A10 - Insufficient Logging & Monitoring

Attackers rely on the lack of monitoring and timely response to achieve their goals without being detected. Exploitation of insufficient logging and monitoring is the bedrock of nearly every major incident. One strategy for determining if you have sufficient monitoring is to examine the logs following penetration testing. The tester’s actions should be recorder sufficiently to understand what damages they may have inflicted. Most attacks start with vulnerability probing. Allowing such probes to continue to raise the likelihood of successful exploit to nearly 100%.

Medication

Ensure all login, access control failures, 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. Developers should ensure that logs are generated in a format that can be easily consumed by a centralized log management solutions. Ensure high-value transactions have an audit trail with integrity controls to prevent tampering or deletion, such as append-only database tables or similar. Developers should establish effective monitoring and alerting such that suspicious activities are detected and responded to in a timely fashion.

Example

An open source project forum software run by a small team was hacked using a flaw in its software. The attackers managed to wipe out the internal source code repository containing the next version, and all of the forum contents. Although source could be recovered, the lack of monitoring, logging or alerting led to a far worse breach. The forum software project is no longer active as a result of this issue. Another one is when an attacker uses scans for users using a common password. They can take over all accounts using this password. For all other users, this scan leaves only one false login behind. After some days, this may be repeated with a different password.