Elective Security in Web Development, KEA

Exam Project

Henrik Kramselund
hlk@zencurity.com

March 7, 2022

Introduction

This material is prepared for use in *Security in Web Development elective course* and was prepared by Henrik Kramselund, xhek@kea.dk.

We will have an exam project in this course, required for the exam! You are expected to present this, and walk us through the features for 10min – focus on security. Then afterwards we will ask questions, and perhaps dig into code too.

Hand in of report and project before May 20, 2022 at 12:00

Provide a small back story for a company, half a page, number of employees, select a business finance, agriculture, pet services provider, what you feel like.

You will build a small web application, consider it a template project for your company. Build a simple and secure project, with some functionality. Something the company can migrate their existing applications over to.

Project description

You are to create a small web site with at least the following features:

- Multilevel (privileges) login with backend authentication
- New user registration
- Data stored in cookie or other form (localStorage etc.) (NOT a Requirement)
- A list of items created by users, with option for setting visible private/public, admin can see everything
- For items have a function for adding data, like adding a comment to an item or similar
- File upload (images), a kind of profile picture might be an idea

NOTE: Apart from most other project I will happily accept existing code, IF source is given, and you can explain it.

Example: validating email address is *impossible*, since the format allows for many features, which are often not used. You are therefore encouraged to find a good implementation of *email validation*, which suit your purposes in this project. You may copy this function/module into your code, including license and references to original.

You MUST be able to walk us through the module, what does it do, and what are the shortcomings of this etc. Explain why THIS version is appropriate for your project. May be simpler to understand, is written in a clear way, your use of email used as a user id for login make it fair to have fewer features etc.

You are not allowed to use a full featured back end framework like Django or similar. You are allowed to use any combination of front end and backend languages. I expect that you will at least use some JavaScript, HTML, CSS etc. You may use existing helper libraries like bootstrap, and any readable/common programming language(s) you decided Java, Python, PHP, ...

Take steps to implement settings, security headers and/or code that prevents or minimizes the risk of the following attacks

- SQLinjection
- Cross-Site Scripting (XSS)
- Cross-Site Request Forgery (CSRF)
- XML External Entity (XXE) – if using XML, not a requirement
- Client side manipulation aka server side validation must happen

Recommendations

You should consider the following

- Firewall – enable the firewall on the server
- Use of SSL
- Use of encryption and hashing
- Configuration settings for your project, if using PHP php.ini, if using Nginx nginx.conf etc.

Deployment

Feel free to deploy on a virtual server somewhere, and configure the server as you like:

- Users, Apache, PHP
- Have a development environment
- Eventually use a repository (source control)
- Make sure you have a running copy on your machine

Deploy the application to a server of your choice Example: Amazon, digitalocean, ...

Hint: using a real name and deploing on a server will allow you to use tools like Mozilla Observatory for checking settings https://observatory.mozilla.org/

Formal

- Report size: 15-20 pages
- Exam project
- Exam project needs to be uploaded to Wiseflow (Not sent via email)
- Report and code ZIPed into a single archive
- Groups should use link on Fronter with group info
- Code blocks should be documented

- Relevant configuration files (httpd.conf, nginx.conf php.ini .htaccess aso) should be included in project if significant changes are done to these. Most relevant parts should perhaps be referenced, but not included in report.
  "The requirement for encryption was done using a configuration setting `add_header` in Nginx allowing us to have a HSTS header."
- Remember references, at least include the book we used for the course

Basically the report should document what you have done, and why you have done that.

Work Load Comments

Please include rough estimate for time spent on this project. We have the last weeks for this project, and there is a lot of work included. I would like to set a maximum number of hours to about 100 hours per person. This is to ensure that above is NOT misunderstood, and result in a stressfull experience.

Best regards

Henrik Kramselund

