Report on 5 real world web application attacks

1. Equifax Data Breach (2017)

Threats: Unpatched vulnerability in the Apache Struts framework was exploited to gain unauthorized access to sensitive customer data.

Vulnerabilities:

- Unpatched software vulnerability (CVE-2017-5638).
- Lack of proper patch management processes.
- Insufficient encryption practices for sensitive data.

Affected Security Pillars:

- **Confidentiality**: Exposure of sensitive personal information of 147 million individuals, including Social Security numbers and credit card data.
- **Integrity**: Possible manipulation of sensitive customer records.
- **Availability**: Service disruptions during remediation efforts.

Risk Analysis:

- Legal Implications: Regulatory fines amounting to more than $700 million.
- Financial Consequences: More costs for response and monitoring breach services.
- Reputation Loss: Customer loss of trust and negative publicity.

Remediation Actions:

- Use of automated patch management.
- Conduct frequent security audits and vulnerability scans.
- Encrypt both in transit and at rest sensitive data.

Mitigation Controls:

- Establish a strong incident response plan.
- Use WAF to prevent exploitation attempts by detecting them.
- Provide frequent security training for employees.

References:

- GAO Equifax Data Breach Report
- Apache Struts CVE documentation.

2. Log4Shell Vulnerability Exploitation (2021)

Threats: Attackers exploited a Remote Code Execution (RCE) vulnerability in the Log4j logging utility, CVE-2021-44228.

Vulnerabilities:

- Unvalidated input processed by logging libraries.
- Default configurations enabling lookups.
- Ignorance of third-party dependencies.

Affected Security Pillars:

- **Confidentiality**: Unauthorized access to sensitive environments.
- **Integrity**: Injection and modification of malicious code into systems.
- **Availability**: Systems that become nonfunctional due to DoS attacks.

Risk Analysis:

- **Legal Consequences**: Potential fines under data protection regulations if sensitive data was accessed.
- **Financial Impact**: Costs of system patching and incident response.
- **Reputation Damage**: Customers may lose trust in organizational security practices.

Remediation Measures:

- Implementing allow list policies for specific environment variables and user inputs.
- Updating Log4j libraries to secure versions immediately.
- Conducting dependency management checks across development pipelines.

Mitigation Strategies:

- Using centralized logging solutions with restricted access controls.
- Implementing runtime security monitoring tools.
- Conducting third-party component audits regularly.

Sources:

- Apache Log4j Security Vulnerabilities
- NCSC advisories.

3. Sony Pictures Hack (2014)

Threats: Nation-state-sponsored actors utilized spear-phishing campaigns and malware to gain access to Sony's network, which included the theft of sensitive emails and data.

Vulnerabilities:

- Weak password policies.
- Poor employee security awareness training.
- Inadequate segmentation of critical network assets.

Security Pillars Impacted:

- **Confidentiality**: Leakage of internal emails, business plans, and employee PII.
- **Integrity**: Tampering with intellectual property.
- **Availability**: Extensive disruption of Sony's operations.

Risk Analysis:

- **Legal Consequences**: Lawsuits from employees and partners.
- **Financial Impact**: Costs associated with investigation, infrastructural repair, and litigation.
- **Reputation Damage**: Long-term loss of brand value and customer trust.

Remediation Measures:

- Implementation of email filtering and monitoring tools.
- Establishment of MFA for all accounts.
- Isolation of sensitive data through network segmentation.

Mitigation Strategies:

- Implementing an APT monitoring system.
- Training sessions on detection of phishing attempts amongst employees.
- Installation of EDR tools.

Sources:

- FBI and private threat intelligence reports
- Industry analyses about the 2014 Sony breach.

4.Uber Data Breach (2022)

Threats: Attackers exploited compromised credentials to breach internal systems.

Vulnerabilities:

- Use of stolen admin credentials.
- Lack of sufficient MFA controls.
- Absence of access segmentation for sensitive data.

Affected Security Pillars:

- Confidentiality: Exfiltration of user data, such as phone numbers and emails.
- Integrity: Possibility of modification of backend processes or records.
- Availability: Partial service disruptions.

Risk Analysis:

- Legal Consequences: Regulatory agencies' investigations and penalties due to failure to safeguard user data.
- Financial Impact: Settlement costs related to lawsuits and additional security measures.
- Reputation Damage: Public trust loss, particularly from the rideshare customers.

Remediation Steps:

- Implementing MFA on all accounts
- Active credential monitoring and response
- High-value data isolation through access policies

Mitigation Steps:

- Adaptive identity solution to track login risky behaviors
- Penetration testing for periodic simulation of attacks
- Post-incident review for identifying weaknesses in current policies

References:

- Uber 2022 incident reports.
- External threat intelligence reviews.

5. Capital One Breach (2019)

Threats:

- Misconfigured WAF enabled the attacker to reach AWS-hosted customer data.

Vulnerabilities:

- Poor cloud security policy configurations.
- IAM roles not restrictive enough.
- Unusual data access behavior was not quickly detected.

Compromised Security Pillars:

- **Confidentiality**: Exposure of 106 million customer accounts and application data.
- **Integrity**: Risk of sensitive credit card application data exposure.
- **Availability**: Few operational disruptions.

Risk Analysis:

- Legal: Fine of $80 million imposed by the U.S. regulators.
- Financial Impact: Costs of sending notifications to customers and ensuring compliance with regulations.
- Reputation Damage: Public exposure to the security of cloud migration.

Remediation Measures:

- Implementing cloud service provider configuration best practices.
- Enabling automated anomaly detection mechanisms for cloud environments.
- Regular updating of WAF configurations and policies.

Mitigation Strategies:

- DevSecOps practice implementation during development and deployment.
- Use of encrypted storage mechanisms and keys rotated periodically.
- Identity and access monitoring tools for enhanced visibility.

Sources:

- Capital One Breach Analysis
- AWS Security Best Practices documentation.