Sony's PlayStation Network Hack (2011)
Vector Attack Type: SQL Injection

Incident Response Plan

1. Detection Methods
    - Automated System Alerts: Configure an Intrusion Detection System (IDS) to monitor for SQL injection signatures, such as unusual or unexpected SQL commands from user input fields.
    - User Reports: Encourage users to report irregularities, such as unexpected changes in their account, loss of access, or account data modifications.
    - Audit Log Analysis: Regularly review logs for unusual access patterns, especially during off-hours or from unknown IP addresses, to detect unauthorized data access or modification.

2. Incident Classification
    - Low (Level 1): Single SQL injection attempt blocked by IDS.
    - Medium (Level 2): Multiple SQL injection attempts from a specific IP or pattern, suggesting persistent probing.
    - High (Level 3): Successful data access or compromise of sensitive user information.

3. NIST Incident Response Lifecycle for SQL Injection Attack
    - Phase 1: Preparation
        - Secure all applications against SQL injection with prepared statements and input validation.
        - Ensure the incident response team is equipped to manage database-related attacks and has access to logging and monitoring tools.
    - Phase 2: Detection & Analysis
        - Detection: An alert is triggered by the IDS for SQL injection attempt detection.
        - Analysis: The incident response team assembles to identify the attack source, assess the attack's scope, and determine if sensitive data was accessed. Classify the severity based on the intrusion's scope.
    - Phase 3: Containment, Eradication & Recovery
        - Containment:
            - Immediately block the IP address or access point associated with the SQL injection attempts.
            - Restrict access to sensitive databases and enforce stricter access controls during containment.
        - Eradication:
            - Apply input sanitization and implement secure coding practices to prevent further SQL injections.
            - Update applications to use parameterized queries, ensuring no user input can modify database queries.

        - Recovery:
            - Restore compromised data from a recent, clean backup.
            - Run integrity checks on the database to ensure all data is intact and no backdoors remain
            - Monitor post-recovery activity to catch any lingering threats.
    - Phase 4: Post-Incident Activity
        - Lessons Learned: Review the incident to identify gaps in SQL injection defenses and improve response time.
        - Improvements: Update IDS to better detect SQL-based anomalies and refine input validation policies.
        - Reporting: Compile a detailed incident report, addressing key points such as the detection method, containment steps, and lessons learned.

Security Rules/Guidelines

Rule 1: Data Access Control

- Purpose: Restrict access to sensitive data to only authorized users.
- Guidelines:
    - Apply the principle of least privilege by granting minimal permissions to users based on their roles.
    - Multi-factor authentication (MFA) should be used for accessing critical systems
    - Regularly audit user permissions to ensure they are up-to-date and relevant.

Rule 2: Input Validation and Parameterized Queries

- Purpose: Protect against SQL injection and data manipulation attacks.
- Guidelines:
    - Implement input validation on all web applications and APIs to ensure data is safe before processing.
    - Use parameterized queries and prepared statements in SQL queries to prevent user input from modifying the query structure.
    - Regularly test applications for SQL injection vulnerabilities through vulnerability assessments and penetration testing.

Rule 3: Data Backup and Recovery Plan

- Purpose: Ensure data availability and continuity in case of a breach or data loss.
- Guidelines:
    - Automate daily backups of all critical data and store backups in a secure, offsite location.
    - Test the backup and recovery process quarterly to verify data restoration procedures.
    - Implement access controls to ensure only authorized personnel can perform or access backups.

Maintaining the CIA Triad

The CIA Triad—Confidentiality, Integrity, and Availability—is maintained through the following policies and procedures:

- Confidentiality: By enforcing data access control and applying the principle of least privilege, we limit access to sensitive data. Multi-factor authentication further protects user credentials, minimizing unauthorized access risks.
- Integrity: Input validation, parameterized queries, and regular security assessments ensure data accuracy and authenticity. Eradication and recovery processes restore data integrity after an incident, verifying that data remains unaltered and secure.
- Availability: Automated backups and tested recovery procedures help ensure data availability even after an attack. Containment strategies limit the scope of an incident, minimizing downtime and maintaining system availability for authorized users.

Legal and Ethical Compliance

Overview

This section ensures the incident response plan meets relevant legal requirements and adheres to ethical principles, safeguarding user rights and maintaining organizational integrity. Legal compliance provides guidelines on how to handle data breaches, while ethical standards uphold the organization's commitment to transparency, privacy, and accountability.

Relevant Laws and Regulations

1. General Data Protection Regulation (GDPR)
    - Scope: GDPR requires organizations that handle the personal data of EU residents to take strict measures to protect that data and report breaches within 72 hours.
    - Requirements:
        - Prompt notification to affected individuals when personal data is compromised.
        - Implementation of technical and organizational security measures to prevent unauthorized access.
2. California Consumer Privacy Act (CCPA)
    - Scope: CCPA mandates data protection standards for California residents and requires organizations to disclose data collection practices and allow consumers to request deletion of their data.
    - Requirements:
        - Protect the privacy and security of consumer data.
        - Notify consumers of any breach involving their personal information.
        - Ensure transparent data processing practices and provide opt-out options.

Ethical Consideration

- Transparency and Accountability: Ethical standards demand that organizations communicate openly with affected parties and stakeholders about any data compromise.

This includes timely, accurate disclosures about the extent of the breach and the steps being taken to protect user data. Acting with transparency builds trust and upholds the organization's reputation.

Upholding Legal and Ethical Standards in the Incident Response Plan

1. Compliance with Notification Requirements
    - The response plan includes immediate detection and analysis steps to quickly identify a breach and determine its scope. This enables the organization to notify affected individuals and relevant authorities within the required timeframe (e.g., 72 hours for GDPR). Such swift action minimizes potential harm to users and ensures adherence to legal notification mandates.
2. Data Protection and Minimization
    - By enforcing access control measures, input validation, and backup strategies, the organization complies with GDPR and CCPA standards on protecting and limiting data access. These safeguards reduce the risk of unauthorized data access, aligning with legal obligations to protect consumer privacy.
3. Ethical Communication and Transparency
    - The post-incident activity includes preparing a report detailing the breach, actions taken, and lessons learned, which can be shared with stakeholders. Clear and honest communication on data breaches ensures accountability, upholding ethical principles and strengthening trust.

SHA256:

- Input: TuMama
- Output: 9bc3c2729e1d9d0a0f06a18eae4f5fd234fb7d19845539e30b5548df9c686670

AES Encryption

- Input: anything
- Passphrase: bruhhh
- Output: 53616c7465645f5f24a879685bb4ece365a6a45e538c0bed29d99dd1f83e8a9e