# Assignment 1

# Meghana D Duttargi

# 241059042

# Web Application Security

# Alternative Report on Real-World Web Application Attacks

## 1. Sony PlayStation Network Breach (2011)

### Incident Details

In April 2011, Sony’s PlayStation Network (PSN) suffered a massive breach that compromised the personal data of approximately 77 million accounts. The breach led to a 23-day service outage, exposing sensitive information such as usernames, passwords, and payment details. Estimated financial losses, including fines, lawsuits, and loss of business, were over $171 million. This attack impacted gaming enthusiasts worldwide, shaking consumer trust in Sony’s ability to secure its platform.

### Threats and Vulnerabilities

Threats: Exploitation of outdated software and poor encryption.

Vulnerabilities: Lack of adequate network segmentation, outdated encryption protocols.

Affected Security Pillars: Confidentiality (user data leaked), Availability (service downtime).

### Risk Analysis

Legal Impact: Fines under data protection regulations.  
Financial Impact: Over $171 million in losses.  
Reputational Impact: Loss of consumer trust and market share.

### Remediation Measures

Regularly update and patch all systems.  
Strengthen encryption mechanisms for user data.  
Conduct regular penetration testing.

### Risk Mitigation Strategies

Implement a robust incident response plan.  
Employ multi-factor authentication (MFA) for all users.  
Ensure continuous monitoring of network activity.

## 2. Uber Data Breach (2016)

### Incident Details

In late 2016, Uber suffered a data breach that exposed the personal information of 57 million riders and drivers. The attackers accessed Uber’s GitHub account and stole credentials for its Amazon Web Services (AWS) environment. Instead of reporting the breach, Uber paid hackers $100,000 to delete the data, leading to regulatory scrutiny and lawsuits. This incident highlighted severe flaws in Uber’s security practices.

### Threats and Vulnerabilities

Threats: Unauthorized access via stolen credentials.

Vulnerabilities: Poor access controls, inadequate credential management.

Affected Security Pillars: Confidentiality (data theft), Integrity (unauthorized data access).

### Risk Analysis

Legal Impact: Fines exceeding $148 million in settlements.  
Financial Impact: Cost of settlements and long-term reputational damage.  
Reputational Impact: Loss of user trust due to delayed breach disclosure.

### Remediation Measures

Enforce secure credential storage practices.  
Adopt a "least privilege" approach for access controls.  
Conduct regular audits of sensitive data repositories.

### Risk Mitigation Strategies

Deploy tools for detecting unusual access patterns.  
Use automated credential rotation systems.  
Ensure compliance with breach notification regulations.

## 3. Target Data Breach (2013)

### Incident Details

In December 2013, hackers breached Target's network using stolen credentials from a third-party vendor. The attackers installed malware on the company's point-of-sale (POS) systems, compromising credit and debit card information of over 40 million customers. Personal data for an additional 70 million customers was also exposed. The breach cost Target approximately $202 million in legal fees, settlements, and technology upgrades.

### Threats and Vulnerabilities

Threats: Cybercriminals exploiting vendor access and POS vulnerabilities.

Vulnerabilities: Insufficient vendor access controls, lack of network segmentation.

Affected Security Pillars: Confidentiality (payment data stolen).

### Risk Analysis

Legal Impact: Significant settlements and lawsuits.  
Financial Impact: Over $202 million in direct costs.  
Reputational Impact: Erosion of customer trust.

### Remediation Measures

Implement strict vendor access controls.  
Segment networks to isolate sensitive systems.  
Use end-to-end encryption for payment data.

### Risk Mitigation Strategies

Regularly audit vendor security practices.  
Deploy network intrusion detection systems (NIDS).  
Train employees on phishing awareness.

## 4. LinkedIn Data Breach (2021)

### Incident Details

In June 2021, data from approximately 700 million LinkedIn users were scraped and leaked on a dark web forum. The attackers exploited LinkedIn’s API to gather public and private information, including email addresses, phone numbers, and employment details. Although no passwords were leaked, the breach raised serious privacy concerns. LinkedIn faced reputational damage and regulatory scrutiny.

### Threats and Vulnerabilities

Threats: Unauthorized data scraping using API endpoints.

Vulnerabilities: Poor API access control policies.

Affected Security Pillars: Confidentiality (user information exposed).

### Risk Analysis

Legal Impact: Potential fines under GDPR.  
Financial Impact: Costs associated with regulatory compliance and user compensation.  
Reputational Impact: Loss of user confidence in data privacy measures.

### Remediation Measures

Strengthen API authentication mechanisms.  
Implement rate limiting to prevent large-scale data scraping.  
Monitor API usage for abnormal activity.

### Risk Mitigation Strategies

Encrypt sensitive user data.  
Provide users with greater control over data visibility.  
Conduct regular API security assessments.

## 5. Colonial Pipeline Ransomware Attack (2021)

### Incident Details

In May 2021, the Colonial Pipeline company fell victim to a ransomware attack by the DarkSide group. The attackers gained access to the company’s IT systems and encrypted critical data, causing a shutdown of fuel distribution along the East Coast of the United States. Colonial Pipeline paid a ransom of $4.4 million to regain access to their systems. The attack resulted in fuel shortages, price hikes, and widespread public concern.

### Threats and Vulnerabilities

Threats: Ransomware deployment targeting critical infrastructure.

Vulnerabilities: Weak password policies, lack of network segmentation.

Affected Security Pillars: Availability (service disruption), Confidentiality (data exfiltration).

### Risk Analysis

Legal Impact: Heightened scrutiny from regulators.  
Financial Impact: Ransom payment and associated recovery costs.  
Reputational Impact: Public backlash due to service disruptions.

### Remediation Measures

Implement regular backups with secure storage.  
Deploy endpoint detection and response (EDR) solutions.  
Train employees to recognize phishing attempts.

### Risk Mitigation Strategies

Adopt a zero-trust security model.  
Enhance network segmentation to limit lateral movement.  
Regularly test and update incident response plans.