Final Project

Web Application Using HTML, PHP and MySQL

Parker Daudt x17118379

M.Sc. Cyber Security

Due Date: 12/11/2017

**Background**

The purpose of this assignment is to develop a web application using HTML, PHP and MySQL with the intent to generate sample content relating to a particular topic, stored in a relational database. The application will exhibit the ability to insert, update and delete information within the database. The web application will take the form of a restaurant web page. The web page will feature a landing page, events page, contact page featuring a contact form, customer login and registration, a review page as well as pages featuring food and drink options available at the establishment.

**Technical Approach**

To accurately account for the security concerns addressed in the OWASP Top 10 research will be conducted with the purpose to investigate and understand the methods used by similar web sites to prevent attacks such as Cross-Site Scripting (XSS), Injection and Cross-Site Request Forgery (XSRF). Steps that will be taken to prevent similar attacks include input sanitation, password storage via encryption methods such as hash and salt, session management and appropriate security configuration.

OWASP Top 10

* Injection
  + Pages: Review, Contact, Customer Login, and Customer Registration are all protected against SQL injection by trimming, escaping and sanitizing each input.
* Broken Authentication
  + User credentials are properly stored, hashed and salted to ensure confidentiality. Pages use server-stored variables and authentication to prevent user credentials from being exposed in the browser.
* XSS
  + Review, Contact, Customer Login, and Customer Registration are properly protected by adding slashes, escaping html special characters, and trimming per input field.
* Insecure Direct Object References
  + Referenced objects are stored directly on the server, preventing a malicious user from gaining access to variables stored by a browser.
* Security Misconfiguration
  + Unnecessary default accounts and default applications were disabled or removed to prevent any unnecessary features from being enabled or installed. All web servers, and database servers are properly configured.
* Sensitive Data Exposure
  + All passwords are salted and hashed, any sensitive information is properly stored and encrypted, should the database be compromised. Extra protection is put in place during transit and at rest.
* Missing Function Level Access Control
  + Access control checks are present and prevent unauthorized access to sensitive information
* XSRF
  + Verification via RECAPTCHA and session variables are put in place on the Review, Contact, Customer Login, and Customer Registration pages to ensure that cross-site request are properly handled and prevented.
* Components with Known Vulnerabilities
  + Libraries and modules are up-to-date and no know vulnerabilities are present in the components being used.
* Unvalidated Redirects and Forwards
  + Destination pages are determined via validated user input and session variables rather than hard-coded links or references.

Several sources used for research:

<https://www.owasp.org/index.php/Top_10_2013-Top_10>

<http://php.net/manual/en/function.hash.php>

<http://php.net/manual/en/faq.passwords.php>

<https://secure.php.net/manual/en/function.password-verify.php>

<https://secure.php.net/manual/en/function.password-hash.php>

<https://www.thesitewizard.com/general/add-captcha-to-feedback-form-script.shtml>

**Project Plan**

1. Research current security techniques to avoid security vulnerabilities. (Week 1)
2. Create website framework using HTML and CSS. (Week 1)
3. Establish/Create Database. (Week 1)
4. Using PHP, connect the website to MySQL database. (Week 2)
5. Test services such as user login, registration, and review form, to confirm functionality and reliability. (Week 2)
6. Implement security measures to prevent OWASP Top 10 attacks (Week 2-3)
7. Test avenues for attack such as login, session manipulation, input manipulation, etc. (Week 3)
8. Review and revise based of finding from tests. (Week 4)
9. Present web site for evaluation. (Week 5)

**Technical Details**

Languages

* HTML
* CSS
* PHP
* MySQL
* JavaScript

Server

* Amazon Web Services

Libraries

* PHP has built in functions such as hash and mysql\_real\_escape\_string that will be used to prevent attacks such as Injection and Sensitive Data Exposure
* Google Map (JavaScript provided from Google to display location)
* RECAPTCHA (Javascript and implementation from Google to validate CAPTCHA input)

Three Features of My Website I Believe I Am Most Proud Of.

1. reCAPTCHA
   1. Learning how to implement and verify the reCAPTCHA request using Google’s API was very valuable and demonstrates the importance in hard-coded external links and preventing automated access to your site.
2. Salt and Hash
   1. I learned how to implement a salt and hash to sensitive information stored in my database. Prior to this assignment I was unaware how to properly store the salted and hashed password, along with the used salt, to properly verify the password when comparing the user’s input.
3. Review Form / Changing Page Elements
   1. The feature of the website I am most proud of is the review forum. Learning how to alter page elements to reflect the status of a user was a difficult challenge, however is important in web design, and creating a pleasant user-interface.