Snyk Top 10: PHP Vulnerabilities 2022

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

01 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

02 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

03 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

04 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

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 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

07 Server Leak

When a server leak occurs, sensitive information is exposed to an actor that isn't authorized to access it. The severity of this vulnerability can vary based on the type of information that is leaked, such as personal information, financial data, business secrets, or proprietary code.

Learn more about this vulnerability

08 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

09 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

10 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