Snyk Top 10: Python Vulnerabilities 2022

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

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 file system.

Learn how to mitigate at Snyk Learn

02 Command Injection

Command injection attacks — also known as operating system command injection attacks — exploit a programming flaw to execute system commands without proper input validation, escaping, or sanitization, which may lead to arbitrary commands executed by a malicious attacker.

Learn more about this vulnerability

03 Improper Restriction of XML External Entity Reference

This mishandling of XXE references occurs when an XML document contains XML entries with URIs that connect to documents outside of the intended sphere of control, causing the application to embed incorrect documents into its output.

Learn how to mitigate at Snyk Learn

04 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

05 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

06 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

07 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 how to mitigate at Snyk Learn

08 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

09 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

10 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