Software Requirements Specification

for

Packet Wars

Prepared by:

Jaagrit Arora (11BCE033)

Parjanya Vyas (11BCE066)

Darshil Patel (11BCE072)

Guided by:

Prof. Zunnun Narmawala

Institute of Technology,

Nirma University

12-Feb-2014

Table of Contents

1. Introduction

1.1 Purpose

Packet Wars is a project aiming to provide a platform to the network security students to learn and understand different computer security algorithms, cryptographic algorithms and their decryption and a few more security concepts.

1.2 Document Conventions

Bold face and bullet points are used to introduce a new topic or a specific subject matter. The rest of the document is written in regular Arial.

1.3 Intended Audience and Reading Suggestions

The SRS is intended for readers who want to understand the working of the software thoroughly and for security analysts who intend to use the functionalities of this software for further understanding. The document contains introduction to the software followed by its functional and non-functional requirements. The document also describes each module of the software in detail with the help of diagrams.

Enthusiasts are encouraged to read the whole document for the sole purpose of the topics included in the project.

2. Overall Description

2.1 Product Perspective

This software is the first release of the stand-alone Packet Wars Platform which will facilitate the interested students to learn the security fundamentals in an interactive and fun way. PHP is used for server side scripting here so that various databases can be maintained into the server. As PHP needs Apache server to execute, proper installation should be done of the software into a centralized server (and in a backup server if fault tolerance is needed) which is in turn connected to each and every system which is supposed to use this software via any kind of (wired/wireless) network.

2.2 Product Functions

The major functions this software performs are:

- Initial login page without the vulnerabilities which cannot be bypassed easily.
- All the learning topics provided as links on the home page.
- An interactive tool with the aim of studying thoroughly with fun.
- Cryptography and Decryption in the form of a competitive game between all connected players providing the sense of competition and arousing the feeling for doing better than peers.

2.3 User Classes and Characteristics

The various classes of users that may use this product are:

- Administrator: The administrator will have full access rights and can use and manipulate every function as well as database of this software. Main purpose of the administrator will be to supervise the users and make sure that any illegal access to any of the database or function is not made.
- Learners: Learners will have access to the databases of only the link they are working upon. They can switch between topics to try out other topics.
- Cryptanalyst: The player of the cryptography game with the aim to decode the encrypted texts and retrieve the plain text using different algorithms as fast as possible.

2.4 Operating Environment

For using this software any advanced and updated web browser is enough. Any specific operating system is not needed for using this software. Though connectivity to the server in which the software is installed is a must and therefore connection via any type of network (wired/wireless) to the server is needed.

A server in which this software is to be installed is needed. In this server Apache 2.4.3 must be enabled as PHP is used for server side scripting. In addition to this, databases are to be used and therefore MySql is required. As per the need sufficient memory is also required.

2.5 Design and Implementation Constraints

As stated earlier, a server in which this software is to be installed is needed. In this server Apache 2.4.3 must be enabled as PHP is used for server side scripting. In addition to this, databases are to be used and therefore MySql is required. As per the need sufficient memory is also required. According to the memory available in the server number of players is limited. Also an advanced and updated web browser (Mozilla Firefox, Google chrome, Internet explorer 8.0 and above, etc) is needed in order to use the functionalities provided by the software. As per the network implemented parallel access to the databases is also limited and varying.

2.6 User Documentation

A printed user manual is provided with this software to facilitate the users and the administrator. It also includes FAQs about the software and their answers. Offline help support is also included in the software which can be used at any time by the users by clicking help icon or accessing help from help menu.

2.7 Assumptions and Dependencies

It is assumed that mandatory access rights are given to the client computers so that they can request data from server and send data to server on LAN. Network settings and access rights must be configured properly in client and server computers in order to ensure complete, smooth and errorless execution of the software. The privilege settings in OS also must be done accordingly. The number of entries in database is highly dependent on the memory space available, as the database software used here can support very huge amount of data. The appearance of the UI may differ a little from browser to browser but functionality remains same.

3. External Interface Requirements

3.1 User Interfaces

The first interface between user and the software is the login screen which will ask the user for their ID and password to authenticate the user.

After logging in successfully, the users have an option of many different topics to choose from in the form of hyperlinks. Once selected, they would be redirected to the respective page wherein they can practically understand the topic.

In case of the selection of cryptographic game, the user would be redirected to a page wherein the cipher texts would be provided to him/her and he/she should provide back the plain text to earn as many points as possible.

3.2 Hardware Interfaces

In order to create a network between client computers and server computers wired or wireless technologies can be used. According to whichever is used hardware interfaces differ drastically. Whichever interfaces are required between computers, routers and switches/hubs according to the network implemented are used by this software. As the web browsers are used to avail the functionalities HTTP and TCP protocols are used by the software.

3.3 Software Interfaces

As stated earlier in the user interfaces section, several databases are used here to store information about the active players. These databases are maintained as SQL databases so that concurrent access is also possible for retrieval of information. As stated above various modules send data to server and request data from server. No necessary precautions are to be exercised by the users for maintaining consistency of the data as all concurrent accesses are managed by the software itself.

3.4 Communications Interfaces

HTTP protocol is used here for all type of communications and client server architecture is implemented. Whole implementation is done on the LAN network therefore no Internet connectivity is mandatory for its use in the campus of the hospital where the established network is already available. All information is submitted to the server as forms by web pages.

4. System Features

4.1 Login module

4.1.1 Description and Priority

This is a high priority module which will enable users to avail various functionalities of the whole project.

4.1.2 Stimulus/Response Sequences

Firstly user has to provide his/her ID and password by which he/she is authenticated. According to the authentication of user, privileges are given to the user and functionalities are made available.

4.1.3 Functional Requirements

REQ-1: The module must accept the user ID and password from the user

REQ-2: It must authenticate the user as one of the classes specified in previous section.

REQ-3: According to the class of the user, appropriate UI should be displayed to the user.

REQ-4: If the login fails due to invalid password or ID, appropriate message should be displayed and login screen should reappear.

REQ-5: No SQL injection attacks should be able to bypass this main login page.

4.2 Sign up module

4.1.1 Description and Priority

This is a high priority module which will enable users to register themselves.

4.1.2 Stimulus/Response Sequences

Firstly user has to provide his/her unique ID and password along with their name and email ID by which he/she will be registered.

4.1.3 Functional Requirements

REQ-1: The module must accept the Name, Email ID, user ID and password from the user. Uniqueness of User ID should be checked.

REQ-2: According to the class of the user, appropriate UI should be displayed to the user.

REQ-3: If the signup fails due to invalid password or ID, appropriate message should be displayed and login screen should reappear.

REQ-4: No SQL injection attacks should be able to modify this main login database using the fields of this page.

4.3 SQL Injection module

4.2.1 Description and priority

This module deals with simulating various types of SQL Injection on a login page. It is also high priority module after the login module.

4.2.2 Stimulus/Response Sequences

Students are the main user of this module. Blind SQL injection, Union queries, etc are injected in the username or password field by the user and accordingly success of the attack is shown.

4.2.3 Functional requirements

REQ-1: It must first provide a dummy login page to the user, and two text fields namely LOGIN and PASSWORD.

REQ-2: It should also accept the malicious entry for any of the field and accordingly respond to the user with either successful attack's information or any SQL error.

REQ-3: Any type of SQL queries should be accepted from the user and proper error messages should be displayed.

REQ-4: It should validate the authentic users with their Username and Password and show them their password only if both the fields match with the corresponding database entry.

REQ-5: It should provide a help/manual page on SQL injection and how it is done to guide the users of the page

4.4 Cryptography module

4.3.1 Description and priority

This module is used to simulate various cryptography algorithms. It is mainly used by the students and cryptanalysts to understand the various cipher techniques and how they work. It is a relatively similar priority module as above all.

4.3.2 Stimulus/Response Sequences

Multiple levels of a game which are defined by various cipher techniques are provided. User have to decode the given cipher text by using a hint, which will provide the key and the technique which is used for encryption, indirectly.

4.3.3 Functional requirements

REQ-1: It must provide cipher text to the user which is to be decoded.

REQ-2: It should also provide a proper hint on what technique is used and what is the key used for encryption.

REQ-3: If user successfully decodes the cipher message, it should increase the points and advance the user to next level.

REQ-4: If user is unable to decode the cipher message then it should provide a link to help and by clicking on it, points should be deducted from the users account.

REQ-5: At the end of the game, total points of the user should be displayed.

4.5 Cross site request forgery module

4.4.1 Description and priority

This module deals with the attack named “Cross Site Request Forgery” and optionally Cross sit scripting. These attacks are simulated using a scenario based attack simulation.

4.4.2 Stimulus/Response Sequences

A quiz on general knowledge is to be given to the users and by observing the URL and using the proxy server, the users will be able to identify the parameters and will be able to attack and fool the quiz manager by fabricating their own URL.

4.4.3 Functional requirements

REQ-1: It must show the questions of quiz to the user and must evaluate the answers given by the user and modify their score accordingly.

REQ-2: Preferably it should pass the parameters by GET method so that they may be visible the end user.

REQ-3: It should include the help/manual page on how this attack works and what user is supposed to do in order to successfully somplete this attack.

4.6 Data forensics and recovery module

4.5.1 Description and priority

This module is basically a passive module which explains the basic techniques of data forensics and data recovery.

4.5.2 Stimulus/Response Sequences

It includes a manual page on how these techniques work and preferably a video on the working of these techniques.

4.5.3 Functional requirements

REQ-1: It must provide user the basic understanding of various file structures and how are they maintained in the optical/magnetic data storages.

REQ-2: It should be able to explain the user how lost data can be recovered, which tools are available for it and how they work.