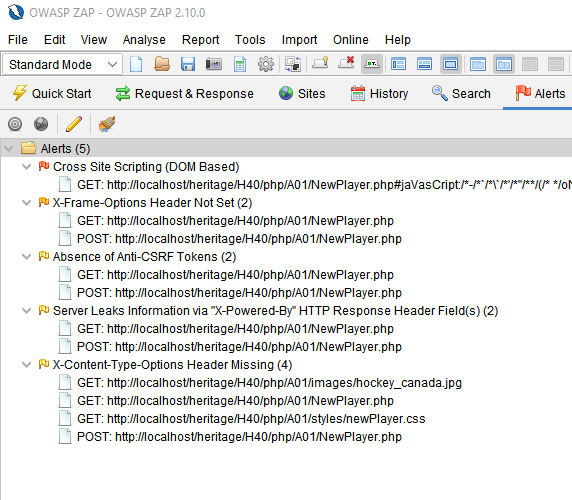
# *Web Programming IV A02 (420-H40)*

Part A - Updating the Application

1. Ensure your program is robust – it should be uncrashable and not have any errors or warnings! Use Postman to ensure you are not making any assumptions about data posted or queried for your assignment.

* htmlspecialchars + issets for fields
* secure/httponly for cookies (if used)

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

|  |  |
| --- | --- |
| Vulnerability | Planned change |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |

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:

<answer here>

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

<answer here>

OWASP ZAP – for details around authentication see: <https://play.vidyard.com/iErtsKxpwKn4m8iRoovtH9>

**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 |  | 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.