Snyk Top 10: Java Vulnerabilities 2022

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

snyk

01 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 filesystem.

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 more about this vulnerability

07 XML External Entity Injection (XXE)

XXE injection is a type of attack against an application that parses XML input. Attacks can include disclosing local files, which may contain sensitive data such as passwords or private user data, using file: schemes or relative paths in the system identifier.

Learn more about this vulnerability

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

02 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

05 SQL Injection

SQL injection is a common method used by attackers to manipulate and access database information. This is done by exploiting application vulnerabilities to inject malicious SQL code that alters SQL queries.

Learn how to mitigate at Snyk Learn

08 Missing Encryption of Sensitive Data

This encryption vulnerability occurs when sensitive, critical information is not encrypted before storage or transmission. This lack of proper data encryption relinquishes confidentiality, integrity, and accountability that properly implemented encryption provides.

Learn more about this vulnerability

10 Improper Access Control

This refers to the failure to properly manage access controls on a computer system or network. When these access controls are not properly preserved, they can allow unauthorized users to access sensitive information or perform actions that they are not supposed to be able to do. This can lead to security breaches, data loss, or system instability.

Learn more about this vulnerability

03 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

06 Use of Implicit Intent for Sensitive Communication

This communication vulnerability occurs when implicit intent is used to transfer sensitive data between applications. Since implicit intent doesn't specify a particular application to receive the data, any untrusted applications can process the intent and obtain sensitive data.

Learn more about this vulnerability

Find and automatically fix vulns in your Java apps for free with Snyk.

Start free

snyk TOP 10