AstroDev Security Requirements

Spoofed Pages

- **Asset**: User accounts
- **Threat**: Spoofing
- **Narrative**: Attackers may create a false page to attempt to gain access to user accounts by getting them to log into the false page to grab their credentials which the attacker can then use to access the legitimate site.
- **Work Required**: All pages must have 2FA (2 factor authentication) to protect against potential spoofing attacks, as well as a separate network to access the web to ensure the safety of the closed network.
- **Verification criteria**: Ensure that the 2FA is working properly though login attempts ensuring that the generated password works rather than a random string of numbers, the password is generated securely, and that the computers on the closed network cannot access the live web.

Data leak from the database

- **Assets**: User data, Sensitive data, Research Data
- **Threat**: Disclosure of information
- **Narrative**: Staff (or an attacker with unauthorised account access) gains access to an area of a dataset that they should not have access to. This could lead to a data leak of sensitive/ personal data from AstroDev which could put the company at risk financially and the employees at risk as their data may have leaked.
- **Work Required**: A minimum privilege access needs to be implemented for accounts. All data is on a need-to-know basis, so only those who require access to specific data on a regular basis will be able to access it. Anyone who needs access to data that is out of scope, will require approval from an administrator to ne able to access the data. Each approval will also require a log to be filled out explaining the why the data is needed.

- **Verification**: Test accounts at each level will attempt to access data that is outside of their scope. They will then request access to the data to a test admin account to verify whether a log has been filled before the data can be released.

Ship Logs being tampered with

- **Assets**: Astro data, spacecraft
- **Threat**: Tampering, repudiation
- **Narrative**: Tampering with the data logs could lead to fatal consequences on the spacecraft. If the navigation logs are tampered with, the ground control systems would produce a false calculation for the ships navigation system which could lead to the spacecraft to get lost in deep space. Should something go wrong, and the data was tampered with, this could hinder any investigation and would lead to destruction of evidence for an investigation.
- **Work Required**: Only the top administrators have modifying privileges to this database, everyone else will only have read-only privileges. All data should be logged when information is altered so that the data cannot be tampered with by an admin. The logs created by this should be un-modifiable by anyone and read-only to those who need access to those logs.
- **Verification**: A test dataset that simulates the actual dataset, using an admin account to test the correct privileges and whether the logging system works correctly based on the requirements of the system.