1. **Authentication and web security**

**Explain how a user login script provides website security?**

First, we must understand how the login work. The concept is very simple: we store ID (username) and PASSWORD in database, then we write a login page contain SQL statement to check against these records in database table (the record cannot have 2 same username). If it match with the records in the database, it will send you to specific page. If it does not match with the database, it will pop up a message (usually wrong password or username)

The reason why it make the website security is that it can provide the ‘access right’ to the user via username. For example, with some specific file or document can only access by user with access level is ‘administrator’ or ‘member’ (depend on the database design and website development strucutre). So, with that concept, we can actually manipulate the database access to any visitor/user or even administrator from the website.

**What is login authentication?**

Login authentication is just the way to identify a specific user. For example, as a student, I have right to access to my personal file via RMIT website. But how can they know that am I a specific student/or just a random guy try to get in my file? We have concept call ‘password’ which is to identify a right login my file as a student.

In summary: username is used to identify the level access (the right to access). Password is used to identify that username.

If the login process is successful, the destination (result page) will pop up. Remember to hide the destination page (if you provide it at the login section, people may get to the destination page without a username).

If the login process is unsuccesful or invalidated, a warning message must pop up.

1. **Session management**

**What is a session?**

Seasions are a simple way to store data for individual users against a unique session ID.

Session ID are normally sent to the browser via session cookies and the ID is used to retrieve existing session data.

**How are sessions managed?**

First, we must understand what is a HTTP requests/response? Hypertransfer Protocoal (HTTP) usually use to ask for a specific file from server to send back to your browser (maybe Chrome, Firefox, etc) and use to send the file from server to specific client.

A web session is a squence of network HTTP request and response transactions associated to the same user.

Session management is a technique used by web developer to make the stateless HTTP protocol support session state. For example: a user already been authenticated to the web server, the next HTTP request from that user SHOULD NOT be ask for verifying username again.

How session work in PHP? When you start a session, a server with send back a session ID. The next request will be identified by the session ID and the server will recognize it unless you ‘destroy the session’ or turn of the browser.

1. **Stateless programming**

**What is meant by the concept “stateless programming”? (refer to HTTP in your answer)**

Stateless is a concept to describe a computer program/application designed NOT to track any previous information/data that occurred.

Stateless programming is to apply the concept of staless to create a web application/computer program which depend from state (no need to keep track on the previous actions). This concept mainly apply on World Wide Web because it use the HTTP protocol which independantly on action to request a new web page without any knowledge of preivous pages requested.

HTTP definition: it stands for HyperText transfer protocol which is a set of rules stating how clients and servers communicate. For example, if British people use English to communicate, so browser (client) and server use HTTP to communicate with each other (with a topic is website).

HTTP (a definition we have been mention above) is called a stateless protocol because each request is executed independently, without any knowledge of the request that came before it.