# *Web Programming IV (420-H40-HR)*

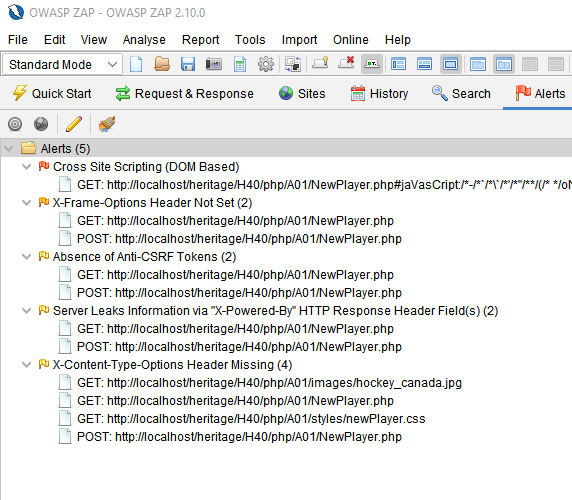
# *Assignment 2*

Date assigned: Wednesday, February 28th

Date due: Tuesday, April 2nd @ 11:59 PM

Part C – Securing your site

1. Run OWASP ZAP’s automated scan attack on your original Assignment 1. **Include the Alerts reports (like below). Ensure when you run it you have players created so that ZAP can test all functionality.**

Sample from Assignment 01: 

**Mine:**

A screenshot of a computer

Description automatically generated

1. **Using the Alert Reports and the techniques learned in class, plan out what changes you will make to your application.**

|  |  |
| --- | --- |
| Vulnerability | Planned change |
| Absence of Anti-CSRF Tokens | Implement a CSRF token for the forms |
| CSP Header Not Set | Set a CSP (excluding bootstrap & fonts) |
| Missing Anti-clickjacking Header | Implement a CSP for clickjacking (form-ancestor) |
| Server Leaks Information | Sanitize Inputs |
| Password Visible | Hash password |
| Strict-Transport-Security Header Not Set | Missing httponly & samesite attributes for cookies |

1. Update your code as planned (if necessary), making it more secure. You must also defend against all the vulnerabilities taught to you.
2. **Run OWASP ZAP against your more secure application. Include the Alerts below and the session files in the zipped up assignment:**

A screenshot of a computer

Description automatically generated

1. **Explain any remaining alerts. Is it a concern that should be addressed? Why or why not?**

Fixed: CSRF token, CSP headers, missing anti-clickjacking header, missing cookie parameters, sanitizing input.

Remaining: CSP alerts are most likely related to the fact that I allow bootstrap and an external source for my fonts. The Cross-Domain Misconfiguration is something we haven’t learned to fix yet. The loosely scoped cookies are referring to the PHPSESSID. CSP line in question:

header("Content-Security-Policy: default-src 'self'; font-src 'self' https://fonts.cdnfonts.com https://db.onlinewebfonts.com data:; style-src 'self' https://fonts.cdnfonts.com https://cdn.jsdelivr.net 'unsafe-inline'; script-src 'self' https://stackpath.bootstrapcdn.com 'unsafe-inline'; frame-ancestors 'none'; form-action 'self'");

**Marking Scheme**

|  |  |  |
| --- | --- | --- |
| **Part A/B - Advanced PHP** |  |  |
| Project Refactor |  |  |
| Using OOP |  | 10 |
| Checking file |  | 2 |
| Using all-in-one form |  | 10 |
| Login/Logout functionality |  |  |
| Create new user/store in file/associated to player |  | 10 |
| Login works as expected |  | 10 |
| Proper use of PHP hash |  | 7 |
| Password management |  | 7 |
|  |  |  |
| **Part C** |  |  |
| ZAP test results – A01 |  | 4 |
| Defense Plan |  | 6 |
| ZAP test results after the defense plan + session files |  | 4 |
| Secure and Robust |  | 6 |
|  |  |  |
|  |  |  |
| **Assignment Organization** |  |  |
| Site Design |  | 10 |
| Code Design/Efficiency/standards |  | 10 |
|  |  |  |
| Organization - Files named correctly; meaningful variable, class, object, method names; code formatting; correct submission to Moodle. |  | 4 |

**To submit**

When you have completed the assignment, zip the files as YourUserName\_H40A02 (including this document) and save the zip file to Moodle.