



Effectiveness of Hacking Mitigation Techniques

Callum Hall - BSC(Hons) Computing(Software Engineering)

Personal: callum.hall2010@gmail.com



This project is about web security and focuses on studying the effectiveness of hacking mitigation techniques on a modern website. Testing was done on these mitigation techniques

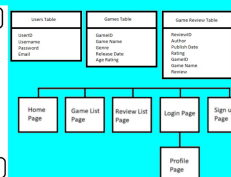
The first aim is to find the most effective method of security against common hacking methods. Another aim was to create two identical websites where one is secure and the other is not to test the mitigation techniques.

The objectives to aid in completion of the aims are:

- To research methods hackers use (SQL, XSS)
- To research mitigation techniques for common attacks
- Develop two websites where one is secure and the other is not
- Test each website by using common attacks such as SQL injection to see how good they are

- Research was done to aid the project.
- The most common type of attacks are injection based attacks
- Injection based attacks are usually done through SQL queries
- Cross-site scripting (XSS) is the second most common type of attack
- XSS can be detected by using automated tools or through technologies such as PHP
- Sensitive data exposure is the third most common type of attack
- This is when sensitive data that is stored on a database is exposed and does not have protection such as encryption

A prototype wireframe design and sitemap layout was made for the website.
A diagram of the database tables was also created to ensure there was no duplicate data.
The two websites were then created following the requirements and specification.

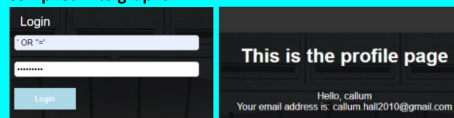
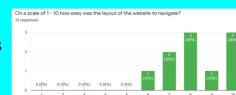


Code for sign up ^

There were various different types of testing done for this project.

- Usability testing was done to test the general usability of the website
- System Testing was done to make sure all the systems such as the login page and the databases all worked
- User testing was done to gather user feedback about the security and overall user experience of the website

There are a variety of results from each set of tests. SQL injection tests were done. Questionnaire results were also compiled into graphs.



In conclusion, a literature review was carried out to aid the project's development. The design and research methodologies were identified. The risks and limitations were also reviewed. The design and implementation stages were covered and the test results were analysed. Further studies could be to look into certain types of attacks more in depth or to propose a new solution to mitigate these attacks such as artificial intelligence.