8/02/2024

Thursday

Podili sunil gopi
B.tech iv year, IT
208X1A1229
KALLAM HARANADHAREDDY
INSTITUTE OF TECH.

TOP 10 OWASP INJECTIONS

TASK-3

OWASP Category: A01:2021 injection -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.

OWASP Category: A02:2021-Cryptographic Failures

Business Impacts: Cryptographic failures can lead to serious security breaches, as attackers may be able to bypass encryption or decrypt sensitive data. A02:2021 highlights the importance of proper implementation and management of cryptographic mechanisms in web applications

OWASP Category: A03:2021-Injection

Business Impacts: injection slides down to the third position. 94% of the applications were tested for some form of injection with a max incidence rate of 19%, an average incidence rate of 3.37%, and the 33 CWEs mapped into this category have the second most occurrences in applications with 274k occurrences.

OWASP Category: A04:2021-Insecure Design

Business Impacts: 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.

The following category reflects the awareness that bringing development and testing together early at the system design stage can improve the quality, readability, and security of the code. This is the ultimate example of the “shift left” testing movement — less waste and more efficiency.

OWASP Category: A05:2021-Security Misconfiguration

Business Impacts: 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.

OWASP Category: A06:2021-Vulnerable and Outdated Components

Business Impacts: applications are prone to threats such as code injection, buffer overflow, command injection and cross-site scripting from unsupported, out of date open-source components and known exploited vulnerabilities.

OWASP Category: A07:2021-Identification and Authentication Failures

Business Impacts: Credential stuffing, the use of lists of known passwords, is a common attack. Suppose an application does not implement automated threat or credential stuffing protection. In that case,

the application can be used as a password oracle to determine if the credentials are valid.

OWASP Category: A08:2021-Software and Data Integrity Failures

Business Impacts: Software and data integrity failures relate to code and infrastructure that does not protect against integrity violations. An example of this is where an application relies upon plugins, libraries, or modules from untrusted sources, repositories, and content delivery networks (CDNs). An insecure CI/CD pipeline can introduce the potential for unauthorized access, malicious code, or system compromise. Lastly, many applications now include auto-update functionality, where updates are downloaded without sufficient integrity verification and applied to the previously trusted application.

OWASP Category: A09:2021-Security Logging and Monitoring Failures

Business Impacts: A major European airline suffered a GDPR reportable breach. The breach was reportedly caused by payment application security vulnerabilities exploited by attackers, who harvested more than 400,000 customer payment records. The airline was fined 20 million pounds as a result by the privacy regulator.

OWASP Category: A10:2021-Server-Side Request Forgery

Business Impacts: SSRF flaws occur whenever a web application is fetching a remote resource without validating the user-supplied URL. It allows an attacker to coerce the application to send a crafted request to an unexpected destination, even when protected by a firewall, VPN, or another type of network access control list (ACL).