For this challenge set I am creating two websites, one that will be used as part accessing another. The two main concepts covered in this challenge set, is cross site scripting which we’ve covered in this course, and corss site request forgery, which is something new I hope to help students learn about in this challenge.

To start, I ask them open webiste A and B in separate tabs. On the website A, the student is given a hint to look at the source code. Inside the html a <form> post will be seen which is set up to delete the restriction on the second website. However, there is missing javascript that the student must inject into the website to perform cross site scripting. An example of the code they will need to inject can be seen here.

Once the correct code has been injected and the webpage automatically reloaded, the user will also refresh website B, but now the first website has sent a POST request to it which included a delete action that removed the earlier subscription. This is an example of cross site request forgery.

With the restriction lifted the user now must perform an SQL injection with the help of the hinted tools burp suite, which will be used to see the format in which the username and password are passwed to the server, and wfuzz which will be used for the automated SQL injection. Both tools can be found in kali linux.

After performing the automated sql injection the user will capture the flag.