Charlotte’s Web 2: The SQL

Web Application Attack Response Plan

The Facts Were These: Hacka Thee Attacka exploits a SQL injection vulnerability to access customer data in the backend database.

Below is a breakdown of each phase of the plan and a rough estimate of the timeline starting from the detection of the threat to the recovery stage.

Immediate Actions (0-30 minutes)

Detection

Web application firewall (WAF) alerts.
Unusual database query patterns.
Application error logs showing injection attempts.
Unauthorized data access alerts.

Initial Response

Block suspicious IP addresses at WAF/firewall.
Enable additional logging and monitoring.
Preserve evidence of attack attempts.
Assess immediate risk to data and systems.

Containment (30 minutes - 2 hours)

Application Security

Implement emergency WAF rules to block attacks.
Restrict database access if necessary.
Disable vulnerable application features.
Implement rate limiting and IP blocking.

Data Protection

Identify potentially compromised data.
Assess scope of data exposure.
Monitor for data exfiltration attempts.
Implement additional database monitoring.

Investigation (2-8 hours)

Attack Analysis

Analyze web server and application logs
Review database logs for unauthorized queries.
Identify attack vectors and methodology.
Assess extent of data compromise.

Vulnerability Assessment

Conduct emergency vulnerability scan.
Test for SQL injection and other web vulnerabilities.
Review application code for security flaws.
Assess related applications for similar vulnerabilities.

Recovery (8-24 hours)

System Patching

Apply security patches to vulnerable applications.
Update WAF rules and signatures.
Implement code fixes for identified vulnerabilities.
Update database security configurations.

Validation

Conduct penetration testing on fixed applications.
Verify WAF effectiveness against known attacks.
Test application functionality after patches.
Validate database integrity and security.

Communication:

.

- **Internal**

    - Notify development and operations teams.
    - Inform legal and compliance teams.
    - Update senior management on incident status.
    - Coordinate with customer service if needed.

- **External**

    - Notify affected customers if data was compromised.
    - Report to regulatory authorities if required.
    - Coordinate with law enforcement if necessary.
    - Update security vendors and partners.

Post-Incident

Implement secure coding practices.
Conduct security code reviews.
Implement regular vulnerability assessments.
Update web application security policies.