Snyk Top 10: Go Vulnerabilities 2022

snyk

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

01

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

02

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

03

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 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

Sensitive Cookie Without 'HTTPOnly' Flag

A sensitive cookie without 'HttpOnly' vulnerability occurs when a cookie that isn't marked with the HttpOnly flag is used to store sensitive information. The HttpOnly flag directs compatible browsers to prevent client-side scripts from accessing cookies.

Learn more about this vulnerability

06

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

07

Cleartext Logging

Cleartext logging is a vulnerability that occurs when unencrypted and non-hashed sensitive information is stored in browser cookies. Malicious users can exploit these cookies by intercepting HTTP traffic or accessing the web browser directly.

Learn more about this vulnerability

08

Use of Hardcoded Credentials

Hardcoded credentials are used for inbound authentication, outbound communication to external components, and encryption of internal data. However, they can create holes that allow attackers to bypass the system authentication, which are often difficult to detect and fix.

Learn more about this vulnerability

09

Sensitive Cookie in HTTPS Session Without 'Secure' Attribute

This HTTPS session vulnerability occurs when the Secure attribute for sensitive cookies in HTTPS sessions is not set, which can allow a user to send those cookies in plaintext over an HTTP session.

Learn more about this vulnerability

10

Server-Side Request Forgery (SSRF)

This a vulnerability that allows attackers to make arbitrary outbound requests from a server. SSRF can be used to pivot throughout corporate networks, exploit otherwise unreachable internal systems, or query metadata endpoints to extract secrets.

Learn more about this vulnerability

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

Start free