National Taiwan Normal University
CSIE Information Security: A Hands-on Approach

Instructor: Po-Wen Chi
Due Date: Jan 3, 2022, AM 11:59

Assignment 6

Policies:

- Zero tolerance for late submission.
- Please pack all your submissions in one zip file. **RAR is not allowed!!**
- I only accept **PDF**. MS Word is not allowed.
- Hand-writing is not allowed.

6.1 SEED Lab (40 pts)

Cross-Site Scripting Attack Lab
https://seedsecuritylabs.org/Labs_20.04/Web/Web_XSS_Elgg/

Please record all your steps with screen captures and answer all questions. Undoubtedly, you need to complete all tasks even they are marked with **optional**.

6.2 Redirection (20 pts)

In the CSRF class, I have shown you how to use Javascript to launch the CSRF attack. Unfortunately, the page will be redirected to the target page and it will make the victim be aware of the attack event. How to make the victim stay at the same page? Please show me your approach.

6.3 HTTPS (20 pts)

Nowadays, we hope that all web services should be protected by the HTTPs channel. If you want to enable a HTTPs service, the certificate is mandatory and I think **Let's Encrypt** is a good candidate. This time, I want you to construct your own certificate.

This is what I want you to do. First, generate your own **root** certificate with the corresponding private key. Then, generate a certificate for a web service, which you may use the seed lab docker instance directly, and sign the certificate with the root key. Third, install the root certificate on your

browser. You must show the you can connect to the web service without any warnings.

6.4 XXE (20 pts)

In this problem, I want to show you how to perform an XML External Entity attack and how it can be abused and protected against. First, you need to download **webgoat**. **Webgoat** is a deliberately insecure application that allows interested developers just like you to test vulnerabilities commonly found in Java-based applications that use common and popular open source components. It is developed by the OWASP community. Start this application and complete the XXE tutorial. Note that there are three assignments there.