Snyk Top 10: JavaScript Vulnerabilities 2022

These are the most prevalent JavaScript vulnerabilities found by Snyk Code researchers in 2022.

01 Document Object Model Cross-Site Scripting

DOM XSS is a vulnerability that allows attackers to manipulate the DOM environment in a user's browser by injecting malicious client-side code. Unlike reflected or stored XSS, where the vulnerability is caused by server-side flaws, DOM XSS is purely client-side.

Learn how to mitigate at Snyk Learn

02 No Rate Limiting

Rate limiting is a method of preventing a user (human or bot) from repeating an action too many times (whether malicious or not). An application without any form of rate limiting is at risk for issues like DoS attacks at the proxy level, locking accounts, and brute-force attacks

Learn how to mitigate at Snyk Learn

03 Cleartext Transmission of Sensitive Information

Cleartext transmission occurs when software transmits sensitive or security-critical data via cleartext in a channel that can be sniffed by unauthorized actors, significantly lowering the difficulty of exploitation by attackers.

Learn how to mitigate at Snyk Learn

04 Cross-Site Request Forgery (CSRF)

Cross site request forgery (CSRF) is a vulnerability where an attacker performs actions while impersonating another user. For example, transferring funds to an attacker's account, changing a victim's email address, or even redirecting a pizza to an attacker's address!

Learn how to mitigate at Snyk Learn

05 Improper Neutralization of HTTP Headers for Scripting Syntax

This syntax vulnerability occurs when a user incorrectly neutralizes the web scripting syntax in HTTP headers that can be used by web browser components to process raw headers, such as Flash. This can lead to cross-site scripting and other attacks.

Learn more about this vulnerability

06 Insecure Hash

An insecure hash vulnerability is a failure related to cryptography, which is the way we encrypt or hash data. By having an insecure hash there is a high chance that your confidential data will be exposed.

Learn how to mitigate at Snyk Learn

07 Cross-Site Scripting (XSS)

Cross-site scripting is a website attack method that utilizes a type of injection to implant malicious scripts into websites that would otherwise be productive and trusted. Generally, the process consists of sending a malicious browser-side script to another user.

Learn how to mitigate at Snyk Learn

08 Directory Traversal

A directory traversal (a.k.a. path traversal) attack aims to access files and directories that are stored outside the intended folder. Manipulating files with "dot-dot-slash (../)" sequences, or absolute file paths, can provide access to arbitrary files and directories stored on the file system.

Learn how to mitigate at Snyk Learn

09 Use of Hardcoded Password

Hardcoded passwords are often used for inbound authentication or outbound communication to external components. However, they can create significant authentication failures that are often difficult for system administrators to detect and fix.

Learn more about this vulnerability

10 Unchecked Return Value

An unchecked return value vulnerability occurs when the app fails to check the return value of a method or function, preventing it from detecting unexpected states and conditions. This can lead developers to assume that the function call will never fail, or that call failures don't matter.

Learn more about this vulnerability