Term Project

EECS 4481 4.0 Computer Security Lab, Winter 2015

Format: Individual

Project Overview

The goal of the project is to develop a secure help-desk web application that allows secure communication over a public network. The application will be used by non-technical persons for online support. Therefore, the application must be resilient to security attacks, as well as user-friendly.

Functional Requirements

The help-desk web application has the functional requirements shown in Table 1.

ID	Requirements
REQ_1	**Users**
REQ_1_1	The application shall support two types of users: anonymous users and help-desk users
REQ_2	**User Authentication**
REQ_2_1	The application shall be able to authenticate help-desk users
REQ_3	**Automatic selection of help-desk user**
REQ_3_1	The help-desk system shall be able to assign for each anonymous user an online help-desk user
REQ_4	**Anonymous users**
REQ_4_1	Anonymous users shall be capable to send text messages to their assigned online help-desk users
REQ_4	**Help-desk users**
REQ_4_1	Help-desk users shall be capable to send text messages to a selected one of their anonymous users
REQ_4_2	A help-desk user shall be capable to send a message to another help-desk user
REQ_4_3	Help-desk user shall be capable to transfer non-authenticated user to another help-desk user
REQ_4_4	The application shall be able to display the help-desk sender and the help-desk recipient for each message between help-desk users
REQ_5	**The application shall be secure**

Table 1: Functional Requirements.

Deliverables

The project will be implemented in four phases with the following due dates and deliverables:

Phase 1: Functional application

Due date: February 1, 2015 at 11:59pm

Deliverable: For this phase, you must deliver a fully functional application, i.e. one that fulfills all requirements except REQ_5. You must also provide a report that includes:

- The server and client software design. Your report must include your rationale for the design choices you made.
- The GUI design of your application (includes rationale as above).
- A testing report.

It is expected that your application design will be carefully thought out. An application with inadequate design will be significantly penalized.

Phase 2: Security report

Due date: February 22, 2015 at 11:59pm

Deliverable: For this phase, you must deliver a report that includes:

1. The security test cases (attacks) that were performed (setup, attack code, analysis of collected data, screen shot of collected data)
2. The security test cases that were designed (setup, test case code) but not executed
3. The security design flaws you found
4. The security bugs you found

Phase 3: Secure application

Due date: March 22, 2015 at 11:59pm

Deliverable: For this phase, you must deliver a version of the help-desk application that contains no known security bugs, i.e. all security issues you identified in Phase 2 have been resolved. You must include a README file explaining how to install your application if you believe this is necessary.
You must also submit a report that includes:

- The revised server and client software design. Your report must include your rationale for the design choices you made.
- The revised GUI design of your application (includes rationale as above).
- A revised testing report. It should include both functional and security tests.
- A report on other ways you could enhance the security of the system, e.g. firewalls, VPN etc.

Phase 4: Final delivery

Due date: April 5, 2015 at 11:59pm

Deliverable: For this phase, you must deliver the final version of the help-desk application including any fixes based on Phase 3 feedback. You must also submit a revised report based on Phase 3 feedback.

How to Submit

Before the deadline, submit electronically the report and/or the source code you created. Place all the files you want to submit in a directory called PhaseX, where X is appropriately 1, 2, 3, or 4. To submit, navigate to the parent directory of PhaseX and give the following command
`submit 4481 PhaseX PhaseX`
Also, drop off a hard copy of the report (if applicable) into the CSE 4481 assignment dropoff box located on the first floor of CSEB. The hard copy will be the one to be marked. The electronic copy will be used for record keeping.
If the source code you would like to submit resides in the Attack Lab, place it in the following directory in the `Submit` virtual machine: `C:/CSE4481/<cse username>/PhaseX`. You will probably need to create this directory.