Cross Site Scripting: Lab Exercise
IN618 Security

Introduction

The marketing manager got a copy of *Head First PHP & MySQL* last week and now he thinks he's a programmer. His first project is a product review page that allows visitors to your company's web site to submit reviews.

Appeals to higher-ups for sanity have failed, so now your team must add this feature to the web site. You have been given the task of reviewing the code and correcting security mistakes before the pages go live.

1 Tasks

The initial code is available in the IN618 directory on the I: drive in a file named `xss-assignment.zip`. Get of copy of the code and assess its vulnerabilities to XSS exploits. Modify it so that

1. Vulnerabilities to XSS exploits are removed;
2. Input data is sanitised appropriately.

You can reasonably determine data validity criteria by inspecting the code.

2 Submission

Upload your completed code to your `public_html` directory on `sec-student.sqrawler.com`. Your files must be in a subdiectory named `xss-assignment`. Leave the filenames as they are in the original source files you received. Failure to follow these instructions will interfere with testing your work and will result in a loss of marks.

Your code must be uploaded and ready for testing by 1:00 PM on Monday, 16 March.

3 Resources

You should already have an account on the web server at `sec-student.sqrawler.com`. Upload your code there for testing and final submission.

4 Marking

There are 10 marks for this exercise:

- Sucessfully resisting XSS attacks performed by the lecturer: 5 marks;
- Correctly handling and sanitising user input data: 4 marks;
- Well formatted and readable code: 1 mark.