What Is Security Testing?

freecodecamp.org/learn/front-end-development-libraries-v9/lecture-understanding-the-different-types-of-testing/what-is-security-testing

The web is a powerful place filled with a wealth of information and activities. But it can also be a dangerous place if you are not careful. There are many hackers and cyber criminals out there looking for new ways to breach websites and compromise data.

You've probably heard of a few high-profile data breaches that affected billion-dollar companies like Meta and Microsoft. When it comes to working on web applications, you will need to do thorough security testing to help identity vulnerabilities and weaknesses.

Here are a few principles to be aware of when it comes to performing security audits and testing:

- Confidentiality: This protects against the release of sensitive information to other recipients that aren't the intended recipient.
- Integrity: This involves preventing malicious users from modifying user information.
- Authentication: This involves verifying the user's identity to ensure that they are allowed to use that system.
- Authorization: This is the process of determining what actions authenticated users are allowed to perform or which parts of the system they are permitted to access.
- Availability: This ensures that information and services are available to authorized users when they need it.

- Non-repudiation: This ensures that both the sender and recipient have proof of delivery and verification of the sender's identity. It protects against the sender denying having sent the information.

Now that we understand the reasoning behind security testing, let's take a look at a few common security threats:

- Cross-site Scripting (XSS): You learned about this in an earlier lesson. But as a refresher, XSS attacks happen when an attacker injects malicious scripts into a web page that is viewed by other users. These scripts can then execute in the context of the victim's browser, potentially stealing cookies and session data or performing other malicious actions without the user's knowledge or consent.

- SQL Injection: SQL is a language for managing and storing information in a relational database. SQL injection allows malicious users to inject malicious code into a database. You will learn more SQL, relational databases, and SQL injection in a future module.

- Denial-of-Service (DoS) attack: This is when malicious users flood a website with a high number of requests or traffic, causing the server to slow down and possibly crash, making the site unavailable to users.

There are many more types of security threats, but there are many tools you can use to help protect your web applications and make them more secure. Here are the broad categories that security testing tools fall into:

- Static application security testing: These tools are used to evaluate the source code for an application to identify security vulnerabilities.

- Dynamic application security testing (DAST): These tools interface with the application's frontend to uncover potential security weaknesses. Unlike static application security testing, DAST tools do not have access to the source code.

Another type of security testing is penetration testing (or pentest for short). This involves creating simulated cyberattacks on the application to identify any vulnerabilities in the system. Mid to large-sized companies might have a team of dedicated cybersecurity professionals that perform pentests on a regular basis as part of their regular security audits.

The world of cybersecurity is very vast and detailed. But every developer should understand a few common threats against web applications and ways to guard against them.

Questions

Which of the following is NOT a core principle when it comes to performing security audits and testing?

Integrity

Cross Scripting

Availability

Non-repudiation

Which of the following involves malicious users to inject malicious code into a database?

SQL injection

Denial-of-Service (DoS) attack

Static application injection

Cross-site Scripting (XSS)

Which of the following involves creating simulated cyberattacks on the application to identify any vulnerabilities in the system?

Penetration testing

Unit testing

Smoke testing

Integration testing

Navigated to What Is Security Testing?