|  |  |
| --- | --- |
| **Attack Type** | **SQL Injection (SQLi)** |
| **Threats** | Attackers inject malicious SQL queries to manipulate databases. |
| **Vulnerabilities** | Lack of input validation and improper query sanitization. |
| **Affected Security Pillars** | Confidentiality, Integrity, Availability |
| **Risks Involved** | Legal: Data breaches violating GDPR. Financial: Regulatory fines, recovery costs. Reputational: Loss of customer trust. |
| **Impact** | Data theft, unauthorized access, potential financial fraud, and reputational damage. |
| **Remediation Measures** | Use prepared statements, parameterized queries, and input sanitization. |
| **Mitigation Strategies** | Regular security audits, code reviews, and developer training. |
| **Sources** | OWASP SQL Injection Guide: https://owasp.org/www-community/attacks/SQL\_Injection |

|  |  |
| --- | --- |
| **Attack Type** | **Cross-Site Scripting (XSS)** |
| **Threats** | Attackers inject malicious scripts into webpages, executed in users' browsers. |
| **Vulnerabilities** | Lack of input sanitization and improper output encoding. |
| **Affected Security Pillars** | Confidentiality, Integrity, Availability |
| **Risks Involved** | Legal: Exposure of personal data. Financial: Legal costs, loss of revenue due to customer churn. Reputational: Brand damage. |
| **Impact** | Session hijacking, data theft, phishing, website defacement. |
| **Remediation Measures** | Use output encoding, CSP (Content Security Policy), and input validation. |
| **Mitigation Strategies** | Employ secure coding practices, regular security testing, and use of frameworks with built-in protections (e.g., React). |

|  |  |
| --- | --- |
| **Attack Type** | **Cross-Site Request Forgery (CSRF)** |
| **Threats** | Attackers trick authenticated users into making unwanted requests, such as changing account details or making payments. |
| **Vulnerabilities** | Lack of anti-CSRF tokens, improper session management, and absence of validation for request origin. |
| **Affected Security Pillars** | Integrity, Confidentiality, Availability |
| **Risks Involved** | Legal: Fraudulent activities leading to potential lawsuits. Financial: Financial loss from unauthorized transactions. Reputational: User trust degradation. |
| **Impact** | Unauthorized actions on behalf of users, fraud, or changes to sensitive information. |
| **Remediation Measures** | Use anti-CSRF tokens, require re-authentication for sensitive actions, validate request origins. |
| **Mitigation Strategies** | Implement multi-factor authentication, regularly audit for CSRF vulnerabilities, and use frameworks with CSRF protection. |

|  |  |
| --- | --- |
| **Attack Type** | **Remote Code Execution (RCE)** |
| **Threats** | Attackers execute arbitrary code on the target server, gaining control over the system. |
| **Vulnerabilities** | Improper input validation, insecure deserialization, or improper configuration of remote services. |
| **Affected Security Pillars** | Confidentiality, Integrity, Availability |
| **Risks Involved** | Legal: Data breach leading to potential violations of compliance standards. Financial: Cost of remediation and recovery. Reputational: Trust loss, brand damage. |
| **Impact** | Full control of the system, data theft, manipulation, or service disruption. |
| **Remediation Measures** | Input sanitization, strict access controls, and regular patching of software. |
| **Mitigation Strategies** | Use least privilege principles, regular vulnerability scanning, and secure coding practices. |

|  |  |
| --- | --- |
| **Attack Type** | **Denial of Service (DoS) / Distributed Denial of Service (DDoS)** |
| **Threats** | Attackers flood the server with traffic to disrupt service availability. |
| **Vulnerabilities** | Lack of rate limiting, weak server configurations, insufficient infrastructure capacity. |
| **Affected Security Pillars** | Availability, Confidentiality, Integrity |
| **Risks Involved** | Legal: Service disruptions impacting customers. Financial: Loss of revenue due to downtime, mitigation costs. Reputational: Customer dissatisfaction. |
| **Impact** | Service disruption, loss of business continuity, and potential loss of revenue. |
| **Remediation Measures** | Implement rate limiting, use DDoS protection services (e.g., Cloudflare), distribute infrastructure for redundancy. |
| **Mitigation Strategies** | Set up traffic monitoring systems, create a DDoS response plan, and ensure infrastructure scalability. |