**CS/SE 611 - Secure Website Design - Final Exam**

**Instructor:    Professor Lozada**  
Class:    CS/SE 611

Student Name: Shobharani Polasa

Date:   04-24-2024

**Instructions** - Please select the best option for each question.

1)        What is a 3-tier application?  
    a.    Microservice, application, server  
    b.    Code, server, microservice  
    c.    Web, app, database ✔

2)        Threat Modeling should be done in the design phase of the?  
    a.    SDLC ✔  
    b.    Product Concept  
    c.    Application

3)        Traditional FWs can analyze Application Traffic?  
    a.    True   
    b.    False ✔

4)        Which Architecture has a large codebase  
    a.    Monolithic Architecture ✔  
    b.    Microservices Architecture  
    c.    Hybrid Cloud Architecture

5)        CLE encryption requires NO application changes  
    a.    True   
    b.    False ✔

          
6)        Security for Microservices begins with?  
    a.    API Gateway ✔  
    b.    Microservices Dependency  
    c.    API

7)        What controls Termination and Scaling polices?  
    a.    Auto-scaling Group ✔  
    b.    CloudWatch  
    c.    CloudFormation Templates

8)        Serverless is more cost effective?  
    a.    True ✔  
    b.    False  
          
  
9)        Which is not an Auto-scale type of management?  
    a.    Fleet Management  
    b.    Zone ✔  
    c.    Dynamic Management

10)        Which is not a STRIDE component  
    a.    Spamming ✔  
    b.    Information Disclosure  
    c.    Tampering

11)        What does GDPR stand for?  
    a.    General Data Protection Regulation ✔  
    b.    General Data Privacy Regulation  
    c.    Global Data Protection Regulation

12)        The two types of OAuth tokens are?  
    a.    Automatic & Renew  
    b.    Authorize & Refresh  
    c.    Access & Refresh ✔

13)        OS Level Access can be controlled by a WAF?  
    a.    True  
    b.    False ✔  
          
  
14)        Whole Database encryption uses multiple keys to encrypt  
    a.    False   
    b.    True ✔

          
15)        OAuth is an Authentication Protocol  
    a.    True  
    b.    False ✔

          
16)        Front-End is also known as?  
    a.    Server Side  
    b.    Client Side ✔  
    c.    Presentation Side

17)        Which is NOT an OAuth Actor  
    a.    Resource Owner  
    b.    Authentication Server ✔  
    c.    Client

18)        Which is NOT a DREAD component  
    a.    Damage potential  
    b.    Exploitability  
    c.    Reputation loss ✔

19)        Which Architecture allows you to write in any coding language?  
    a.    Monolithic Architecture  
    b.    Microservices Architecture ✔  
    c.    API Platform Architecture

20)        Which OAuth Flow is the most Vulnerable  
    a.    Implicit ✔  
    b.    Client Credential Flow  
    c.    Authorization Code

21)    Where should a privacy policy go on a website and why? Also, provide highlights of what the privacy policy should state. Please limit your answer to 2 paragraphs or less.

A privacy policy on a website is essential to ensure compliance and build user trust. This should be clearly placed, usually at the bottom of the webpage, to ensure that it can be accessed from any page. This selection process helps maintain transparency and meets the legal requirements of the European Union General Data Protection Regulation (GDPR), the California Consumer Privacy Act (CCPA in the United States), and other laws on data protection, best practice is global. This visibility ensures that users can easily see the policy to understand how their data is managed whenever they interact with the website Availability of the privacy policy does not necessarily force a website not only strengthens its guarantee of data security but also helps users make informed decisions about the use of their personal data on the web

The information in a privacy policy should be comprehensive and accessible, avoiding technical details that could obscure its message. At a minimum, the policy should describe the types of personal information the website collects, such as name, address, email address, payment information, browsing behavior and describe the purposes of each type of data collection, how it is used will use and for clearly those who can be shared The policy should also describe the security measures in place to protect personal information, including encryption and secure server information. Furthermore, users must be informed of their personal data rights, including the right to access, correct, update, or delete their information upon request Should the Regulation provide for them user instructions are used for exercising these rights, as well as the contact details of someone with internal organization In order to disclose, the privacy policy should be updated on a regular basis, and contact a clarity for users about any significant changes to how their data is handled

22)  An US based e-commerce website has been compromised and 6 million user records, including payment information has been leaked, some users records are from customers in the EU, also the data was not encrypted.  After some initial investigation it was determined that the website had been probed for several months by nation state actors.  It was also determined the US based e-commerce website company had several Security technologies mis-configured or missing. Below is a list of the technologies.  Please highlight where these technologies go and why.  Please limit your answer to 3 paragraphs or less.

* Web Application Firewall
* Firewall
* Antivirus
* HSM (Hardware Security Module)
* IDS & IPS

It has been destroyed on the US-based e-commerce website. on each of the listed security technologies plays a key role in protecting data and infrastructure, their proper configuration and implementation is essential for improved security First, Web Application Firewall (WAF) Filtering, HTTP traffic a maintained between web applications and the Internet and designed to protect web applications. In order to protect against vulnerabilities such as SQL injection, cross-site scripting (XSS), and others that must be implemented at the application level to monitor incoming web traffic it is important to configure a WAF to block requests bug edge before it reaches the web server .

The firewall operates at the network layer and can be configured to define and control what traffic is allowed in and out of the network. It acts as the first line of defense against unauthorized access, helping to prevent attackers from accessing the network where they can access sensitive data such as payment information Firewall codes a well-organized system based on the principle of least privilege ensures that only appropriate vehicles are allowed. In addition, all endpoints and servers should use antivirus software to detect, hide, and remove malicious software that could be used to dump data or as part of a ransomware attack For regular updates and real-time scanning needed to remain effective against new and emerging threats.

Hardware security modules (HSMs) are physical devices that manage digital keys for strong authentication and provide encryption functionality. HSMs are used in environments that require high levels of security for the storage and manipulation of encryption keys. Placed where sensitive data such as payment information is processed or stored, to ensure encryption and key management where potentially compromised operating systems cannot reach the final destination, the Intrusion Detection System ( IDS) and Intrusion Prevention System (IPS) activities suspicious, potential threats f It is critical to detect and respond to IDS monitors network traffic for unique operating systems that indicate potential attacks, while IPS proactively prevent such threats based on known anomalies IDS and IPS together enhance the level of security through real-time monitoring of network activity Actors and third parties including advanced persistent threats