ASSIGNMENT-4

OWASP 10:

The OWASP Top 10 is a well-known document that outlines the top ten most critical web application security risks. OWASP stands for the Open Web Application Security Project, a non-profit organization focused on improving software security.

The OWASP Top 10 list is updated periodically to reflect the evolving landscape of web application security threats. As of my last update, the most recent version is OWASP Top 10 2021. Here's a brief overview of the OWASP Top 10 as of that version:

1. Injection: Injection flaws, such as SQL, NoSQL, OS, and LDAP injection, occur when untrusted data is sent to an interpreter as part of a command or query. Attackers can manipulate these inputs to access or modify data.

2. Broken Authentication: This refers to security vulnerabilities related to authentication and session management. Weaknesses in this area can allow attackers to compromise passwords, keys, or session tokens, leading to unauthorized access to user accounts.

3. Sensitive Data Exposure: When sensitive data such as financial information, healthcare records, or personal identifiable information (PII) is not adequately protected, it can be exposed to unauthorized parties. This often occurs due to weak encryption or insufficient access controls.

4. XML External Entities (XXE): XXE vulnerabilities occur when an XML parser processes XML input that contains references to external entities. Attackers can exploit these vulnerabilities to access sensitive data, execute arbitrary code, or perform denial-of-service attacks.

5. Broken Access Control: Inadequate access control mechanisms can allow unauthorized users to view sensitive data, perform actions, or access functionality that should be restricted. This includes bypassing authentication, authorization, or other security controls.

6. Security Misconfiguration: Security misconfigurations can occur at any level of the application stack, including the web server, application server, database, or framework. These misconfigurations can lead to unauthorized access, data exposure, or other security vulnerabilities.

7. Cross-Site Scripting (XSS): XSS vulnerabilities occur when attackers inject malicious scripts into web pages viewed by other users. These scripts can steal sensitive information, hijack user sessions, or deface websites.

8. Insecure Deserialization: Insecure deserialization vulnerabilities arise when untrusted data is deserialized without proper validation. Attackers can exploit these vulnerabilities to execute arbitrary code, conduct denial-of-service attacks, or tamper with application logic.

9. Using Components with Known Vulnerabilities: Many web applications rely on third-party components such as libraries, frameworks, or plugins. If these components contain known vulnerabilities, attackers can exploit them to compromise the security of the application.

10. Insufficient Logging and Monitoring: Inadequate logging and monitoring make it difficult for organizations to detect and respond to security incidents effectively. Without sufficient visibility into system activity, attackers can operate undetected for extended periods.

Addressing the vulnerabilities outlined in the OWASP Top 10 is crucial for building and maintaining secure web applications. Developers, security professionals, and organizations should prioritize understanding and mitigating these risks to protect against common attack vectors and safeguard sensitive data.

Vulnerabilities in altoromutual website

Website is vulnerable to both sql and xss vulnerabity

Commands used to exploit to website:

' or "

-- or #

' OR '1

' OR 1 -- -

" OR "" = "

" OR 1 = 1 -- -

' OR '' = '

Commands used for xss vulnerability

<image/src/onerror=prompt(8)>

<img/src/onerror=prompt(8)>

<image src/onerror=prompt(8)>

<img src/onerror=prompt(8)>

<image src =q onerror=prompt(8)>

<img src =q onerror=prompt(8)>

**Impact of sql vulnerability:**

SQL (Structured Query Language) injection vulnerabilities can have significant impacts on both the security and functionality of a web application. Here are some of the potential impacts:

1. Data Breaches: One of the most severe consequences of SQL injection vulnerabilities is the potential for data breaches. Attackers can exploit these vulnerabilities to gain unauthorized access to databases, allowing them to view, modify, or delete sensitive information such as user credentials, personal data, financial records, or intellectual property.

2. Data Loss or Corruption: SQL injection attacks can lead to data loss or corruption if attackers manipulate SQL queries to delete or modify database records unintentionally. This can disrupt business operations, cause financial losses, or damage an organization's reputation.

3. Unauthorized Access: By exploiting SQL injection vulnerabilities, attackers can bypass authentication mechanisms or escalate privileges, gaining unauthorized access to restricted areas of the application or administrative functionalities. This can result in further exploitation, data theft, or system compromise.

4. Account Takeover: SQL injection attacks can enable attackers to hijack user accounts by extracting login credentials or session tokens stored in the database. Once authenticated, attackers can impersonate legitimate users, perform unauthorized actions, or access sensitive data.

5. Denial of Service (DoS) Attacks: In some cases, attackers may exploit SQL injection vulnerabilities to execute resource-intensive queries or manipulate database operations, leading to performance degradation or system unavailability. This can result in denial of service (DoS) conditions, preventing legitimate users from accessing the application.

6. Reputation Damage: The discovery of SQL injection vulnerabilities can damage an organization's reputation and erode customer trust. Public disclosure of security incidents or data breaches resulting from SQL injection attacks can lead to negative publicity, legal consequences, and financial penalties.

7. Regulatory Compliance Violations: Organizations may be subject to regulatory requirements or industry standards that mandate the protection of sensitive data and the prevention of security vulnerabilities such as SQL injection. Failure to address SQL injection vulnerabilities can result in non-compliance, leading to fines, legal actions, or loss of business partnerships.

8. Financial Losses: The consequences of SQL injection vulnerabilities can result in direct financial losses for organizations, including costs associated with incident response, forensic investigations, legal proceedings, data recovery, and regulatory fines. Additionally, businesses may suffer indirect financial losses due to reputational damage, decreased customer confidence, or loss of revenue opportunities.

Overall, SQL injection vulnerabilities pose significant risks to the security, integrity, and availability of web applications and the sensitive data they process. Addressing these vulnerabilities through secure coding practices, input validation, parameterized queries, and web application firewalls (WAFs) is essential to mitigate the potential impacts and protect against SQL injection attacks.

**Impact of xss vulnerability:**

Cross-Site Scripting (XSS) vulnerabilities can have significant impacts on both users and organizations:

1. Data Theft: One of the primary goals of XSS attacks is to steal sensitive information from users. Attackers can craft malicious scripts that steal cookies, session tokens, or other credentials stored in the browser, allowing them to impersonate users or access their accounts.

2. Account Hijacking: By exploiting XSS vulnerabilities, attackers can hijack user sessions, gaining unauthorized access to their accounts. This can lead to various malicious activities, such as sending spam, stealing personal information, or conducting fraudulent transactions.

3. Defacement: XSS attacks can be used to deface websites by injecting malicious scripts that alter the appearance or content of web pages. This can damage the reputation of the affected organization and erode trust among users.

4. Phishing: Attackers can leverage XSS vulnerabilities to launch phishing attacks, tricking users into disclosing sensitive information or performing actions they wouldn't typically do. For example, an attacker could inject a fake login form that captures credentials and sends them to the attacker-controlled server.

5. Malware Distribution: XSS vulnerabilities can be exploited to distribute malware to unsuspecting users. Attackers can inject malicious scripts that redirect users to websites hosting malware or initiate drive-by downloads, infecting users' devices with malicious software.

6. Session Hijacking: XSS attacks can be used to steal session cookies or tokens, allowing attackers to impersonate legitimate users and perform actions on their behalf. This can lead to unauthorized access to sensitive data or functionality within the application.

7. Data Manipulation: In addition to stealing data, attackers can use XSS vulnerabilities to manipulate data displayed to users. This can include modifying the content of web pages, injecting fake advertisements, or altering form submissions, leading to data corruption or unauthorized transactions.

8. SEO Manipulation: Attackers can use XSS vulnerabilities to inject hidden links or keywords into web pages, manipulating search engine rankings for malicious purposes. This can negatively impact the visibility and reputation of the affected website.

9. Regulatory Compliance Violations: Exploiting XSS vulnerabilities to access or expose sensitive information may result in violations of data protection regulations such as GDPR (General Data Protection Regulation) or HIPAA (Health Insurance Portability and Accountability Act), leading to legal repercussions and financial penalties for organizations.

10. Reputation Damage: Publicly known XSS vulnerabilities can damage an organization's reputation and credibility, eroding trust among users, customers, and partners. Failure to promptly address and mitigate such vulnerabilities can result in negative publicity and loss of business opportunities.

Overall, XSS vulnerabilities pose a significant threat to the security, integrity, and reputation of web applications and the organizations that own them. It's essential for developers and organizations to prioritize XSS prevention measures to mitigate these risks effectively.