Lab 12

Chetan Sahrudhai Kimidi - ckimidi

***Abstract*—Learning about cross-site scripting and related attacks.**

I. Introduction

In this lab, I learnt about cross site scripting, XSS. I completed all the 1-12 sections, in WebGoat 8.

II. XSS: Steps 1-12

In Step 2, I used the console in Developer Tools, to enter the command ”alert(document.cookie);”. And this displayed the session id as seen in Fig. 1.
In Step 7, I used the alert() method in the credit card field to find that it was vulnerable, as suggested in the instructions. I used the following command, ”alert(1);”, in script tag, as seen in Fig. 2.
In Step 10, to find the test module, like the start.mvc#lesson, I used the Developer Tools Debugger, to find the MVC (Model View Controller) file hierarchy, and checked the files in view, to find a particular GoatRouter.js, in which I found the test route, as seen in Fig. 3, and finished the step as seen in Fig. 4.
I completed Step 11, in two ways, The first one was using/invoking the function in the console, and then entering that unknown number in the field, as seen in Fig. 5 and Fig. 6. But, it was advised to not use this way, instead use the test-route and find a way to find that number.
So, continuing from the section 10 , I used ”test route” and called webgoat.customjs.phoneHome(). Since the input after the ”test/” in the URL gets reflected, I can use that to call the javascript function webgoat.customjs.phoneHome(), using an XSS Payload. The payload I would use is as follows - ”webgoat.customjs.phoneHome()” in a script tag.
I ensured to URL Encode the payload before injecting it. Then, I visited the URL, and checked for a triggered HTTP request by the payload, found its response, and found the number, entered it and completed the task successfully. This whole process can be seen in Fig. 7, Fig. 8, Fig. 9 and Fig. 10.
In Step 12, I finished the quiz as seen in Fig. 11.

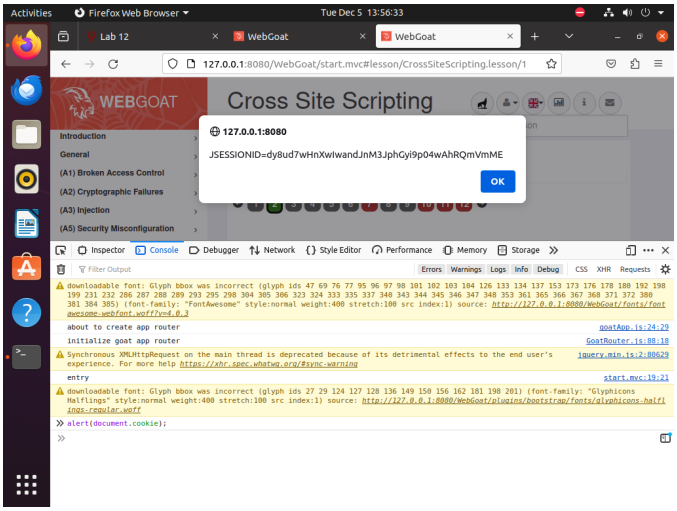

Fig. 1. JSESSION_ID

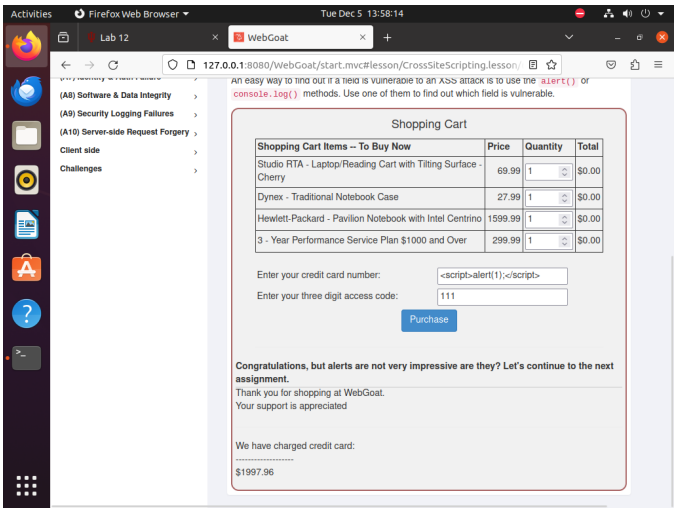

Fig. 2. Alert!

III. Conclusion

To conclude this lab exercise, I learnt about XSS, finished steps 1-12 in WebGoat 8 and successfully completed this lab and course.

References

[1] Cloudflare XSS
[2] OWASP XSS

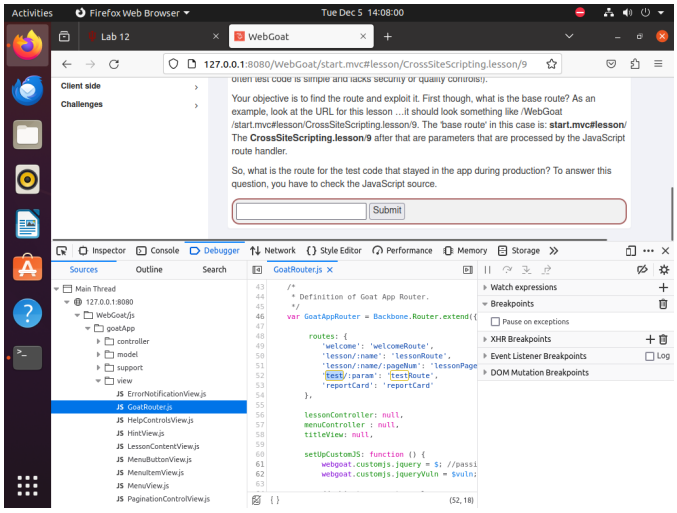

Fig. 3. Test Route

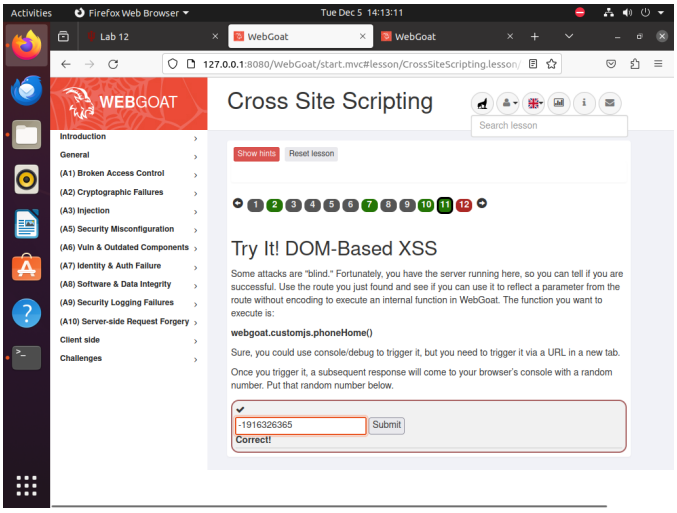

Fig. 6. Number found , BUT...

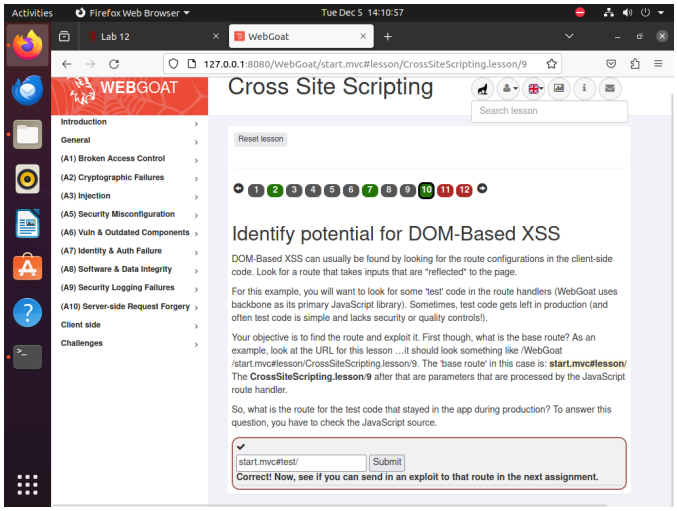

Fig. 4. #test found

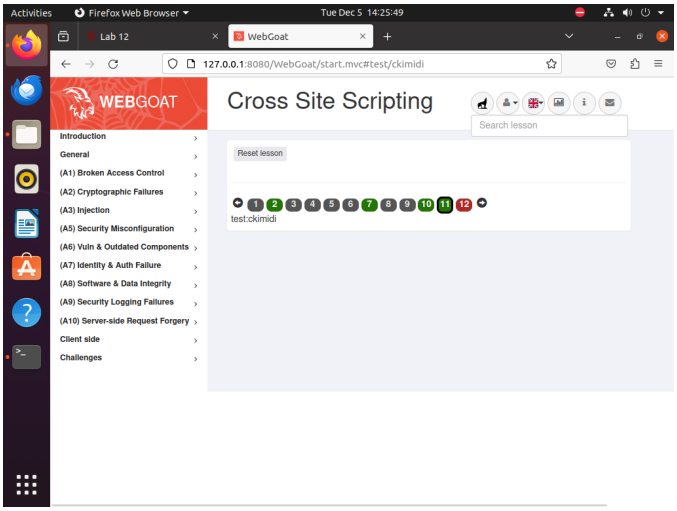

Fig. 7. test ckimidi

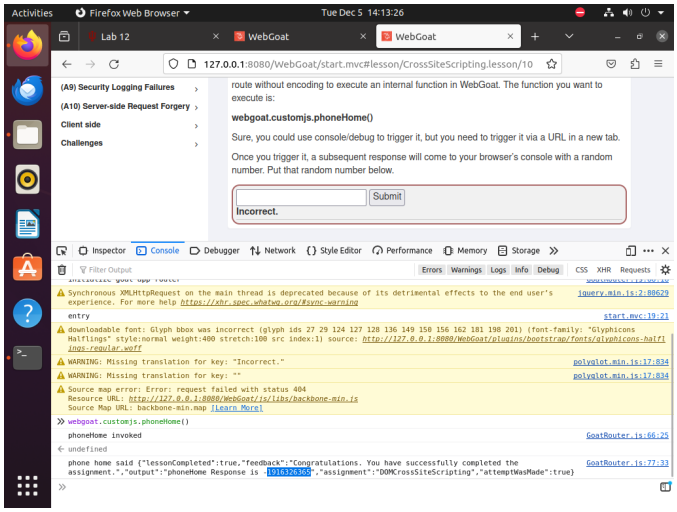

Fig. 5. Function invoked

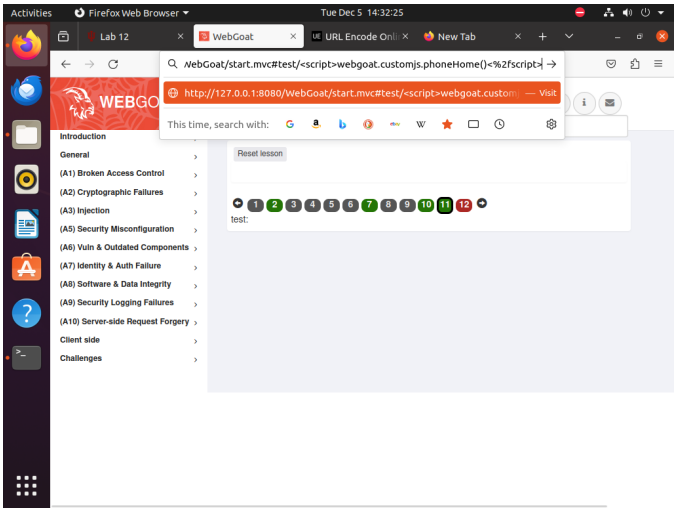

Fig. 8. URL injection

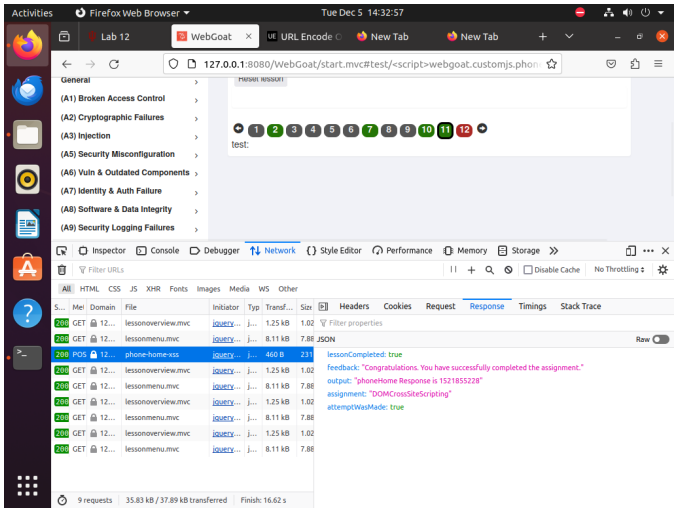

Fig. 9. HTTP response

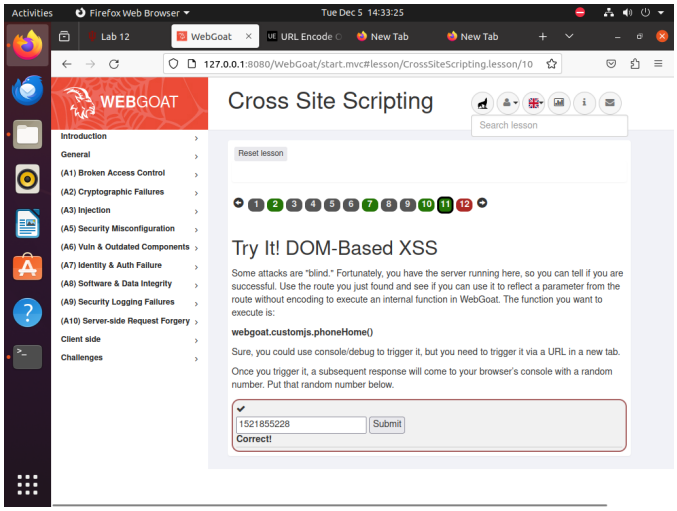

Fig. 10. Solved!

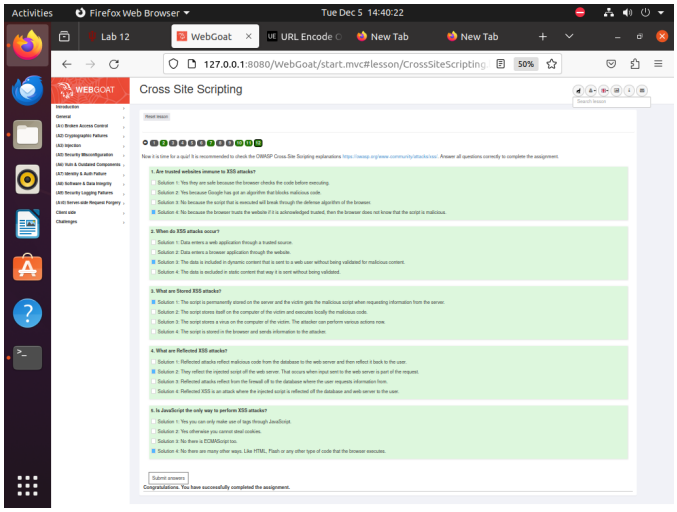

Fig. 11. Quiz done