1. **Real world web application attacks**

- Identify the Threats, Vulnerabilities, and Affected Security Pillars (Confidentiality, Integrity, Availability).

- Analyze the Risks Involved and discuss the impact of each attack, including potential legal, financial, and reputational consequences for the affected organization.

- Propose remediation measures or security best practices that could have prevented each attack

- Recommend strategies to mitigate the associated risks.

- Cite the sources used to describe each attack.

1. **MySpace Samy Worm Data Breach**

The Samy Worm, created by Samy Kamkar in 2005, is a notable example of a cross-site scripting (XSS) attack that propagated rapidly through the MySpace social networking platform.

**Threats & Vulnerabilities**

1. Threats: The Samy Worm exploited a vulnerability in MySpace's handling of JavaScript. It allowed the worm to execute without user consent, automatically adding Samy as a friend and displaying the message "but most of all, samy is my hero" on infected profiles.
2. Vulnerabilities: The worm took advantage of MySpace's lack of adequate input validation and output encoding, allowing malicious scripts to be executed when users viewed infected profiles.

**Affected Security Pillars**

1. Confidentiality: The worm did not directly steal sensitive data but compromised user profiles and privacy by spreading without consent.

2. Integrity: The integrity of user profiles was compromised as the worm altered them to include unauthorized content and friend requests.

3. Availability: MySpace experienced significant downtime as the site struggled to handle the surge in traffic caused by the worm's rapid propagation.

**Risks Involved**

1. Samy Kamkar faced legal repercussions for his actions, including a felony charge and a plea agreement that included probation, community service, and restitution.
2. Although specific financial losses for MySpace were not publicly detailed, the incident likely incurred costs related to damage control and system recovery.
3. MySpace's reputation suffered due to its inability to prevent such a widespread attack, leading to decreased user trust and engagement.

**Proposed Remediation Measures**

1. Input Validation: Implement strict input validation to ensure that user-generated content does not contain executable scripts.
2. Output Encoding: Use output encoding techniques to prevent scripts from being executed when displaying user content.
3. Security Audits: Regularly conduct security audits and penetration testing to identify and address vulnerabilities in web applications.

**Recommended Strategies for Risk Mitigation**

1. Educate users about the risks of clicking on unknown links or viewing suspicious profiles on social networking sites.
2. Content Security Policy (CSP): Implement CSP headers to restrict the execution of untrusted scripts and mitigate XSS risks.
3. Establish monitoring systems to detect unusual activity on user accounts and respond quickly to potential threats.

<https://www.vice.com/en/article/the-myspace-worm-that-changed-the-internet-forever/>

<https://en.wikipedia.org/wiki/Myspace>

1. **Yahoo Data Breach (2013-2014)**

**Threats & Vulnerabilities**

1. Threats: The breaches involved unauthorized access to Yahoo's systems, with attackers employing various techniques, including cookie manipulation and exploiting security flaws in the platform.
2. Vulnerabilities: The primary vulnerabilities included inadequate security measures to protect user data and a lack of timely updates regarding known threats. In particular, the 2014 breach was attributed to the copying of a backup of Yahoo's User Account Database by attackers.

**Affected Security Pillars**

1. Confidentiality: The breaches compromised sensitive user information, including names, email addresses, phone numbers, birth dates, and hashed passwords. In some cases, unencrypted security questions and answers were also exposed.
2. Integrity: The integrity of user accounts was at risk as attackers could potentially manipulate account settings or access personal information.
3. Availability: Although there were no direct reports of service outages due to the breaches, the aftermath led to significant scrutiny and operational disruptions as Yahoo worked to address the security flaws.

**Risks Involved**

1. Legal Consequences: Yahoo faced multiple lawsuits resulting in a $117.5 million class-action lawsuit settlement and a $35 million fine from the U.S. Securities and Exchange Commission for failing to disclose the breaches promptly.
2. Financial Impact: The breaches led to a decrease in Yahoo's acquisition price by Verizon from $4.8 billion to $4.5 billion due to the fallout from the incidents.
3. Reputational Damage: The breaches severely damaged Yahoo's reputation, leading to a loss of user trust and confidence in their ability to protect personal data.

**Proposed Remediation Measures**

1. Enhanced Security Protocols: Implement stronger encryption methods for sensitive data and ensure that all user information is adequately protected.
2. Regular Security Audits: Conduct frequent security assessments and penetration testing to identify vulnerabilities within the system proactively.
3. Incident Response Plan: Develop and maintain a comprehensive incident response plan to quickly address any future breaches or security incidents.

**Recommended Strategies for Risk Mitigation**

1. User Education: Educate users on best practices for password management and recognizing phishing attempts that may lead to unauthorized access.
2. Multi-Factor Authentication (MFA): Encourage or mandate the use of MFA for all user accounts to add an additional layer of security against unauthorized access.
3. Transparency with Users: Maintain open communication with users regarding data security practices and promptly inform them of any potential breaches or vulnerabilities.

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

**Threats & Vulnerabilities**

1. Threats: The breach was primarily caused by hackers exploiting a known vulnerability in Apache Struts (CVE-2017-5638) used in Equifax's online dispute portal. Attackers gained access to sensitive databases by sending malicious HTTP requests.

Vulnerabilities: Failure to apply a critical security patch for Apache Struts. Inadequate network segmentation, allowing attackers to move laterally within the network.

**Affected Security Pillars**

1. Confidentiality: Sensitive personal information of 147.9 million Americans was compromised, including names, Social Security numbers, birth dates, addresses, and in some cases, driver's license numbers.
2. Integrity: The integrity of user data was threatened as attackers could potentially manipulate or misuse the compromised information.
3. Availability: Although there were no direct service outages reported during the breach, the investigation and remediation efforts caused operational disruptions within Equifax.

**Risks Involved**

1. Legal Consequences: Equifax faced numerous lawsuits and regulatory scrutiny due to the breach. In October 2019, they settled a class-action lawsuit for $117.5 million.
2. Financial Impact: The breach resulted in substantial financial losses estimated at over $4 billion when considering legal fees, settlements, and loss of business.
3. Reputational Damage: The breach severely impacted Equifax's reputation, leading to a loss of customer trust and confidence in their data protection capabilities.

**Proposed Remediation Measures**

1. Patch Management: Implement a robust patch management policy to ensure timely updates for all software components, particularly those with known vulnerabilities.
2. Network Segmentation: Improve network architecture by segmenting sensitive systems to limit lateral movement by attackers once they gain access.
3. Enhanced Monitoring: Deploy advanced monitoring tools that can inspect encrypted traffic to detect data exfiltration attempts.

**Recommended Strategies for Risk Mitigation**

1. User Education: Educate users on best practices for protecting their personal information and recognizing phishing attempts that could lead to unauthorized access.
2. Multi-Factor Authentication (MFA): Encourage or mandate the use of MFA for all accounts to add an additional layer of security against unauthorized access.
3. Incident Response Plan: Develop and regularly update an incident response plan that outlines procedures for quickly addressing data breaches and minimizing damage.
4. **WannaCry Ransomware Attack (2017)**

**Threats & Vulnerabilities**

1. Threats: WannaCry exploited a vulnerability in Microsoft Windows known as EternalBlue, which allowed the ransomware to spread rapidly across networks without user interaction.
2. Vulnerabilities: The attack primarily targeted systems that had not applied critical security patches released by Microsoft prior to the attack. Many organizations were using outdated versions of Windows or had not updated their software due to operational constraints.

**Affected Security Pillars**

1. Confidentiality: The ransomware encrypted sensitive files on infected machines, rendering them inaccessible to users.
2. Integrity: Data integrity was compromised as files were encrypted and could only be restored by paying the ransom.
3. Availability: The attack caused widespread disruptions, particularly in critical sectors like healthcare, where systems were rendered unusable.

**Risks Involved**

1. Legal Consequences: Organizations affected by the attack could face legal repercussions for failing to secure user data adequately.
2. Financial Impact: The estimated damages from the attack ranged from hundreds of millions to billions of dollars. Notable victims included the UK's National Health Service (NHS), FedEx, and various other organizations.
3. Reputational Damage: The attack severely impacted the reputation of affected organizations, leading to a loss of trust among customers and stakeholders.

**Proposed Remediation Measures**

1. Patch Management: Organizations should implement a robust patch management policy to ensure timely updates for all software components, particularly those with known vulnerabilities.
2. Network Segmentation: Improve network architecture by segmenting sensitive systems to limit lateral movement by attackers once they gain access.
3. User Education: Regular training for employees on recognizing phishing attempts and understanding the importance of software updates.

**Recommended Strategies for Risk Mitigation**

1. Multi-Factor Authentication (MFA): Encourage or mandate the use of MFA for all accounts to add an additional layer of security against unauthorized access.
2. Incident Response Plan: Develop and regularly update an incident response plan that outlines procedures for quickly addressing ransomware attacks and minimizing damage.
3. Backup Solutions: Implement regular backup solutions that allow organizations to restore data without paying ransoms if an attack occurs.

**5.Twitter Account Hijacking Incident (July 15, 2020)**

**Threats and Vulnerabilities**

1. Threat: The incident involved a coordinated social engineering attack that compromised high-profile Twitter accounts to promote a cryptocurrency scam.
2. Vulnerabilities: The attackers exploited weaknesses in Twitter's internal security protocols, particularly through social engineering techniques that targeted lower-level employees to gain access to administrative tools.

**Affected Security Pillars**

1. Confidentiality: Unauthorized access to sensitive user accounts led to the exposure of personal information.
2. Integrity: The integrity of the affected accounts was compromised as attackers posted fraudulent messages.
3. Availability: The incident disrupted Twitter's service as it struggled to regain control over the compromised accounts.

**Risks and Impact**

1. Legal: The attackers faced charges including wire fraud, money laundering, and unauthorized computer access. Twitter itself could face legal scrutiny for failing to protect user data adequately.
2. Financial: The scam resulted in the theft of approximately $110,000 worth of Bitcoin. Additionally, Twitter incurred costs related to incident response and potential regulatory fines.
3. Reputational: The breach severely damaged Twitter's reputation, raising concerns about its security measures and the safety of user accounts on the platform.

**Remediation Measures**

1. Enhanced Employee Training: Regular training on social engineering tactics and phishing awareness for all employees, especially those with access to sensitive tools.
2. Stronger Authentication Protocols: Implementing more robust multi-factor authentication (MFA) methods for internal tools to prevent unauthorized access even if credentials are compromised.
3. Access Control Review: Conducting thorough reviews of who has access to administrative tools and limiting that access based on necessity.

**Risk Mitigation Strategies**

1. Incident Response Plan: Develop and regularly update an incident response plan that includes protocols for quickly addressing unauthorized access incidents.
2. Regular Security Audits: Conduct frequent audits of security practices and employee access levels to ensure compliance with best practices.
3. Monitoring and Alerts: Implement real-time monitoring of account activity, especially for high-profile accounts, to detect unusual behavior promptly.