1. **Broken Access Control**

Business Impact: -

Broken access control can affect companies severely by hurting them financially as well as damaging their reputation and business relationships. To prevent broken access control, it's important to implement and validate that your access controls are working properly on a continuous basis.

1. **Cryptographic Failures**

Business Impact: -

Attackers can get hold of a complete database having thousands of sensitive information, data theft, public listing, breaches, and many critical problems with business-related data.

1. **Injection**

Business Impact: -

Injections into the circular flow of income are a result of money borrowed by households and firms from different external sources, like financial institutions. However, this additional income does not result in an immediate expenditure.

1. **Insecure Design**

Business Impact: -

Insecure design vulnerabilities result from non-adherence to security best practices during the design process. Today, it is one of the leading causes of functionality failures, data breaches, broken policies, and tarnished reputations.

1. **Security Misconfiguration**

Business Impact: -

Security misconfigurations can allow attackers to gain unauthorized access to the networks, systems and data which in turn can cause significant monetary and reputational damage to your organization.

1. **Vulnerable and Outdated Components**

Business Impact: -

A vulnerable and outdated component is a software component that is no longer being supported bythe developer, making it susceptible to security vulnerabilities. Many times, a component has known vulnerabilities that don't get fixed due to a lack of maintainer.

1. **Identification and Authentication Failure**

Business Impact: -

The failure of a system to identify and/or authenticate leaves the application susceptible to attacks and leaves user accounts/data at risk. Authentication failure poses a stringent and profound threat to an organization's security.

1. **Software and Data Integrity Failure**

Business Impact: -

Addressing software and data integrity failures is crucial for maintaining the security of web applications. Failure to address these vulnerabilities can result in significant financial losses, reputational damage, legal liabilities, loss of customer trust, etc.

1. **Security Logging and Monitoring Failure**

Business Impact: -

Insufficient logging and monitoring of systems can impact visibility, incident alerting, login failures, system failures and breaches. This makes it essential to have a fully operational logging and monitoring system to collect logs and give out alerts to Security Operation Center (SOC) staff and administrators.

1. **Server Side Request Forgery (SSRF)**

Business Impact: -

successful SSRF attack can often result in unauthorized actions or access to data within the organization. This can be in the vulnerable application, or on other back-end systems that the application can communicate with.