OWASP
TOP 10 2021

BROKEN ACCESS CONTROL

SENCODE
CYBER SECURITY

BROKEN ACCESS CONTROL

SENCODE
CYBER SECURITY

Restrictions on what authenticated users are allowed to do are often not properly enforced.

Attackers can exploit these flaws to access unauthorized functionality and/or data, such as access other users' accounts, view sensitive files, modify other users' data, change access rights.

CRYPTOGRAPHIC FAILURE

SENCODE
CYBER SECURITY

CRYPTOGRAPHIC FAILURE

SENCODE
CYBER SECURITY

Many web applications and APIs do not properly protect sensitive data, such as financial, healthcare, and PII. Attackers may steal or modify such poorly protected data to conduct credit card fraud, identity theft, or other crimes.

Sensitive data may be compromised without extra protection, such as encryption at rest or in transit, and requires special precautions when exchanged with the browser.

INJECTION

SENCODE
CYBER SECURITY

INJECTION

SENCODE
CYBER SECURITY

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.

The attacker's hostile input can trick the interpreter into executing unintended commands or accessing data without proper authorization.

INSECURE DESIGN

SENCODE
CYBER SECURITY

INSECURE DESIGN

SENCODE
CYBER SECURITY

Insecure design is a wide term that encompasses a variety of flaws and is defined as "missing or poor control design".

Even if a design is secure, implementation flaws might lead to vulnerabilities that can be exploited. Because appropriate security safeguards were never built to fight against specific threats, an unsafe design cannot be repaired by a perfect implementation.

SECURITY MISCONFIGURATION

SENCODE
CYBER SECURITY

SENCODE
CYBER SECURITY

SECURITY MISCONFIGURATION

Security misconfiguration is the most commonly seen issue. This is commonly a result of insecure default configurations, incomplete or ad hoc configurations, open cloud storage, misconfigured HTTP headers, and verbose error messages containing sensitive information.

Not only must all operating systems, frameworks, libraries, and applications be securely configured, but they must be patched/upgraded in a timely fashion.

VULNERABLE AND OUTDATED COMPONENTS

SENCODE
CYBER SECURITY

SENCODE
CYBER SECURITY

VULNERABLE AND OUTDATED COMPONENTS

Components, such as libraries, frameworks, and other software modules, run with the same privileges as the application. If a vulnerable component is exploited, such an attack can facilitate serious data loss or server takeover.

Applications and APIs using components with known vulnerabilities may undermine application defenses and enable various attacks and impacts.

7

IDENTIFICATION & ATHENTICATION FAILURE

SENCODE
CYBER SECURITY

SENCODE
CYBER SECURITY

IDENTIFICATION & AUTHENTICATION FAILURE

Application functions related to authentication and session management are often implemented incorrectly, allowing attackers to compromise passwords, keys, or session tokens, or to exploit other implementation flaws to assume other users' identities temporarily or permanently.

SOFTWARE AND DATA INTEGRITY FAILURE

SENCODE
CYBER SECURITY

SOFTWARE AND DATA INTEGRITY FAILURE

SENCODE
CYBER SECURITY

Code and infrastructure that do not protect against integrity violations are referred to as software and data integrity failures. An application that uses plugins, libraries, or modules from untrusted sources, repositories, or content delivery networks is an example of this (CDNs). Unauthorized access, malicious code, or system compromise can all be risks of an unsecured CI/CD pipeline.

9

SECURITY LOGGING AND MONITORING FAILURES

SENCODE
CYBER SECURITY

SENCODE
CYBER SECURITY

SECURITY LOGGING AND MONITORING FAILURES

Insufficient logging and monitoring, coupled with missing or ineffective integration with incident response, allows attackers to further attack systems, maintain persistence, pivot to more systems, and tamper, extract, or destroy data.

Most breach studies show time to detect a breach is over 200 days, typically detected by external parties rather than internal processes or monitoring.

SERVER-SIDE REQUEST FORGERY

SENCODE
CYBER SECURITY

10

SENCODE
CYBER SECURITY

SERVER-SIDE REQUEST FORGERY

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).

As modern web applications provide end-users with convenient features, fetching a URL becomes a common scenario.

WORRIED ABOUT YOUR WEB-APPLICATIONS?

CONTACT US

Email: office@sencode.co.uk

Phone: 01642 716680

Website: sencode.co.uk


SENCODE
CYBER SECURITY
SECURITY BEYOND COMPLIANCE