Lab 4 – Web Security Testing and Countermeasures

CS296N, Web Development 2: ASP.NET

Objectives

Get practice:

- Testing your web app using the Zed Attack Proxy
  - Passive testing
  - Active testing
- Reducing or eliminating security vulnerabilities in your app's code.

Instructions

Use OWASP ZAP to do both passive and active testing of your web app, then fix at least three of the security vulnerabilities identified in the alerts. Preferably, solve the highest priority issues. Only solve issues that can be fixed in your app's code, not issues that require changes to the server.

In order to solve the security issues, you will first need to do some research. Each pair of lab partners should choose one issue to research. Post a description of the issue you are researching in the course Moodle forum so that others will know to research different issues. When you have finished your research, share it with the class in the forum.

See the instructor's example posts in the forum for an idea of what to include in your posts.

Submission to Git and Moodle

Beta Version, Test Results and Code Review

1. Submit a document containing:
   a. A copy of the security alerts found by ZAP (just the alert descriptions, not all the web app endpoints).
   b. A copy of your security research.
2. Commit your security code fixes to a branch of your Git repository named lab4-security.
3. Send a pull request to your lab partner and to the instructor.
4. When you get pull request from your lab partner, do a review of their code.
5. On Moodle, enter the URL of your lab partner's git branch with your code review using "online text". Please do not put it in a comment.

Production Version

1. Merge your work into a branch named lab4-master.
2. Enter the URL of your master branch on Moodle using "online text". Please do not put it in a comment.
3. Optional: Enter the URL of your web site running online.

Written by Brian Bird, Lane Community College, winter 2019