Software industry: Top vulnerabilities in 2024 and what to watch for in 2025

BY JENNIFER CHANEY · FEBRUARY 17, 2025 · LAST UPDATED ON JANUARY 2, 2026

What you will learn

- **Which software security vulnerabilities dominated in 2024,** from access control flaws and API weaknesses to common web bugs like Cross Site Scripting (XSS), and why they posed significant risks for modern software ecosystems.
- **Why these vulnerabilities matter for your business and how to prioritise them effectively**, including practical insights on enforcing RBAC, securing APIs, and fixing high impact issues before attackers exploit them.
- **What proactive strategies should you adopt in 2025** to stay ahead of evolving threats and embrace bug bounty programs for dynamic testing beyond traditional tools.

Driven by the adoption of cloud services, increasingly complex SaaS ecosystems, and the reliance on open-source components, the software industry isn't slowing down. But with innovation comes risk: vulnerabilities are being exploited at an alarming rate, threatening billions of dollars in operations, data, and trust.

In 2024, the software industry was rocked by cyber threats ranging from API misconfigurations to access control failures and cloud service vulnerabilities. These issues underscored the urgent need for organizations to strengthen their defenses—and to embrace more preventative solutions such as bug bounty programs to proactively address security risks before they can become a real problem.

This blog outlines the top vulnerabilities that came to light in 2024 in the software industry, provides actionable insights for addressing emerging threats, and explores how bug bounty programs provide a critical advantage in staying ahead of attackers.

2024's software security landscape: Vulnerabilities found

Behind every breach is a vulnerability—a misstep in development, a misconfiguration, or overlooked weaknesses waiting to be exploited. Here are a few of the most prevalent issues from 2024:

1. Access control vulnerabilities

Access control flaws, such as Insecure Direct Object References (IDOR), accounted for a staggering portion of breaches in 2024. These bugs allow attackers to manipulate sensitive resources—viewing, modifying, or even deleting data that wasn't meant to be accessible.

Last year, one of Intigriti's bug bounty researchers found an access control flaw that allowed attackers to alter API connections across multiple organizations. The result? The potential for **massive service**

disruption, data losses, and leaks of sensitive details. Such vulnerabilities remind organizations to rigorously enforce **role-based access controls (RBAC)** and ensure policies surrounding least-privilege principles are well-implemented.

Actionable tips:

- Implement least-privilege access principles.
- Perform rigorous role-based access control (RBAC) testing.
- Regularly audit and patch API access pathways for injection risks.

2. API vulnerabilities and information leakage

APIs are the cornerstone of modern software ecosystems, enabling communication between systems and services. However, a 2023 report showed that **94% of organizations had experienced security problems in production APIs**, with 17% having experienced an API-related breach

In one case case last year, a researcher on Intigriti's platform reported an API endpoint leaking sensitive user data, such as names, email addresses, and even password reset tokens. By chaining this data together, attackers could request a password reset and hijack user accounts. This highlights the importance of limiting exposed data, enforcing strict API input validation, and conducting regular pentests on endpoints.

Actionable tips:

- Use minimal response models—return only the data actively required for the user's request.
- Obfuscate or encrypt sensitive fields where feasible.
- Perform regular API audits and penetration tests to identify unnecessary exposed data points.

3. Cross-Site Scripting (XSS): Low complexity, high Impact

Often underestimated as a low-priority issue, Cross-Site Scripting (XSS) ranked as the **second most common High/Critical Security Vulnerability in 2023**. It accounted for 10.5% of all such vulnerabilities and required an average of 100 man-days to remediate.

In 2024, Intigriti researchers unearthed a dangerous XSS case where a malicious script, sent via a support form, allowed an attacker to hijack an administrator's session. This opened the door to unauthorized access to internal tools and sensitive data extraction.

Lesson learned? Even low-complexity bugs can have severe consequences when privileged users are targeted. Organizations need to take XSS vulnerabilities seriously by using Content Security Policies (CSPs), systematically sanitizing inputs, and testing employee-facing workflows.

Actionable tips:

- Utilize Content Security Policies (CSP) to limit JavaScript execution.
- Validate and sanitize all input fields—especially those visible in admin or high-privilege workflows.

- Employ advanced browser-side security features like Subresource Integrity (SRI).

Bug bounty programs: Staying one step ahead

The migration to SaaS and cloud-based services has transformed software company operations, but also massively expanded the attack surface. One example is web application breaches, often involving stolen credentials and exploited vulnerabilities, which account for 25% of all breaches.

In a world where these types of vulnerabilities are inevitable, proactive discovery is the best defense. Below are three reasons why embracing bug bounty programs is a smart move for the software industry moving forward:

1. Dynamic security testing beyond traditional tools

Static scanners and traditional vulnerability assessments often fail to identify hidden risks in real-world scenarios. Bug bounty programs empower skilled, creative security researchers to test for vulnerabilities in production environments, including cloud platforms, APIs, and SaaS applications. This dynamic approach is ideal for areas like:

- Finding misconfigured cloud services.
- Testing open-source dependencies for vulnerabilities.
- Uncovering injection flaws (SQLi, XSS) that go undetected in code scans.

And much more.

2. Discovery of high-impact vulnerabilities

Bug bounty programs specialize in surfacing high-priority issues, such as RCE bugs, insecure permissions, and IDOR exploits, which have been behind some of the largest breaches in 2024. By incentivizing ethical hackers to actively search for these vulnerabilities, organizations gain real-time intelligence that can stop vulnerabilities before they're weaponized.

3. Cost-effective security augmentation

The average cost of a cyber breach in 2024 was $4.88 million, but the ability to uncover and remediate a critical flaw before exploitation can cost as little as a four-figure bug bounty reward. Bug bounty programs effectively reduce the long-term financial burden of cyber incidents while augmenting internal security teams with the expertise of global ethical hackers.

2025: How to stay secure in an evolving threat landscape

Looking forward, staying ahead of cyber threats in 2025 requires a proactive and multilayered approach. Here are some key measures for software organizations to implement:

1. Adopt secure development practices (shift-left security)

Integrate security testing earlier in the development lifecycle, including:

- Implementing **automated code checks** for common vulnerabilities.
- Using **secure coding frameworks** and dependency monitoring.

2. Embrace bug bounty programs

Start or expand your bug bounty program to identify vulnerabilities that automated tools often overlook. Bug bounty platforms provide access to a talented crowd of ethical hackers who can dynamically test applications, APIs, and services in real-world scenarios.

3. Focus on cloud and SaaS security

With cloud and SaaS adoption accelerating, companies must:

- Regularly audit configurations and permissions in cloud environments.
- Use **zero-trust principles** to limit access wherever possible.
- Monitor third-party dependencies for emerging vulnerabilities.

4. Prepare for supply chain risks

Implement measures like:

- Using a **Software Bill of Materials (SBOM)** to track dependencies.
- Conducting penetration testing of third-party integrations.

Conclusion

The escalating complexity of software ecosystems demands a shift from reactive security to proactive strategies. Lessons from 2024 show that attackers are commonly exploiting gaps caused by rapid SaaS adoption, cloud misconfigurations, and overlooked vulnerabilities in APIs and access controls.

Bug bounty programs provide a crucial advantage in this fight, empowering organizations to stay one step ahead by surfacing vulnerabilities before they're exploited. As software companies gear up for 2025, those who embrace dynamic security testing and crowd-sourced ethical hacking through bug bounty platforms will be better prepared to protect their systems, their data, and their reputation from the next wave of cyber threats.

Take action now—because prevention is the best defense.

AUTHOR

Jennifer Chaney

Head of Marketing, Intigriti

REQUEST A DEMO

intigriti.com/demo

VISIT THE WEBSITE

intigriti.com

GET IN TOUCH

hello@intigriti.com