Tutorial (Topic 1)

Q1.

Your IT company is implementing an Online-Booking system for Condo facilities. Only the condo

residences are allowed to use the Booking system. There are several security attributes to think

about for this system.

1. Define the Security terms Confidentiality, Integrity and Availability (CIA) and Authenticity

C – Ensures that only authorized individuals can view information

I – Ensures that only authorised individuals can change or delete information

A – Ensures that data, or the system, is available for the authorized user when required.

ii. Describe the security attributes that is related to CIA. (e.g What constitutes to

Confidentiality in the Booking system as a whole?)

C – Encryption of data or communication. Login feature of the website.

I – update profile page information with authorisation check. Users are allowed to make changes to ONLY their own account.

A – security system is reliable, and website has proper backup system for disaster recovery.

Q2.

Describe the following terms and explain how are they related?

1. Vulnerability

Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source.

Common web app vulnerability can be in e.g. <http://cve.mitre.org/>

1. Threat

Any circumstance or event with the potential to adversely impact organisational operations (including mission, functions, image, or reputation), organisational assets. Or individuals through an information system via:

* Unauthorised access
* Destruction
* Disclosure
* Modification of information
* Denial of service

Relationship between threat and vulnerability; threats exploit vulnerabilities in order to obtain, damage or destroy assets.

Q3.

For the security formula: Protection = Prevention + (Detection + response), describe how you would

implement Preventive, Detective as well as Responsive behaviour to protect your website.

Prevention

* Firewalls to monitor user activities and control access to web server
* Access control such as login or authorization
* Encryption to hide data from unauthorized users

Detection

* Audit logs to record user activities which can be used for immediate or post hacking activities.
* Intrusion detection system to detect any anomalies in user activities.

Response

* Web application backups are required for recovery process after the hacking activity.
* Incident Response Teams to analyse security breaches and take any necessary responsive measures. (e.g. decision to continue web site operation or disconnect from Internet after an attack?)
* Computer forensics is required to gather evidence of the attack either on the network, website or server.

Q4.

“You do not need to worry about Network level and Host level security while developing a web

application as it is running on the application layer”.

Provide arguments in favour or against for the above statement.

Firewall is a network level device that enforce secure network traffic by providing application-specific filtering to block malicious communications.

Hosts such as windows 10 or windows server only provides OS-level security. (E.g network or local accounts, apply OS patches etc)

As a web developer, you should not be overly concerned by network and host level security. However, developers need to be aware of Web Server configuration as the website is hosted on a web server.

Q5.

Explain the differences between Authentication and Authorization. Provide examples to your

Explanation

Authentication

* Ensures that an individual is who he claims to be
* Login does not ensure the authenticity of a user (e.g. password can be shared)
* Enhanced login such as 2FA, biometric are good examples

Authorization

* Restricted access to specific users
* More about roles and permissions