Sreeharinaidu rangani
Z23749310
Exam

1 A.What is the FPR at threshold 2?

FPR= FP / (FP + TN). (at threshold 2 FP=7, TN=63)

= 7/7+63 => 7/70 = 0.1
FPR=0.1

B.What is the FRR at threshold 5?

TPR= TP / (TP + FN). (at threshold 5 TP=24, FN=6)

= 24/24+6 => 24/30 = 0.8
FRR=1-TPR
FRR=1-0.8
FRR=0.2

1) A. What is anomaly detection?

Finding behavior that deviates from the norm is the aim of anomaly detection. Anomaly detection can identify fresh, undiscovered threats.

B.

By recognizing specific patterns and comparing them to known vulnerabilities, Signature Detection enhances system security by preventing threats and identifying them. This process also helps to create a counterattack strategy by comparing recorded patterns of known vulnerabilities to known vulnerabilities.

3)

Well from my past assignment experiences in CDS , I know some of the common security flaws and avoidance measures. Like cross – site- scripting and broken access control (recent my personal project). Below screenshot showing BST page with payment method but we don't know any backend functionality like input handling and api functionality.

A)

Well its just one input filed you know. If programmer doesn't sanitize the coming inputs, the attacker might attack this site by injecting Javascript code into that input filed. By simply injecting js code in the input filed the attacker can take over your application. I would say if input input filed doesn't sanitized properly then XSS attack will occur.

b)
to assess the vulnerability to CSRF, we would need to understand the site's handling of state-changing requests and whether it uses anti-CSRF tokens. If the site processes state-changing actions without requiring a unique token, which the server has to verify, it may be susceptible to CSRF attacks.

c)

XSS Mitigation Methods:
Sanitize input by escaping special characters or any Tags, thus preventing the execution of HTML and JavaScript.
Use Content Security Policy (CSP) headers (use HTTP only cookie) to restrict the sources of executable scripts.
And implement best security methods to input sanitization. And Use strict organization security ploicy to review client requirements.

CSRF Mitigation:

Use anti-CSRF tokens that are unique to each user session and validate them for each state-changing request.
Ensure that requests are accepted only from authenticated and authorized users.
Employ the SameSite cookie attribute to prevent the browser from sending cookies with requests initiated by third-party websites.

For the BST website to be robustly secured, essential defenses must be established. Furthermore, incorporating periodic security audits and vulnerability assessments into the development process is crucial for maintaining continuous defense against various security risks.

4)

a.) It looks that the vulnerability in this comic is a lack of input validation or data sanitization, which could lead to data corruption or loss.
b.) Losing student records might be a serious consequence of this vulnerability, with potentially dire consequences for both the school and the impacted students. In addition to possible legal and reputational repercussions, this may result in administrative difficulties and the loss of important data.

c) Adequate data sanitization or input validation approaches could have prevented the harm depicted in the cartoon. This could be cleaning and verifying user input to stop unexpected or harmful material from being processed or stored, setting up suitable authentication and access controls to stop unauthorized access, and regularly backing up and protecting sensitive data to stop damage or loss.

5)

A)Validating user input involves ensuring that the data is entered in the correct format, type, and range and that no unexpected or dangerous characters are present that could lead to unexpected behavior, security issues, or mistakes. The accuracy, security, and stability of a program are the result of input validation, which is a crucial component of software development.
When incoming data is validated, it is often compared to a predetermined set of standards or criteria. The format (such as regular expressions), allowable values, length or size restrictions, and data type (such as date, text, or numeric) may all be specified by these rules.

B)

Client-side validation: This method uses JavaScript or other client-side scripting languages to validate user-input data on the client-side. Using this method, the data is sent to the server after being verified by the user's web browser.

Server-side validation: This method uses a server-side programming language like PHP, Python, or Ruby to verify user-input data on the server. With this method, the data is sent to the server, where it is validated. Because hostile users cannot defeat server-side validation, it is more secure than client-side validation.

Mixture of the two: Client-side and server-side validation can be used together to maximize their benefits and minimize their disadvantages. This approach uses server-side validation to provide a more thorough and secure validation procedure, while client-side validation is used to give users rapid feedback and lessen server load.

C)

It's generally accepted that the most secure method of input validation is server-side validation. Server-side validation prevents attackers from easily changing or evading the validation process because it is done on the server.

As attackers with the capacity to alter client-side code or intercept data being transmitted to the server can easily get around it, client-side validation shouldn't be the only approach

used for input validation, even if it can benefit users by giving them fast feedback and lowering server demand.

6)

Privacy: Each person's right to manage their personal data, including the freedom to decide who can access it and how.
Puts emphasis on a person's right to control their personal information.
.Relevant to persons and their personal data in a variety of circumstances, the three primary privacy issues are autonomy, data control, and protection of personal information.

Security is the application of extensive procedures and processes to guard resources, data, and assets against loss, theft, and illegal access.
- Incorporates a wide range of precautions to shield resources, data, and assets from different threats.

Applyable to organizations, systems, and resources to prevent illegal access, damage, or theft. - Encompasses integrity, availability, and confidentiality of information and resources.

Confidentiality: A subset of security that aims to stop sensitive data from being disclosed without authorization.
*a portion of security that is especially focused on protecting private information so that only authorized parties can access it.
- Mainly applied to specific information, frequently related to business, legal, or sensitive data requiring restricted access; - Prevents unauthorized disclosure of sensitive data, upholds trust, and ensures limited access to specific information.

7)

A)
Symmetric encryption uses a single key.
- The key sizes are 128 to 256 (AES) and 56 to 112 (DES).
- The key needs to remain a secret.
- The distribution of keys needs to be out of band.

This place has quicker speed.
Asymmetric Cryptography: Two keys are used.
- The key size is unrestricted, provided that it is at least 256.
- One key needs to be kept private, while the other can be distributed.
- Distribution to other keys is done via the public key.

Here, the pace is slower.

B) The symmetric encryption algorithms DES and AES are examples of this.

One popular symmetric encryption method for safe data transfer is AES. It can handle keys with lengths of 128, 192, or 256 bits and works with fixed-size data blocks.
Older symmetric encryption standard DES is now seen as less secure because of its little key size (56 bits).
In both scenarios, the encryption and decryption processes employ the same key.
You have to keep the key hidden.

C)
RSA is a popular asymmetric encryption method that uses a public key for encryption and a private key for decryption to provide secure communication.
Public key cryptography, sometimes referred to as asymmetric cryptography, includes the following features: • Every user has two keys—one public and one private—and messages encrypted using a user's public key can only be unlocked with that user's private key.
RSA is a popular asymmetric encryption method that uses a public key for encryption and a private key for decryption to provide secure communication.
Public key cryptography, sometimes referred to as asymmetric cryptography, includes the following features: • Every user has two keys—one public and one private—and messages encrypted using a user's public key can only be unlocked with that user's private key.

8)

a) A hacked system could allow an attacker to run their code with elevated privileges if the code is run with "Prog Ctr" on the stack. Unauthorized access to the system's resources follows from this.

b) Vulnerabilities related to buffer overflows can let attackers inject any code into the stack. An attacker can take advantage of this by overwriting the program counter with a new value that refers to malicious code they have injected into the stack. This occurs when the data flows beyond what the buffer can hold, which can subsequently overwrite nearby memory space, including the program counter.

c) It can be found using code analysis tools, which examine the source code to track how the program behaves while running.

d) Programmers should use safe library functions, validate input sizes, perform bounds checking, and use languages and compilers with overflow protection in order to develop secure code. Additionally, buffer overflow vulnerabilities can be successfully prevented from being exploited with the use of mitigation measures like stack canaries and non-executable stack space.

9)

a) Consider a security kernel to be the head of a safe operating system, acting as its principal protector. It determines who has access to what resources, ensures that security

regulations are obeyed, and segregates and secures critical security responsibilities. It serves as the main barrier ensuring the security of the system.
b.) To implement and uphold the system's security policy, a security kernel should have the fundamental security features and methods, such as process isolation, auditing, authentication, and access control.
c.) To lower the risk of security flaws and the possible attack surface, it shouldn't have extraneous complexity or non-essential features.

10)

The above figure illustrates an assault on the TCP three-way handshake.
SYN, or synchronize:To establish a connection, the source sends a TCP packet to the destination with the SYN flag.
The destination receives the SYN packet and responds with a packet containing both the SYN and ACK flags to signal that it is prepared to establish a connection. This protocol is known as SYN + ACK (Synchronize + Acknowledge).
ACK stands for acknowledgement.After receiving the SYN and ACK packets, the source device confirms the TCP connection by sending an ACK back to the destination.
By taking these three steps, you can be sure that before transferring data, the source and destination systems agree on the creation of a trustworthy and organized communication channel.

11)

My project is on **broken access control** . Nothing I guess my project is better . if I wanted to change I feel I need to take different example. For my project demonstration I have used student result portal. If I wanted to change something I would do a bigger project example like organization level