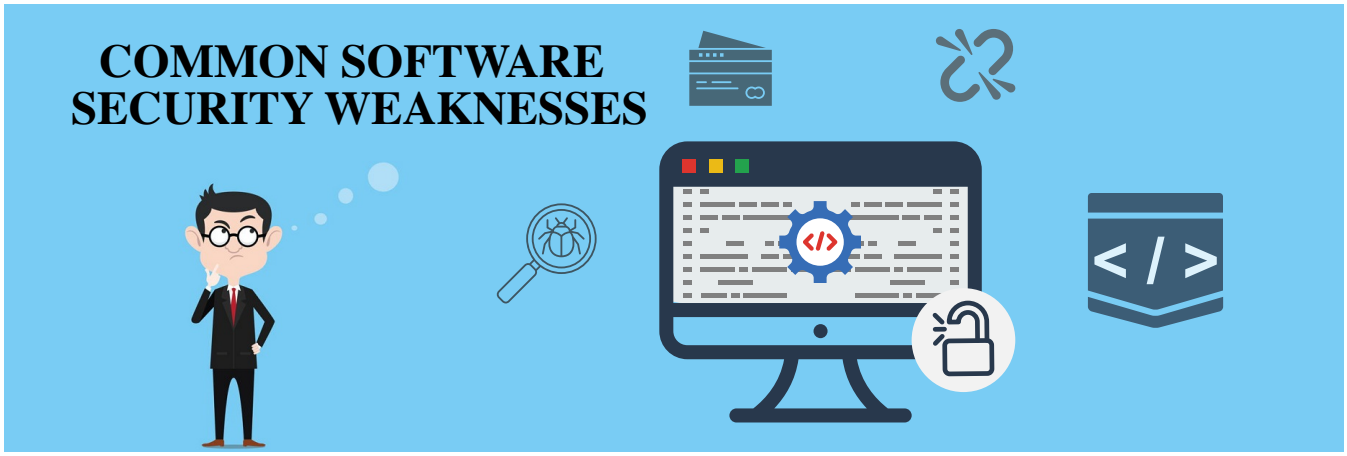
Common Software Vulnerabilities in 2022 and Ways to Prevent Them



List of Software Security Vulnerabilities

List of Software Security Vulnerabilities and Weaknesses

If you want to protect your customers and your brand, it's important to identify and prevent software security vulnerabilities before shipping software. In order to do so, you first need to be **aware of the different types of security weaknesse**s and ways to avoid them. This article aims at showing you common types of software security weaknesses and it also includes tips on preventing these vulnerabilities.

1. Bugs

Software bugs are an error or failure in software and they're very common. Some bugs will result in serious issues like information theft and some will lead to system failure. But some less serious bugs will result in error messages or incorrect results. Bugs, in general, cause the software to behave in an unexpected manner. Pretty much all software contains minor (or major) bugs. Hackers can easily take advantage of some software bugs and cause much harm if you do not fix security vulnerabilities. While it's usually impossible to ship software with 0 bugs, it's important to find and fix any serious bugs, especially ones that could pose a security risk.

2. Exposure of sensitive data

Sensitive data includes things such as account numbers, addresses, financial data, health information, usernames, and passwords. All this data must be protected to keep it from

falling into the wrong hands. Personal or sensitive data has to be protected with encryption and access controls to prevent unauthorized people from accessing it. If the [software fails to protect this personal data due to security < https://codesigningstore.com/tips-for-software-developers-to-enhance-software-security>] vulnerabilities, hackers who gain access to this information can use it to commit fraud and other crimes.

3. Flaws in Injection

Injection flaws result in **cyber attackers injecting malicious code** into an application. This kind of software security vulnerability occurs when untrusted data is sent along with a query or command to an interpreter, which in turn will make the targeted system to execute unexpected commands. This kind of attack can also result in hackers gaining access to protected data stored in the database without the right authorization.

4. Buffer overflow

Yet another common type of software security weakness, **buffer overflow** occurs when an attempt is made to store data that is too big for the memory space allocated. Attackers can use this software coding mistake, where the storage capacity of a program is overwritten, to take control of or to access your system. This vulnerability tends to be more common in software written in **C and C++**. Many programming languages have automatic protection against buffer overflow attacks.

5. Security misconfiguration

One of the most common issues in software development, **security misconfiguration** is a result of incomplete configurations and default configurations that are not secure. For example, **open cloud storage or misconfigured HTTP** headers. In order to avoid this kind of software security weakness, you need to make sure you have properly configured your OS, frameworks, and applications. Likewise, all this must be updated whenever necessary.

6. Broken access control

Broken user restrictions can cause severe software weaknesses. For example, if you

have an admin panel for your website, you want to restrict that area so only admin users can access it. If such restrictions are not enforced properly, hackers and other unauthorized people can easily take advantage of that vulnerability and access sensitive data or gain control of your system.

7. Insecure deserialization

Insecure deserialization is a security weakness that is used by hackers to carry out injection attacks and DDoS attacks. In this type of vulnerability, untrusted data is used to implement attacks.

8. Broken/Missing Authentication

Weaknesses in session management and credential management result in **broken authentication**, which means an **attacker is able to compromise passwords** or other information to access a user's account. Improperly implemented authentication and session management can result in this kind of software vulnerability.

There are a lot of adverse effects that can occur as a result of software security weaknesses. But you can prevent these problems if you take all the necessary security precautions while developing the software. It's important for software developers to use different methods to detect weaknesses in their software automatically. The **following are good ways** to prevent software security vulnerabilities.

How to Prevent Software Vulnerabilities

1. Test Your Software

It's a **good practice to test your software** often as this will help you find and get rid of vulnerabilities quickly. You can test your software using code analysis tools, white box testing, black box testing, and other techniques.

2. Update the Software Regularly

It is important to **regularly update software** as outdated software is prone to vulnerabilities. By making sure your software uses up to date components and dependencies, you can prevent security issues and **software vulnerabilities < https://www.companionlink.com/blog/2021/03/6-quick-tips-to-protect-your-iphone/>** .

3. Set Up Software Design Requirements

Define a set of principles that need to be followed while developing each software release. These principles will show the developers how to write, inspect, and demonstrate their **code to ensure security best practices are followed < https://codesigningstore.com/best-practices-for-code-signing-certificates>** . Following the latest information from organizations such as **CWE, OWASP, and CERT** will also help you detect and prevent vulnerabilities.

4. Use a Code Signing Certificate

Digitally signing your code using a code signing certificate will make your code tamper-proof, making it impossible for third parties to tamper with your code. A **code signing certificate** will make sure your files remain secure and it will also prevent hackers from adding security vulnerabilities to your code.

Effects of Software Security Vulnerabilities

Hackers make use of security vulnerabilities in software to attack and damage a system. **Defects in software** allow these attacks to succeed.

Software security vulnerabilities don't just result in **hackers attacking a system** but can also result in financial losses.

Hackers often **ruin the reputation of the companies** they attack.

Attackers use security weaknesses to steal and access an individual's personal details including bank accounts to steal money.

Summary

It is important to understand what the common software security vulnerabilities are and how to prevent them. One of the most effective ways to make your software tamper-proof is by **signing it using a code signing certificate < https://codesigningstore.com/code-signing-certificates>** . In addition, you will want to **enforce security standards** during development to prevent software security vulnerabilities. We hope this article helped you understand the different kinds of software security weaknesses and how to prevent them.

powered by digicert

Chat Now

Contact

+1 (727) 291-0611

146 2nd St. N. #201C St. Petersburg, FL 33701 United States

Code Signing Certificates

OV Code Signing Certificates < https://codesigningstore.com/ov-code-signing-certificates >

EV Code Signing Certificates < https://codesigningstore.com/ev-code-signing-certificates >

Cloud Signing Certificates < https://codesigningstore.com/cloud-signing>

24/7 Customer Support

FAQs < https://codesigningstore.com/faqs>

+ 1 (727) 291-0611

support@codesigningstore.com

We Accept:

24/7 Customer Support

LIVE CHAT

PHONE

EMAIL