

# Three Software Vulnerability Types to Watch For

Using anonymized data from three years of tests on software systems and applications, the [2023 Software Vulnerability Snapshot report](#) found persistent vulnerabilities that are significant challenges to web and software application security.



## Information leakage

An average 19% of the total vulnerabilities found over three years were related to information leakage.

Vulnerabilities in this category include exposure of sensitive information to an unauthorized actor, exposure of sensitive information through sent data, and cross-site request forgery.

## Security misconfigurations

Server misconfigurations represented an average 18% of the total vulnerabilities found over three years of testing. Five percent were related to application misconfigurations.

Developer features such as debug and QA can be dangerously unsafe if not deactivated when deployed. Configuration files need to be set with security in mind.



## Insufficient transport layer protection

An average 11% of vulnerabilities found over all three years of testing were related to insufficient transport layer protection.

Applications may use SSL/TLS during authentication, but fail to use it elsewhere in the application, leaving data and session IDs exposed.

## How to protect your code

1.

### Implement a multilayered security approach.

Use static analysis to identify coding flaws, dynamic analysis to examine running applications, software composition analysis to identify vulnerabilities in third-party components, and pen testing for issues that may be missed by other tests.

2.

### Supplement your security testing.

Does your team have sufficient skills to test for security defects with a multilayer approach? Do they have the time to test at the level demanded by customers?

3.

### Augment your team with on-demand, expert security testing.

Boost your security testing coverage with on-demand resources to protect your software, your business, and your customers.

Synopsys offers a full spectrum of testing services, including penetration testing, dynamic application security testing, static application security testing, mobile application security testing, network penetration testing, red teaming, IoT and embedded software testing, and thick client testing.

[Contact Synopsys today to schedule a free consultation](#)

## The Synopsys difference

Synopsys provides integrated solutions that transform the way you build and deliver software, accelerating innovation while addressing business risk. With Synopsys, your developers can secure code as fast as they write it. Your development and DevSecOps teams can automate testing within development pipelines without compromising velocity. And your security teams can proactively manage risk and focus remediation efforts on what matters most to your organization. Our unmatched expertise helps you plan and execute any security initiative. Only Synopsys offers everything you need to build trust in your software.