CSCE 4560 Secure E-Commerce Website Proposal:

**AI-Powered Study Guide Website**

Group 9: Edward Tomlinson, Bhargav Reddy, Benjamin Murley

**E-Commerce Selection**

The reason we chose a study guide website was it was unique and it roughly relates to our class as a whole. It keeps it relevant to the class as well as provides a great example for what we have learned.

**Project Scope**

Our focus is on making a study guide website. Designed to aid users in knowing important information on their subject. Use ai to generate study guide content. Have User registration, ai software, and the ability to buy a subscription service.The focus on security will be oriented around establishing multi factor authentication and secure payment gateways to make user data and transactions safe.

**Security Challenges**

Security challenges should be oriented around setting up a secure and safe website for us to do a subscription transaction. Protecting user data, and making a secure login. Our most important security challenge is guaranteeing secure payment for users, as insecurity of financial data is an instant turn-off for many consumers. Our subscription transaction, likely handled through a payment gateway, will need to implement a way to securely hold the user’s payment information and charge it monthly without exposing it to outside attackers. For user data and secure login functionality, our challenge will be to balance security measures with responsiveness and functionality. Users will want to be confident in the security of their data while still being able to access it quickly when they want to.

**Security Solutions**

Addressing the security challenges above will require a focus on safe data storage. We will need to use industry standard safety protocols such as encryption (AES), antivirus software, and zero trust architecture. These solutions will need to be balanced with the need for a responsive site, since security tends to degrade performance. We will need to evaluate the difference in processing time between different security solutions, leaning toward more secure for things like bank data and faster performance for less secure information such as names or study guide information. The most effective and common method for database encryption is Transparent Data Encryption (TDE) which is supported natively in many database engines.

Implementation of a multifactor authentication (MFA) service will address many basic authentication security issues by significantly reducing the likelihood of illicit access by bad actors. We will use a mandatory MFA service when creating user accounts to guarantee a layer of security, rather than having it be optional.

**Risk Assessment**

Our goal is to identify key risks -- such as unauthorized access, data breaches, payment fraud-- along with their direct and subsequent consequences. We plan to inform our users of what is possible, we will reassure them that we are committed to protecting their data, in a simple yet memorable way so users will be more inclined to take action when necessary. Some examples of risks include:

* Unauthorized Access
  + Immediate:
    - Account taken over
    - Lost control
  + Subsequent:
    - Identity theft
    - Financial fraud
* Data Breach
  + Immediate:
    - Sensitive data exposed
    - Lost trust

Strategies to Slow/Prevent them from happening:

* Unauthorized Access:
  + Multi-Factor Authentication (MFA)
  + AI-Powered login monitoring
* Data Breach:
  + End-to-end encryption
  + Control access policies

**14-Week Timeline for Secure E-Commerce Website Project**

**Week 1-2: Project Planning and Setup**

- **Member 1**: Research and finalize the website's core features (e.g., product catalog, user registration, shopping cart, checkout).

- **Member 2**: Set up the development environment (e.g., choose a framework like React/Django, set up version control, and create a project repository).

- **Member 3**: Research and select tools/libraries for MFA and payment gateway integration (e.g., Auth0 for MFA, Stripe for payments).

---

**Week 3-4: Basic Website Structure and User Registration**

- **Member 1**: Design and implement the product catalog (e.g., product listings, categories, and search functionality).

- **Member 2**: Implement user registration and login functionality (basic authentication without MFA).

- **Member 3**: Design and implement the shopping cart (e.g., add/remove items, update quantities).

---

**Week 5-6: Checkout Process and Payment Gateway Integration**

- **Member 1**: Design and implement the checkout process (e.g., shipping details, order summary).

- **Member 2**: Integrate the secure payment gateway (e.g., Stripe) for processing payments.

- **Member 3**: Implement order confirmation and history functionality for users.

---

**Week 7-8: Multifactor Authentication (MFA) Integration**

- **Member 1**: Research and implement MFA for user login (e.g., using Auth0 or a similar service).

- **Member 2**: Test and refine the MFA implementation to ensure seamless user experience.

- **Member 3**: Update the user profile page to allow users to enable/disable MFA.

---

**Week 9-10: Security Enhancements and Testing**

- **Member 1**: Implement data encryption for sensitive user information (e.g., passwords, payment details).

- **Member 2**: Conduct security testing (e.g., penetration testing, vulnerability scanning) to identify weaknesses.

- **Member 3**: Fix any identified security vulnerabilities and optimize the website for performance.

---

**Week 11-12: User Interface (UI) and User Experience (UX) Improvements**

- **Member 1**: Improve the UI design (e.g., responsive layouts, modern styling).

- **Member 2**: Enhance the UX (e.g., streamline navigation, add error handling, and improve loading times).

- **Member 3**: Conduct user testing with a small group to gather feedback and make adjustments.

---

**Week 13: Final Testing and Bug Fixes**

- **Member 1**: Test the product catalog and shopping cart for functionality and usability.

- **Member 2**: Test the checkout process and payment gateway for reliability and security.

- **Member 3**: Test the MFA and user authentication flow for robustness.

- Collaborative Task: Fix any remaining bugs and ensure all features work seamlessly together.

---

**Week 14: Deployment and Final Review**

- **Member 1**: Deploy the website to a hosting platform (e.g., AWS, Heroku, or Netlify).

- **Member 2**: Perform a final security review to ensure all vulnerabilities are addressed.

- **Member 3**: Conduct a final user acceptance test to confirm the website is ready for use.

---

**Summary of Responsibilities**

- **Member 1**: Product catalog, checkout process, MFA implementation, data encryption, UI improvements, and deployment.

- **Member 2**: User registration/login, payment gateway integration, security testing, UX improvements, and final security review.

- **Member 3**: Shopping cart, order confirmation/history, MFA user profile updates, bug fixes, user testing, and final acceptance testing.