Snyk Top 10: Ruby Vulnerabilities 2022

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

01 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

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 Open Redirect

An open redirect vulnerability occurs when an application allows a user to control a redirect or forward to another URL. If untrusted user input isn't validated, an attacker could supply a URL that redirects an unsuspecting victim from a legitimate domain to an attacker's phishing site.

Learn more about his vulnerability

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 more about this vulnerability

05 Sensitive Cookie Without 'HttpOnly' Flag

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 more about this vulnerability

06 Cleartext Transmission of Sensitive Information

This is a type of broken access control vulnerability in which a user or attacker gains access to information that they are not explicitly authorized to view, including PII, company data, system data/metadata, and more.

Learn more about this vulnerability

07 Improper Certificate Validation

Improper certificate validation when a certificate is incorrectly validated or not validated at all. When a certificate is invalid or malicious, it might allow an attacker to spoof a trusted entity by interfering with communication between the host and client.

Learn more about this vulnerability

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 filesystem.

Learn more about this vulnerability

09 Authentication Bypass

This specific variant of authentication bypass in Ruby occurs when the application modifies the SSL context after connection creation has begun. If the program modifies the SSL_CTX object after creating SSL objects, older SSL objects created from the original context could all be affected by that change.

Learn more about this vulnerability

10 Use of Weak Credentials

Weak credentials (such as a default key or hardcoded password) are ones that can be calculated, derived, reused, or guessed by an attacker. When credentials are easily predictable or even fixed, an attacker can breach the system without relying on brute force.

Learn more about this vulnerability