Snyk Top 10: PHP OSS Vulnerabilities 2022

These are the most prevalent **critical and high** open source vulnerabilities found by Snyk scans of PHP apps in 2022.

01 Information Exposure

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.

Top vuln: CVE-2022-31043
Fix: Upgrade `guzzlehttp/guzzle` to version 7.4.4, 6.5.7 or higher.

02 Improper Input Validation

Improper input validation is when an application receives input (or data), but it does not take the necessary steps to validate the input or it simply incorrectly validates the input. This can lead to your application receiving unintended input which may result in altered data or arbitrary code execution.

Top vuln: CVE-2022-23614
Fix: Upgrade `twig/twig` to version 2.14.11, 3.3.8 or higher.

03 Directory Traversal

A directory traversal attack aims to access files and directories that are stored outside the intended folder. By manipulating files with "dot-dot-slash (../)" sequences and their variations, or by using absolute file paths, it may be possible to access arbitrary files and directories stored on the filesystem.

Top vuln: CVE-2022-39261
Fix: Upgrade `Debian:10 twig` to version 2.6.2-2+deb10u1 or higher.

04 Insecure Encryption

Insecure encryption is the use of cryptographic algorithms or protocols that have known weaknesses or vulnerabilities, which makes it possible for an attacker to break the encryption and access the sensitive information that is being protected.

Top vuln: CVE-2021-46743
Fix: Upgrade `firebase/php-jwt` to version 6.0.0 or higher.

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.

Top vuln: CVE-2022-40832
Fix: There is no fixed version for `codeigniter/framework`.

06 Deserialization of Untrusted Data

This is when an application deserializes untrusted data without sufficiently verifying that the resulting data will be valid, thus allowing the attacker to control the state or the flow of the execution.

Top vuln: CVE-2021-29476
Fix: Upgrade `Debian:10 wordpress` to version 5.0.11+dfsg1-0+deb10u1 or higher.

07 Remote Code Execution (RCE)

Remote code execution (RCE) allows an attacker to execute arbitrary code on a remote device. This is often done through injection attacks. In 2022, the big RCE vulnerability was Spring4Shell.

Top vuln: CVE-2022-28368
Fix: Upgrade `dompdf/dompdf` to version 1.2.1 or higher.

08 Arbitrary Code Execution (ACE)

Arbitrary code execution (ACE) happens when an attacker is able to run commands or execute code of their choice on a target machine. If this code is executed over a network, it is sometimes referred to as remote code execution.

Top vuln: CVE-2022-25277
Fix: Upgrade `drupal/core` to version 9.3.19, 9.4.3 or higher.

09 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.

Top vuln: CVE-2020-19316
Fix: Upgrade `laravel/framework` to version 5.8.17 or higher.

10 PHP Remote File Inclusion (RFI)

Remote file inclusion (RFI) vulnerabilities occur when malicious code in a web app attempts to reference an insecure external file. This can be used as a backdoor for malware.

Top vuln: CVE-2022-41343
Fix: Upgrade `dompdf/dompdf` to version 2.0.1 or higher.

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

Start free