Lab name: [Clickjacking with form input data prefilled from a URL parameter](https://portswigger.net/web-security/clickjacking/lab-prefilled-form-input)

Severity: Critical

Lab description:

* The aim of this lab is to update the user’s email address just by creating another frame over the webpage. The attacker has to give their mail in the input form, so that the mail is updated to theirs.
* The vulnerability occurs because, there are no proper security headers or CSRF token that validates each session.

Impact:

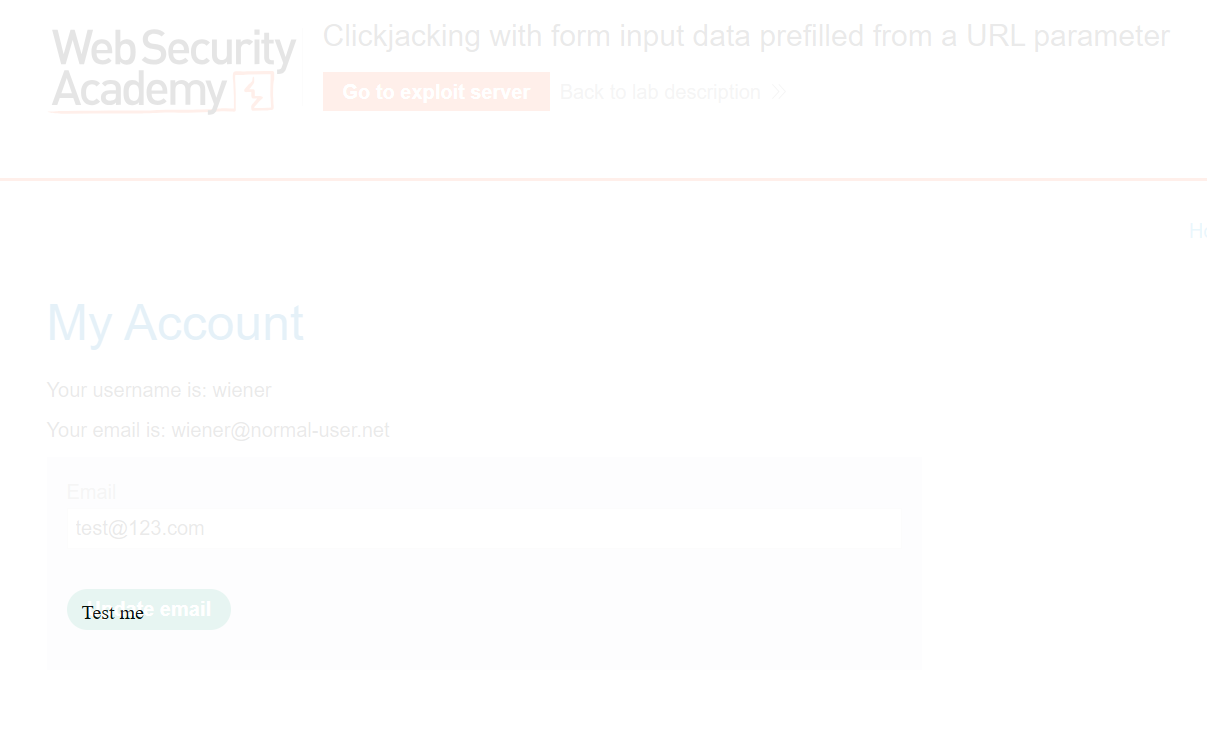
* Confidentiality and integrity both are affected in this case, so the severity is critical.
* Even though there are CSRF tokens, It can be bypassed because the form is submitted by the user itself.
* The browser sends the cookies which are the users.

Recommendations:

* Use X-Frame-options to prevent the webpage from loading the iframes.
* Use content-security-policy with frame-ancestors to avoid these types of issues.
* Ask user for confirmation to perform any actions.
* Don’t prefill sensitive fields using URL parameters.

Steps to reproduce:

1. Access the lab and login with the username and password provided.
2. Notice that after logging in, there is an update email button.
3. Go to the exploit server and check if the iframe tag works.
4. As it works, write a HTML code where the “click me” button is kept above the update email button and in the form set desired email.



1. Store and deliver this to victim, so solved the lab.