CS-499: Computer Science Capstone

24 November 2024

3-2 Milestone Two: Enhancement One: Software Design and Engineering

The artifact is a **secure login system** that I developed as part of a project to demonstrate my skills in implementing secure authentication methods. It was created in **2023** as a practical solution to help users securely log into web applications by validating credentials through hashing and implementing session management to protect user data. The system uses industry-standard practices, such as bcrypt for password hashing and JWT (JSON Web Tokens) for maintaining secure user sessions.

I selected this artifact because it demonstrates critical aspects of **software security**, **backend development**, and **secure coding practices**, all of which are fundamental in my career goals. The artifact showcases several of my skills and abilities in software development, including:

* **Authentication Mechanisms**: Implementing password hashing and session management reflects my understanding of security fundamentals, essential for preventing unauthorized access.
* **Secure Code Practices**: By using bcrypt and JWT, I’m demonstrating my commitment to secure coding practices, ensuring data protection through encryption and secure token-based session management.
* **Web Development**: The system is built using a web framework (e.g., Node.js with Express), illustrating my proficiency in building robust and secure web applications.

The artifact was improved by refining the session handling and ensuring that the password hashing process was more secure by upgrading to a stronger hashing algorithm (bcrypt). Additionally, I implemented error handling and logging to make the system more resilient and easier to debug, addressing potential vulnerabilities in the process.

Yes, I successfully met the course outcomes I planned to meet with this enhancement, particularly in the following areas:

* **Outcome 5**: *Develop a security mindset that anticipates adversarial exploits in software architecture and designs to expose potential vulnerabilities, mitigate design flaws, and ensure privacy and enhanced security of data and resources.*

The enhancement directly addresses this outcome, as I focused on securing the login system against common exploits (e.g., brute force, session hijacking) and ensuring the system adheres to best practices in security.

Additionally, I’m now refining the artifact to further align with **Outcome 3**: *Design and evaluate computing solutions that solve a given problem using algorithmic principles and computer science practices and standards appropriate to its solution while managing the trade-offs involved in design choices.*

By optimizing the system’s performance and ensuring it adheres to industry standards for scalability and security, I’m enhancing the solution’s design to better meet these standards.

The process of enhancing and modifying this artifact provided significant learning opportunities, particularly in the areas of **security design** and **session management**. Here are the key takeaways:

* **Security Implementation**: I deepened my understanding of how to implement secure authentication and authorization systems. Learning how to hash passwords and securely store sessions was invaluable.
* **Testing and Debugging**: I learned the importance of thorough testing and error handling to ensure that the system could withstand common vulnerabilities. By testing the login system for security flaws, such as brute force attacks, I was able to make necessary improvements.
* **Session Management**: One challenge I faced was ensuring that session management was both secure and efficient. Implementing JWT tokens was initially confusing, but I learned how to manage token expiration and refresh mechanisms effectively.

Some of the challenges included balancing security with system performance. For example, while bcrypt is secure for password hashing, it can be slow if not configured correctly, especially with high volumes of user requests. I had to carefully adjust the hash cost parameter to balance security and performance.

Overall, enhancing the artifact gave me a deeper understanding of secure web development and reinforced the importance of following industry best practices when handling user data and authentication systems.