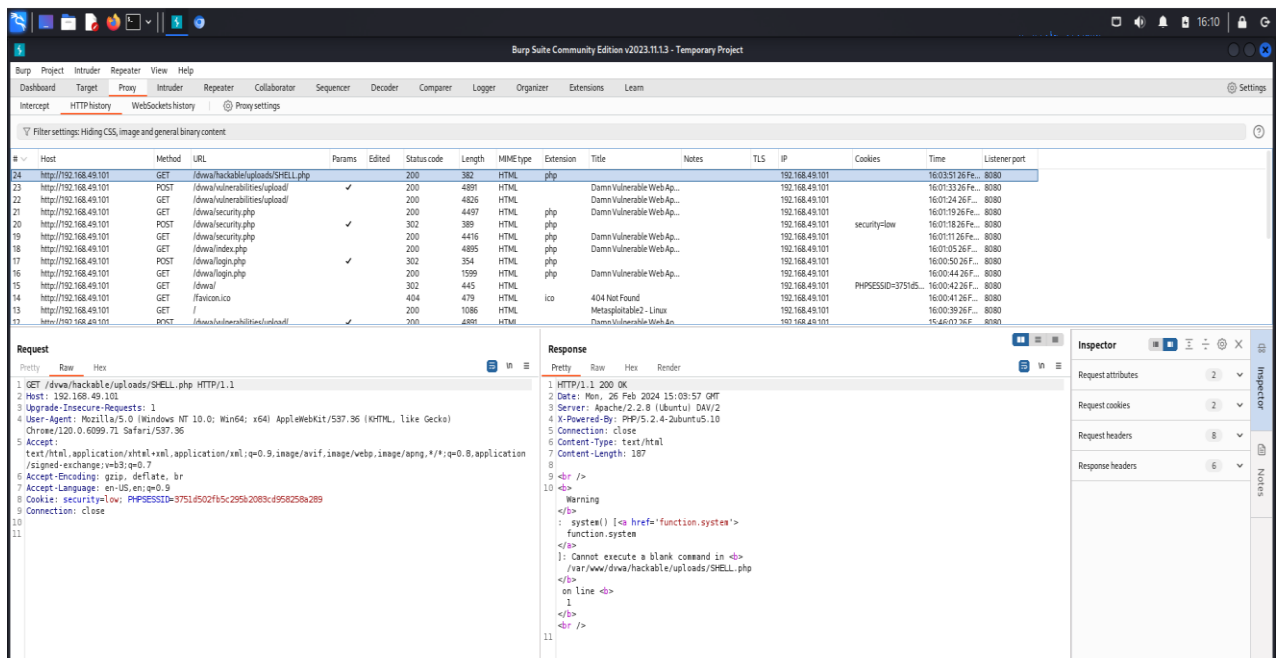


Una SHELL.PHP che ci permetterà la dimostrazione

Per l'intercettazione di tutto usiamo Burpsuite.

Se la shell verrà caricata correttamente visualizzeremo la seguente immagine.

Intercettazione Burpsuite:



Quando eseguiamo il comando `ls` nella barra url. La shell utilizzata ci permette di inserire un comando qualsiasi ed eseguirlo.

The screenshot shows a web browser window on the left with the address bar displaying `192.168.49.101/dwa/hackable/uploads/SHELL.php?cmd=ls`. The page content shows the output of the `ls` command: `SHELL.php ciao.php dwa_email.png`. On the right, the Burp Suite interface is open, showing the HTTP history and the details of the request and response. The request is a GET request to `/dwa/hackable/uploads/SHELL.php?cmd=ls` with a status code of 200. The response is an HTML document with a status code of 200, containing the output of the `ls` command.

The screenshot shows a web browser window on the left with the address bar displaying `192.168.49.101/dwa/hackable/uploads/SHELL.php?cmd=whoami`. The page content shows the output of the `whoami` command: `www-data`. On the right, the Burp Suite interface is open, showing the HTTP history and the details of the request and response. The request is a GET request to `/dwa/hackable/uploads/SHELL.php?cmd=whoami` with a status code of 200. The response is an HTML document with a status code of 200, containing the output of the `whoami` command.