Web Security

Prof. Yinzhi Cao
Fall 2018
Homework 2: Cross-site Scripting: Attack and Defense
Project due on October 9th in Blackboard

In this homework, we will explore and understand cross-site scripting (XSS) attacks, a type of Web-level injection attacks to bypass the same origin policy, from both the attack and defense perspectives.

We will finish the project via three steps:

(1) XSS exploit generation,
(2) vulnerability patching, and
(3) defense via Content Security Policy (CSP).

XSS Exploit Generation: In this step, we are going to play an XSS game (https://xss-game.appspot.com/) designed by Google. The game has six levels in total and you will need to finish all six levels, i.e., generating exploits for all six vulnerable websites, to finish this step.

Note that you need to write a report describing the logics behind the exploits, such as (i) where the vulnerable source code locates and (ii) how to trigger the vulnerability.

You need to submit both the report and the exploit code.

Vulnerability Patching: In this step, we will patch the vulnerable code that you exploited in the first step. Specifically, we have three sub-tasks here:

(i) Export all six vulnerable websites and rebuild them at your own server
(ii) Patch the vulnerable code
(iii) Write a report detailing your patches and instructions about how to run your website

Defense via Content Security Policy: Content Security Policy is an added layer of security to prevent XSS attacks. In this step, you are going to write CSP rules to defend against XSS attacks while still maintaining the website functionality. We will have two sub-tasks here:

(i) Write a set of CSP rules following CSP 1.0 (note that unsafe-eval and unsafe-inline, according to their name, should not be used; nonce and hashes are not supported in CSP 1.0.)
(ii) Write a set of CSP rules following CSP Level 2 or above (i.e., nonce derivative is allowed for inline scripts.)

[Bonus] Is your code secure? Once every group finishes their project, we are going to publish all the submissions on blackboard. If you find an additional vulnerability on defenses written by other groups, you will obtain bonus points.

Notes:

- For all three tasks, Please use Git to version-control your code development and submit your code as a ZIP file **through Blackboard**.