**Author:** *Alessandro Ferro*

**ICTWEB502**

**Task 1**

**Student ID:** 83126277

Question 1: Explain the web-programming concept - authentication and web security in your own words.

**Answer**

Authentication is the process of verifying the identity of an actor interacting with a system.

There are three main ways in which authentication is implemented nowdays:

* User credentials – Probably the most common and widespread method. When accessing a website or a web application for the first time, the user sign-up and provide a username and a password. To access the resources of the website, the user then needs to login using the correct couple of username and password.

For this method to work effectively in providing a decent level of security, the password has to be articulated enough to be an hard guess for any malicious attacker. There are several website that show the ‘strength’ of a password when the user creates one, or that implement minimum requirements to be met in order to accept the creation of a password.

* Tokens – When a user request access to a resource, the application generate a one-time token, often in the form of a pin, which is sent to the user through text, email, authentication app, or by other means. The user is then prompted to insert the token and if the value of the token sent to the user and of the token entered by the user match, access is granted.
* Two-Factor authentication – It implements both of the previous mentioned methods. The use of matching username and password doesn’t give access straight away. Instead it triggers the creation of a token that also needs to be entered to be authenticated by the system.

The subject of authentication is also strictly related to session management. Because http is a staless protocol, it is important to implement ways to keep the state consistent during the transactions between the client and the server. This is mostly achieved by using session cookies, which work in a way non dissimilar from the token seen above, with the only difference that it is not a human receiving and providing them to the application.

Authentication is only the first step to consider when implementing web security measures. The second step, once the identity of someone or something has been proven, is to establish the level of authorization of that entity, which means what resources it can or cannot access.

Question 2: What is hypertext transfer protocol (HTTP)? What are the basic features of HTTP? What are the header fields in HTTP?

**Answer**

The Hyper Text Transfer Protocol (HTTP) defines how information are tranmitted over the web. It folllows a request-rresponse model, in which a client request resources to a server and the server handle the request and send back the response in a format that the client can process.

The requests sent by the client contain a request method, URI, protocol version and a MIME-like message with the modifiers, the client information and an optional body content sent over a TCP/IP connection.

The server response consists of a status line, protocol version, status code and MIME-lide message with server information, entity meta information and optional enntity-body content.

The basic features of http are:

* http is connectionless – client and server do not keep a connection open. Each request sent by the client is treated as a new one.
* http is media independent – http can be used t send any type of data that the client and the server can handle.
* http is stateless – as a result of being connectionless, http is also stateless. Client and server know of each other only during the request-response cycle. Outside of that cycle, no memory is kept and every request is treated as anew one.

HTTP headers provide additional information about the request, the response, the object sent in the message body, the client or the server.

In the request, the headers follow the request line, which contains the method, the URI and the protocol version.

In the response the headers follow the status line containing the protocol version, the nusmeric status code and the associated textual phrase.

The http headers can be grouped in four different categories:

* General headers – apply to both request and response and provide information and control over the message itself and how it is processed.
* Request headers – apply only to the request. They contain additional infromation about the resources requested or about the client, offering more context to the request and allowing to performm additional requests.
* Response headers – apply only to the response. They contain additional information about the server and the response to offer a better context.
* Entity headers – apply to both the request and the response. They contain information about the body of the message, such as content length, language, encoding or MIME type.

Question 3: Explain the web-programming concept – session management in your own words.

**Answer**

Sessions are a method adopted to work around the statelessness of the http protocol. Sessions allow to persist data between different client-server interactions, thus allowing dynamic content to be provided over the web.

For this to be possible, a user needs to be identified, recognized and authorized by the server and those authentication and authorization levels need to be kept consistent throughout the session by sending and receiving security tokens at every transaction.

This back and forth of sensitive information raises security concerns and session management addresses them by providing strategies and methods to prevent malicious attackers from appropriating them.

Some of these methods are:

* Applications should accept only cookies to identify sessions.
* The use of an encrypted communication channel (TSL)
* The security features of the cookies based exchange mechanism, such as Secure attributes, HttpOnly attribute, SameSite attribute, Domain and Path attributes, Expire and Max-Age attributes.
* HTML5 Web Storage API.

Question 4: What are the disadvantages of stateless programming?

**Answer**

A stateless program doesn’t persist any data between client-server interactions, thus the content provided by the server has some limitations.

The content provided by a stateless program cannot be personalized. Every time a client connect to the server, the server treat it as a new client. The server has no knowledge of previous interactions with that client and the content provided is the same as for any other client.

This represents a limit to the functionalities provided by a statelss program. User specific features, such the shopping cart of an ecommerce website, require the content to be unique for every user, and the same applies to online banking systems and any other security heavy program.

Persisting data in stateless programmming requires the use of session and cookies, which represent possible vulnerabilities that could compromise the security of a system and need to be carefully managed by the program.

Question 5: identify and describe internet technologies - programming control structures and provide three sample structures.

Control structures in programming refers to the logical blocks that determine the flow of a program.

A program rarely execute in a linear manner. There are several reasons why a block of code may need to be repeated for a certain number of times or until a condition is satisfied, or there are cases where one of either two or more blocks on code can be executed instead of the others.

These structures are the tools used to determine this behaviour and can be considered as the building blocks in the creation of algorythms.

There are three kind of control structures:

* Sequence control structures – The code gets executed line by line as it appears in the script, usually fromm top to bottom. It encompass any operation that follow the flow of a program without incurring in any of the other two types of control structures.
* Decision control structures – It evaluate a condition and depending on the outcome it executes/not execute a block of code, or execute one block instead of one or more others.

In this category there are:

* + If-the statements 🡪 IF condintion true THEN execute code
  + If-then-else statements 🡪 IF condintion true THEN execute code ELSE execute other code
  + Switch-case 🡪 BASED ON CASE execute SEQUENCE
* Iteration control structures. A block of code is repeated for a specified number of times or until a condition is met. Iteration control structures are usually (but not always) used in sinergy with collections to manage data.

Under this category fall:

* + For-loop 🡪 FOR number iterations EXECUTE code
  + While-loop 🡪 WHILE condition true EXECUTE code
  + Do-while-loop 🡪 DO execute code WHILE condition true
  + Foreach-loop 🡪 FOREACH item in array EXECUTE code

Question 6: identify and describe internet technologies - object-oriented programming and list three languages.

OOP is a programming model in which data are organised in structures called objects. Objects do not allow to directly manipulate the data; instead they expose methods (functions) created appositely.

This approach leaves the control over the data and their access, to the object.

The starting point to create an object is a class. A class is a blueprint. It defines attributes (data) the object will have, how they will be organized and it will deterrmine the methods to access and manipulate those data. An object is an instance of a class.

Object Oriented Programming follows four principles:

* Encapsulation 🡪 data are private to the class and are accessible only through the apposite methods.
* Abstraction 🡪 It abstracts the internal implementation of a class from its use. The inner mechanisms that make a class work are hidden, but mehod to make use of them are exposed.
* Inheritance 🡪 It allows to derive a child class from a parent class. The parent keeps all all the fields (attributes) and methods of the parent class and additionally can implement some of its own.
* Polymorphism 🡪 The same interface can be implmented in different ways by different classes.

Three OOP languages are:

1. Java
2. C#
3. Swift

Question 7: list and compare the following web browsers in different aspects.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Name | Creator | Platforms | Written in | Engines |
| Microsoft Edge | Microsoft | Cross-platform | C++, C# | Blink, v8 Javascript engine |
| Chrome | Google | Cross-platform | C, C++, Java, Javascript, Python | Blink, V8 Javascript engine |
| Safari | Apple | Apple | C++, Objective-C, Swift | WebKit, Nitro |

Question 8: Provide the differences between the Client-side scripting and Server-side scripting

**Answer**

Server side

* It constitutes the back end of an application
* It processes requests from the client
* It creates and manages sessions
* It provides authentication and authorization
* Can connect to a databse to retrieve data
* It processes the data from the database to make them mmeaningful to the client
* Has access to the file system of a server to create, read and write on a file
* It is compiled by the computer

Client side

* It represents the front end of an application
* It can send requests to the server
* It can manipulate cookies
* It can validate forms and other user inputs
* Update browser asynchronously
* Manipulate the DOM (either physical or virtual)
* Has access to the browser local storage
* Is platform independent
* Is interpreted by the browser.

# **Unit Assessment Result Sheet (UARS)**

## **Assessment Task 1 – Unit Knowledge Test (UKT)**

## **Student and Trainer/Assessor Details**

|  |  |
| --- | --- |
| **Unit code** | ICTWEB502 |
| **Unit name** | Create dynamic web pages |
| **Outcome of Unit Assessment Task (UAT)** | |  | | --- | | **First attempt:** |   Outcome (please make sure to tick the correct checkbox):  Satisfactory (S)  or Not Satisfactory (NS)  Date: \_\_\_\_\_\_\_(day)/ \_\_\_\_\_\_\_(month)/ \_\_\_\_\_\_\_\_\_\_\_\_(year)   |  | | --- | | **Second attempt:** |   Outcome (please make sure to tick the correct checkbox):  Satisfactory (S)  or Not Satisfactory (NS)  Date: \_\_\_\_\_\_\_(day)/ \_\_\_\_\_\_\_(month)/ \_\_\_\_\_\_\_\_\_\_\_\_(year) |
| **Feedback to Student** | |  | | --- | | * **First attempt:** |  |  | | --- | | * **Second attempt:** | |
| **Student Declaration** | * I declare that the answers I have provided are my own work. Where I have accessed information from other sources, I have provided references and or links to my sources. * I have kept a copy of all relevant notes and reference material that I used as part of my submission. * I have provided references for all sources where the information is not my own. I understand the consequences of falsifying documentation and plagiarism. I understand how the assessment is structured. I accept that all work I submit must be verifiable as my own. * I understand that if I disagree with the assessment outcome, I can appeal the assessment process, and either re-submit additional evidence undertake gap training and or have my submission re-assessed. * All appeal options have been explained to me. |
| **Student Signature** |  |
| **Date** |  |
| **Trainer/Assessor Name** |  |
| **Trainer/Assessor Declaration** | I hold:  🗹 Vocational competencies at least to the level being delivered  🗹 Current relevant industry skills  🗹 Current knowledge and skills in VET, *and undertake*  🗹 Ongoing professional development in VET  *I declare that I have conducted an assessment of this candidate’s submission. The assessment tasks were deemed current, sufficient, valid and reliable. I declare that I have conducted a fair, valid, reliable, and flexible assessment. I have provided feedback to the above-named candidate.* |
| **Trainer/Assessor Signature** |  |
| **Date** |  |
| **Office Use Only** | Outcome of Assessment has been entered onto the Student Management System on \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ (insert date)  by (insert Name) \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |