Title: Web Application Attack - Incident Response Playbook

* Question: You are a security operations system analyst and helpful cybersecurity assistant that generates detailed incident response playbooks based on NIST guidelines. please generate a playbook for a web application attacks effectively?
* Answer:

1. Preparation:

Objective: Establish contacts, define procedures, and gather information to save time during an incident.

- \*\*Cybersecurity Incident Response Team (CSIRT)\*\*:

- \*\*Core Members\*\*: Include individuals responsible for cybersecurity, possibly supplemented by IT roles depending on organization size. Limit size to maintain confidentiality and efficiency.

- \*\*Extended Members\*\*: Include Legal, Compliance, Public Relations, and Executive Leadership.

- \*\*Roles and Responsibilities\*\*: Assign clear roles to core and extended team members.

- \*\*Escalation Paths\*\*: Define escalation paths for incidents starting as events or lower-severity issues.

- \*\*Third-Party Web Hosting Contacts\*\*:

- Document contact details for web hosting providers.

- \*\*Logging\*\*:

- Ensure logging levels for account login systems are set appropriately (minimum 90 days).

- Store logs securely on secondary systems like a SIEM.

- \*\*Backups\*\*:

- Ensure web application backups are functioning as expected.

2. Detection and Analysis:

Objective: Detect the incident, determine its scope, and involve appropriate parties.

- \*\*Hosting Service Communication\*\*:

- Contact hosting providers to report issues and inquire about recent security concerns.

- Obtain and preserve logs from the hosting service.

- \*\*Evidence Analysis\*\*:

- Determine next steps based on evidence of compromise (e.g., abnormal web application behavior, client reports, phishing attacks).

- \*\*Method of Compromise\*\*:

- Interview impacted users to gather details on potential points of compromise.

- Search for phishing emails and malicious web history indicators.

- Investigate malware presence (e.g., credential harvesters, keystroke recorders).

- Use Indicators of Compromise (IoCs) to identify other potential victims.

- \*\*Log Review\*\*:

- Search logs for anomalies (e.g., login activity from unusual locations).

- Assess victim accounts for sensitive data exposure.

- \*\*Web Application Vulnerabilities\*\*:

- Perform security scans and review vendor notifications and community threat intelligence.

3. Containment:

Objective: Mitigate the attack’s effects on the environment.

- \*\*Account Compromise\*\*:

- Reset all management/administrative account passwords.

- Enable Multi-Factor Authentication (MFA) for impacted accounts.

- Revoke authentication tokens and reset alternative authentication methods.

- \*\*Malware Discovery\*\*:

- Preserve malware samples for analysis.

- Block IoCs in email systems, firewalls, and endpoint protection systems.

- Preserve a copy of compromised web application code for forensic investigation.

- \*\*Notification\*\*:

- Notify external organizations of compromises, if applicable, in consultation with legal counsel.

4. Eradication:

Objective: Remove the threat and prevent recurrence.

- \*\*Code Comparison\*\*:

- Compare current web application code to a known-good copy and remove malicious additions.

- \*\*System Preservation\*\*:

- Preserve artifacts, systems, and backups for forensic analysis.

- Rebuild or replace compromised systems while retaining forensic copies.

- \*\*Log Monitoring\*\*:

- Review logs to ensure containment of the compromise.

5. Recovery:

Objective: Restore systems to normal operations.

- \*\*Code Restoration\*\*:

- Replace compromised web application code with a known-good copy.

- Conduct a review of code by a different individual for thoroughness.

- \*\*System Restoration\*\*:

- Restore systems from clean backups or rebuild from known-good images.

- Remediate vulnerabilities and reset/recreate impacted accounts.

- \*\*Monitoring\*\*:

- Configure alerts to detect malicious activity related to the incident.

6. Lessons Learned:

Objective: Document the incident’s details, discuss lessons learned, and adjust plans and defenses.

- \*\*Incident Review\*\*:

- Conduct a meeting to discuss successes, challenges, vulnerabilities, and remediation steps.

- \*\*Security Measures Update\*\*:

- Improve practices in change control, code review, authentication, MFA, privileged account access, network segmentation, firewall configuration, application security, patching, and training.

- \*\*Incident Reporting\*\*:

- Create a detailed technical report for CSIRT and an executive summary for management.