Group 8

Secure eCommerce, CSCE 5560

Final Project Proposal, due 9/10/24

E-Commerce Selection:

We have selected a small international tutoring service website aimed at high/secondary school and college students that allows users to schedule, view and register for available tutoring services. It allows students to make payments through different payment gateways, it handles security via MFA and a secure payment system.

In the present world, seeking knowledge and updating ourselves has been considered as the most important thing to meet the job market. Even in the world of AI, nothing can replace a tutor who is there to solve every problem and help you in every step of the journey in learning new things. Our website helps these knowledge seekers to find their tutors to guide them in the right path.

Project Scope

Our website will provide a secure e-commerce platform supporting the tutoring activity. Primary functionalities planned and enabled by the sub-item features are:

- Customer registration & accounting for students to track classes, schedule, plan
    - **User accounts** with demographics facilitating user activity records like class scheduling, shopping cart etc.
    - **User feedback** is used to provide input for business improvement.
- Customer data security supporting user trust.
    - **User authentication** with Multi-Factor Authentication (MFA).
    - **User financial data partitioning via a payment gateway e.g. PayPal**
- Service purchasing.
    - **Services catalogue** with pricing and availability, and
    - **Secure Point of Sale (POS).**
    - **Invoice generation**

Security Challenges:

To create a secure e-commerce platform, frequent security vulnerabilities that jeopardize website functionality and user confidence must be found and mitigated. Some of the challenges are below (Gusain, 2024).

1. Protecting User Data

The website will handle personal information like names, addresses, and payment details. If this data isn't properly secured, hackers can steal it and misuse it.

Challenge:

- Preventing data breaches and unauthorized access to sensitive information.
- Hackers can steal personal data in a data breach.
- Information can be intercepted during transmission, like in a man-in-the-middle attack.

2. Transaction Security

Customers need to know that their payments are processed securely. If the payment system isn't safe, users could experience fraud or unauthorized charges.

Challenge:

- Protecting financial transactions from attacks that could lead to stolen payment information.
- Insecure payment gateways can lead to payment fraud.
- Scammers use phishing to trick users into giving away their payment information.
- Hackers use cross-site scripting and SQL Injection attacks to weaken the database

3. User Authentication

Password-based logins are not always enough to protect user accounts. Attackers can use weak passwords to break into accounts or trick users into giving away their passwords.

Challenge:

- Ensuring that users' accounts are protected from unauthorized access.
- Poor password policies make it easy for hackers to guess or steal passwords.
- Brute force attacks happen when hackers repeatedly try to guess login details.
- Weak authentication systems are prone to phishing attacks, where login credentials are stolen.

4. Building Customer Trust

Users need to trust the website before they share their personal information or make a purchase. If they don't feel confident about the security, they won't use the platform.

Challenge:

- Gaining and maintaining customer trust by showing the website is safe and secure.
- Inconsistent security measures can cause customers to lose trust in the platform.
- A lack of clear communication on how data and payments are handled raises concerns.
- Fear of data theft or fraud can make customers hesitant to use the service.

Security Solutions:

To solve these security issues, we will implement the following solutions

1. Multi-Factor Authentication (MFA) & Web Application Firewall

We will utilize multi-factor authentication (MFA) (NIST, 2022), which requires users to authenticate their identities in two steps (e.g., by entering a password and receiving a code via email or SMS) to ensure that only authorized users may access their accounts.

Solution: In addition to a password, users will need to log in using a one-time code that is texted to their phone as an extra security measure.

Web Application Firewall to monitor and block suspicious activity preventing SQL Injections and XSS attacks

2. Secure Payment Gateway

We will use PayPal (PayPal, 2024) to handle payments and ensure that transactions are safe and reliable. PayPal is known for its strong security and is trusted by many businesses for online payments.

Solution:

PayPal will securely process all payments by encrypting the information so hackers can't access it. PayPal also follows PCI-DSS guidelines, which are industry rules for keeping payment data safe. Additionally, PayPal uses tokenization, which replaces sensitive payment information with a special code, making it useless to attackers.

3. User Data Encryption

Every piece of personal data will be encrypted during transmission and storage to prevent hackers from accessing or reading it.

Solution: To secure sensitive data, we'll encrypt it securely and do routine security audits to identify and address any weaknesses.

4. Developing User Trust

By demonstrating to users that their data is secure, and the website complies with the best security procedures, we want to earn their trust.

Solution: To let users know that their connection is secure, the website will show trust marks like SSL certificates. In addition, we will inform consumers about safe online practices including choosing secure passwords and spotting phishing schemes, and we will clearly outline our privacy rules.

Risk Assessment

- **Exploitation of vulnerabilities:** Hackers can exploit unpatched or old/legacy software and devices. Keeping software and devices up to date, additionally, we

can look for more “comprehensive solutions based on our protection needs” (Bader, 2023)

- **Human error:** Find or create an employee training program to ensure the risks of human errors are minimized
- **Man in the middle (Mitm):** Attackers can sniff and spoof to manipulate the network traffic; a solution to this problem would be implementing TLS, which uses HTTPS to encrypt packets using cryptographic algorithms.
- **Data compliance/privacy:** Ensure the E-commerce website aligns and follows “HIPPA, GDPR, PCI DSS, and many other laws and legislations” (Sarah Bader, 2023).

Project Timeline.

- Week 1 - 4: Submit proposals, brainstorm e-commerce (EC) website pages and design the website
- Week 5 - 8: Find and select the MFA solution that fits best for the EC website and integrate it with EC
- Week 9: Test and review the MFA integration, documenting the process
- Week 10 - 11: Implement payment gateway
- Week 12 - 14: Implement HTTPS and SSL for secure communications and transactions
- Week 15: Review documentation and test the functionality of each added secure and communication mechanism.

References

American Express. (2022, December 19). *E-Commerce Security Threats and Their Solutions*. American Express. Retrieved September 8, 2024, from https://www.americanexpress.com/en-ca/business/trends-and-insights/articles/ecommerce-security-threats-and-their-solutions/

Bader, S. (2023, April 19). *Common Risks with E-commerce | How to Avoid Them | Rewind*. Rewind Backups. Retrieved September 7, 2024, from https://rewind.com/blog/common-risks-with-ecommerce-and-how-to-avoid-them/

Gusain, S. (2024, September 2). *Ecommerce Security - Key Threats And How To Prevent Them*. Binmile. Retrieved September 8, 2024, from https://binmile.com/blog/ecommerce-security/

NIST. (2022, January 10). *Multi-Factor Authentication | NIST*. National Institute of Standards and Technology. Retrieved September 8, 2024, from https://www.nist.gov/itl/smallbusinesscyber/guidance-topic/multi-factor-authentication

PayPal. (2024, June 25). *Secure Logins with Multi-Factor Authentication*. PayPal. Retrieved September 6, 2024, from https://www.paypal.com/us/money-hub/article/how-secure-authentication-works