## Esercizio S3-L3 Epicode

Studente: Simone Mininni

BurpSuite e DVWA

Attacco BruteForce:

Login page...



admin	
Password	

## Burpsuite Post method interception...

```
Forward Drop Interceptis on Action Openbrowser

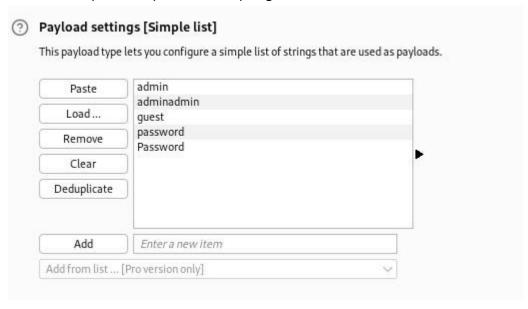
Pretty Raw Hex 

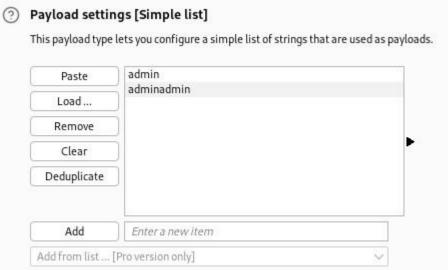
1 POST /DVMA/Login.php HTTP/1.1
2 Content-Length: 85
4 Cache-Control: max-age-0
5 sec-ch-ua: "Chromium";v="117", "Not;A=Brand";v="8"
6 sec-ch-ua-mobile: ?0
7 sec-ch-ua-platform: "Linux"
8 Ubgrade-Insecure-Requests: 1
9 Origin: http://127.0.0.1
0 Content-Type: application/x-ww-form-urlencoded
1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/117.0.5938.132 Safari/537.36
2 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
8 Sec-Fetch-Mode: navigate
5 Sec-Fetch-Mode: navigate
5 Sec-Fetch-Dest: document
7 Referer: http://127.0.0.1/DVMA/Login.php
8 Accept-Lendoding: gzjp, deflate, br
9 Accept-Language: en-US,en;q=0.9
0 Cookie: PHPSESSID=vr7r5Sefhfvug5k9f09444leie; security=lov
1 Connection: close
2 username=admin&passvord=admin&Login=Login&user_token=52fd86476ad167e81ad1cb4795e2733c
```

Send to Intruder per testare l'attacco brute force di tipo cluster bomb, identificando 2 payloads(username e password).



Inserisco le possibili password e poi gli username nella lista...





Procedo con l'attacco, individuando il payload1 admin e payload2 password restituiscono la pagina index.php.

