Question 1 0.1 / 0.1 points

The majority of web application attack occurs through cross site scripting (XSS) and SQL injection attack which typically result from flawed coding:

- ✓ ● True
- ○ False

Question 2 0 / 0.1 points

XSS needs authentic session.

- ✗ ○ True
- ➡ ● False

Question 3 0.1 / 0.1 points

The feature which ensuring that data is real, accurate and safeguarded from unauthorized user modification:

- ○ Authorization
- ○ Availability
- ✓ ● Integrity
- ○ Authentication

Question 4 0.1 / 0.1 points

The majority of web application attacks occur through cross-site scripting (XSS) and SQL injection attacks which typically result from flawed coding.

- ✓ ● True
- ○ False

Question 5 0 / 0.1 points

After establishing a TCP connection between browser and webserver, they communicate each other using _____ protocol

- ✗ ○ IP
- ○ TCP/IP
- ○ TCP
- ➡ ● HTTP

Question 6 0 / 0.1 points

WebGoat is a deliberately _____ maintained by OWASP (Open Web Application Security Project).

- ○ secured web application
- ➡ ● insecure web application
- ✗ ○ intercepting proxy tool
- ○ None of them

Question 7 0.1 / 0.1 points

Authorization is a process of verifying a correct user.

- ○ True
- ✓ ● False

Question 8 0.1 / 0.1 points

In cyber security, the web security deals with -

- ○ security of web applications only.
- ✓ ● security of websites, web applications and web services.
- ○ security of web developers.
- ○ security of IT product of an organization.

Question 9 0.1 / 0.1 points

The most common usage of ZAP is:

- ○ It encrypts the message.
- ○ It decrypts the secret message.
- ✓ ● It operates as an intercepting proxy.
- ○ It intercepts all the IP packets on the network.

Question 10 0.1 / 0.1 points

Cross-site scripting (XSS) targets an web application's users by _____, into a web application's output

- ✓ ● injecting JavaScript code
- ○ secret message
- ○ None of them.
- ○ sql query

Question 1 0.1 / 0.1 points

Denial-of-service attacks often use IP spoofing to overload networks.

- ✓ ● True
- ○ False

Question 2 0.1 / 0.1 points

An email from your manager asking for some information like name, credit card information of the company's top clients. The email says it's urgent and to please reply right away. You should reply right away. True or False?

- ○ True
- ✓ ● False

Question 3 0.1 / 0.1 points

Which one of these statements is correct?

- ○ If you get a message from a colleague who needs your network password, you should never give it out unless the colleague says it's an emergency.
- ○ If you get an email that looks like it's from someone you know, you can click on any links as long as you have a spam blocker and anti-virus protection.
- ○ You can trust an email really comes from a client if it uses the client's logo and contains at least one fact about the client that you know to be true.
- ✓ ● If you get an email from Human Resources asking you to provide personal information right away, you should check it out first to make sure they are who they say are.

Question 4 0.1 / 0.1 points

The security controls that are primarily implemented and executed by the system through the system's hardware, software, or firmware is:

- ○ None of them.
- ✓ ● Technical Controls
- ○ Management Controls.
- ○ Operational Controls.

Question 5 0.1 / 0.1 points

_____ is a table defining what access permissions exist between specific subjects and objects.

- ○ An access control list
- ○ Security Policy
- ✓ ● An access control matrix
- ○ None of them

Question 6 0.1 / 0.1 points

Physical access control limits access to computer networks, system files and data.

- ○ True
- ✓ ● False

Question 7 0.1 / 0.1 points

Email authentication can not protect against phishing attacks. True or False?

- ○ True
- ✓ ● False

Question 8 0.1 / 0.1 points

The WebGoat is a secured web application.

- ○ True
- ✓ ● False

Question 9 0.1 / 0.1 points

Defense in depth is an information assurance (IA) concept in which multiple layers of security controls (defense) are placed throughout an information technology (IT) system.

- ✓ ○ True
- ○ False

Question 10 0.1 / 0.1 points

Web applications can handle many HTTP requests simultaneously. Developers often use common resources like variables that are accessible by multiple threads. The race condition arises when multiple threads compete each others to get access those common resources. To avoid such race condition as a web developer you need to employ proper Synchronization.

- ✓ ● True
- ○ False

Question 1 0.1 / 0.1 points

Which statement is true for SQL injection attack:

- ○ The attacker must find a parameter that the web application passes through to a database.
- ○ It is a particularly widespread and the most dangerous form of injection.
- ✓ ● All of them
- ○ SQL Injection is a trick to inject SQL script/command as an input through the web front-end.

Question 2 0.1 / 0.1 points

Which one is a common security threat to a web server?

- ✓ ● All of them.
- ○ Unauthorized access.
- ○ Improper usage.
- ○ Denial of service.

Question 3 0.1 / 0.1 points

A firewall is a combination of hardware and software, located at a network gateway to filter all network packets to determine whether to forward them toward their destination or discard them.

- ✓ ● True
- ○ False

Question 4 0.1 / 0.1 points

A Web Hosting Network should have at least 2 segments

- ○ True
- ✓ ● False

Question 5 0.1 / 0.1 points

Web development tools (i.e. Web Developer) allow web developers to test and debug their code.

- ✓ ● True
- ○ False

Question 6 0.1 / 0.1 points

It is always bad practice to sanitize all input data, especially data that will used in OS command, scripts, and database queries', even if the threat of SQL injection has been prevented in some other manner.

- ○ True
- ✓ ● False

Question 7 0.1 / 0.1 points

Which statement is true for a web server:

- ✓ ● All of them.
- ○ Web Server is a computer host configured and connected to Internet, for serving web pages on request.
- ○ Since web servers are open to public access they can be subjected to attempts by hackers to compromise the server.
- ○ Web Server is a program that serves Web pages to Web browsers using the Hyper Text Transfer Protocol (HTTP).

Question 8 0.1 / 0.1 points

Server side applications are written in various programming languages, however, flaws in the scripts may allow attackers to penetrate a Web server.

- ✓ ● True
- ○ False

Question 9 0.1 / 0.1 points

Defense in depth is defined as the practice of layering defenses to provide added protection.

- ✓ ● True
- ○ False

Question 10 0.1 / 0.1 points

Which statement is true in secure coding practices:

- ○ Input data received through a web page form should be filtered for malicious input.
- ○ Encryption mechanism should be deployed to encrypt passwords.
- ✓ ● All of them
- ○ The code should use explicit path names when invoking external programs and not rely on the PATH environment value.

Question 1 1 / 1 point

_____ requires you to have a second device that will give you a one-time, temporary code that helps limit access to the account

- Multiple threads
- Multilevel passwords
- ✔ Two factor authentication
- All of them

Question 2 0 / 1 point

Database access control enables you to store data for many users in a single database and table, while at the same time restricting row-level access based on a user's identity, role, or execution

- ✖ True
- ➡ False

Question 3 1 / 1 point

To secure your servers,

- ✔ All of them
- sanitize the input in your application .
- Only communicate with the server with encrypted protocols.
- Employ WAF (Web Application Firewall), IDS (Intrusion Detection System), and IPS (Intrusion Protection System) for a multi-layered approach to security.

Question 4 1 / 1 point

In database access control, which principle should be followed to protect your database:

- ✔ Least privilege principle
- CEO's decision is the best decision
- Most privilege principle
- None of them

Question 5 0 / 1 point

In _____, a single specified type of statement (such as SELECT) on a specified schema object table Employees

- ➡ schema object auditing
- privilege auditing
- fine grained auditing
- ✖ statement auditing

Question 6 1 / 1 point

System integrity refers both to data integrity (correct and accurate data) and system is in operation and works correctly.

- ✔ True
- False

Question 7 1 / 1 point

Database security should be in place to ensure data access to authorized users and protect the data.

- ✔ True
- False

Question 8 0 / 1 point

_____ monitors the actions of database users to ensure the authorized access to the database.

- All of them
- ✖ Access Control
- ➡ Auditing
- Encryption

Question 9 1 / 1 point

There are two privileges in database, system privileges and object privileges.

- ✔ True
- False

Question 10 1 / 1 point

Database row level security is responsible to control the rules determined by security policies for all direct accesses to the database system.

- True
- ✔ False

Question 1 1 / 1 point

WebGoat is a free online tool used to test and uncover application flaws that might otherwise go unnoticed.

- ✔ ● True
- ○ False

Question 2 1 / 1 point

A clear description of responsibilities for every user at every possible step should be specified in your web application security policy.

- ✔ ● True
- ○ False

Question 3 1 / 1 point

Common Criteria (CC) is a local set of guidelines and specifications developed for evaluating information security products, specifically to ensure they meet an agreed-upon security standard for government deployments.

- ○ True
- ✔ ● False

Question 4 0 / 1 point

The basic components of a good security policy are: access policy, privacy policy, authentication policy, Availity statement.

- ➡ ● True
- ✖ ○ False

Question 5 1 / 1 point

In web application security policy, you should specify about database input sanitization.

- ✔ ● True
- ○ False

Question 6 1 / 1 point

An information security policy is a set of rules and guidelines that dictate how information technology (IT) assets and resources should be used, managed, and protected.

- ✔ ● True
- ○ False

Question 7 1 / 1 point

An acceptable use policy is a document stipulating constraints that a user must agree to for access to a corporate network or the Internet or to use any IT devices say, laptop, wifi access, etc.

- ✔ ● True
- ○ False

Question 8 1 / 1 point

Common Criteria has two key components: Protection Profiles, Evaluation Assurance Levels.

- ✔ ● True
- ○ False

Question 9 1 / 1 point

The goal of CC certification is to assure customers that the products they are buying have been evaluated and that the vendor's claims have been verified by a vendor-neutral third party.

- ✔ ● True
- ○ False

Question 10 1 / 1 point

Information security policies provide a framework for best practice that can not be followed by all employees of an organization.

- ○ True
- ✔ ● False