

Intercettazione Login e Password sulla DVWA attraverso BurpSuite

Burp Suite Community Edition v2024.4.5 - Temporary Project

Menu: Burp, Project, Intruder, Repeater, View, Help

Sub-menu: Dashboard, Target, Proxy, Repeater, Intruder, Collaborator, Sequencer, Decoder, Comparer, Logger, Organizer, Extensions, Settings

Intercept: HTTP history, WebSockets history, Proxy settings

Request to http://127.0.0.1:80

Forward, Drop, Intercept is on, Action, Open browser

Add notes, HTTP/1

Inspector

- Request attributes: 2
- Request query parameters: 3
- Request body parameters: 0
- Request cookies: 2
- Request headers: 16

Request details (Pretty view):

```
1 GET /DVWA/vulnerabilities/brute/?username=admin&password=password&Login=Login HTTP/1.1
2 Host: 127.0.0.1
3 sec-ch-ua: "Chromium";v="125", "Not.A/Brand";v="24"
4 sec-ch-ua-mobile: ?0
5 sec-ch-ua-platform: "Linux"
6 Upgrade-Insecure-Requests: 1
7 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
8 Gecko) Chrome/125.0.6422.112 Safari/537.36
9 Accept:
10 text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;
11 q=0.8,application/signed-exchange;v=b3;q=0.7
12 Sec-Fetch-Site: same-origin
13 Sec-Fetch-Mode: navigate
14 Sec-Fetch-User: ?1
15 Sec-Fetch-Dest: document
16 Referer:
17 http://127.0.0.1/DVWA/vulnerabilities/brute/?username=admin&password=admin&Login=Login
18 Accept-Encoding: gzip, deflate, br
19 Accept-Language: en-US,en;q=0.9
20 Cookie: PHPSESSID=270kk187vrr3brobhnnqesnsc; security=low
21 Connection: keep-alive
```

Event log (2) All issues

Memory: 122.6MB