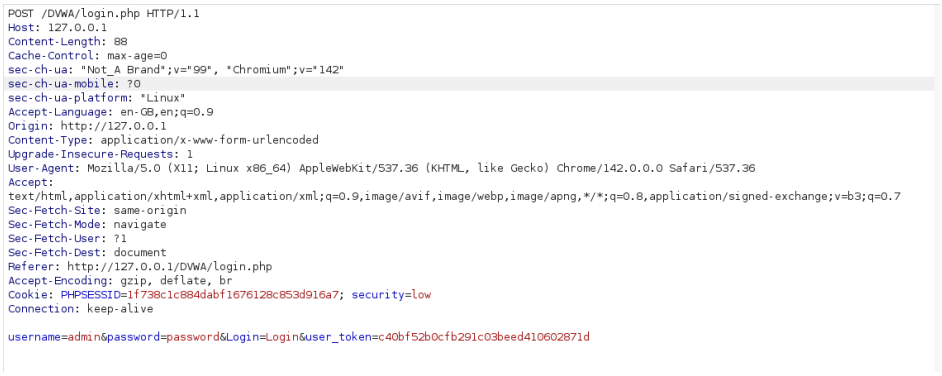
Raul Pastor

BURPSUITE

Per l'esercizio su Burpsuite ho installato Burpsuite (perché non era presente su Kali) e ho impostato la DVWA settando Mysql e Apache2.
Per ogni livello di sicurezza ho verificato le differenze.

Livello low:



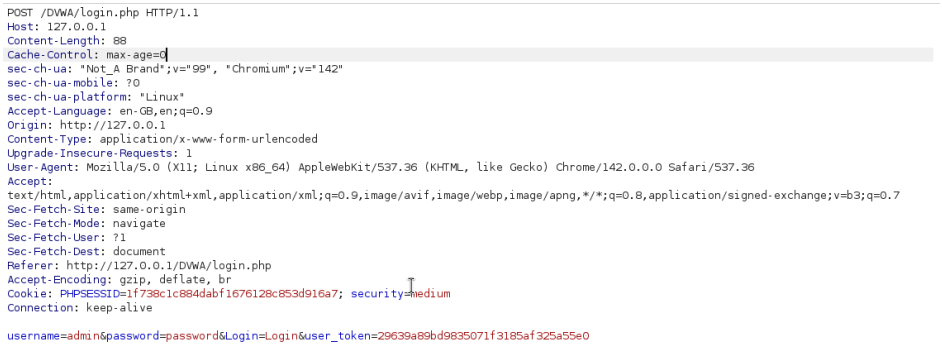
```
POST /DVWA/login.php HTTP/1.1
Host: 127.0.0.1
Content-Length: 88
Cache-Control: max-age=0
sec-ch-ua: "Not_A Brand";v="99", "Chromium";v="142"
sec-ch-ua-mobile: ?0
sec-ch-ua-platform: "Linux"
Accept-Language: en-GB,en;q=0.9
Origin: http://127.0.0.1
Content-Type: application/x-www-form-urlencoded
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/142.0.0.0 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: PHPSESSID=1f738c1c884dabf1676128c853d916a7; security=low
Connection: keep-alive

username=admin&password=password&Login=Login&user_token=c40bf52b0cfb291c03beed410602871d
```

In questo livello:

- L'applicazione accetta quasi qualsiasi modifica fatta con Burp Suite.
- Se si inviano credenziali sbagliate o manipolate, semplicemente compare **"Login failed"**.

Livello medium:



```
POST /DVWA/login.php HTTP/1.1
Host: 127.0.0.1
Content-Length: 88
Cache-Control: max-age=0
sec-ch-ua: "Not_A Brand";v="99", "Chromium";v="142"
sec-ch-ua-mobile: ?0
sec-ch-ua-platform: "Linux"
Accept-Language: en-GB,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/142.0.0.0 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: PHPSESSID=1f738c1c884dabf1676128c853d916a7; security=medium
Connection: keep-alive

username=admin&password=password&Login=Login&user_token=29639a89bd9835071f3185af325a55e0
```

In questo livello:

- Se provi a inviare richieste modificate da Burp, a volte non funzionano più.
- L'app effettua un po' più di controlli, quindi alcune alterazioni non hanno alcun risultato visibile.

Raul Pastor

Livello high:

```
POST /DVWA/login.php HTTP/1.1
Host: 127.0.0.1
Content-Length: 88
Cache-Control: max-age=0
sec-ch-ua: "Not_A Brand";v="99", "Chromium";v="142"
sec-ch-ua-mobile: ?0
sec-ch-ua-platform: "Linux"
Accept-Language: en-GB,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/142.0.0.0 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: PHPSESSID=1f738c1c884dabf1676128c853d916a7; security=high
Connection: keep-alive

username=admin&password=password&Login=Login&user_token=065fdaa1e8562fb3ed7eeb0e41c615a6
```

In questo livello:

- Anche se modifichi username e password in Burp, l’applicazione continua sempre a rispondere con **“Login failed”**.
- Qualsiasi richiesta “strana” tende a essere rifiutata senza dare messaggi speciali.