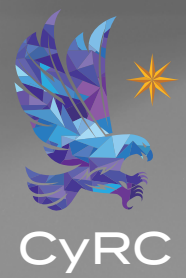
SYNOPSYS®

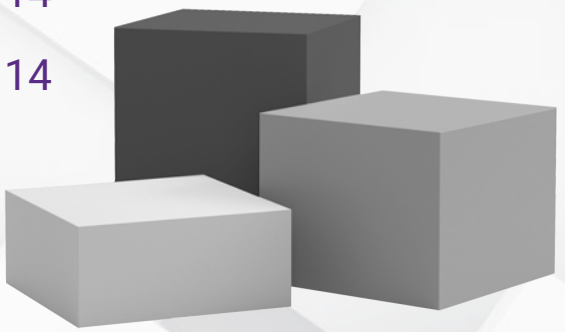
Software Vulnerability Snapshot

The 10 Most Common Web Application Vulnerabilities



Analysis by Synopsys Security Testing Services and the Synopsys Cybersecurity Research Center

Table of contents



Overview

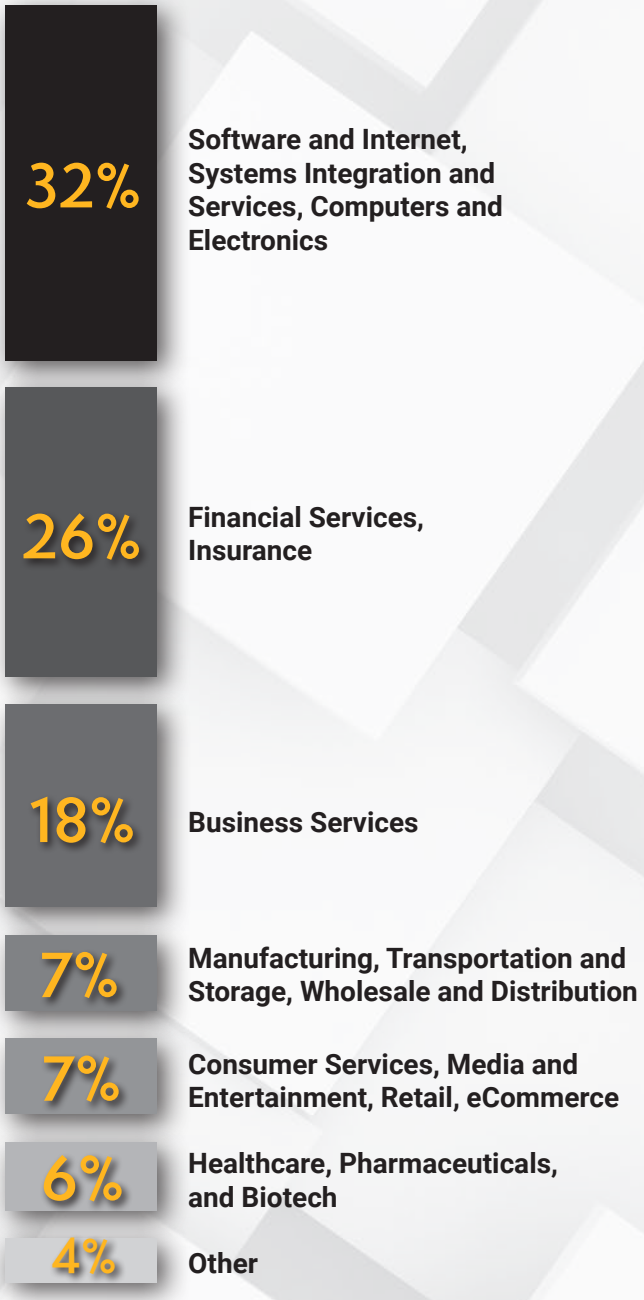
To produce the annual "Application Vulnerability Snapshot" report, Synopsys Cybersecurity Research Center (CyRC) researchers examine anonymized data from commercial software systems and applications tested by Synopsys Application Security Testing (AST) services. This year's report includes data from 4,398 tests conducted in 2021 on 2,711 targets (i.e., software or systems). Almost all the tests (95%) were intrusive "black box" and "gray box" tests, including penetration (pen) tests, dynamic application security testing (DAST), and mobile application security testing (MAST) analyses.

Black box testing approaches the target's security state from an outsider's perspective, whereas gray box testing simulates an authenticated user with credentials—essentially extending black box testing with deeper insights. The Synopsys AST services tests probe running applications as a real-world attacker would, with the goal of identifying vulnerabilities that could then be triaged and remediated as necessary.

The targets tested were largely web (82%) and mobile (13%) applications, with the remaining 5% either source code or network systems/applications tests. The industries represented included software and internet (32%), financial services (26%), business services (18%), manufacturing (7%), consumer services (7%), and healthcare (6%). The remaining 4% of test targets represented travel and leisure, education, energy and utilities, and other verticals.

The Synopsys AST services tests probe running applications as a real-world attacker would, with the goal of identifying vulnerabilities that could then be triaged and remediated as necessary.

Industries represented in the study



Who Should Read This Report

If you're in charge of a software security program, getting a deeper view into software risk can help you plan strategic improvements in your security efforts. If you're looking at a security program from the tactical side, you can use the information in this report to present a business case for expanding security testing in your software security initiative, for example, by enhancing static application security testing (SAST) and software composition analysis (SCA), or by testing running applications with DAST, pen or fuzz testing, or MAST.

According to the Forrester report, "The State of Application Security: 2022," web application exploits are the third-most-common attack (see Figure 1). With that much exposure, it's clear that organizations need to test their running web applications in the same way that attackers will, and then identify and eliminate vulnerabilities before they are exploited by outside agents.

"How was the attack carried out?"

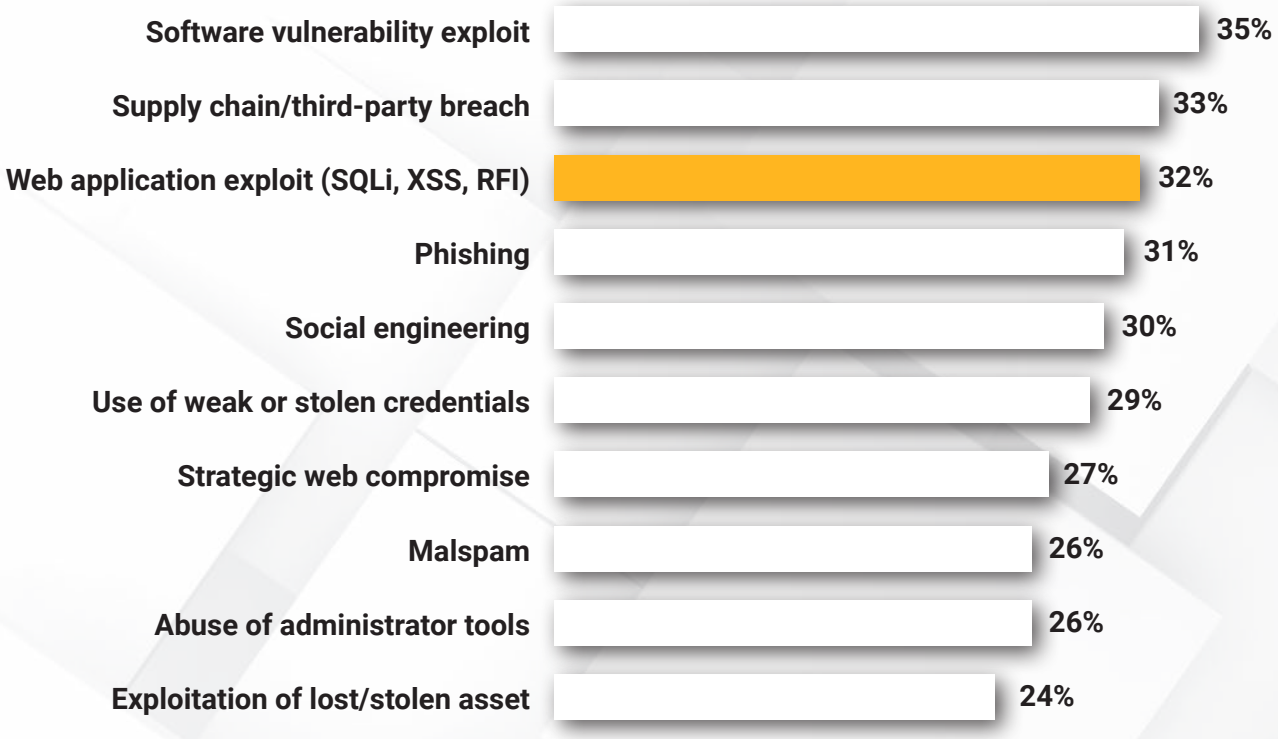


Figure 1. Web application exploits comprise over 30% of attacks

88% of organizations participating in the BSIMM project use external penetration testers to find problems.

Who Uses Third-Party Application Security Testing

Businesses use third-party application security testing services for a variety of reasons, one of the largest being a lack of trained or experienced security professionals.

Some organizations may also want to validate their own testing and ensure that their internal security controls are working. Others may need to extend their software security testing capabilities but don't want to add dedicated tools and staff to their budgets. Still others may need to comply with regulatory or business requirements that mandate third-party assessments. For example, the Payment Card Industry Data Security Standard (PCI DSS) requires pen testing on a regular schedule or after any significant changes to the software or system.

The "2022 BSIMM13 Trends and Insights report" found that 88% of the organizations participating in the Building Software in Maturity Model (BSIMM) project, a program examining the strategies organizations employ to build security into software development, use external penetration testers to find problems. These tests can uncover issues that might have been missed by internal testing and may highlight a weak link in an organization's security toolset. If a static analysis tool is failing to capture security defects that surface during DAST or penetration testing, for example, there may be a problem in the organization's overall security testing portfolio.

For those wanting to learn more about the BSIMM project, the "BSIMM13 Foundations" report provides in-depth detail on BSIMM background and data, and the "BSIMM13 Trends and Insights" report offers a distillation of current BSIMM findings.

Types of Tests Mentioned in This Report

Sixty-four percent of the tests conducted in 2021 by Synopsys AST services were **pen tests**—simulated attacks designed to evaluate the security of an application or system. Pen testing enables organizations to find and fix runtime vulnerabilities in the final development stages of software or after deployment. Pen tests are often a compliance requirement of security standards. As noted earlier in this report, compliance with PCI DSS requires pen testing on a regular schedule.

Pen testing also introduces a needed human element into the security equation. Some vulnerabilities can't be easily detected by automated testing tools—they need human oversight to be uncovered. For example, the only effective way to detect an insecure direct object reference (IDOR), an issue that allows attackers to gain access to unauthorized data, is by performing a manual test.

Benefits of Third-Party Application Security Testing

Third parties can provide expertise, scale, trust in findings, and remediation guidance. They can also lower your overall risk posture while saving you time and money in the long run. Third-party testing is useful when you need to

Enhance your security coverage

Fulfill compliance requirements

Increase your security reputation with customers

Improve your response to software security threats

Dynamic application security testing (DAST) and **mobile application security testing (MAST)** were 18% and 12% of the total tests respectively. MAST is used to uncover authentication and authorization issues, client-side trust issues, misconfigured security controls, cross-platform development framework issues, and vulnerabilities in application binaries running on mobile devices and corresponding server-side systems.

The primary objective of DAST is to test running web applications for vulnerabilities such as SQL injection and cross-site scripting. The vulnerabilities that are exploited in web applications don't exist in source code; they arise only after deployed into production. This makes DAST an essential component of any application security testing program.

As noted earlier, human oversight is sometimes needed to develop a full software security picture. Synopsys DAST evaluations include manual testing to uncover vulnerabilities that typically can't be found by out-of-the-box tools, such as some vulnerabilities pertaining to authentication and session management, access control, and information leakage.

There is often confusion regarding the use of static application security testing (SAST) and software composition analysis (SCA) versus the need for DAST and pen testing. SAST and SCA test the application code and are used to discover a different set of vulnerabilities than DAST and pen testing. Organizations need to utilize multiple testing techniques at various points in the software development process for comprehensive security coverage.

Security Issues Found in the Synopsys AST Services Tests

Of the 4,398 tests Synopsys AST services conducted in 2021, 95% uncovered some form of vulnerability in the target applications. Twenty-five percent of the total were high- or critical-risk vulnerabilities.

With more attackers using automated exploitation tools that can attack thousands of systems in a matter of seconds, fixing high- and critical-risk vulnerabilities is urgent whenever those vulnerabilities are discovered. For example, vulnerabilities allowing cross-site scripting (XSS) can give attackers the entry they need to access application resources and data. Synopsys AST services found that 22% of the 2021 test targets had exposure to reflected, stored, or DOM-based cross-site scripting vulnerabilities (see Figure 2).

Critical-risk vulnerabilities allow attackers to execute code on a web application or application server and access sensitive data. Common critical-risk vulnerabilities include remote code execution and SQL injection—insertion of a SQL query via the input data from the client to the application. While not shown in Figure 2, 4% of the total test targets were vulnerable to some type of SQL injection.

Of the 4,398 tests Synopsys AST services conducted, 95% uncovered some form of vulnerability in the target applications.

Synopsys Application Security Testing Services by the Numbers

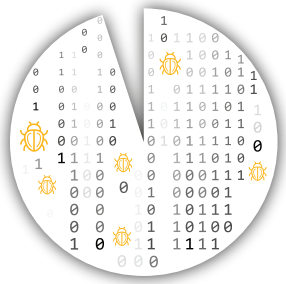
2,711

Test Targets

4,398

Tests

4,194



Tests That Uncovered Vulnerabilities (95%)

30,731

Vulnerabilities Discovered

1,420

Tests with High- or Critical-Risk Vulnerabilities (25%)

Types of Tests (Excludes Retests)

64% Pen Testing

18% Dynamic Analysis

12% Mobile Testing

6% Other*

*Static Analysis, Network Pen Testing

Validation of Fixes Retests: 34% of Total Tests

Fresh Assessment of Previously Tested Application: 26% of Total Tests

Top Vulnerability Discovered	Weak SSL/TLS Configuration (82%)
Top High-Risk Vulnerability Discovered	Reflected, Stored, or DOM-Based Cross-Site Scripting (22%)
Top Critical-Risk Vulnerability Discovered	SQL Injection/Blind SQL Injection (4%)

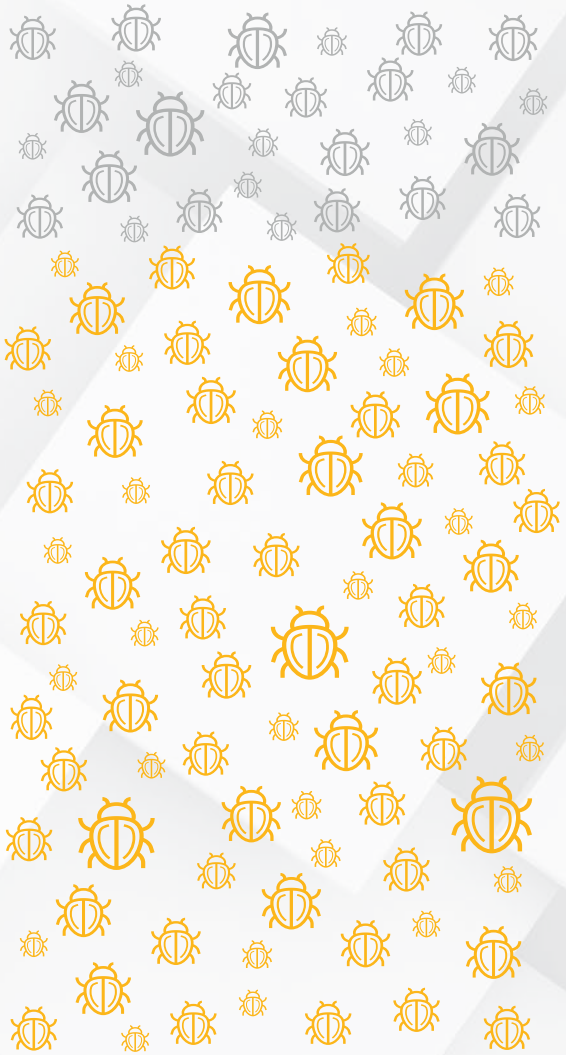
Vulnerability	Percentage of Vulnerability in Total Test Targets
Weak SSL/TLS Configuration	82%
Missing Content-Security-Policy Header	46%
Verbose Server Banner	45%
HTTP Strict Transport Security (HSTS) Not Implemented	40%
Cacheable HTTPS Content	34%
Insecure Content-Security-Policy Header	28%
Weak Password Policy	26%
Excessive Session Timeout Duration	25%
Clickjacking	22%
Reflected, Stored, or DOM-Based Cross-Site Scripting	22%

Figure 2. Top 10 vulnerabilities found in 2021 tests

Vulnerabilities Breakdown by the OWASP Top 10

The Open Web Application Security Project (better known as OWASP) Top 10 list represents a consensus among a large group of developers and web application security teams of the most critical security risks to web applications. In late 2021, the Top 10 list was updated with three new categories added and others consolidated or with name and scope changes.

While intended by OWASP as an awareness document, many organizations use the list as a de facto application security standard. Of the total 30,731 vulnerabilities discovered in the Synopsys AST services tests, 78% fell into an OWASP Top 10 category.



Of the total 30,731 vulnerabilities discovered in the Synopsys AST services tests, 78% fell into an OWASP Top 10 category.

Figure 3 lists the 10 most prevalent vulnerabilities Synopsys found, matched against the OWASP Top 10, and in two cases, the OWASP Mobile Top 10.

Description	OWASP Family Top 10 Category	Percentage of Vulnerability in Total Vulnerabilities
Information Disclosure: Information Leakage	A01:2021—Broken Access Control	18%
Server Misconfiguration	A05:2021—Security Misconfiguration	18%
Insufficient Transport Layer Protection	M3: Insufficient Transport Layer Protection	11%
Authorization: Insufficient Authorization	M6: Insecure Authorization	7%
Application Privacy Tests	A07:2021—Identification and Authentication Failures	5%
Client-Side Attacks: Content Spoofing	A03:2021—Injection	4%
Fingerprinting	A07:2021—Identification and Authentication Failures	4%
Authentication: Insufficient Authentication	A07:2021—Identification and Authentication Failures	4%
Application Misconfiguration	A05:2021—Security Misconfiguration	4%
Authorization: Insufficient Session Expiration	A07:2021—Identification and Authentication Failures	3%
Total		**78%**

Figure 3. Vulnerabilities matched against 2021 OWASP Top 10 and OWASP Mobile Top 10 categories

Figure 3 lists the 10 most prevalent vulnerabilities Synopsys found, matched against the OWASP Top 10, and in two cases, the OWASP Mobile Top 10.

OWASP Categories in Detail

A01:2021—Broken Access Control

Eighteen percent of the total vulnerabilities were related to the OWASP A01:2021—Broken Access Control category. The OWASP team notes more occurrences of vulnerabilities that fit into this category than any other category. Notable 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."

Many of the vulnerabilities contained in the Broken Access Control category are more failures in business logic than actual vulnerability types, and they cannot be easily detected by automated testing tools. For example, IDOR issues, which allow attackers to manipulate references in order to gain access to unauthorized data, are included in the Broken Access Control category. As mentioned earlier in this report, the only effective way to detect IDOR issues is by having a human perform a manual test.

A05:2021—Security Misconfiguration (Server Misconfiguration)

Server misconfigurations, part of the OWASP A05:2021—Security Misconfiguration category, represented 18% of the vulnerabilities found in the tests. Security misconfigurations can happen at any level of an application stack, including the network services, platform, web server, application server, database, frameworks, custom code, and preinstalled virtual machines, containers, or storage. Such flaws frequently give attackers unauthorized access to some system data or functionality, occasionally even resulting in a complete system compromise.

A05:2021—Security Misconfiguration (Application Misconfiguration)

The flip side of server misconfigurations, application misconfigurations are also members of the A05:2021—Security Misconfiguration category. Four percent of the total vulnerabilities were related to application misconfigurations.

M3: Insufficient Transport Layer Protection

Many mobile applications have specific issues with insufficient transport layer security, to the point where OWASP has dedicated a category in the OWASP Mobile Top 10 to it. As OWASP notes, "mobile applications frequently do not protect network traffic. They may use SSL/TLS during authentication but not elsewhere. This inconsistency leads to the risk of exposing data and session IDs to interception." Eleven percent of vulnerabilities found in the tests were related to insufficient transport layer protection.

M6: Insecure Authorization

Seven percent of the test targets contained insecure authorization vulnerabilities, another OWASP Mobile Top 10 category. Authentication is the act of identifying an individual. Authorization is the act of checking that the individual has only needed permissions. A mobile app transmitting a user's roles or permissions to a back-end system as part of a request is an example of insecure authorization.

OWASP notes that the presence of IDOR vulnerabilities is often indicative of code not performing a valid authorization check. Again, this is an example of the need to have human involvement in testing for comprehensive security. As a general rule, only manual testing can uncover most IDOR issues.

A07:2021—Identification and Authentication Failures

Previously known as Broken Authentication, the A07:2021—Identification and Authentication Failures category now includes vulnerabilities related to identification failures.

Sixteen percent of the total vulnerabilities found in the tests belonged to this OWASP category, including what is identified in the tests as "fingerprinting," a security measure sometimes used to authenticate users. However, unless web servers are properly configured and monitored, fingerprinting can also provide attackers with valuable information such as OS type, OS version, SNMP information, domain names, network blocks, VPN points, and more. Insufficient session expiration, another member of this category, occurs when an application permits the reuse of old session credentials or session IDs for authorization.

A03:2021—Injection (Client-Side Attacks: Content Spoofing)

The A03:2021—Injection category includes well-known vulnerabilities such as cross-site scripting and SQL injection. "Content spoofing," an attack closely related to cross-site scripting, modifies a web page for malicious reasons. Four percent of the total vulnerabilities found in the tests fell into this category.

Testing with a Full Spectrum of Security Tools

Vulnerability	Percentage of Vulnerability in Total Pen Tests	Vulnerability	Percentage of Vulnerability in Total DAST Scans
Weak SSL/TLS Configuration	77%	Weak SSL/TLS Configuration	81%
Missing Content-Security-Policy Header	46%	Missing Content-Security-Policy Header	56%
Verbose Server Banner	42%	Verbose Server Banner	49%
HTTP Strict Transport Security (HSTS) Not Implemented	36%	HTTP Strict Transport Security (HSTS) Not Implemented	48%
Cacheable HTTPS Content	32%	Cacheable HTTPS Content	40%
Insecure Content-Security-Policy Header	30%	Excessive Session Timeout Duration	38%
Weak Password Policy	25%	Clickjacking	30%
Reflected, Stored, or DOM-Based Cross-Site Scripting	22%	Insecure Content-Security-Policy Header	28%
Excessive Session Timeout Duration	21%	Weak Password Policy	27%
Vulnerable Third-Party Libraries in Use	21%	Reflected, Stored, or DOM-Based Cross-Site Scripting	22%
Clickjacking	21%	Session Not Invalidated After Logout	22%
Verbose Error Messages (with Stack Trace)	19%	Unmasked NPI Data	22%
Verbose Error Messages	18%	Password Reset Username Enumeration	21%
Unmasked NPI Data	16%	Improper Restriction of Excessive Authentication Attempts	19%
Session Not Invalidated After Logout	16%	X.509 Certificate About to Expire (SSL/TLS)	19%

Figure 4. Top 15 vulnerabilities found by pen and DAST scans (excluding retests)

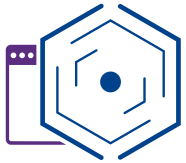
Figure 4 makes it clear that applications often fail in their duty to protect the integrity of sensitive network traffic. Weak SSL/TLS configurations were the top vulnerability found in the overall tests, with 82% of the test targets containing some form of that vulnerability. Broken down by types of tests, pen testing found that 77% of its targets had weak SSL/TLS configurations, with 81% found by DAST scans and 32% found by MAST scans.

Both the pen tests and DAST scans found 22% of the total test targets had some exposure to cross-site scripting attacks, one of the most prevalent and destructive high- and critical-risk vulnerabilities impacting web applications. While SAST can detect many common vulnerabilities, it is limited to discovering vulnerabilities that occur in the code itself. Most XSS vulnerabilities occur only when the application is running.

WhiteHat Dynamic

In June 2022, Synopsys acquired WhiteHat Security, an application security pioneer and market-segment-leading provider of dynamic application security testing solutions. WhiteHat™ Dynamic expands the Synopsys portfolio of application security testing services that deliver subscription-based static analysis, dynamic analysis, and mobile testing services.

During 2021, WhiteHat was used to scan over 16,000 applications and conducted over 5 million scans that uncovered a quarter-million flaws and vulnerabilities in customer web applications. It's interesting to see that the WhiteHat findings closely correspond to those conducted by Synopsys AST services and with the OWASP Top 10.



Top 10 Vulnerabilities in WhiteHat Scans

1. Information Leakage
2. Frameable Resource (Clickjacking)
3. Insufficient Transport Layer Protection
4. Fingerprinting
5. Application Misconfiguration
6. Insufficient Authorization
7. Cross-Site Scripting
8. Server Misconfiguration
9. Improper Input Handling
10. Directory Indexing (Broken Access Control)

Figure 5. WhiteHat top 10 software flaws/vulnerabilities found in 2021

Description	Percentage of Vulnerability in Total Vulnerabilities—Synopsys AST Services
Information Disclosure: Information Leakage	18%
Server Misconfiguration	18%
Insufficient Transport Layer Protection	11%
Authorization: Insufficient Authorization	7%
Application Privacy Tests	5%
Client-Side Attacks: Content Spoofing	4%
Fingerprinting	4%
Authentication: Insufficient Authentication	4%
Application Misconfiguration	4%
Authorization: Insufficient Session Expiration	3%

Figure 6. Percentage of vulnerability found in all Synopsys AST services tests

Vulnerability	Percentage of Vulnerability in Total MAST Scans
Weak SSL/TLS Configuration	32%
Lack of Binary Obfuscation (iOS)	31%
Credential Kept in Memory After Login	30%
Application Allows Sensitive Data to be Copied (iOS)	26%
Application Allows Sensitive Data to be Copied	22%
Unmasked NPI Data	22%
Application Screenshot Information Disclosure	21%
Lack of Certificate Pinning (iOS)	20%
Lack of Binary Obfuscation	19%
Insecure Configuration of Application Transport Security (iOS)	19%
Vulnerable Minimum OS Version Supported (iOS)	18%
Sensitive Data Stored Unencrypted in Local Storage (iOS)	18%
iOS Keychain Used Without Security Access Control	17%
Application Screenshot Information Disclosure (iOS)	16%
Application Screenshot Information Disclosure (Android)	16%

Figure 7. Top 15 vulnerabilities found by MAST scans (excluding retests)

Even Lower-Risk Vulnerabilities Can Be Exploited to Facilitate Attacks

Many of the vulnerabilities the tests uncovered are considered minimal, low, or medium risk. That is, the issues found are not directly exploitable by attackers to gain access to systems or sensitive data. Nonetheless, surfacing these vulnerabilities is not an empty exercise, as even lower-risk vulnerabilities can be exploited to facilitate attacks. For example, verbose server banners—found in 49% of the DAST scans and 42% of the pen tests—provide information such as server name, type, and version number that could allow attackers to perform targeted attacks on specific technology stacks.

It's clear when looking at the results from the Synopsys AST services tests that the best approach to security testing is using a spectrum of tools to help ensure an application or system is secure.

Implementing or securing protections such as a content security policy (CSP) can provide an added layer of security that helps detect and mitigate certain types of attacks, including cross-site scripting and data injection attacks. An insecure or absent CSP might be considered a low-risk concern. However, the prevalence of cross-site scripting, clickjacking, and cross-site leak exploits makes a strong argument for having a CSP—and more importantly, a secure CSP—as an effective second layer of protection against various types of attacks, especially cross-site scripting.

The Danger of Vulnerable Third-Party Libraries

As shown in Figure 4, the pen tests and DAST scans, although run on different applications, found many of the same types of vulnerabilities. On the other hand, both types of testing revealed vulnerabilities either not found or found far less frequently than the other test. For example, the Vulnerable Third-Party Libraries in Use category was found in 21% of the pen tests but it doesn't appear in the top 15 vulnerabilities found in the DAST scans. Although not detailed in this report, the same vulnerability category was found in 27% of the static analysis tests Synopsys AST services conducted in 2021.

The Vulnerable Third-Party Libraries in Use category correlates with OWASP Top 10 category A06:2021—Vulnerable and Outdated Components. OWASP notes that software is likely vulnerable if

- You do not know the versions of all components you use (both client-side and server-side). This includes components you directly use as well as nested dependencies.
- The code being used is unsupported or out-of-date. This includes the OS, web/application server, database management system, applications, APIs, and all components, runtime environments, and libraries.

In light of high-profile supply chain attacks, software supply chain security has become a major concern for organizations dependent on third-party software. Most programs managing software supply chain risk focus on identifying and securing third-party software—often open source software—that is destined for integration into software developed in-house. A recent report from Synopsys and the Enterprise Strategy Group (ESG) found that 73% of survey respondents have increased their efforts to secure their organizations' software supply chain through a variety of initiatives.

Software supply chain security has become a major concern for organizations dependent on third-party software.

Managing Supply Chain Risk with a Software Bill of Materials

To better manage supply chain risk, more organizations are using automated tools to generate a software Bill of Materials (SBOM) to fully identify the third-party software they use and improve their ability to respond to disclosed vulnerabilities. Evidence of the movement toward SBOMs can be seen in the 30% growth of the "create Bills of Materials for software" BSIMM activity recorded in the "BSIMM13 Foundations" report. BSIMM13 data also indicates a 35% increase in both the "identify open source" and "control open source risk" activities due to the prevalence of open source components in modern software and the rise of attacks using vulnerable open projects as vectors.

With many companies having hundreds of applications or software systems in use, each themselves likely dependent on hundreds to thousands of different third-party and open source components, an accurate, up-to-date SBOM is urgently needed to effectively track those components.

The Need for a Holistic AppSec Program to Manage Risk at Scale

Businesses that sell software, or products that include embedded software, can't afford security, compliance, or quality issues compromising those products. Even businesses not directly engaged in selling software or software-driven products depend on software quality and security. Software drives the administrative systems for most payroll, billing, receivables, sales-tracking, and customer records. Software controls production, manages inventories, directs warehousing, and runs the distribution systems that keep business running.

Software is also the way most businesses interact with customers. As noted earlier, the Forrester report, "The State of Application Security, 2022," states that web application exploits are the third-most-common type of software attack. The giant credit risk assessment firm Equifax fell prey to such an exploit when an attacker's breach of the underlying software framework of an Equifax web portal exposed the personal data of 143 million U.S. citizens.

It's obvious that organizations not only should test web applications for common flaws, vulnerabilities, and misconfigurations with static analysis and software composition analysis tools, but also test their running web applications in the same way that attackers probe them.

A full spectrum of application security testing is an essential component of managing software risk in today's world. When an organization lacks the needed human resources or tools to perform high-level black and gray box security testing or needs to validate its own security controls, working with a third party such as Synopsys Application Security Testing services may be the ideal solution.

Recommendations

Plan a strategy of a full spectrum of security testing tools.

Bolster your in-house testing through third-party AST services that might include build-time static analysis, manual code review, dynamic scanning in a QA/integration test, and preproduction and postproduction penetration testing. A full spectrum of testing tools can help you remedy defects and identify known vulnerabilities in your software, whether that software is commercial third-party software, open source, or developed in-house.

Collect and combine data from your security testing tools and use that data to create and enforce software security policies.

Gather data on what testing was performed and what issues were discovered to drive security improvements in both the software development life cycle and your governance processes.

Use a mixture of automated and manual security testing.

There is no one best approach to application security testing. Some vulnerabilities can't be easily detected by automated testing tools—they need human oversight to be uncovered. Humans should perform the security tests they're the most effective at carrying out, with their efforts augmented by automated testing.

Choose the right vendor.

Choose a vendor that can develop a comprehensive risk posture report for your executives and for regulatory/compliance purposes.

CyRC

About CyRC Research

The mission of the Synopsys Cybersecurity Research Center (CyRC) is to publish security research that helps organizations better develop and consume secure, high-quality software.

SYNOPSYS®

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.

For more information, go to www.synopsys.com/software.

Synopsys, Inc.
690 E Middlefield Road
Mountain View, CA 94043 USA

Contact us:
U.S. Sales: 800.873.8193
International Sales: +1 415.321.5237
Email: sig-info@synopsys.com