Lab name: [CSRF vulnerability with no defenses](https://portswigger.net/web-security/csrf/lab-no-defenses)

Severity: Critical

Lab description:

* This lab demonstrates the CSRF vulnerability. This lab contains no CSRF tokens, or cookies.
* The goal is to create a webpage where the victim’s email is automatically updated to a malicious email that is set by the attacker.

Impact:

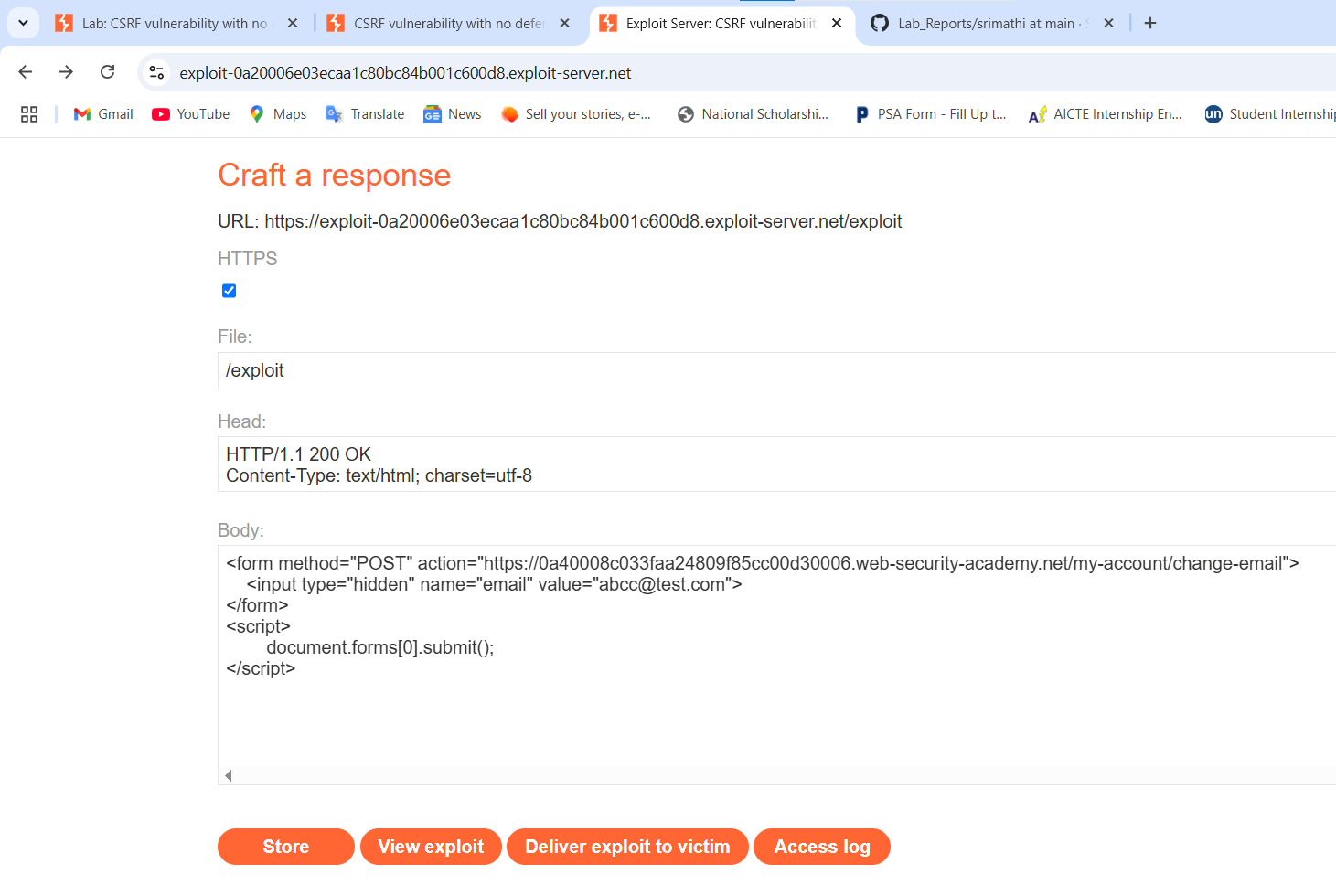
* The data is changed in the server without user’s knowledge, thus affecting the integrity.
* The user’s data might be extracted, thus affecting the confidentiality too.
* As integrity and confidentiality affected, the severity is critical.

Recommendations:

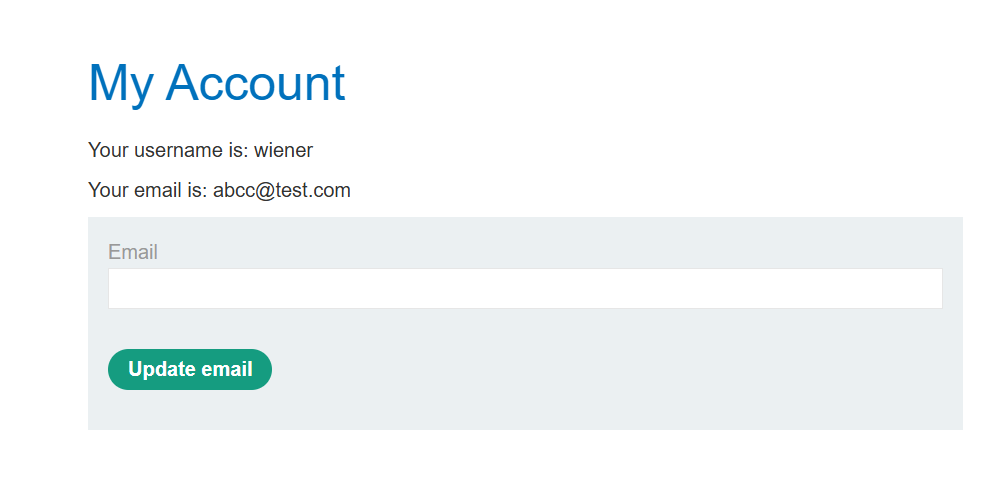
* In this case there are no CSRF tokens that are added, CSRF tokens are unique and unpredictable which adds more security by checking for the token each time the user tries to access anything.
* Use POST/PUT for making any changes because it is used to change data.
* Check referrer origins and other security headers.

Steps to reproduce:

1. Access the lab and login with the username and password
2. In the exploit server, enter the desired email in the input.



1. View and deliver the exploit to the victim.
2. This will update the email to the desired email.



1. Later, we cannot update the email too, it is because the URL that is provided in the form doesn’t exist.

