## Activity 9: Web Security Scanner

Instructors: Krerk Piromsopa, Ph.D

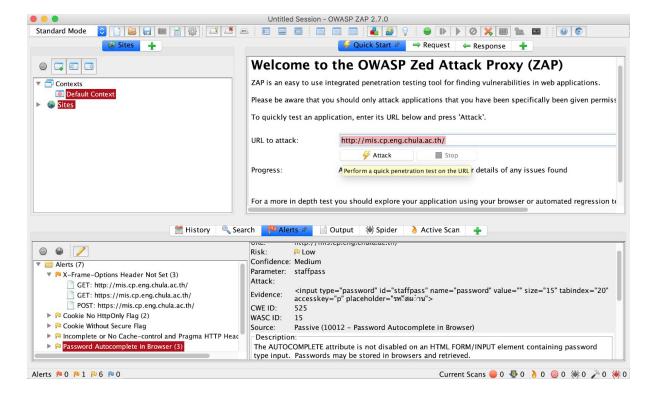
## Overview

With the web everywhere, we should learn the fundamentals of secure web application. In this activity, we will use OWASP Zed Attack Proxy<sup>1</sup> to test web applications.

## Exercise

- 1. We will try to test sites with OWASP ZAP. Run OWASP in ZAP in standard mode. \*\*\* Don't try attack mode with real sites. \*\*\* Test the following sites:
  - a. https://www.chula.ac.th/
  - b. https://www.eng.chula.ac.th/
  - c. https://www.cp.eng.chula.ac.th/
  - d. ... (You name it.) Facebook, Google?

What do you see?



<sup>&</sup>lt;sup>1</sup> https://www.zaproxy.org/

Computer Security
Dept. of Computer Engineering,
Chulalongkorn University.

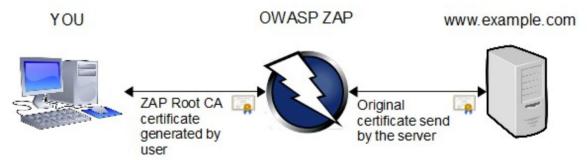
2. Use OWASP ZAP in proxy mode. (Install Web Driver Add-ons) Browse a web site (e.g. facebook) What do you see?

ZAP as proxy. By default, ZAP uses:

Address: localhost

Port: 8080

Do ZAP certificate (if needed)



3. Suppose that you are now a security analysis. Please scan 3 sites in the domain **chula.ac.th**. Identify possible security issues. Write a report (1-page A4) to suggest to the admin how to improve the security.

Owasp. org