SWE 314

Let's Start

GROUP 1 -
WASSETIK

OUR TEAM

Lama Alnasser	442201852
Layan Aluwaishiq	442201814
Nouv B. Al-Qahtani	442201905
Alanoud Alfakhri	442200434
Nada Alkubra	442202368

INTRODUCTION

What is wassetik?

Wassetik is a leading e-commerce website that provides customers with a wide variety of products and services at competitive prices and makes purchasing as easy as possible.

Idea

It is an enterprise for online selling, serving as an intermediary between other retailers and customers. Its web services business includes renting data storage, computing resources, managing payments, and facilitating delivery. The idea behind our website was to create an online marketplace where people could buy and sell goods easily and conveniently.

INTRODUCTION

TARGET USERS

With a global customer base, our website caters to anyone looking to purchase a product or service online, including individuals, families, and businesses seeking to save time, money, and effort by shopping online.

PLATFORM

The system will be programmed using web languages such as HTML, CSS, and JavaScript

INTRODUCTION

PROJECT GOALS AND IMPORTANCE

We aspire to make the customer experience more reliable by protecting the customer and vendor’s rights, such as verifying the vendor’s information, guaranteeing the right to return and payment.

REFERENCE WEBSITES

-eBay https://www.ebay.com
-AliExpress https://ar.aliexpress.com/

PROJECT SCOPE

Wassetik is a website that acts as a facilitator between customers and vendors by providing a platform for vendors to display their products to customers. In addition to offering customers a hassle-free method of browsing and buying products from multiple vendors, Wassetik will offer customers a secure payment gateway that supports various payment methods to simplify the purchasing process.

The estimated cost of developing “Wassetik” project using web development languages is around 60,000 SR, and the development period is expected to be approximately 6 months.

PRODUCT SCOPE

FUNCTIONAL REQUIREMENTS

The Customer functional requirements:

1. The customer shall be able to create an account using their email address, phone number, and password.
2. The customer shall be able to log in using their credentials (email address and password).
3. The customer shall be able to edit their account information.
4. The customer shall be able to browse all the products.
5. The customer shall be able to view product details (price, description, specifications).
6. The customer shall be able to add products to their shopping cart.
7. The customer shall be able to view their shopping cart.
8. The customer shall be able to modify product quantities.
9. The customer shall be able to remove products from the shopping cart.
10. The customer shall be able to choose from different delivery options, such as standard and express shipping.

PRODUCT SCOPE

FUNCTIONAL REQUIREMENTS

The Customer functional requirements:

11. The customer shall be able to checkout using different payment methods such as Apple Pay, credit card, and PayPal.
12. The customer shall be able to track their order status.
13. The customer shall be able to return products after completing a purchase.
14. The customer shall be able to exchange products after completing a purchase.
15. The customer shall be able to review the products they have purchased.
16. The customer shall be able to rate the products they have purchased.
17. The customer shall be able to communicate with the vendor.
18. The customer shall be able to access their order history.
19. The vendor shall be able to create an account using their email address, phone number, and password.

PRODUCT SCOPE

FUNCTIONAL REQUIREMENTS

The Vendor functional requirements:

1. The vendor shall be able to log in using their credentials (email address and password).
2. The vendor shall be able to add new products, including (product name, price, specifications, and description)
3. The vendor shall be able to provide an expected delivery date for each product.

The System functional requirements:

1. The system should be able to send emails containing ads and offers to customers.
2. The system should check the availability of an item in the shopping cart when it is added to the cart.
3. The system should remove the product from the shopping cart if it is out of stock.
4. The system should inform the customer of the removal of the out-of-stock products from their shopping cart.

PRODUCT SCOPE

NON-FUNCTIONAL REQUIREMENTS

1. The user must be able to login into the system within 1 second.
2. The system downtime should not be more than 1 hour per month.
3. The system should be available to the users 99.9% of the time.
4. The system should be user-friendly (clear, easy to use, and navigate).
5. The system should be available in multiple languages and support different currencies.
6. The system should be able to handle the increased amount of data and usage.
7. The system should be capable of handling a high volume of transactions, 1000 or more simultaneously while maintaining a high level of security.
8. The system should be accurate in order fulfillment, ensuring each customer gets their order.
9. The system shall be able to load all products as the user scrolls down within 1.5 seconds.
10. The system shall be able to integrate with third-party tools such as payment gateways.
11. The system shall be able to handle 1,000,00 concurrent users while maintaining optimal performance.

PRODUCT SCOPE

SECURITY REQUIREMENTS

1. The system must be able to encrypt all personally identifiable information before storing it in the database.
2. The system should remain accessible and operate dependably, even when subjected to denial-of-service attacks.
3. The system payment processing gateway must be PCI DSS (Payment Card Industry Data Security Standard) compliant.
4. The system shall have authentication measures at all the entry points, front panels, or inbound network connections to avoid unauthorized access.
5. The backup system shall store the recovered data in a network system to help in case of failure or intruder action.
6. The system shall ensure system-level accounts have limited privileges to avoid attackers escalating users' accounts to access administrators' features.

OWASP VULNERA-BILITIES

1. Cryptographic Failures:
The hashed passwords stored in the database could be vulnerable to cryptographic failures.

2. Broken Access Control:
The customer login credentials stored in the database could be at risk of being vulnerable to broken access control.

3. Identification and Authentication Failures:
User login process, which involves using an email address and password, is vulnerable to identification and authentication failures.

4. SQL Injection:
User inputs during the process of reviewing products could be vulnerable to SQL injection attacks.

OWASP VULNERA-BILITIES

5. Software and Data Integrity Failures:
Using modules from untrusted sources in software increases the potential for risks related to software and data integrity failures.

6. Security Logging and Monitoring Failures:
Visible logging to the system could be vulnerable to security logging and monitoring failures risk.

7. Server-Side Request Forgery:
If an attacker can manipulate the URL of a third-party service that a web application uses, it may be vulnerable to server-side request forgery.

8. Security Misconfiguration:
Displaying an error message when the user inputs invalid data could be vulnerable to security Misconfiguration.

SECURITY CONSIDERATIONS

1. The **integrity** and **confidentiality** of the hashed passwords stored in the database should be preserved.
2. The **integrity** and **confidentiality** of customer login credentials stored in the database should be preserved.
3. The **authenticity** and the **confidentiality** of user login credentials should be preserved
4. The **integrity** and **confidentiality** of user inputs during the reviewing process should be preserved.
5. The **integrity** of software should be upheld when relying on modules from untrusted sources.
6. The Integrity and Confidentiality of the system should be protected.
7.
a. The user's **authenticity** should be preserved.
b. Secure communication **confidentiality** should be preserved.
8. The system's private information **confidentiality** should be preserved.

SECURITY TECHNIQUES TO BE IMPLEMENTED

1. Cryptographic Failures:

a. Strong Password Hashing Algorithms:

Implement robust cryptographic hash functions like bcrypt, Argon2, or scrypt to protect hashed passwords. These algorithms resist brute-force and dictionary attacks.

b. Salted Hashes:

Generate unique random salts for each user and combine them with passwords before hashing. Salting prevents attackers from using precomputed tables and enhances password security.

2. Broken Access Control:

Principle of Least Privilege (PoLP):

Follow the PoLP, means users should only be granted the minimum privileges necessary to perform their tasks.

SECURITY TECHNIQUES TO BE IMPLEMENTED

3. Identification and Authentication Failures:

a. Strong Password Policies:

Enforce the usage of strong passwords that meet specific complexity requirements, such as a minimum length and a combination of uppercase and lowercase letters, numbers, and special characters. This helps prevent easy guessing or brute-force attacks on user passwords.

b. Multi-Factor Authentication (MFA):

Implement MFA by requiring users to provide something they know (password) and something they have (one-time password sent to their mobile device) or something they are (biometric authentication like fingerprint or facial recognition).

4. SQL Injection:

Input Validation and Sanitization:

Implement comprehensive input validation and sanitization mechanisms to ensure that user inputs are validated for expected formats and sanitized to eliminate any potentially malicious content.

SECURITY TECHNIQUES TO BE IMPLEMENTED

5. Software and Data Integrity Failures:
To verify the software or data is from the expected source and has not been altered we can use digital signatures or similar mechanisms.
a. Digital Signing Process the software or data is signed using a cryptographic algorithm by the entity that created it, typically the software developer or data owner. The signing process involves generating a unique digital signature based on the contents of the software or data.

b. Signature Verification to verify the integrity and authenticity of the software or data, the digital signature is checked using the corresponding public key. If the signature is valid, it means the software or data has not been tampered with since it was signed and that it indeed originated from the expected source.

SECURITY TECHNIQUES TO BE IMPLEMENTED

6. Security Logging and Monitoring Failures:

a. By using Snort tool to generates detailed logs that capture network traffic and any suspicious or malicious activities it detects. These logs contain valuable information about the source and destination IP addresses, timestamps, protocols used, and specific rules triggered by the detected activity.

b. SIEM systems provide a range of additional features that further enhance the detection and response capabilities for logging attacks, SIEM systems have more features to help detect and respond to logging attacks, and detect unusual user behavior. These capabilities enhance the ability to identify and address logging attacks.

7. Server-Side Request Forgery:

a. Input validation by validating all user input and ensuring that it is within the expected range of values before making a request. This can help prevent attackers from manipulating the URL to inject malicious code or execute unauthorized actions.

b. Applying Secure communication by using secure communication protocols (such as HTTPS) to encrypt data in transit and prevent attackers from intercepting or modifying requests.

SECURITY TECHNIQUES TO BE IMPLEMENTED

8. Security Misconfiguration:
Limit error messages by Ensuring that error messages are concise and do not reveal sensitive information about the system or underlying code. Avoid displaying detailed error messages and other technical details that are useful to an attacker and could be used to exploit vulnerabilities in the system.

RECORDED VIDEO FOR OUR CRYPTOSYSTEM

THANK YOU FOR LISTENING!

HAVE A GOOD DAY