Lab1: CSRF vulnerability with no defenses

**1. Summary**

**Bug Title:** Cross-site request forgery (CSRF).

**Severity:** Medium.

**Description:** Cross-Site Request Forgery (CSRF) is an attack that forces an end user to execute unwanted actions on a web application in which they’re currently authenticated. With a little help of social engineering (such as sending a link via email or chat), an attacker may trick the users of a web application into executing actions of the attacker’s choosing. If the victim is a normal user, a successful CSRF attack can force the user to perform state changing requests like transferring funds, changing their email address, and so forth. If the victim is an administrative account, CSRF can compromise the entire web application.

**Date Discovered:** 29/7/2024

**Status:** Solved.

**2. Bug Details**

**Vulnerability Type:** CSRF.

**Affected URL/Endpoint:** /my-account/change-emai endpoint

**Description:** There is a feature that allows authenticated users to change their email address by submitting a form. This feature is vulnerable to CSRF, enabling an attacker to forge the same request and execute it on behalf of the target user, leading to an unauthorized email change.

**Steps to Reproduce:**

1. Visit this URL: <https://portswigger.net/web-security/csrf/lab-no-defenses>

2. Click access lab to open the vulnarble application

3. Click on my account button and login using the following credentials: wiener:peter

4. After login there is a form to update the user email which us vulnarabe to CSRF

5. type any email then click submit and intercept the requet via burp suite and copy this request

6. visit this site: <https://csrf-poc-generator.vercel.app/> and paste the requet in the upper part and click generate PoC

7. copy result and change the vlaue of input filed to lol@lol.com or any email

8. click "Go to exploit server"

9. paste the generated HTML code into "Body" section and click "Deliver exploit to victim" button

10. Congratulations, you solved the lab!

**Impact:**  unwanted email change of the target account without knowing (Unauthorized Actions) which negatively impact the security posture if the application and lead to loss of control and reputation damage

**3. Recommendations**

* Use CSRF tokens.
* Use Strict SameSite cookie restrictions
* Validating the Referrer Header

**4. Conclusion**

**Summary:** The application has a feature allowing authenticated users to change their email addresses via form submission. However, this feature is vulnerable to Cross-Site Request Forgery (CSRF). An attacker can exploit this vulnerability to craft a malicious request that changes the user's email address without their consent which negatively impact on Security Posture by Unauthorized Actions, Loss of Control, Privacy Breach and Reputation Damage so it important to fix the bug to Protect User Accounts, Maintain Trust and Prevent Exploitation:

**5. Appendices**

**Tools Used:**

* burp suite.
* <https://csrf-poc-generator.vercel.app/>

**References:**

* <https://portswigger.net/web-security/csrf>
* <https://owasp.org/www-community/attacks/csrf>