

ESERCIZIO LEZIONE 3

In questo esercizio ci viene chiesto di utilizzare BURPSUIT per andare ad intercettare i dati tra noi ed un server su un applicazione web creata *ad ok* per questo esercizio.

Dopo aver installato mysql e apache2, come da slide, e aver impostato il nostro sito andiamo a lavorare:

Setup Check

Web Server SERVER_NAME: **127.0.0.1**

Operating system: ***nix**

PHP version: **8.2.7**

PHP function display_errors: **Disabled**

PHP function display_startup_errors: **Disabled**

PHP function allow_url_include: **Disabled**

PHP function allow_url_fopen: **Enabled**

PHP module gd: **Missing - Only an issue if you want to play with captchas**

PHP module mysql: **Installed**

PHP module pdo_mysql: **Installed**

Backend database: **MySQL/MariaDB**

Database username: **kali**

Database password: *********

Database database: **dvwa**

Database host: **127.0.0.1**

Database port: **3306**

reCAPTCHA key: **Missing**

Writable folder /var/www/html/DVWA/hackable/uploads/: **Yes**

Writable folder /var/www/html/DVWA/config: **Yes**

Status in red, indicate there will be an issue when trying to complete some modules.

If you see disabled on either `allow_url_fopen` or `allow_url_include`, set the following in your `php.ini` file and restart Apache.

`allow_url_fopen = On`

`allow_url_include = On`

These are only required for the file inclusion labs so unless you want to play with those, you can ignore them.

Create / Reset Database

DVWA Security

Security Level

Security level is currently: **impossible**.

You can set the security level to low, medium, high or impossible. The security level changes the vulnerability level of DVWA:

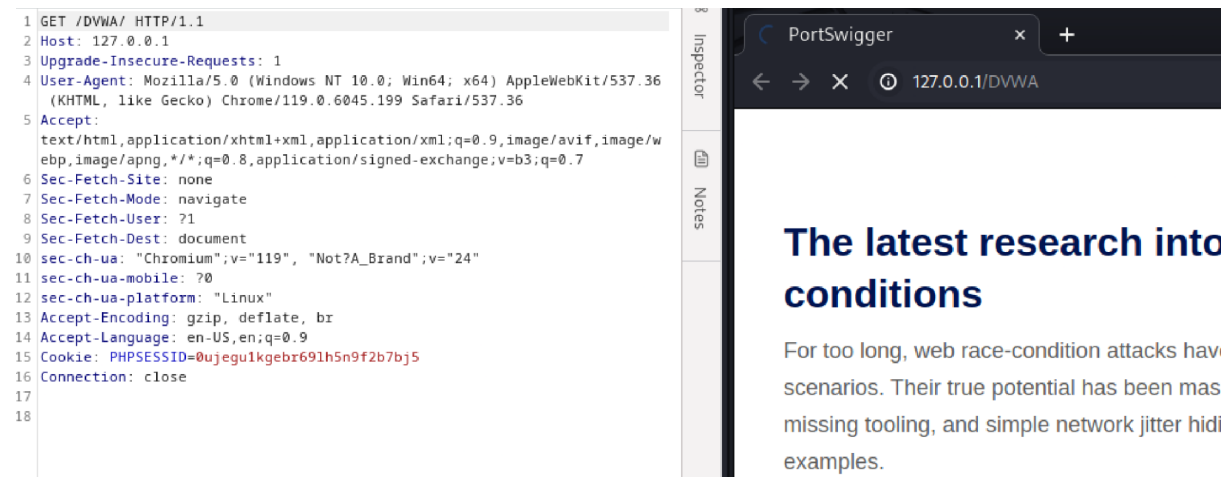
1. Low - This security level is completely vulnerable and **has no security measures at all**. It's use is to be as an example of how web application vulnerabilities manifest through bad coding practices and to serve as a platform to teach or learn basic exploitation techniques.
2. Medium - This setting is mainly to give an example to the user of **bad security practices**, where the developer has tried but failed to secure an application. It also acts as a challenge to users to refine their exploitation techniques.
3. High - This option is an extension to the medium difficulty, with a mixture of **harder or alternative bad practices** to attempt to secure the code. The vulnerability may not allow the same extent of the exploitation, similar in various Capture The Flags (CTFs) competitions.
4. Impossible - This level should be **secure against all vulnerabilities**. It is used to compare the vulnerable source code to the secure source code.
Prior to DVWA v1.9, this level was known as 'high'.

Low

Submit

>>>Apriamo un nuovo browser con Burpsuit

>>>Digitiamo il sito 127.0.0.1/DVWA

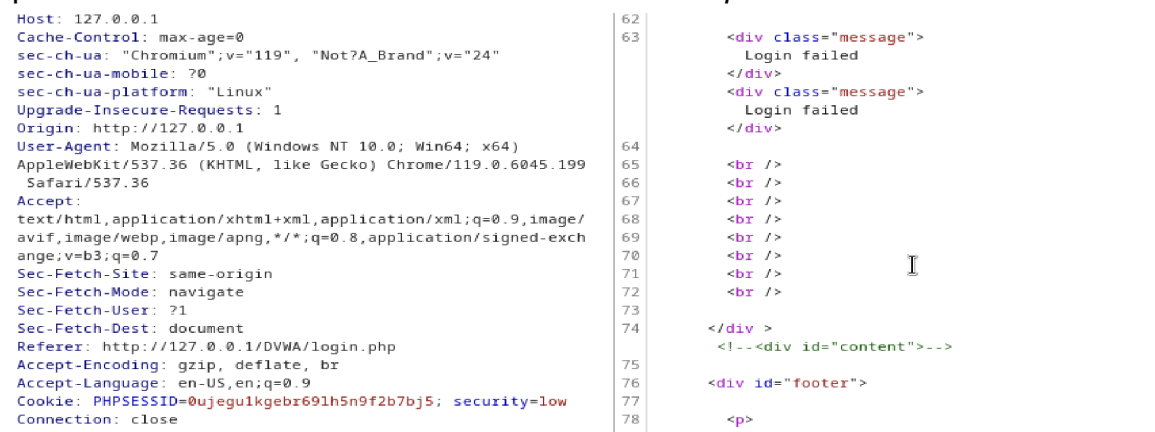


Nella parte di sinistra possiamo vedere tutti i dati di chrome che sta cercando di raggiungere il sito DVWA. Con il comando Forward, cliccando 2 volte andiamo avanti nella procedura del sito(confermiamo che la pagina web può proseguire).



Quindi arriviamo alla pagina di login inseriamo i dati e Burpsuite ci rimanda nuovamente quello che abbiamo inserito.

A questo punto della procedura noi potremmo andare a cambiare username e password inseriti attraverso il comando *sent to reaper* modifichiamo il e inviamo.



Nella parte destra del html ci darà l'informazione che il login è fallito in quanto user e password non sono quelli corretti.

Mentre con user e password corretti possiamo entrare alla pagine e andare a cambiare al suo interno quello che preferiamo.

The image shows a Burp Suite interface on the left and a web browser on the right. The browser displays the 'Welcome to Damn Vulnerable Web Application' page. The Burp Suite interface shows the 'Proxy' tab selected, with the 'Intercept' button highlighted. Below the browser, a list of HTTP request details is visible, including headers like 'Sec-Fetch-Site', 'Sec-Fetch-Mode', 'Sec-Fetch-User', 'Sec-Fetch-Dest', 'Referer', 'Accept-Encoding', 'Accept-Language', 'Cookie', and 'Connection'. The 'Cookie' header shows 'PHPSESSID=0ujegu1kgebr69lh5n9f2b7bj5; security=impossible'. The 'Referer' header shows 'http://127.0.0.1/DVWA/security.php'. The 'Accept-Encoding' header shows 'gzip, deflate, br'. The 'Accept-Language' header shows 'en-US,en;q=0.9'. The 'Connection' header shows 'close'. The 'security=low&seclev_submit=Submit&user_token=2c5a307544da8d55c5c09efb4ba488e3' is visible in the request body.

3 Sec-Fetch-Site: same-origin
4 Sec-Fetch-Mode: navigate
5 Sec-Fetch-User: ?1
6 Sec-Fetch-Dest: document
7 Referer: http://127.0.0.1/DVWA/security.php
8 Accept-Encoding: gzip, deflate, br
9 Accept-Language: en-US,en;q=0.9
0 Cookie: PHPSESSID=0ujegu1kgebr69lh5n9f2b7bj5; security=impossible
1 Connection: close
2
3 security=low&seclev_submit=Submit&user_token=2c5a307544da8d55c5c09efb4ba488e3

in questo caso il livello di sicurezza.