Cross-Site Scripting Attack

11.1. In Listing 10.2 of the book, we added a check before sending the Ajax request to modify Samy's own profile. What is the main purpose of this check? If we do not add this check, can the attack be successful? How come we do not have such a check in the add-friend attack (Listing 10.1)? (3 points)

11.2. To defeat XSS attacks, a developer decides to implement filtering on the browser side. Basically, the developer plans to add JavaScript code on each page, so before data are sent to the server, it filters out any JavaScript code contained inside the data. Assume that the filtering logic is perfect. Can this approach prevent XSS attacks? (4 points)

11.3. A fellow student recommends implementing the secret token and same-site cookie countermeasures to be used to defeat XSS attacks. Which of these, if any, would help against such attacks? Why or why not? (2 points)

11.4. If you can modify browser's behavior, what would you add to the browser, so you can help reduce the risks of XSS attacks? Explain why your countermeasure would work. (4 points)

11.5. Why is the CSP (Content Security Policy) effective in defeating the Cross-Site Scripting attack? What is the downside of this approach? (2 points)

11.6. The following PHP code returns a web page. It also sets the CSP (Content Security Policy) for the JavaScript code running inside the page. Which JavaScript code is allowed to execute inside this page? Explain your answer. (6 points)

```
<?php
  $cspheader = "Content-Security-Policy:".
               "default-src 'self';".
               "script-src 'self' 'nonce-1rA2345' 'example.com'".
               "";
  header($cspheader);
?>
<html>
<script type="text/javascript" nonce="1rA2345">
  ... JavaScript Code ...                                          ❶
</script>

<script type="text/javascript" nonce="2rB3333">
  ... JavaScript Code ...                                          ❷
</script>

<script type="text/javascript">
  ... JavaScript Code ...                                          ❸
</script>

<script src="script.js"> </script>                                 ❹
```

```
<script src="https://example.com/script2.js"> </script>        ❺

<button onclick="alert('hello')">Click me</button>             ❻
</html>
```