Individual report: Airline Website Development

Introduction

This is an individual report on the production activity of the website development group project “Airline website system”. We were assigned with four members as a team. Everyone also be counted as developer and have primary roles as per the agile methodology. My primary role is a red hat tester which is want to test the vulnerability of the project and working with technical lead for the website development.
This report included requirements that are client want, the development process, my responsibilities in team and analyzes the website system. Further, the report then explores the testing that were carried out for the vulnerability, assesses the security optimization of the website system and reviews the knowledge and skill that I had learnt in the project development process.
Lastly, the report analyzes our project management with the action for system implementation after we got the feedback from each interim review. And conclude the project development process, final product before the deadline, what functions are not finish or in process and the reason of delay if it occurs.

Background to the project

Ivy Wong is our client and want to develop the airline website system for management team to handle booking, managing flights. Generally, the system has two role account: customer and management team. Ivy wishes the customer can book a flight ticket through the system and send the enquiry to the management team of the airline company. The other side, the management team can control the flight booking request/changes, handle the customer enquiry and the payment can be done through the system.
There was four team meeting, four interim review and final presentation of project process and outcomes. Basic on the above information, we would try to analyzed different case and other requirements on our meeting, and present our mind in the interim review for our client, Ivy Wong.
Especially, the airline website system which would follow by the feedback from client in each interim review to optimize the function, ui design and the security feature. After four interim review, the airline website system would be showed to client and test all functions in the final presentation.

Individual report: Airline Website Development

Requirements

For me, figure out all requirement is the important thing in developing the system. According the initial meeting with client is not enough to analyzes what is the client really want. So, the following interim review is suitable time for me to realize what is the client expected and which part in the website system is not fit for the client requirement.

Especially**,** we have analyzed kind of problems to ask to Ivy in the review for the project implementation and I also prepared some advice to improve the website security for data protect and hacker prevention.

We have used the application called “trello” as our product backlog to maintain our project schedule, stored the user stores, update the process. According the information in our trello, client told that the security requirement is the most important part of the system and also figured some user stores. Here are lists of security requirements and user stores after client feedback:

Security requirement

The login function should be secure in the system. It means that hacker cannot hack the account in the system.

Hacker can not access and get our database’s data.

Hacker cannot client-side scripts into web pages viewed by other users.

To avoid hacker get the right login account and login password.

User stores

Users can login to the system by using different kind of the user types (E.g. Admin, staff, Manager etc...)

as a customer I want to view the flight information on the system and purchase the ticket online

as a manager/senior staff of the company I will like to check/edit the customer’s information on system.

As a user I want to use the system by using different types of device (mobile, PC)

as a customer I want a channel to send out enquires

As a customer I want a channel to send out enquires

Individual report: Airline Website Development

Design and implementation

Collectively we have designed an airline booking system website. And my missions are to create the login function, register function and design the interface of the website.

Basic on the user stores, client said she wants the system consists different kind of role which content at least admin, senior, junior for management team and user for customer. We create some tables in database called “roles”, “relation_user_role”, “relation_role_func” to design the role level of users in the airline website system. Using “roles” table to store a list of role type, “relation_user_role” is used to match up the account and the role type, “relation_role_func” is used to authorize the permission of using function with which roles. Since the role is authorized the permission of function in the table, it is a secure work to protect the edit information function and edit booking function will not get accessed by using the account of user role.

Since account was stored many user information of customer and management team, I have set some policy on the password. In our register function, user need customize their account name and password, the system will check is It the valid name that is not exist in the database. On the password level, the password must have at least 8 characters in length, and also should have at least one uppercase and one lowercase character. This setting can protect the account not easy to hack by someone using brute-force attack to get the user name and password.

Continuing on the register function, the system will send the email for confirmation to make sure that the email is correct when user used to register. The account could not book the flight ticket before user take the confirmation by email. It would make sure that management team can find the user correctly after user is booked a ticket, or get something problem and wants management team member follow up.

We have created the page let the user can view the flight information in the system, user need input the departure and destination, depart time, arrive time, and also can select it is one-way trip or return trip. Users can see the flight information on the page after they type the search flight button. if user is confirm to book the flight ticket, they can click the button called ”order” which is also showed in the search result page. Then the system will show the selected flight ticket information for user confirmation and noticed user can select the seat or later, and user can click a button to payment page and pay using credit card. Since the system is not formally used for business for real customer to booking, so the payment function would not really take the credit card permission.

Individual report: Airline Website Development

Moreover, users can see their account information and booking record in the system, they can also edit their profile in any time. And they had no permission on edit booking record, and it means that user can't change the booking record.
On the admin level, admins had all permission in the system, they can manage the information of flight, booking record, user profile, and also can book for user if some user had any problem on booking. We have created the manage page in the website and give the permission of admin to edit the flight, booking and user information. It means admin can do the management on the website.

Testing

As a red hat tester, to test the vulnerability of the product is my most responsibility. And since client deep concern on the security of the system. I had list out kind of common vulnerability of the website system. Such as "SQL injection", "Cross-site scripting", "Brute-force attack", these are very common attack action for the hacker to get the data from another website. I will describe what vulnerability I have found and how to avoid these happened.

SQL injection

This is code injection technique, used to attack data-driven applications, in which malicious SQL statements are inserted into an entry field for execution. Using the following code for example:

```
statement = "SELECT * FROM users WHERE name = '" + userName + "';"
```

if the username is varied by malicious user like this:

```
' OR '1'='1
```

Then the code will be becoming like this:

```
statement = "SELECT * FROM users;"
```

then the malicious user can login the system even he has not got the correct account. For this problem, our website is used python to developed. Using SQLAlchemy to avoid SQL injection vulnerabilities. And manage the permission to access database strictly, minimize the need of permission to user basic on their feature.

Individual report: Airline Website Development

Cross-site scripting

it enables attacker to inject client-side script into web pages viewed by other users. To prevent this problem happen, some important data in our system would not show on the url and it would send out using session.

Brute-force attack

Brute force attack is an attempt to crack a password or username or find a hidden web page, or find the key used to encrypt a message, using a trial and error approach and hoping, eventually, to guess correctly. This is an old attack method, but it's still effective and popular with hackers.

To prevent this, I made the policy password that need suit at least 8 characters and at least 1 uppercase and one lowercase character, hacker need more to crack a password or username.

Further, implement a feature that if login failed more than 3 times, the account would be locked and send notification email to user email account is the stronger secure to stop the brute-force attack immediately. If I had more time to complete the project this would be a feature, I implemented to strengthen the system.

Further, I also used the application called “Vega vulnerability scanner” to analyzed our airline website system and found the bug called “Cleartext password over http.” And we used the Hypertext Transfer Protocol Secure(https) to prevent the problem, it is using Transport Layer Security (TLS) or Secure Sockets Layer (SSL) to encrypt the communication protocol in HTTPS.

I have learnt more knowledge on the security level of the website system such as how to protect the data would not hacked by malicious users and how to protect the website that not be attacked easily.

Project Management

Project management is the stronger factor in project development process. I have updated our system each time after we end the interim review. For the initial system, client feedback that the system design was not good look. So, I redesign the structure of the website and add the background in every pages.

And client said that she wants more secure action in the system, so that I updated the function of login and register system, and other action to protect the communication protocol such as using https.

We tried to met the target by the feedback of the client, although some function may be in processing, but using the trello to be product backlog and follow the timeline to guide the system implementation can make sure that the processing would not delay too much.

Individual report: Airline Website Development

Conclusions

In conclusions, the system fulfills the system and security requirement which are client request and ready to used. Following the agile development to implement the project is safely and quickly to fix the requirement if it is wrong. Although some features may in process or need to improve the effect. But we can change our process to do the important function/requirement first if the project is delay.
The agile development is helpful to manage our project and we learnt a lot of thing on the project management.

Individual report: Airline Website Development

Marks allocation

Team working can cause concern amongst students. They worry that their marks will be lower if working with people who do not have the same approach to team working than they. To account for this, students must claim their marks using the mark claim grid shown below. This should be added as an appendix in their individual reflection. For each category, evidence must be provided such as hyperlinks to minutes, documents and commits to the repository for the category.

Please record below the % of the category marks being claimed as justified by the evidence provided.

Marking Category	% claimed	Justification/evidence	Final mark (Please leave blank)
Process - Project Management - Objectives - V&V - Approach	25	https://github.com/cpass19999/PRCO204HK-Project---Airline-Team-7-/blob/master/Documentation/Project%20Management%20Review_.docx https://github.com/cpass19999/PRCO204HK-Project---Airline-Team-7-/blob/master/Documentation/PROC204_Group7_Group%20Report.pdf	
Product - Background - Communications - Implementation - LSEP	25	https://github.com/cpass19999/PRCO204HK-Project---Airline-Team-7-/blob/master/Documentation/minutes%20of%20the%20group%20meeting.docx https://github.com/cpass19999/PRCO204HK-Project---Airline-Team-7-/blob/master/Documentation/offical%20meeting%20minutes%20with%20the%20client.docx	