**Report on 5 Real-World Web Application Attacks**

In this report, we will examine five well-known real-world web application attacks, identify their threats and vulnerabilities, and discuss the affected security pillars: Confidentiality, Integrity, and Availability (CIA). We will also analyze the risks involved, their impact, and propose security best practices for remediation, along with strategies to mitigate associated risks.

**1. Equifax Data Breach (2017)**

**Threat and Vulnerabilities:**

* The attack exploited a vulnerability in the Apache Struts framework, which was used in Equifax’s web applications.
* Failure to apply critical security patches in a timely manner left the system exposed to attackers.

**Affected CIA Pillars:**

* **Confidentiality:** Sensitive personal data, including Social Security Numbers, dates of birth, and credit card information, was compromised.
* **Integrity:** Attackers could have potentially altered data during the breach.

**Impact:**

* Over 147 million individuals were affected.
* Estimated financial loss exceeded $1.4 billion.

**Security Best Practices and Mitigation Strategies:**

* Implement a robust patch management process to address vulnerabilities promptly.
* Conduct regular security audits and penetration testing.
* Use web application firewalls (WAFs) to monitor and block suspicious traffic.

**2. Sony Pictures Hack (2014)**

**Threat and Vulnerabilities:**

* Attackers used spear-phishing emails to gain access to Sony’s network.
* Lack of robust access controls allowed attackers to move laterally within the system.

**Affected CIA Pillars:**

* **Confidentiality:** Confidential emails and employee data were leaked.
* **Integrity:** Internal records and systems were manipulated.
* **Availability:** Systems were rendered inoperable for an extended period.

**Impact:**

* Financial and reputational damage to Sony.
* Sensitive corporate information and unreleased films were exposed.

**Security Best Practices and Mitigation Strategies:**

* Educate employees on recognizing phishing attacks.
* Implement strong multi-factor authentication (MFA).
* Use network segmentation to limit lateral movement of attackers.

**3. Capital One Data Breach (2019)**

**Threat and Vulnerabilities:**

* A misconfigured firewall in the AWS cloud environment allowed unauthorized access to sensitive data.
* Exploitation of an SSRF (Server-Side Request Forgery) vulnerability.

**Affected CIA Pillars:**

* **Confidentiality:** Personally identifiable information (PII) of over 100 million customers was compromised.

**Impact:**

* Estimated cost of the breach was around $300 million.
* Regulatory fines and customer trust issues.

**Security Best Practices and Mitigation Strategies:**

* Regularly audit cloud configurations and access controls.
* Implement principle of least privilege for data access.
* Employ automated tools to detect and remediate misconfigurations.

**4. Twitter Celebrity Account Hijacking (2020)**

**Threat and Vulnerabilities:**

* Social engineering attacks targeted Twitter employees to gain access to internal tools.
* Weak internal controls and inadequate monitoring of privileged accounts.

**Affected CIA Pillars:**

* **Integrity:** Malicious tweets were posted from compromised accounts.
* **Availability:** Temporary lockdown of verified accounts disrupted service.

**Impact:**

* Loss of user trust and reputational damage.
* Fraudulent cryptocurrency scheme promoted via compromised accounts.

**Security Best Practices and Mitigation Strategies:**

* Implement rigorous employee training on social engineering threats.
* Enforce strict access controls and logging for administrative tools.
* Conduct regular reviews of privileged account activity.

**5. Log4j Vulnerability Exploitation (2021)**

**Threat and Vulnerabilities:**

* Attackers exploited the Log4Shell vulnerability (CVE-2021-44228) in the widely used Log4j library.
* Insufficient input validation allowed remote code execution (RCE).

**Affected CIA Pillars:**

* **Confidentiality:** Attackers could gain unauthorized access to sensitive data.
* **Integrity:** Data could be modified or corrupted.
* **Availability:** Systems were at risk of being taken offline.

**Impact:**

* Thousands of organizations worldwide were affected.
* Critical systems in industries such as healthcare and finance faced disruption.

**Security Best Practices and Mitigation Strategies:**

* Immediately update vulnerable Log4j versions and apply security patches.
* Implement intrusion detection and prevention systems (IDPS).
* Conduct thorough application security testing to identify and mitigate similar vulnerabilities.