

Sri Lanka Institute of Information Technology.

**Exploiting cross-site scripting to steal Cookies**

Web Security – IE2062

Group – 13.1 ( Y2S2 Cyber Security)

Student Details :

|  |  |
| --- | --- |
| Student ID | Student Name |
| IT20153540 | Abeywickrama O.D. |

B.Sc. (Hons) in Information Technology

specializing Cyber Security.

Go to the ports wigger website, then to academy, then to cross-site scripting, then to stealing cookies lab.

Then Before picking an access course, make a selection on the main page. Then Go to the solution section and copy the <script> that is mentioned. Then go to the lab.

Graphical user interface, text, application

Description automatically generated

When you first enter the lab, you'll see a few commercials. Choose one of them and click it.

A picture containing text, screenshot, person, person

Description automatically generated

Then Go to the comment section and paste the script you copied from the main page into the comment section.

Graphical user interface, text, application

Description automatically generated

Then launch the Burp collaborator client by turning on Burp Suite and going to the top left Burp column.

Graphical user interface, text, application

Description automatically generated

Then, under the Generate collaborator payload column, select "copy to clipboard."

And then put the link into the relevant path provided in the website's comment box.

A picture containing text

Description automatically generated

Then I submitted the remark, along with the code for getting the payloads.

Graphical user interface, text, application, email

Description automatically generated

Then go to Burp collaborator and press the poll button right now.

Graphical user interface, text, application

Description automatically generated

The collaborator will get the payloads, and we must select the appropriate http payload to proceed to the proper session. By scrolling down to the bottom of the http payload link.

Graphical user interface

Description automatically generated

Following some investigation, I discovered that some payloads had connections that have been closed, as well as a single session that states that the connection is kept alive.

So, I went ahead and copied the Session Code from that particular session.

Then I activated the interceptor and reloaded the page where I had left my remark.

Graphical user interface, application

Description automatically generated

Then I copied the burp collaborator's open session code and placed it into the interceptor's session column.

I also used interceptor to send the modified code.

Graphical user interface, text, application, email

Description automatically generated

It led me to another large source code after uploading, which I assumed was the session cookies.

As a result, I went through the cookies and discovered "Congratulations You Solved the Lab" as one of them.

Graphical user interface, text, application, email

Description automatically generated

After that, I disabled the interceptor and passed the retrieved code to the main site, which allowed me to finish the lab.

Chart

Description automatically generated with medium confidence

**Thank you.**

**IT20153540**

**Abeywickrama O.D.**