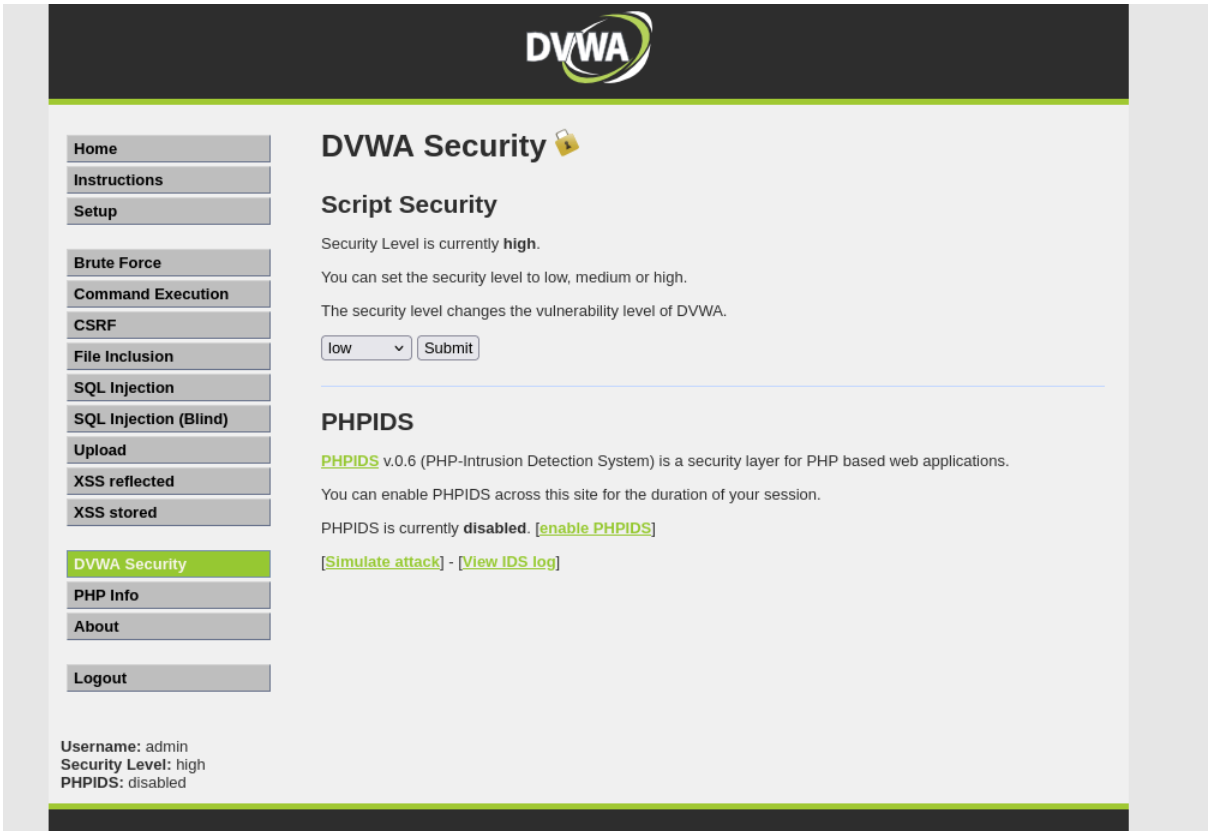
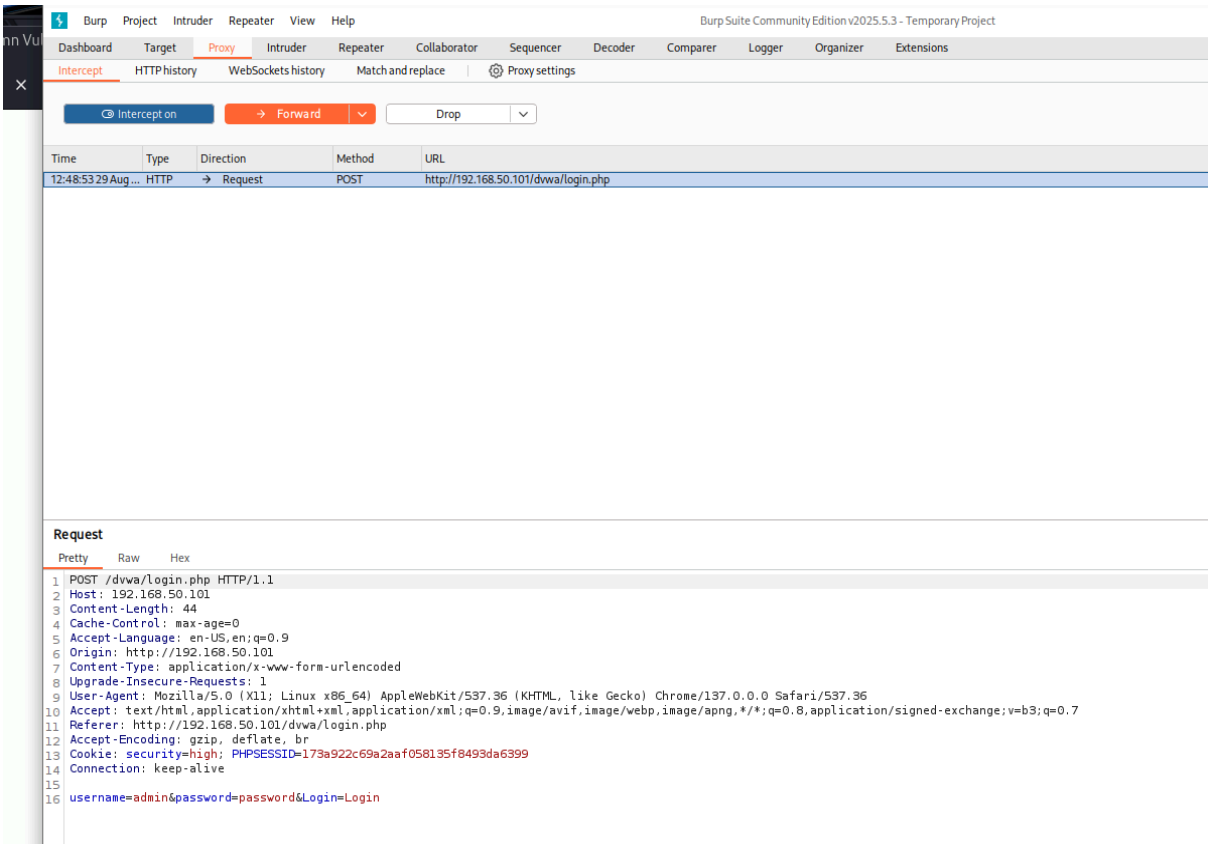
DVWA E BURPSUITE

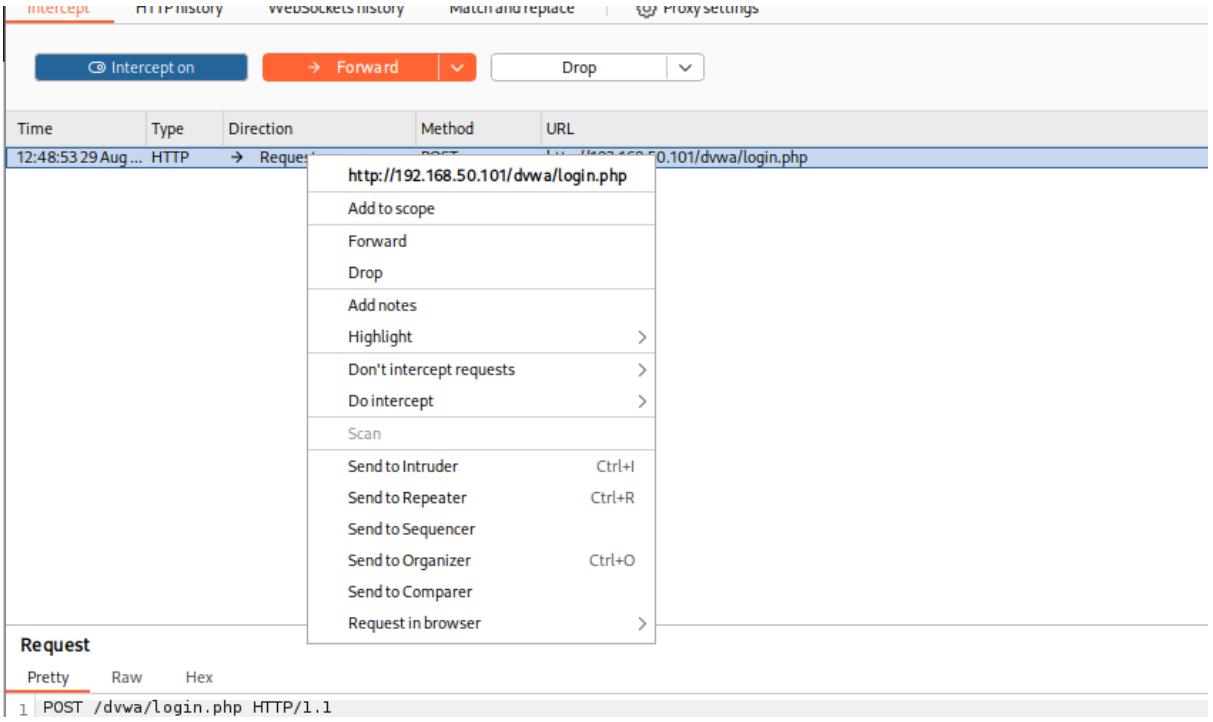
ho acceso la macchina di metaspoitable2 per accedere al servizio DVWA

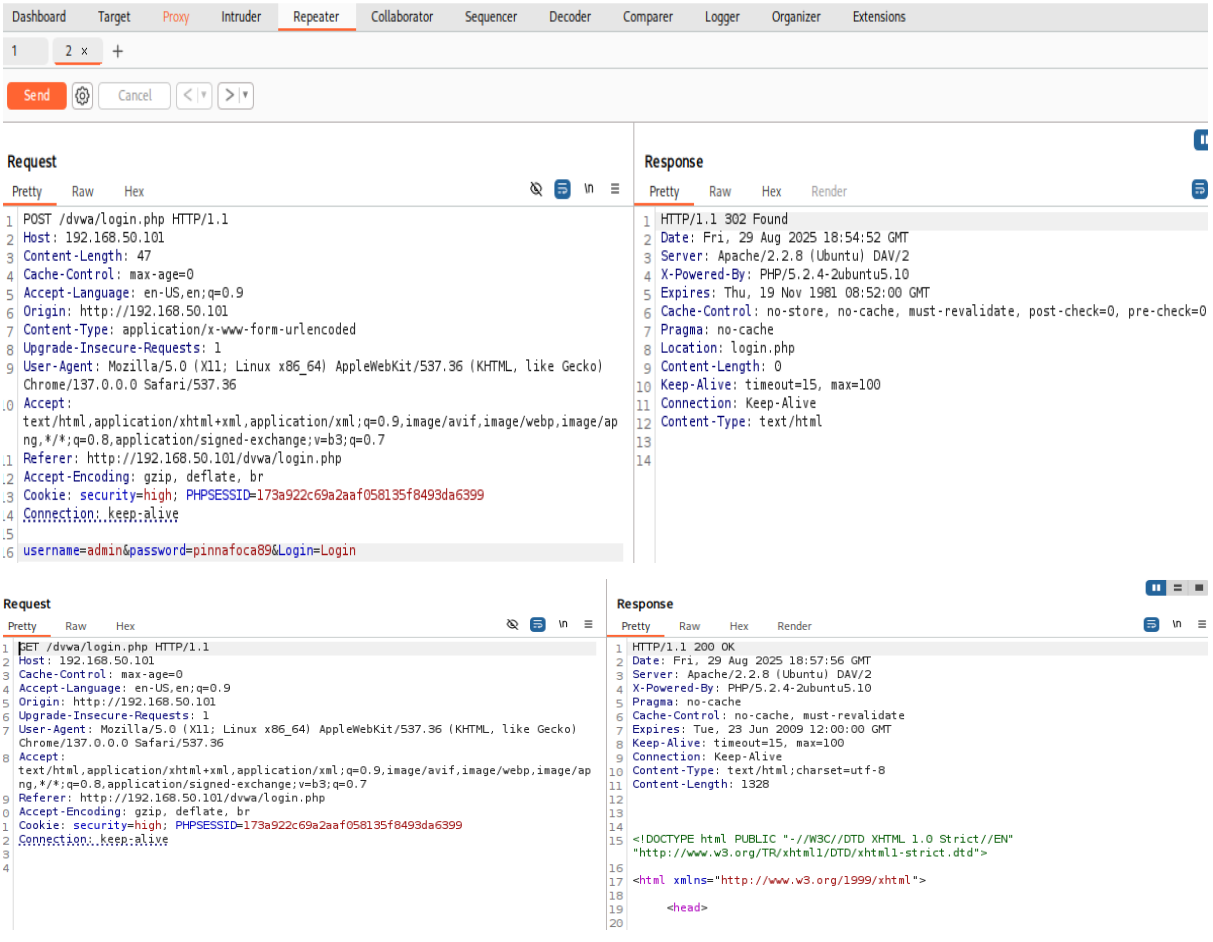


ho impostato il livello di sicurezza basso



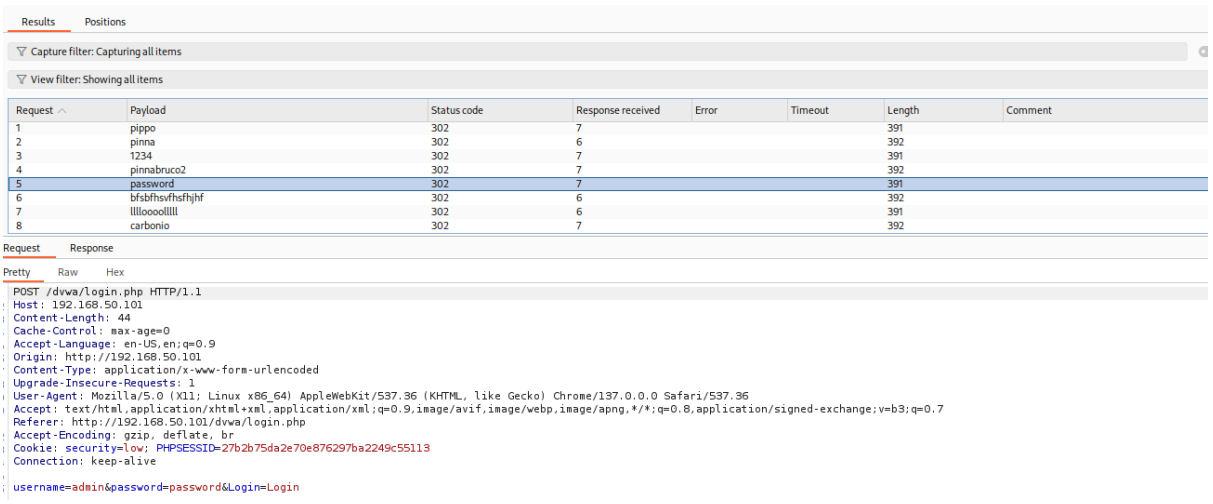
ho selezionato la proxy andando con il pulsante forward sono andata fino alla pagina del login e con le credenziali giuste sono entrata.





```
                    </p>
50
51              </fieldset>
52
53          </form>
54
55
56          <br />
57
58          <div class="message">
                Login failed
            </div>
59
60          <br />
61          <br />
62          <br />
63          <br />
64          <br />
65          <br />
```

sono andata poi su send to repeter ho modificato i parametri della pagina l'ho mandato e nelle risposta si legge login failed



View filter: Showing all items

Request	Payload	Status code	Respor
1	pippo	302	7
2	pinna	302	6
3	1234	302	7
4	pinnabruco2	302	7
5	password	302	7
6	bfsbfhsvfhsfhjhf	302	6
7	lllloooollllll	302	6
8	carbonio	302	7

Request Response

Pretty Raw Hex Render

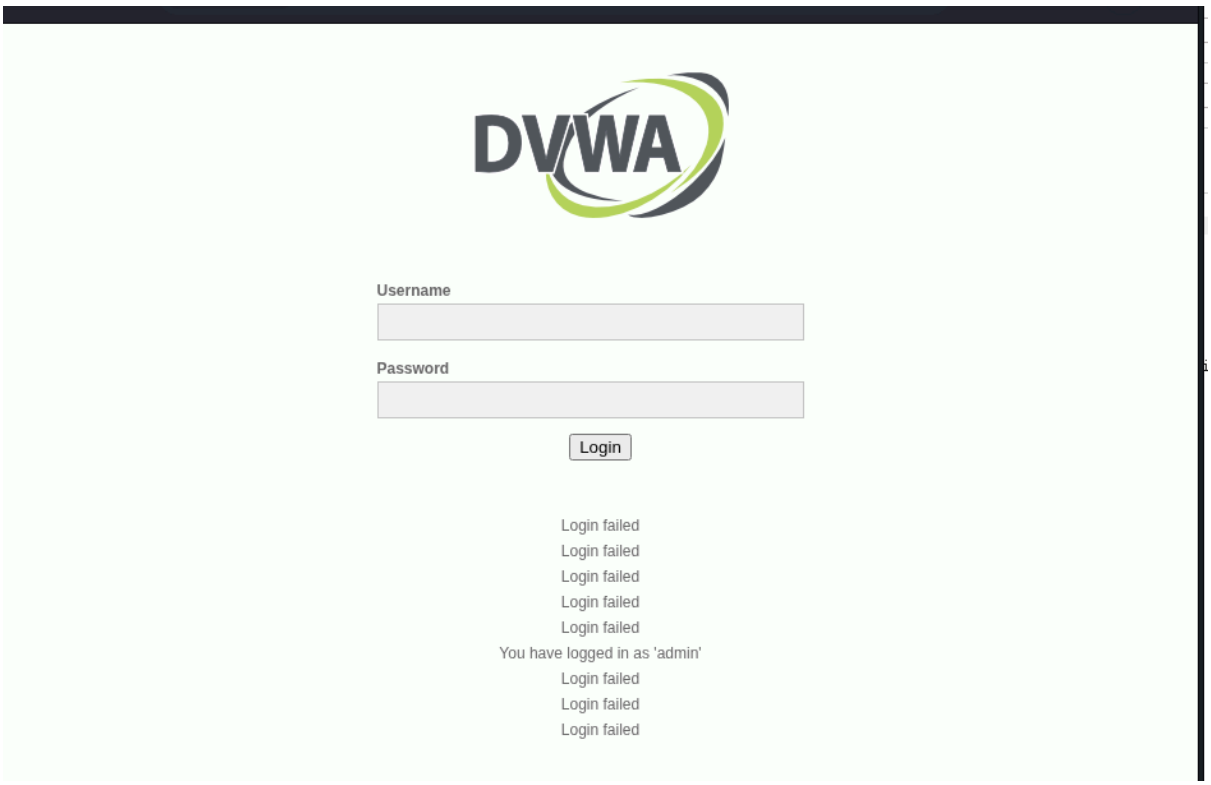
```
1 HTTP/1.1 302 Found
2 Date: Sun, 31 Aug 2025 12:49:33 GMT
3 Server: Apache/2.2.8 (Ubuntu) DAV/2
4 X-Powered-By: PHP/5.2.4-2ubuntu5.10
5 Expires: Thu, 19 Nov 1981 08:52:00 GMT
6 Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
7 Pragma: no-cache
8 Location: login.php
9 Content-Length: 0
10 Keep-Alive: timeout=15, max=97
11 Connection: Keep-Alive
12 Content-Type: text/html
```

Request	Payload	Status code
1	pippo	302
2	pinna	302
3	1234	302
4	pinnabruco2	302
5	password	302
6	bfsbfhsvfhsfhjhf	302
7	lllloooollllll	302
8	carbonio	302

Request Response

Pretty Raw Hex Render

```
1 HTTP/1.1 302 Found
2 Date: Sun, 31 Aug 2025 12:49:33 GMT
3 Server: Apache/2.2.8 (Ubuntu) DAV/2
4 X-Powered-By: PHP/5.2.4-2ubuntu5.10
5 Expires: Thu, 19 Nov 1981 08:52:00 GMT
6 Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
7 Pragma: no-cache
8 Location: index.php
9 Content-Length: 0
10 Keep-Alive: timeout=15, max=99
11 Connection: Keep-Alive
12 Content-Type: text/html
```



per modificare i parametri sono andata su send to intruder, sono andata poi su position ho fatto add selezionando il parametro password sono andata su payloads ho aggiunto una simple list caricato una lista di parole tra cui anche password ovvero quella giusta ho fatto start attack, ho cliccato una password sbagliata sono andata su response login.php ovvero login fallito poi ho cliccato sulla password giusta response index.php ovvero login riuscito.