**Incident Response Plan**

### **1. Overview**

This Incident Response Plan outlines the necessary steps to address the security breach that occurred due to an unpatched vulnerability in a web application. The plan focuses on containment, eradication, and recovery strategies to mitigate the impact and prevent future incidents. Additionally, it includes a list of AWS and Azure security services that can assist in executing these response measures.

### **2. Containment**

The goal of containment is to limit the attacker's access and prevent further damage.

#### **2.1 Immediate Actions**

* **Disable Compromised Accounts:**
  + Revoke access for affected user accounts.
  + Reset credentials and enforce **Multi-Factor Authentication (MFA)**.
* **Block Malicious IPs:**
  + Configure **AWS WAF / Azure Firewall** to block attacker IPs.
  + Monitor real-time traffic for additional indicators of compromise (IoC).
* **Isolate Affected Systems:**
  + Disconnect **infected AWS EC2 / Azure Virtual Machines** from the network.
  + Restrict access to **database services (AWS RDS / Azure SQL)** to limit data exposure.
* **Activate Security Monitoring Tools:**
  + Enable **AWS GuardDuty / Azure Sentinel** to detect ongoing malicious activity.
  + Use **AWS CloudTrail / Azure Log Analytics** for forensic analysis.

### **3. Eradication & Recovery**

Once the attack has been contained, the next step is to remove threats and restore normal operations.

#### **3.1 Threat Eradication**

* **Apply Security Patches & Updates:**
  + Update all **web applications, databases, and operating systems**.
  + Ensure auto-patching is enabled on **AWS Systems Manager / Azure Update Manager**.
* **Scan for Malware & Vulnerabilities:**
  + Use **AWS Inspector / Azure Security Center** to scan for vulnerabilities.
  + Remove any backdoors or unauthorized scripts left by attackers.
* **Restrict Network Access:**
  + Implement **least privilege access** for all users and services.
  + Reconfigure **AWS Security Groups / Azure NSGs** to limit external access.

#### **3.2 Recovery Steps**

* **Restore Systems from Backups:**
  + Deploy **AWS Backup / Azure Backup** to restore secure copies of data.
  + Verify backups are **free of malware** before restoration.
* **Conduct Post-Incident Testing:**
  + Perform **penetration testing** to confirm vulnerabilities are fixed.
  + Run automated security scans using **AWS Inspector / Azure Defender**.
* **Improve Logging & Monitoring:**
  + Enhance **SIEM capabilities** with **AWS Security Hub / Azure Log Analytics**.
  + Enable real-time alerting for unusual login attempts and unauthorized access.

### **4. AWS & Azure Security Services for Incident Response**

| **Security Measure** | **AWS Service** | **Azure Service** |
| --- | --- | --- |
| Threat Detection | GuardDuty | Sentinel |
| Network Firewall | AWS WAF | Azure Firewall |
| Access Control | AWS IAM | Azure AD |
| Log Analysis | CloudTrail | Log Analytics |
| Vulnerability Scanning | AWS Inspector | Azure Defender |
| Backup & Recovery | AWS Backup | Azure Backup |

### **5. Conclusion**

The incident response plan provides a structured approach to mitigating security breaches caused by vulnerabilities in web applications. By following **containment, eradication, and recovery** steps, the organization can limit damage, restore systems, and implement preventive security controls. Additionally, leveraging **AWS and Azure security tools** enhances the overall defense posture against future threats.

Regular security audits, proactive monitoring, and continuous employee training should be conducted to maintain a strong security framework and minimize cybersecurity risks.

### **6. References**

* [AWS Security Hub](https://aws.amazon.com/security-hub/)
* [Azure Security Center](https://azure.microsoft.com/en-us/services/defender-for-cloud/)
* [NIST Incident Response Guide](https://csrc.nist.gov/publications/detail/sp/800-61/rev-2/final)