

Ho provato a fare un intruder sul login, con qualche risultato

The screenshot displays the Burp Suite Community Edition v2023.10.3.5 interface. The main window shows the 'Intruder' tab with a list of payloads. A modal window titled '3. Intruder attack of http://127.0.0.1 - Temporary attack - Not saved to project file' is open, showing the results of the attack. The modal window has a table with columns: Request, Position, Payload, Status code, Error, Timeout, Length, and Comment. The table shows 10 requests, all with a status code of 302. The payloads are: admin:password123, user1:pass1, user2:pass2, guest:guest123, username:password, admin:password123, user1:pass1, user2:pass2, guest:guest123, and username:password. The modal window also has a 'Finished' bar at the bottom.

Payload settings [Simple list]

You can define one or more payload sets. The number of payload sets depends on the attack.

Payload set: 1 Payload count: 5
Payload type: Simple list Request count: 10

Payload processing

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

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: ./:=<>+&*~:~[]^*#

Choose an attack type

Attack type: Sniper

Payload positions

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

Target: http://127.0.0.1 Update Host header to match target

```
1 POST /DVWA/login.php HTTP/1.1
2 Host: 127.0.0.1
3 Content-Length: 75
4 Cache-Control: max-age=0
5 sec-ch-ua: "Chromium";v="119", "Not?A_Brand";v="24"
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/119.0.6045.159 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/DVWA/login.php
18 Accept-Encoding: gzip, deflate, br
19 Accept-Language: en-US,en;q=0.9
20 Cookie: security=impossible; PHPSESSID=ui48b0mj6e73lgrte6mlbb57p
21 Connection: close
22
23 username=556password=556Login=Login&user_token=c58fbe3466221d23422e04f8489b4187
```

2 payload positions

2 highlights Length: 957

KaliLinux con server giu [In esecuzione] - Oracle VM VirtualBox

File Macchina Visualizza Inserimento Dispositivi Aiuto

10. 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	Payload1	Payload2	Status code	Error	Timeout	Length	Comment
0			302	<input type="checkbox"/>	<input type="checkbox"/>	476	
1	admin	password	302	<input type="checkbox"/>	<input type="checkbox"/>	476	
2	user1	password	302	<input type="checkbox"/>	<input type="checkbox"/>	476	
3	user	password	302	<input type="checkbox"/>	<input type="checkbox"/>	476	
4	guest	password	302	<input type="checkbox"/>	<input type="checkbox"/>	476	
5	username	password	302	<input type="checkbox"/>	<input type="checkbox"/>	475	
6	admin	password123	302	<input type="checkbox"/>	<input type="checkbox"/>	476	
7	user1	password123	302	<input type="checkbox"/>	<input type="checkbox"/>	476	

Request Response

Pretty Raw Hex

```
1 POST /DWA/login.php HTTP/1.1
2 Host: 127.0.0.1
3 Content-Length: 91
4 Cache-Control: max-age=0
5 sec-ch-ua: "Chromium";v="119", "Not?A_Brand";v="24"
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/119.0.6045.159 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: security=impossible; PHPSESSID=jsq1d1ml8qp9ugt0q822esua0
21 Connection: keep-alive
22
23 username=username&password=password&Login=Login&user_token=eddc82b4a854280aef0efa0701497f01
```

0 highlights

Finished

CTRL (DESTRA)


Inspector

Request attributes 3 34 In

```

1 HTTP/1.1 200 OK
2 Date: Wed, 10 Apr 2024 16:52:48 GMT
3 Server: Apache/2.4.58 (Debian)
4 Expires: Tue, 23 Jun 2009 12:00:00 GMT
5 Cache-Control: no-cache, must-revalidate
6 Pragma: no-cache
7 Vary: Accept-Encoding
8 Content-Length: 1342
9 Connection: close
10 Content-Type:
text/html; charset=utf-8
11
12 <!DOCTYPE html>
13
14 <html lang="en-GB">
15
16   <head>
17
18     <meta http-equiv="
Content-Type" content="
text/html; charset=UTF-8" />
19
20     <title>
Login :: Damn Vulnerable
Web Application (DVWA)
</title>
21
22     <link rel="stylesheet" type=
"text/css" href="
dwa/css/login.css" />
23
24   </head>
25
26   <body>
27
28     <div id="wrapper">
29
30       <div id="header">
31
32         <br />
33
34         <p>

```

Request attributes	2	▼	Inspector
Request query parameters	0	▼	
Request body parameters	0	▼	
Request cookies	2	▼	 Notes
Request headers	18	▼	
Response headers	9	▼	