- Cross-site scripting (XSS)

  OWASP's top 10, XSS is now categorized alongside insecure deserialization, A03:2021-Injection. According to OWASP, an application is vulnerable to attack when user-supplied data isn't sanitized, filtered, or validated by the application, hostile data is used within object-related mapping search parameters to extract sensitive records. The most common injections are SQL, NoSQL, OS command, object-relational mapping, LDAP, and expression language. The risk of this vulnerability is that attackers will inject malicious code into our app and try to gain sensitive information that would otherwise be unavailable to them. Remediation includes; the use of a safe API, which avoids using an interpreter entirely, provides a parameterized interface or migrates to object relational mapping. Using LIMIT and other SQL controls within queries to prevent mass disclosure of records in case of SQL injection. Severity level: medium. Because remediation also includes the use of automation to prevent injection code, this lowers the severity level of this threat.

- Cross-site request forgery (CSRF)

  Tho not listed in OWASP's top 10, cross-site request forgery is still a major vulnerability that can be used as an attack by malicious actors. A CSRF attack is one that forces an end user to perform unwanted actions on a web app on which they are currently authenticated. The objective is to have the user perform a state changing action. Remediation includes checking if our framework has built-in CSRF protection and using it. Don't use GET requests for state-changing operations. Using custom request headers and verifying the origin with standard headers. Also using cross-site scripting remediations as well because XSS can be used to bypass all CSRF mitigation. This vulnerability is high because the entire application is compromised if an admin account were to be compromised.

- SQL injection

OWASP top 10 has placed SQL injection into A03 injection. Applications are vulnerable to attack when hostile data is directer used or concatenated. The SQL or command is structured with malicious code in dynamic queries, commands, or stored procedures. Refer to cross-site scripting for remediations.

- Sensitive data exposure

Referred to A02:2021-Cryptographic Failures in OWASP top 10. This vulnerability focuses on the lack of cryptography for data at rest and transit. It looks at if data is transmitted in clear text, are cryptographic algorithms up to date or not. OWASP has the following for remediation. Classify data that is stored, processed, or transmitted by an application. Id what data is sensitive according to privacy laws, regulations requirements, and business needs. Ensure that all sensitive data at rest is encrypted. Don't use FTP or SMTP for transporting sensitive data. Always use authenticated encryption instead of just encryption. These are just some of the required remediations that OWASP recommends using. The risk level for this vulnerability is critical. If data isn’t secured properly then it will be easily available for malicious actors to access it and cause damage to our company and our clients.

- Insufficient logging and monitoring

  Labeled as A09:2021- Security Logging and Monitoring Failures in OWASP top 10. This vulnerability is related to the lack of logging and monitoring and how a lack of them can lead to breaches going undetected until it's too late. Risks involved are audit event logs like logins, failed logins, and high-value transactions that aren’t logged. Warnings and errors generate no, inadequate, or unclear log messages. The application cannot detect, escalate or alert for active attacks in real-time. Remediation includes ensuring all login, access control, and server-side input validation failures can be logged with enough information to determine if it's a malicious actor behind that activity and also held long enough for forensic analysis. DevSecOps teams should have effective monitoring and alerting in place so that any suspicious activity is detected and responded to quickly. Have or adopt an incident response and recovery plan like NIST 800-61r2 or updated. This is a high-rated vulnerability because if we are unaware of an attack or breach then all the safeguards we have are for nothing. It is important to beware of suspicious activity before it can grow into a problem that we can’t handle later on.