Lab name: [Basic clickjacking with CSRF token protection](https://portswigger.net/web-security/clickjacking/lab-basic-csrf-protected)

Severity: High

Lab description:

* Clickjacking is an attack where a malicious page tricks the user into clicking something on a different website, usually hidden inside an <iframe>.
* Clickjacking is a method where users are manipulated to perform certain tasks, and user gains something out of it.

Impact:

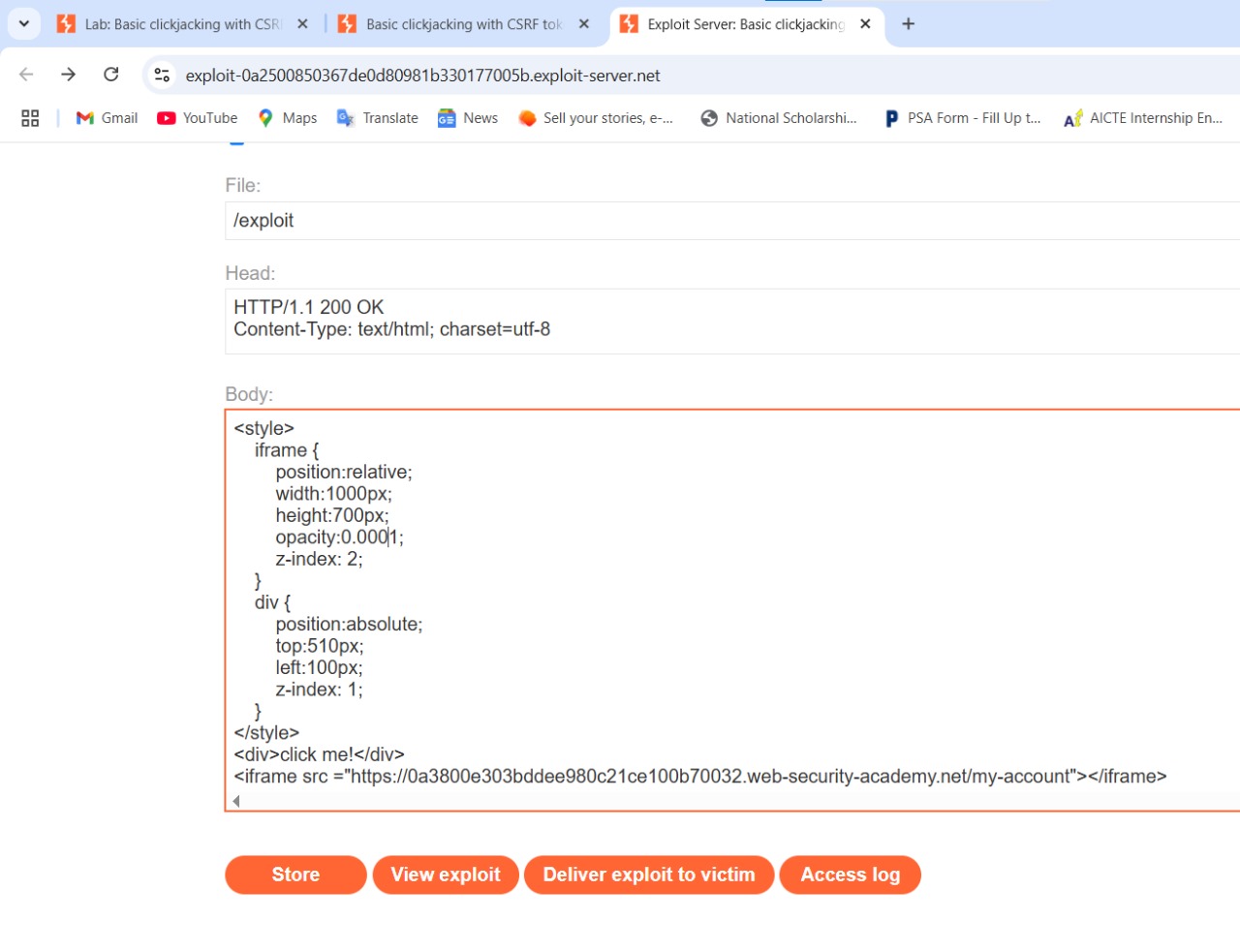
* The victim is triggered to perform some malicious actions, in this case the victim’s account gets deleted, the victim might not know how and why it happened.
* Although the application has CSRF tokens are available, the button is placed just above the delete button where CSRF token is sent along automatically
* If the user is logged in, the attacker can perform any actions through the user.
* This impacts integrity, which is why severity is high in this case.

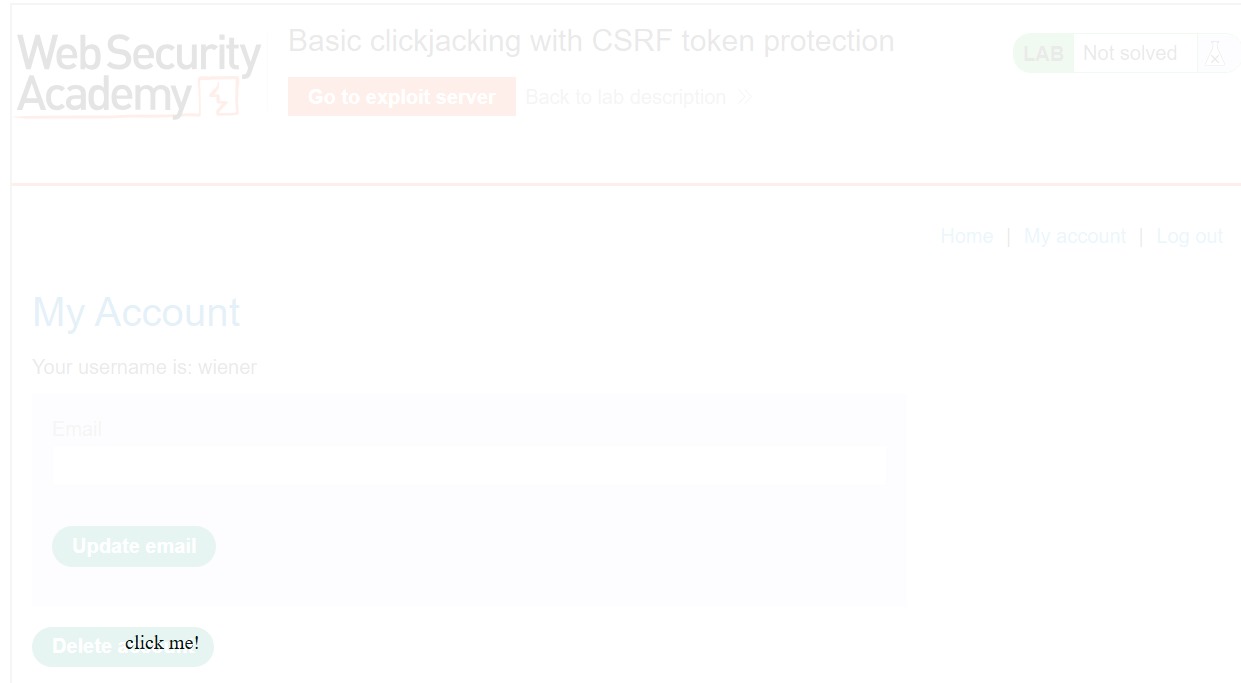
Recommendations:

* Usage of security headers like X-Frame-options header with same-origin value will prevent from performing this type of attacks.
* Use content-security-policy header with value frame-ancestors none to prevent embedding in the application.
* Avoid all allowing HTTP request methods like GET.

Steps to reproduce:

1. Open the lab, and login using the username and password provided.
2. Now notice that there is delete button after the user has logged in.
3. If the button is clicked, the user is vanished from the server.
4. In the exploit server, create a <iframe> tag just to check if it is working.
5. The tag works, now add a body and place a click me button which attracts the user.





1. Deliver this to the victim, thus the lab is solved.

The above picture can be more attractive to a normal user and if they click it, it deletes the account.