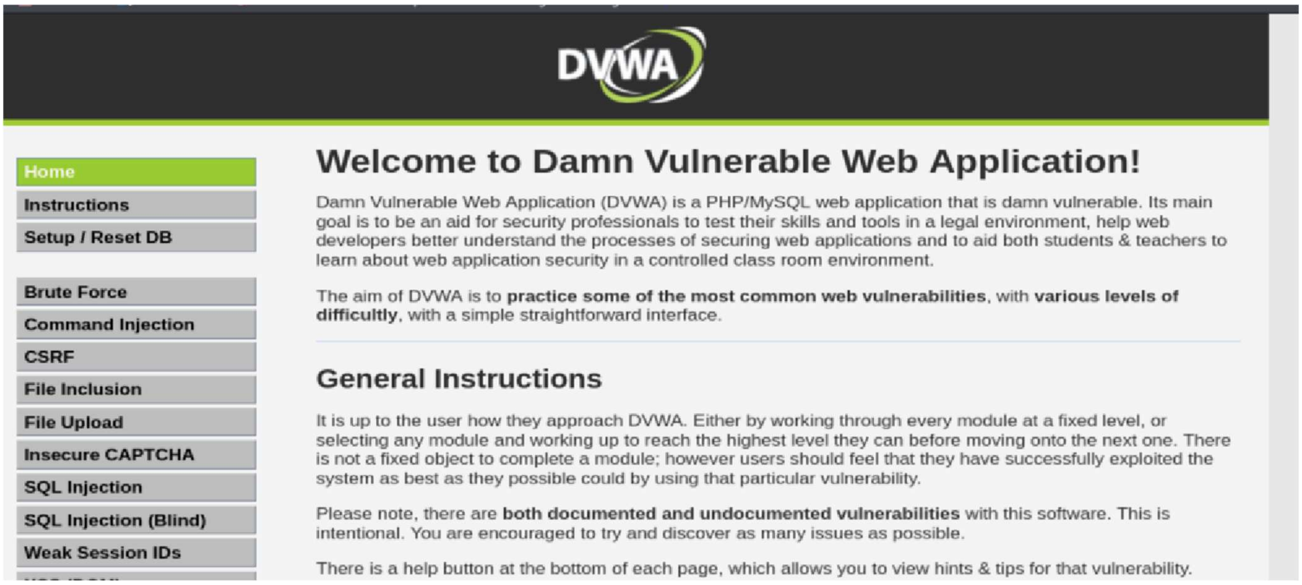
127.0.0.1/DVWA/login.php



Username
admin

Password
●●●●●●●●

Il login funziona:



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.

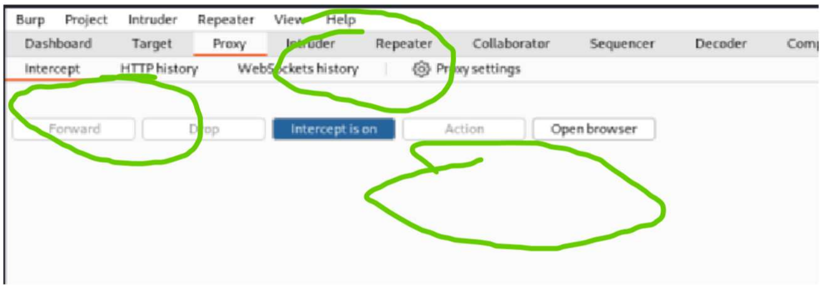
General Instructions

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.

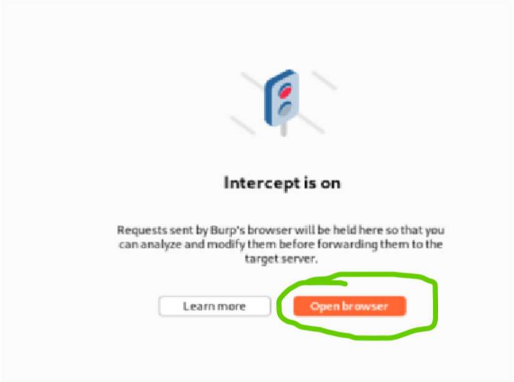
Please note, there are **both documented and undocumented vulnerabilities** with this software. This is intentional. You are encouraged to try and discover as many issues as possible.

There is a help button at the bottom of each page, which allows you to view hints & tips for that vulnerability.

Avvio burpsuite con le impostazioni di default, poi vado in proxy > intercept e avvio l'intercept dei pacchetti

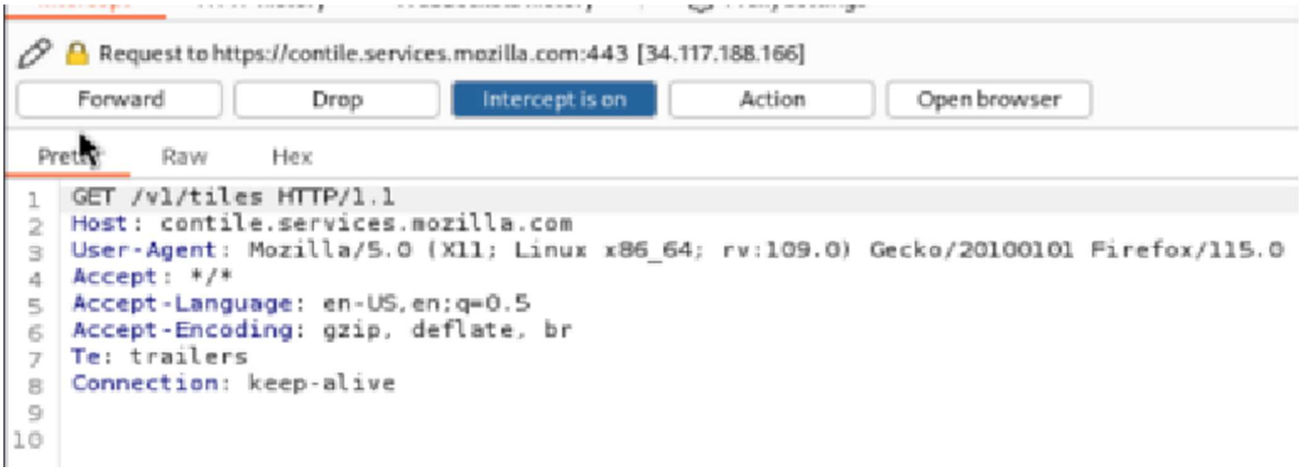


Apro il default browser (chromium) usando il pulsante:



Requests sent by Burp's browser will be held here so that you can analyze and modify them before forwarding them to the target server.

Ora provo ad andare di nuovo sulla pagina di DVWA. Dentro burpsuite vedo la richiesta

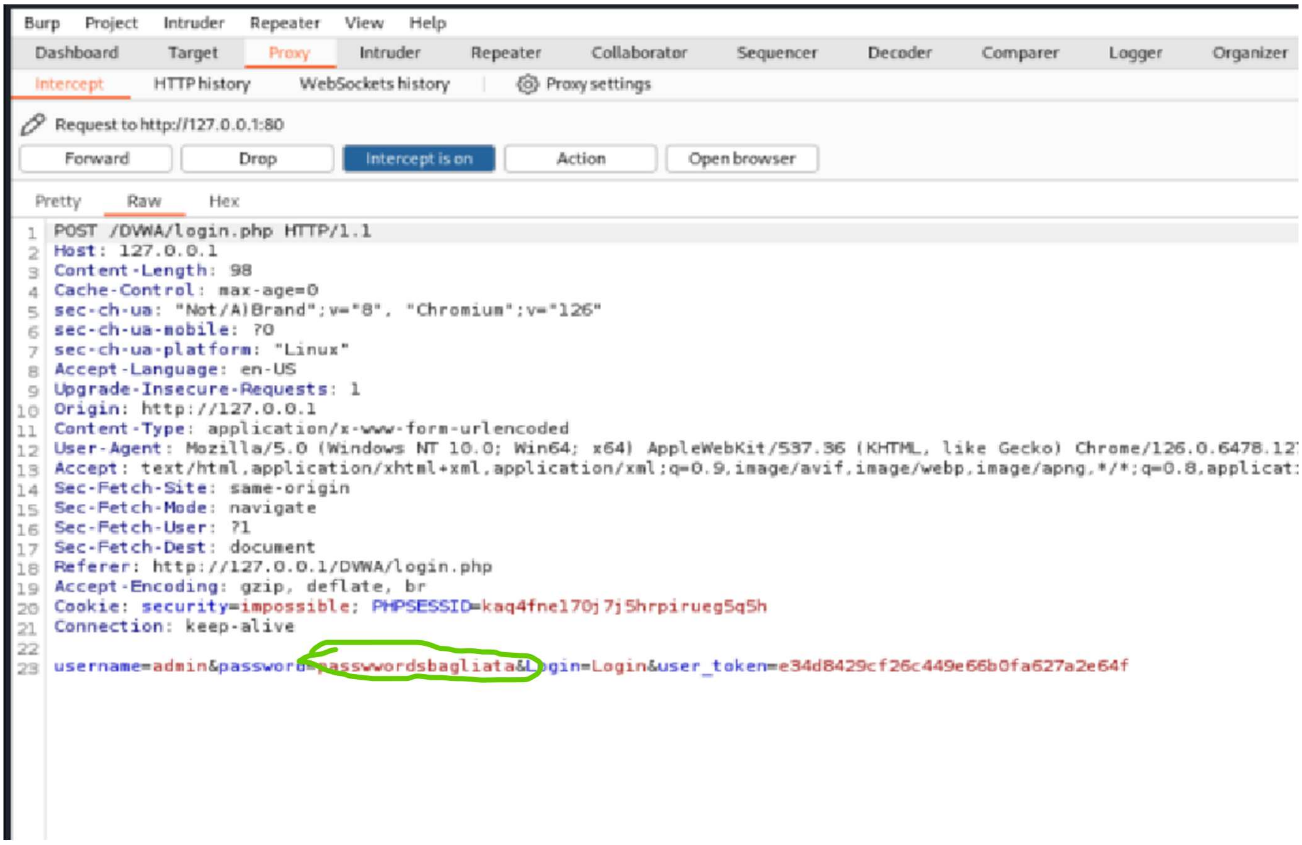

Request to https://contile.services.mozilla.com:443 [34.117.188.166]
Forward
Drop
Intercept is on
Action
Open browser
Pretty
Raw
Hex

```
GET /v1/tiles HTTP/1.1
Host: contile.services.mozilla.com
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
Te: trailers
Connection: keep-alive
```

Premo Forward per farla passare

Nella pagina di login inserisco come credenziali “admin” e “passwordsbagliata”.

Mi si apre burpsuite con la password in plain text (sono in http)

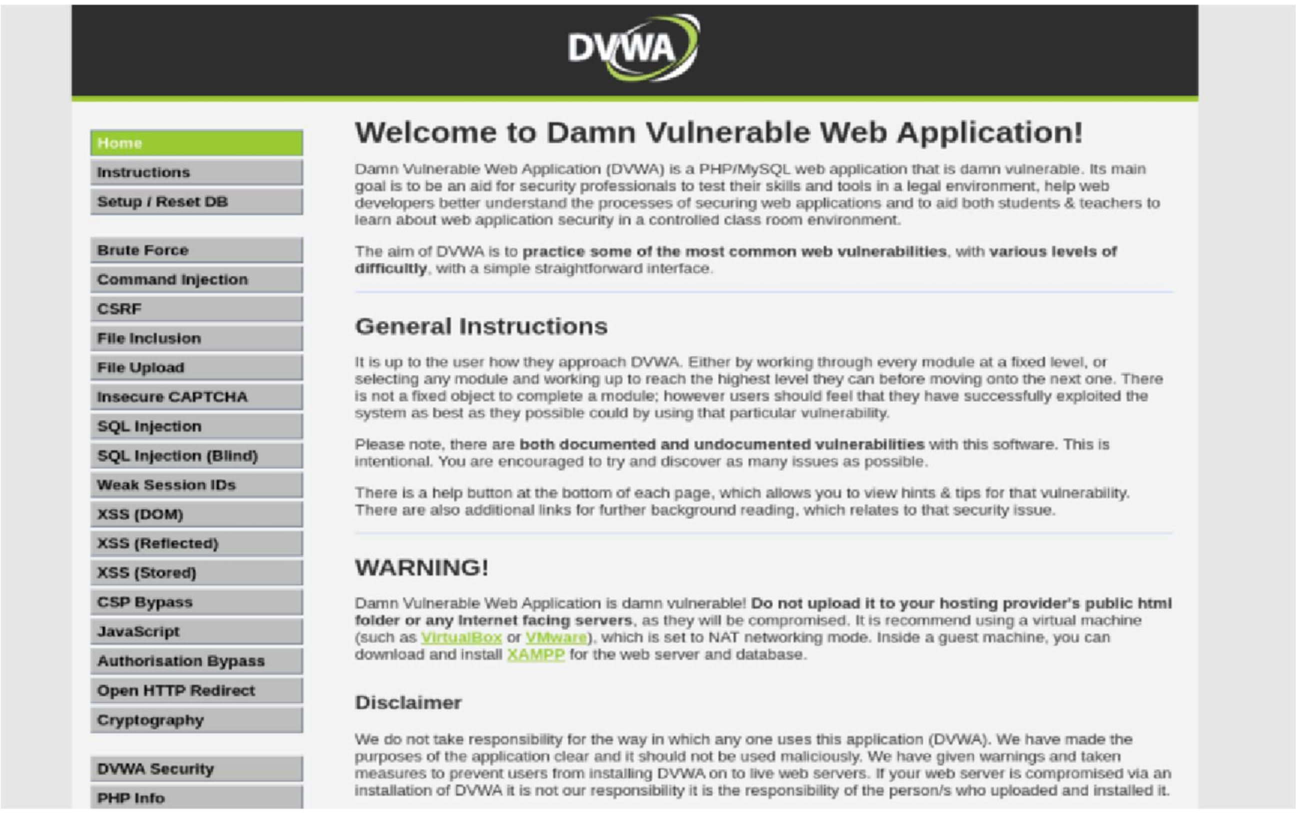


```
POST /DVWA/login.php HTTP/1.1
Host: 127.0.0.1
Content-Length: 98
Cache-Control: max-age=0
sec-ch-ua: "Not/A)Brand";v="8", "Chromium";v="126"
sec-ch-ua-mobile: ?0
sec-ch-ua-platform: "Linux"
Accept-Language: en-US
Upgrade-Insecure-Requests: 1
Origin: http://127.0.0.1
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/126.0.6478.12
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,applicat
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=kaq4fne170j7j5hrpirueg5q5h
Connection: keep-alive

username=admin&password=passwwordsbagliata&Login=Login&user_token=e34d8429cf26c449e66b0fa627a2e64f
```

Sostituisco la password in “password” e poi inoltro.

La password è stata sostituita rispetto a quella inserita nella pagina di login, il login è andato a buon fine:



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 purposes of the application clear and it should not be used maliciously. We have given warnings and taken measures to prevent users from installing DVWA on to live web servers. If your web server is compromised via an installation of DVWA it is not our responsibility it is the responsibility of the person/s who uploaded and installed it.