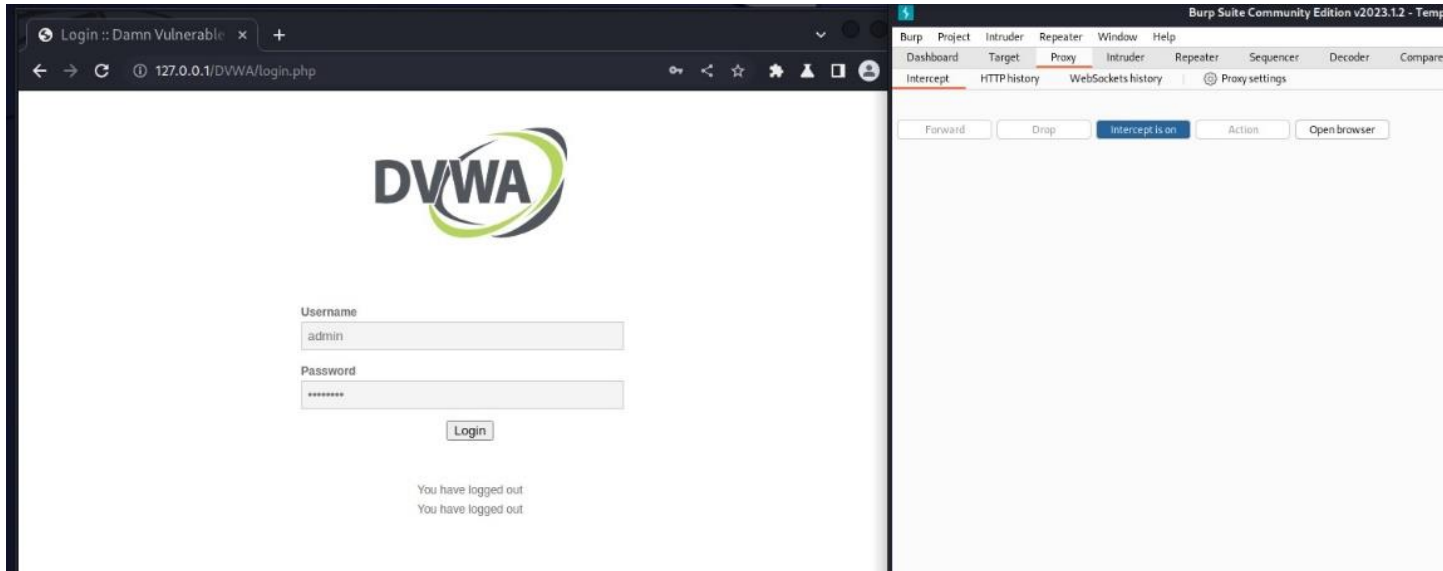
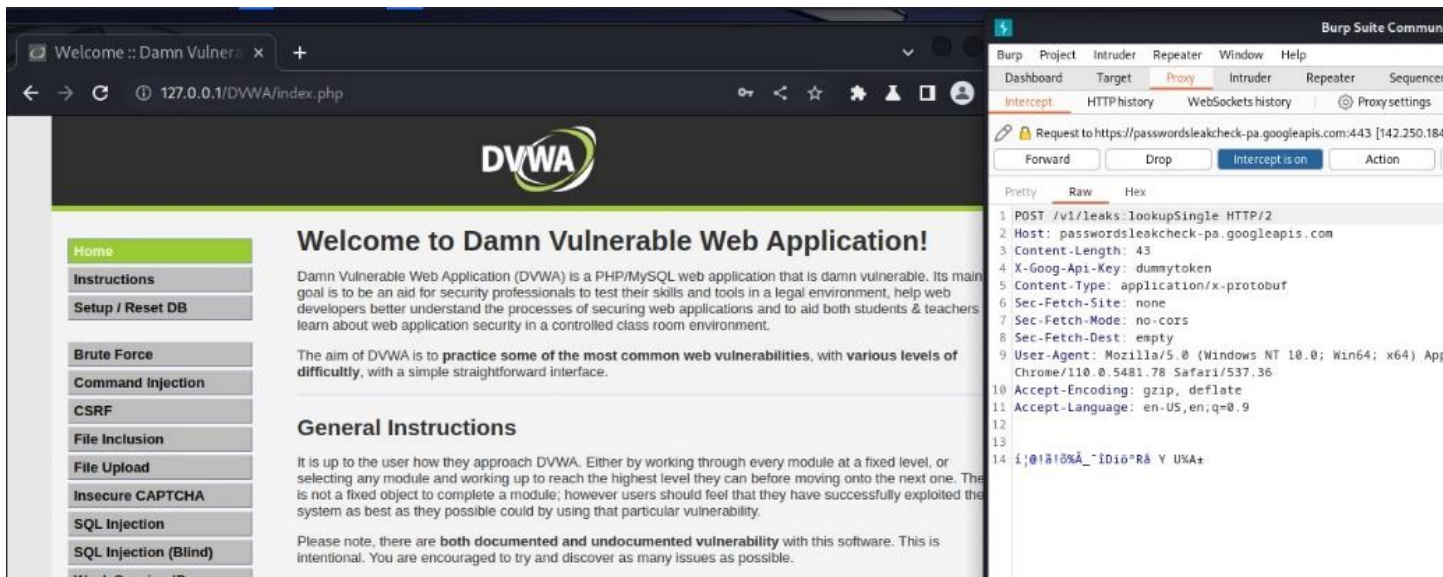


DVWA E BURPSUITE

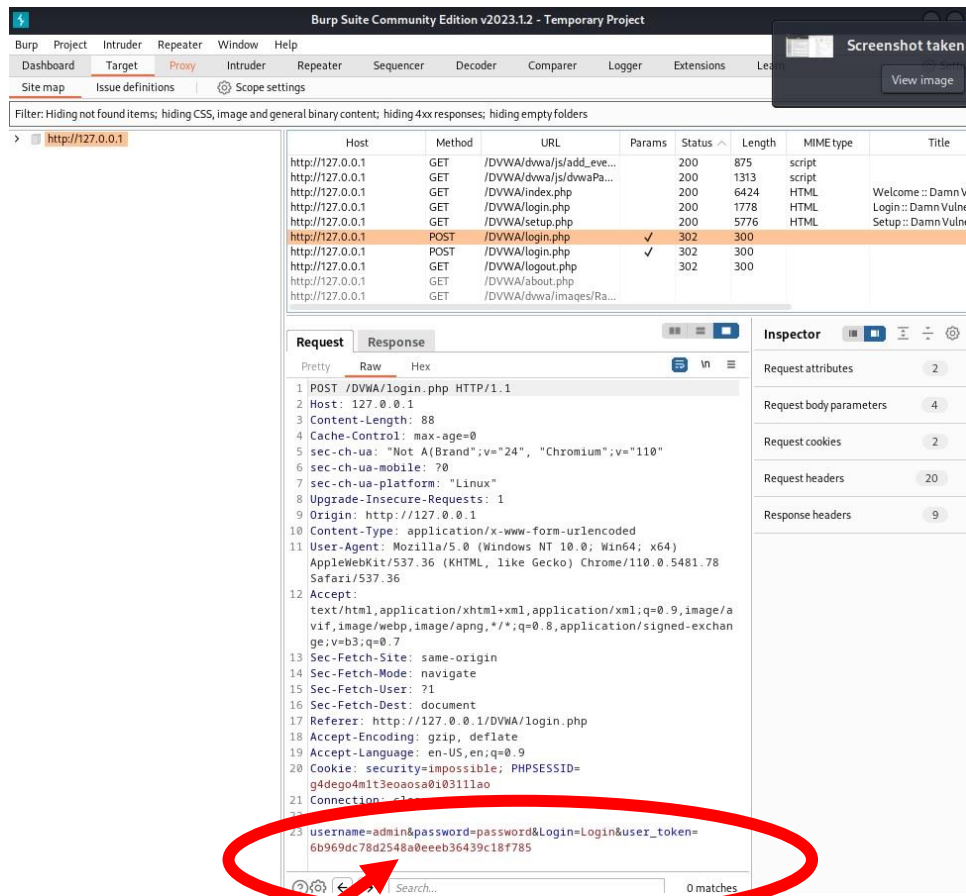
1) Ho effettuato il login con utente e password giusti (rispettivamente “admin” e “password”)



2) Ho intercettato la request con Burpsuite



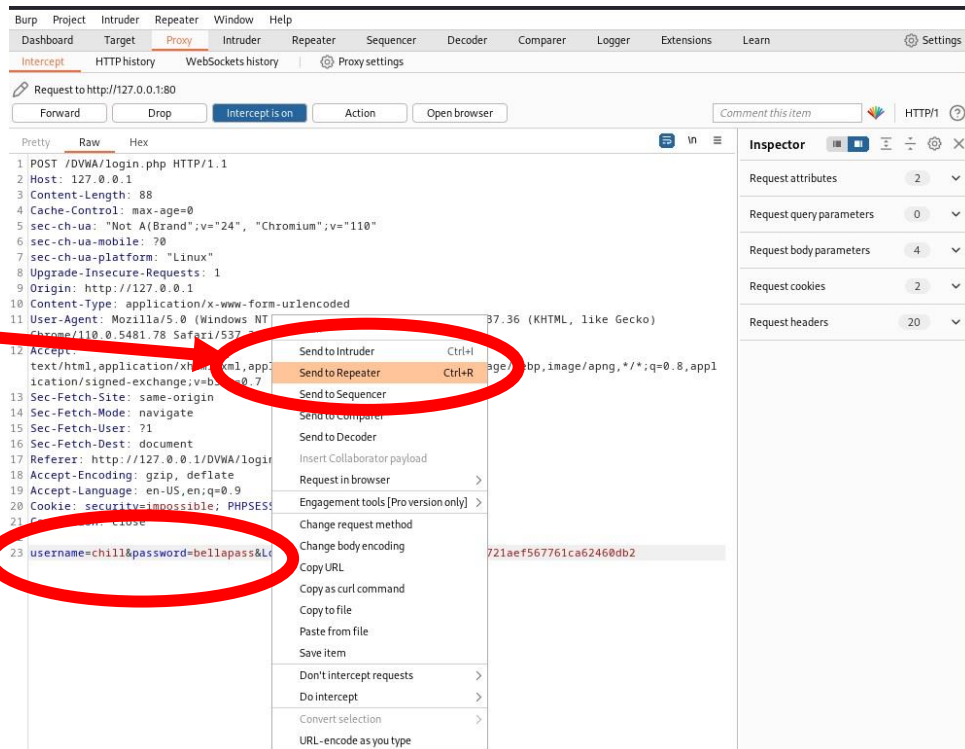
3) Mi sono spostato nella finestra Target dove ho aperto la request con metodo POST DVWA/login.php, che mi ha mostrato nome utente e password



Nello specifico ho trovato

- username = admin
- password = password

4) Ho modificato username e password (rispettivamente “chill” e “bellapassword” e ho inviato il risultato al Repeater



5) Ovviamente con le credenziali sbagliate che ho modificato non riesco ad accedere all'area riservata. Nel body dell' "http response" troviamo scritto **"login failed"**

The screenshot shows the Burp Suite interface with the 'Repeater' tab selected. The 'Request' section displays an HTTP GET request to /DVWA/login.php. The 'Response' section displays the HTML response, which contains multiple 'Login failed' messages. A red circle highlights the response body, and a red arrow points to it.

Request

```
1 GET /DVWA/login.php HTTP/1.1
2 Host: 127.0.0.1
3 Cache-Control: max-age=0
4 sec-ch-ua: "Not A(Brand";v="24", "Chromium";v="110"
5 sec-ch-ua-mobile: ?0
6 sec-ch-ua-platform: "Linux"
7 Upgrade-Insecure-Requests: 1
8 Origin: http://127.0.0.1
9 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
  Chrome/110.0.5481.78 Safari/537.36
10 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
11 Sec-Fetch-Site: same-origin
12 Sec-Fetch-Mode: navigate
13 Sec-Fetch-User: ?1
14 Sec-Fetch-Dest: document
```

Response

```
58
59 </form>
60
61 <br />
62
63 <div class="message">
  Login failed
</div>
<div class="message">
  Login failed
</div>
<div class="message">
  Login failed
</div>
<div class="message">
  Login failed
</div>
```

6) Infine, nella sezione “INTRUDER”, ho provato infine a fare un tentativo di “brute forcer” (con minimo e massimo 8 caratteri, con lettere da A alla Z e numeri da 0 a 9) per trovare la password dell’utente admin, invano.

Positions Payloads Resource pool Settings

Payload sets

You can define one or more payload sets. The number of payload sets depends on the attack type defined in the Positions tab. Various payload types are available for each payload set, and each payload type can be customized in different ways.

Payload: Payload count: unknown

Payload type: **Brute forcer** Request count: unknown

Payload settings [Brute forcer]

This payload set generates payloads that contain all permutations of a specified character set.

Character set:

Min length:

Max length:

Payload processing

You can define rules to perform various processing tasks on each payload before it is used.

Enabled	Rule
---------	------

Payload encoding

This setting can be used to URL-encode selected characters within the final payload, for safe transmission within HTTP requests.

☒ URL-encode these characters:

2. Intruder attack of http://127.0.0.1 - Temporary attack - Not saved to project file

Attack Save Columns

Results Positions Payloads Resource pool Settings

Filter: Showing all items

Request	Position	Payload	Status	Error	Timeout	Length	Comment
0			302	<input type="checkbox"/>	<input type="checkbox"/>	300	
1	1	aaaaaaaa	302	<input type="checkbox"/>	<input type="checkbox"/>	351	
2	1	baaaaaaa	302	<input type="checkbox"/>	<input type="checkbox"/>	351	
3	1	caaaaaaa	302	<input type="checkbox"/>	<input type="checkbox"/>	351	
4	1	daaaaaaa	302	<input type="checkbox"/>	<input type="checkbox"/>	351	
5	1	eaaaaaaa	302	<input type="checkbox"/>	<input type="checkbox"/>	351	
6	1	faaaaaaa	302	<input type="checkbox"/>	<input type="checkbox"/>	351	
7	1	gaaaaaaa	302	<input type="checkbox"/>	<input type="checkbox"/>	351	
8	1	haaaaaaa	302	<input type="checkbox"/>	<input type="checkbox"/>	351	
9	1	iaaaaaaa	302	<input type="checkbox"/>	<input type="checkbox"/>	351	
10	1	jaaaaaaa	302	<input type="checkbox"/>	<input type="checkbox"/>	351	
11	1	kaaaaaaa	302	<input type="checkbox"/>	<input type="checkbox"/>	351	
12	1	laaaaaaa	302	<input type="checkbox"/>	<input type="checkbox"/>	351	

59