OWASP Top Ten
A2:2017-Broken Authentication

Risk - If an attacker gains access to multiple accounts or an admin account, they can compromise a system. This can lead to the disclosure of highly sensitive information.

Severity = 3
Justification - Because of the design and execution of most identity and access restrictions, faulty authentication is common. Session management, which is inherent in all stateful systems, is the foundation of authentication and access restrictions.Broken authentication may be detected manually and exploited using automated methods such as password lists and dictionary attacks.

Remediation

1. Use multi factor authentication to avoid credential stuffing, brute force attacks, and stolen credentials being used.
2. Default credentials should not be used.
3. Implement password-strengthening measures, such as comparing new or modified passwords against a list of the top 10,000 worst passwords.
4. Decrease the number of unsuccessful login attempts by limiting or delaying them.
5. Use random session IDs for logins, but don't include them in URLs. they should be kept secret.

A10:2017-Insufficient Logging & Monitoring

Risk - Failure exposes all data that's meant to be kept safe. Health records, credentials, credit cards and personal data are usually in this data.

Severity = 2
Justification - The issue is that sensitive data is not encrypted. Poor key creation, and management, as well as weak algorithms.

Remediation

1. Classify the data that an application processes, stores, or transmits. Determine which information is sensitive in light of privacy rules, regulatory obligations, or commercial considerations.
2. Implement controls in accordance with the categorization.
3. Don't keep critical information around needlessly. It should be discarded as quickly as feasible, or it should be tokenized or truncated in accordance with PCI DSS. It is impossible to steal data that is not saved.
4. Make sure all sensitive data is encrypted at rest

A3:2017-Sensitive Data Exposure

Risk - Vulnerability probing is the starting point for the majority of successful attacks. Allowing such probes to run can increase the chances of a successful exploit to nearly 100%.

Severity = 2
Justification - According to an industry poll, this issue is among the top ten.
Examining the logs after penetration testing is one approach for assessing if you have enough monitoring. The actions of the testers should be documented in order to know the extent of any harm they may have caused.

Remediation

1. Logs are generated in a format that can be easily consumed by a centralized forensic analysis system.
2. Establish or implement an incident response and recovery strategy, such as NIST 800-61 rev 2 or later, to ensure that suspicious actions are recognized and reacted to in a timely manner.
3. Ensure that all login, access control, and server-side input validation failures can be logged with sufficient user context to identify suspicious or malicious accounts, and held for sufficient time to allow delayed forensic analysis, according to the risk of the data stored or processed by the application.