Secure Software Development Coursework 1 Individual Reflection

AstroDev Security Requirements

1. **Preventing Denial of Services from Spaceships to Ground Control**
    - Asset: Datasets
    - Threat: Denial of Service
    - Narrative: Datasets may deny its services to the spaceship, which will prevent ground control from accessing the flight logs to then provide the next coordinates for the spaceship to fly to.
    - Work Required: Implement appropriate authentication and authorisation methods to prevent authorised users from being locked out of access, whilst also prevent unauthorised users from access.
    - Verification: Test different users, from authorised to unauthorised, to investigate if the datasets deny its services appropriately.
2. **Preventing Unauthorised Access and Updates to the User Credentials Database**
    - Asset: User Credentials Database
    - Threat: Tampering and Elevation of Privilege
    - Narrative: An unauthorised user has access to the confidential user credentials database. From there, they can modify user information and indirectly affect operations between spaceships and ground control.
    - Work Required: Encrypt data within the database, where only authorised users can decrypt requested data.
    - Verification: Attempt to access data with an unauthorised user account. Rework the solution based on findings, if any at all.
3. **Verifying User Identity to Prevent Unwanted Access to Chat Logs**
    - Asset: Chat Data
    - Threat: Spoofing
    - Narrative: Attackers may pose as authorised users to access chat logs between ground control and spaceships.
    - Work Required: Implement Multi-Factor Authentication during account login, so that unauthorised users are locked out of confidential chat logs
    - Verification: Test Multi-Factor Authentication amongst different accounts.

DefenceVenture Security Requirements

1. **User Authorisation for Database Access**
    - Asset: Databases

- Threat: Tampering
- Narrative: An attacker abuses the application to perform unintended updates to a database.
- Work Required: Implement appropriate authorisation measures and introduce integrity checks, such as Hashes and Digital Signatures.
- Verification: Test the integrity methods using unauthorised accounts to update the database with. Rework the solution accordingly based on results.

2. **Monitor Network Packets to Authorise Users**
    - Asset: Network
    - Threat: Denial of Service
    - Narrative: Attacker launches a denial of service (DDoS) attack, preventing the network from being used.
    - Work Required: Network monitoring to ensure packets are from an authorised user.
    - Verification: Send malicious data packets in a closed network to test the system. Rework the solution based on the effect of the packets. Ensure users sending packets are authorised with the network through checks.
3. **Restrict Privileges from Users to Prevent Unwanted Activity**
    - Asset: Defence System
    - Threat: Elevation of Privilege
    - Narrative: A user may access more data than they need, allowing them to have too much control over a system.
    - Work Required: Give a user the minimum number of permissions to be able to do their job.
    - Verification: Test accounts with different levels of privileges and see which ones can perform certain tasks.