Synack

AI EDITION

Synack 2026

State of Vulnerabilities

WHAT 11,000 VULNERABILITIES REVEAL ABOUT THE AI-ERA ATTACK SURFACE

Table of Contents

In 2025 time to exploit and remediation shrunk, signaling a shift to continuous security validation

THE RULES CHANGED IN 2025, AND NOW TIME IS YOUR BIGGEST VULNERABILITY.

This isn't because attackers found new vulnerabilities (spoiler: they always do) but because the time between discovery and exploitation collapsed to a matter of hours. For security teams, that means the traditional model of periodic testing and manual review isn't just inefficient, it's structurally inadequate.

This shift shows up in the data where AI and LLM systems are primary targets and active testing priorities. In fact, Synack customers launched 120% more AI/LLM security missions in 2025 than the year before. That growth shows that organizations are taking AI infrastructure seriously as an attack surface.

Every new AI system introduced into an environment expands the perimeter in ways that static scanning can't adequately map. On top of that, agentic AI systems that can act autonomously across systems also introduce new classes of risk that require human expertise to find and understand. While automated scanning finds known signatures, it can miss logic flaws, misconfigurations, and emergent behaviors.

To understand what that active testing needs to account for, we have to first understand what attackers are capable of. Models like Anthropic's Mythos can compress a reconnaissance timeline from days to hours. Our red team researchers are already studying what tools like Mythos mean for the attack surface to understand how we can stay ahead of AI-enabled adversaries.

The good news is that the organizations in this report are responding. In 2025, Synack customers cut their remediation time nearly in half from an average of 63 days in 2024 to just 38 days. Overall mean time to remediation dropped by approximately 47% across all severity levels. Faster remediation is one output of a more continuous, coverage-focused approach to security. Taken together, these shifts suggest the industry is moving closer to continuous security validation as the working model, with periodic testing increasingly playing a supporting role rather than carrying the program on its own.

The vulnerability data in this report isn't just a record of what happened in 2025. It's a map of where attackers are going next. We hope it helps you get there first.

MARK KUHR
CO-FOUNDER & CTO, SYNACK

BY THE NUMBERS

2025 in Review

47%

AVERAGE REDUCTION IN MTTR ACROSS SYNACK CUSTOMERS

63 → 38

AVERAGE DAYS TO REMEDIATE CRITICAL VULNERABILITIES

37%

OF VULNERABILITIES FOUND WERE CRITICAL OR HIGH-SEVERITY

120%

INCREASE IN AI/LLM MISSION ADOPTION ON THE SYNACK PLATFORM

48,244

PUBLISHED CVE RECORDS INDUSTRY-WIDE IN 2025

11,646

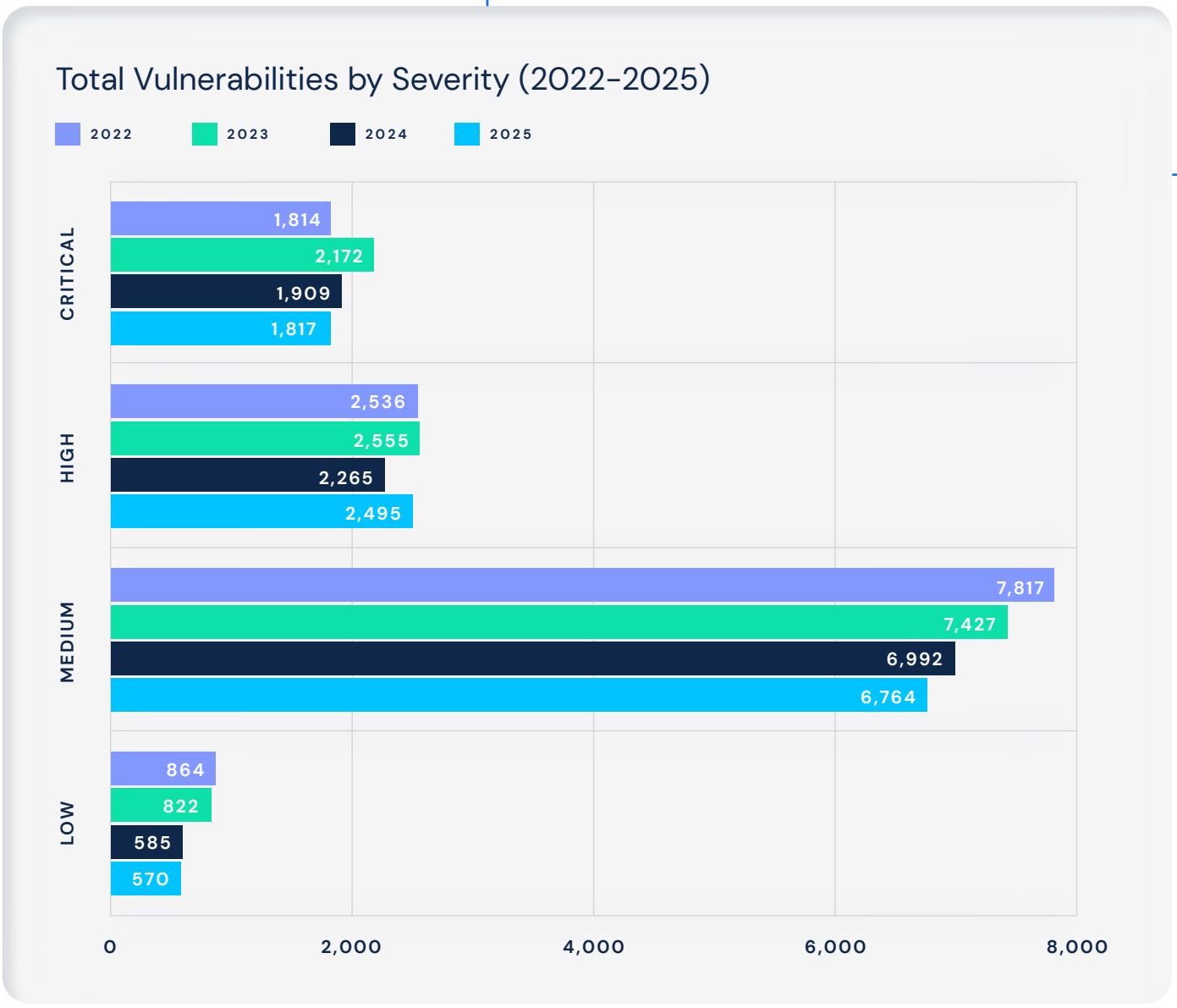
VULNERABILITIES FOUND FOR SYNACK CLIENTS IN 2025

Stable posture in a worsening landscape

IN 2025, MOST VULNERABILITY METRICS TRACKED CLOSELY WITH 2024, WHERE VOLUME AND DENSITY REMAINED STABLE. THAT'S A GOOD SIGN.

Industry-wide, the threat surface expanded. Published CVEs reached 48,244 in 2025, a 20% year-over-year increase (cve.org). Customer programs holding flat against that backdrop means security posture is keeping pace with a faster-moving environment.

The mix tells the rest of the story. Lows and mediums continued to decline while high-severity findings ticked back up. This is a pattern we consistently see in mature programs, which tend to have less noise.



Synack

Meanwhile, AI-enabled adversaries are closing the window between a CVE's public disclosure and the first observed threat actor exploitation.

Looking back on 2025, the year also presented unexpected zero-day vulnerabilities, such as React2Shell [CVE-2025-55182]. This flaw allowed unauthenticated attackers to initiate a malicious HTTP request, ultimately resulting in remote code execution on the server. Synack ran 53 on-demand CVE checks to check for the vulnerability across 14 potentially impacted customers within days of the disclosure. We also checked for this CVE across 348 Synack365 assessments.

When an organization partners with Synack, we work tirelessly to help security teams process and prioritize vulnerability data.

It's critical to our business, but we also want our customers to address systemic vulnerabilities that are recurring in their environments and reduce findings over time. That's why our platform provides strategic insights, such as: which vulnerabilities types occur the most, the time to remediate by class and type of vulnerability, and which assets have the highest and lowest attacker resistance.

SEARCHING ACROSS SYNACK'S VULNERABILITY DATASET, WE IDENTIFIED TRENDS ACROSS ORGANIZATIONS AND INDUSTRIES.

SOME AGE-OLD VULNERABILITIES PERSIST (WE'RE LOOKING AT YOU, XSS) AND SOME INDUSTRIES EXCEL OVER OTHERS AT FAST AND EFFECTIVE REMEDIATION.

Vulnerability volume remains stable, but the stakes are higher

In 2025 the total vulnerability volume remained relatively flat, but **high-severity vulnerabilities increased by 10%** since 2024. At Synack, we prioritize high and critical findings rather than noise from low-severity volume. CVSS is a useful proxy, but it doesn't always represent true risk. We still accept medium and low vulnerabilities because lower-severity findings often chain together or take on different weight once additional context is factored in.

Total Vulnerabilities by Severity in 2024 and 2025

Synack

Old threats, new urgency

What's declining

Cross-Site Scripting (XSS) remains the most frequently found vulnerability, with authorization and permissions as a close second. However, both are declining year over year, which could signal that security programs focused on reducing structural vulnerabilities are working. If your organization has invested in secure coding training and consistent code review, these are the categories where you're likely seeing results.

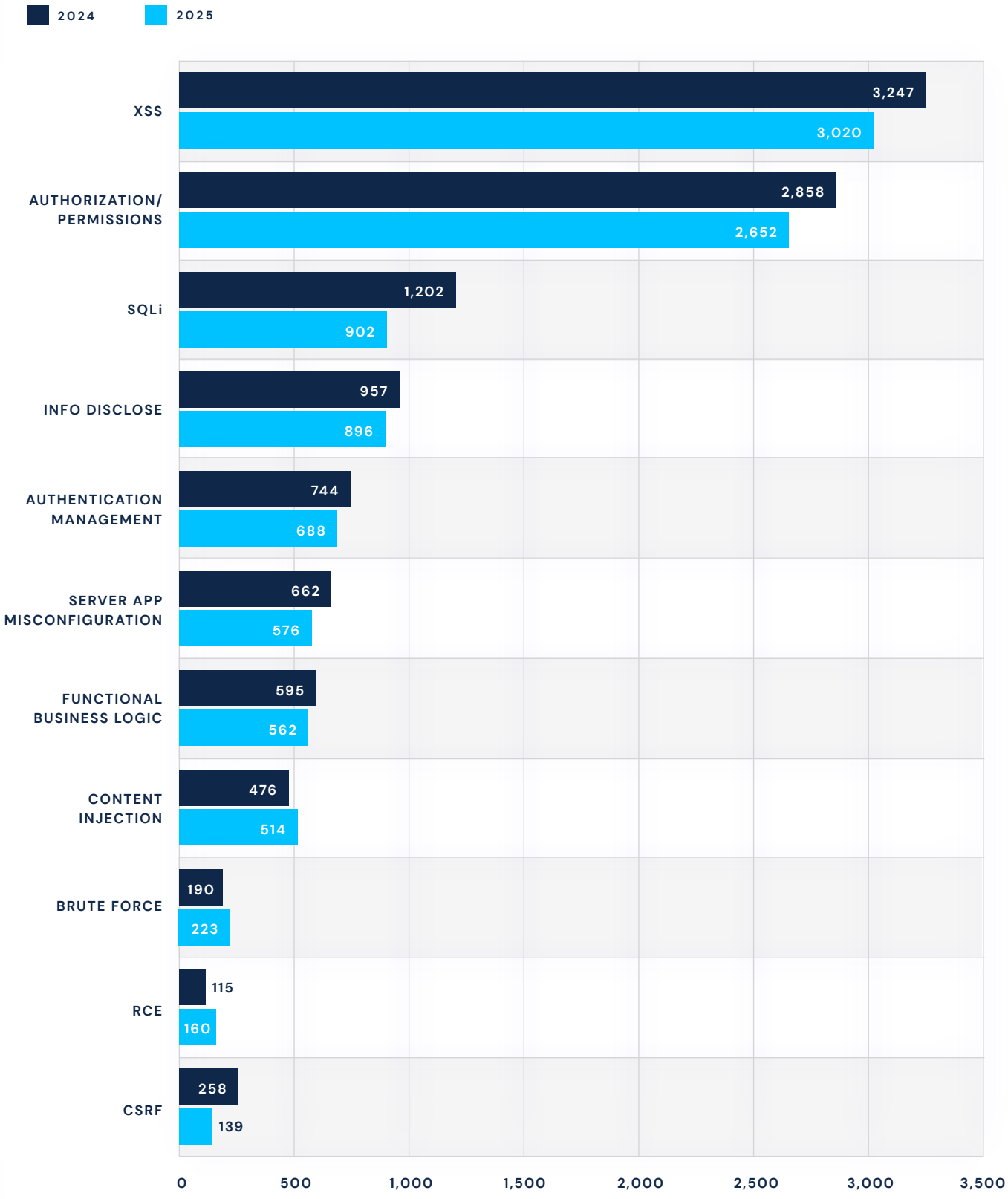
What's growing

THREE CATEGORIES SHOWED GROWTH THROUGHOUT 2025:

1. CONTENT INJECTION: 8% YOY INCREASE
2. BRUTE FORCE ATTACKS: 17.4% YOY INCREASE
3. REMOTE CODE EXECUTION (RCE): 39% YOY INCREASE

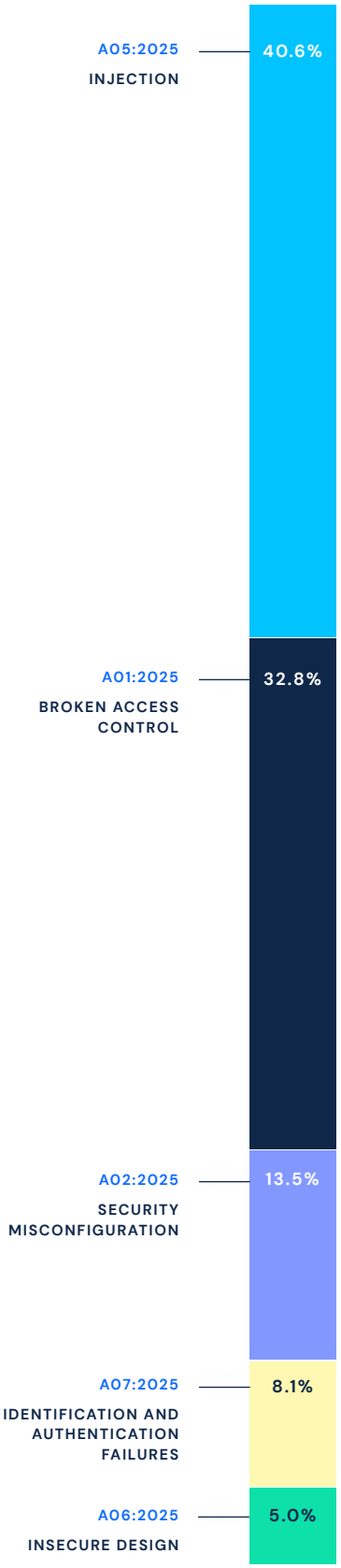
These reflect a pivot by threat actors toward social engineering, identity-based exploitation, and supply chain vulnerabilities. It also signals increased targeting of authentication boundaries—consistent with AI-enabled adversaries systematically testing access controls at scale.

Total Vulnerabilities by Type in 2024 and 2025



Synack

SYNACK 2025 FINDINGS DISTRIBUTED ACROSS OWASP TOP 10:2025 CATEGORIES



THE VULNERABILITY LANDSCAPE

Where Synack findings align with the OWASP Top 10

This chart shows how Synack's 2025 findings distribute across the OWASP Top 10:2025 categories, which represent the industry's standard for benchmarking application security risk. Injection and broken access control consistently account for the largest share of what we find.

OWASP TOP 10 CATEGORIES

- A01:2025 - Broken Access Control
- A02:2025 - Security Misconfiguration
- A03:2025 - Software Supply Chain Failures
- A04:2025 - Cryptographic Failures
- A05:2025 - Injection
- A06:2025 - Insecure Design
- A07:2025 - Authentication Failures
- A08:2025 - Software or Data Integrity Failures
- A09:2025 - Security Logging and Alerting Failures
- A10:2025 - Mishandling of Exceptional Conditions

THE AI ATTACK SURFACE

OWASP Top 10 for LLMs

The 2025 update to the OWASP LLM Top 10 added categories that reflect how AI architectures have evolved. For organizations running LLM-integrated applications, the following three are worth considering:

- Excessive Agency (LLM06) shows the risk of agentic AI systems acting beyond their intended scope, which is particularly relevant as AI agents move into production workflows.
- System Prompt Leakage (LLM07) was added based on real-world exploits because system prompts are not as isolated as developers assume.
- Vector and Embedding Weaknesses (LLM08) addresses the RAG pattern specifically, now standard in enterprise AI deployments.

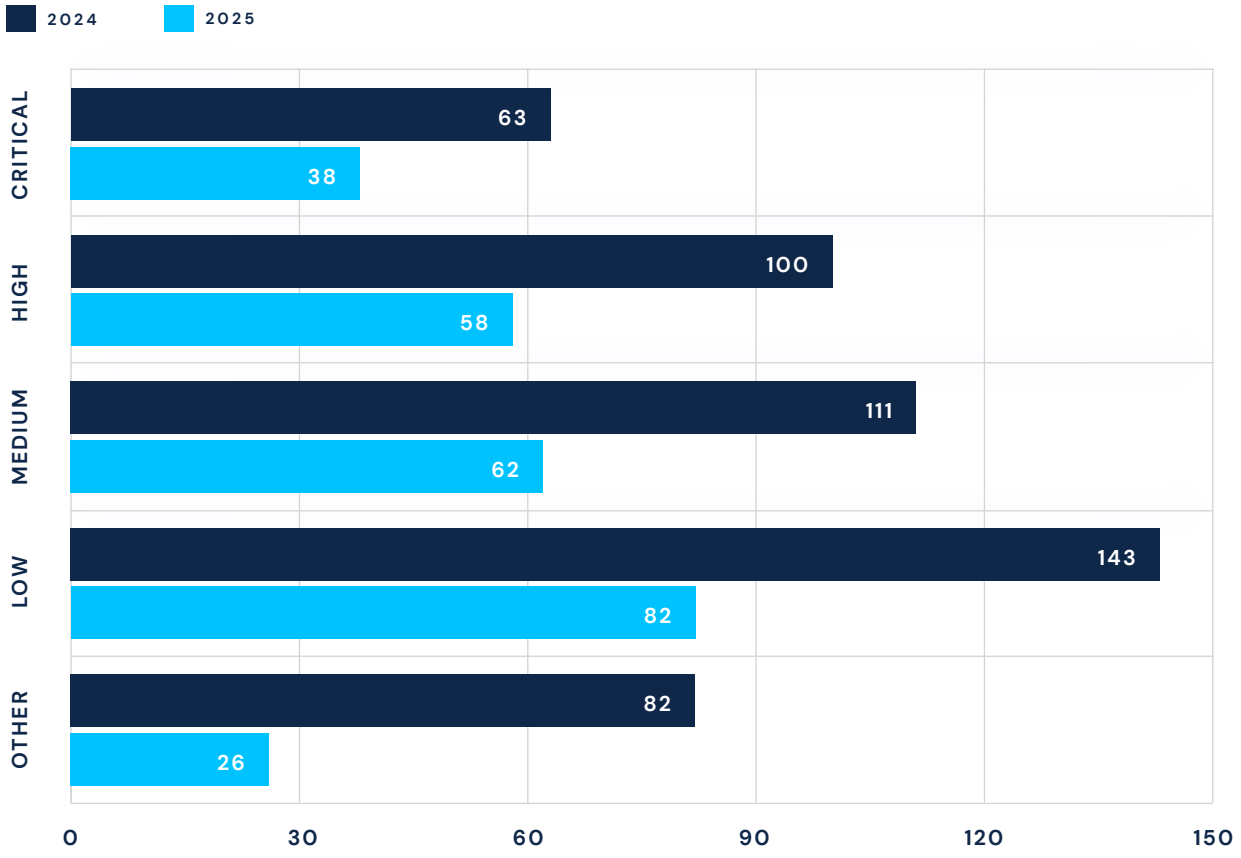
Ultimately, AI infrastructure doesn't replace traditional attack surfaces, it extends them. In fact, OWASP LLM05 (Improper Output Handling) explicitly notes that LLM-generated SQL queries without proper parameterization lead to SQL injection, which is the same category still topping our vulnerabilities charts.

Synack

Synack customers cut MTTR for critical and high vulnerabilities nearly in half

Despite significant headwinds, Synack clients reduced their mean time to remediate (MTTR) high vulnerabilities by 42 days from 2024 to 2025, while critical vulnerabilities were remediated in 25 fewer days. **On average Synack customers reduced their MTTR by 47%.**

Average Number of Days to Remediate Vulnerabilities by Severity in 2024 and 2025



WHAT'S DRIVING FASTER REMEDIATION?

Two forces are likely driving faster remediation. First, AI-enabled attackers are shortening Average Time to Exploit (TTE) and security teams are feeling pressure to close critical windows faster. Second, PTaaS platforms like Synack enable teams to correlate vulnerability data across assets and business units, improving prioritization and workflow efficiency.

Industry Overviews

RETAIL

FINANCIAL SERVICES

GOVERNMENT

TECHNOLOGY

MANUFACTURING

INDUSTRY COMPARISON

The industry sections on the following pages cover retail, financial services, government, technology, and manufacturing, which is just a sampling of the industries Synack supports.

FOR INFORMATION ON HOW YOUR SECTOR COMPARES, VISIT SYNACK.COM.

The exposed attack surface in 2025

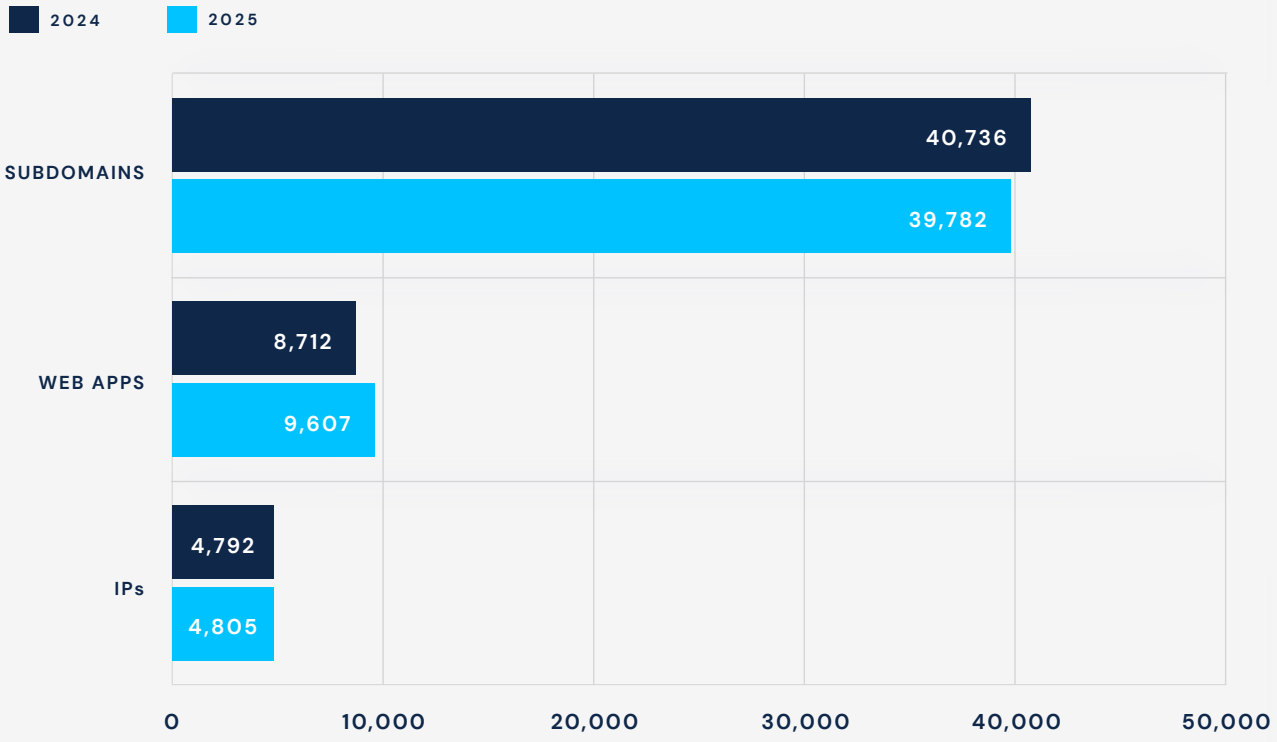
MAPPING IT ASSETS AND INFRASTRUCTURE IS ONE OF THE BIGGEST CHALLENGES FACING SECURITY TEAMS—AND THE TARGET KEEPS MOVING.

Across the five industries in this report, average total assets grew or held steady in 2025, with the exception of retail. Manufacturing saw the sharpest increase at 21%, from 2,053 to 2,486 assets per organization.

Average Total Assets by Industry in 2024 and 2025

Synack

Average Total Assets by Type in 2024 and 2025



Looking across asset types, subdomains remain the dominant category by volume, averaging roughly 40,000 per organization. Web applications grew modestly year over year, consistent with the faster development cycles driven by AI coding assistants.

Closing the coverage gap with continuous pentesting

OUR RESEARCH WITH OMDIA SHOWS THAT ON AVERAGE, ORGANIZATIONS ARE ONLY TESTING ABOUT 32% OF THEIR ATTACK SURFACE.

With average subdomain counts near 40,000 and web application counts growing, that coverage gap translates to thousands of untested assets per organization—each one a potential blind spot for AI-driven adversaries.

Synack

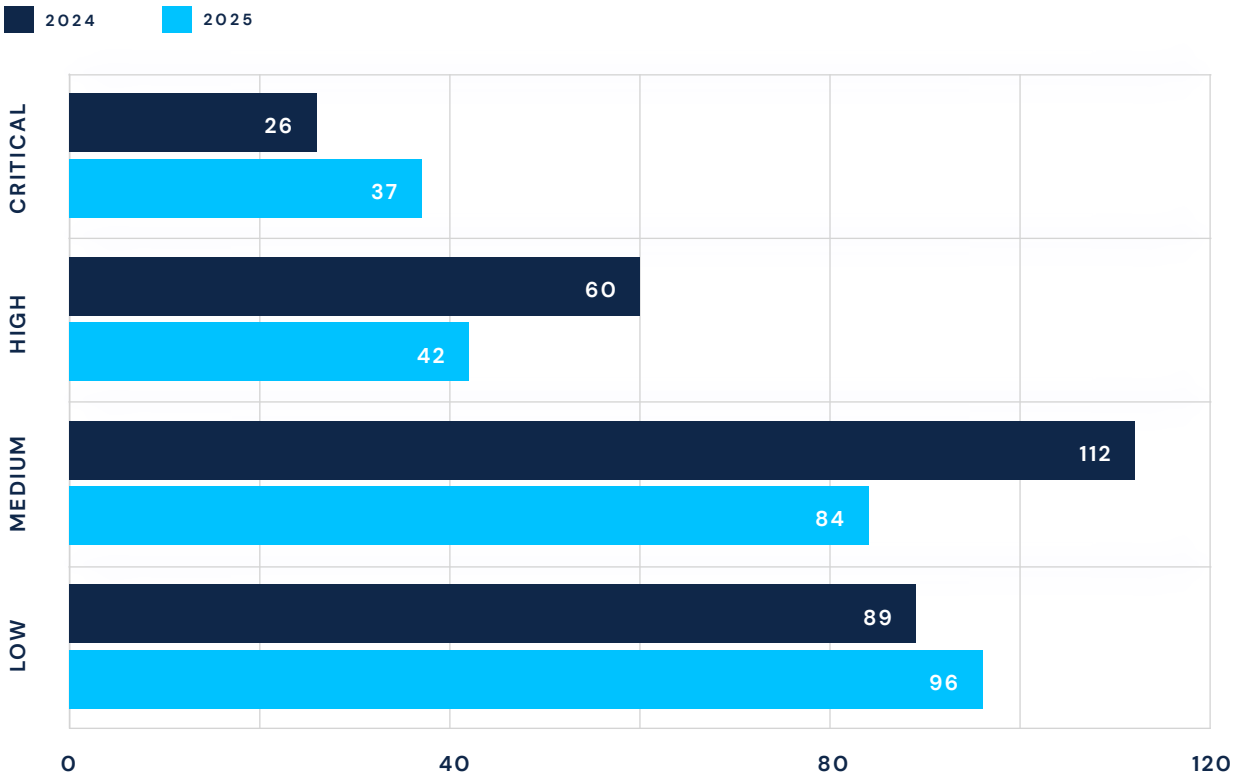
INDUSTRY OVERVIEW

Retail

RETAIL ORGANIZATIONS CUT HIGH-SEVERITY REMEDIATION TIME BY 18 DAYS IN 2025— FROM AN AVERAGE OF 60 TO 42 DAYS.

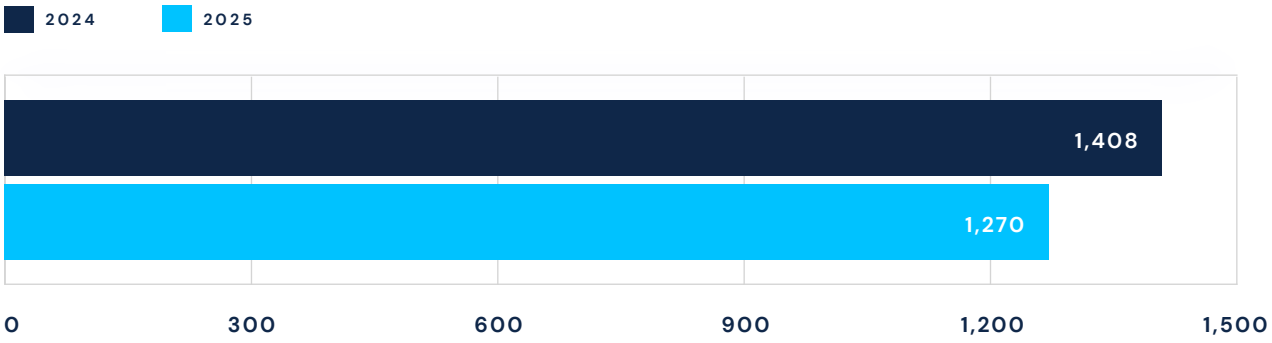
Critical vulnerability remediation extended somewhat, from 26 to 37 days, reflecting the growing complexity of the highest-severity findings as attackers increasingly target harder-to-exploit entry points in consumer-facing infrastructure.

Average Number of Days to Remediate Vulnerabilities by Severity for Retail Clients in 2024 and 2025



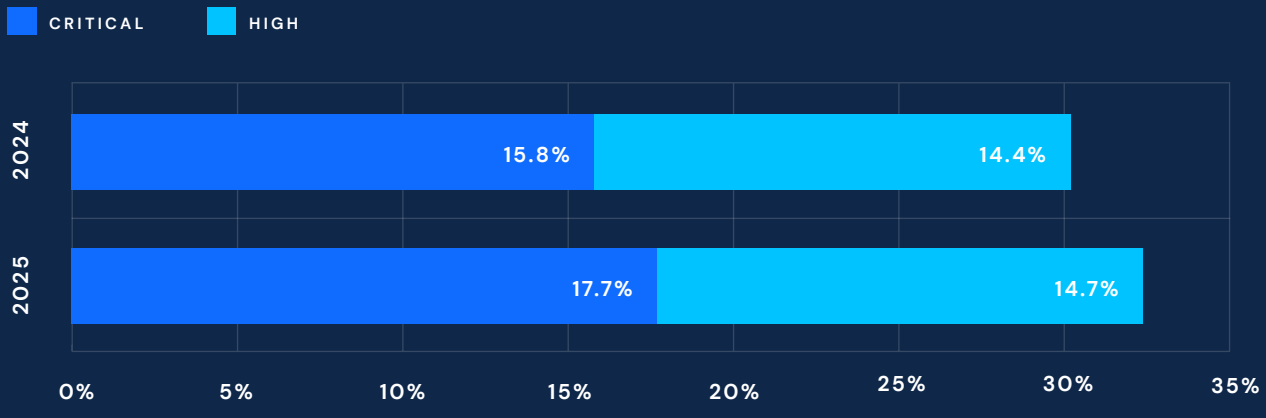
Synack

Total Vulnerabilities for Retail Clients in 2024 and 2025



In total, the retail customers that Synack supports identified 1,270 total vulnerabilities in 2025—a 10% decline from 1,408 the prior year.

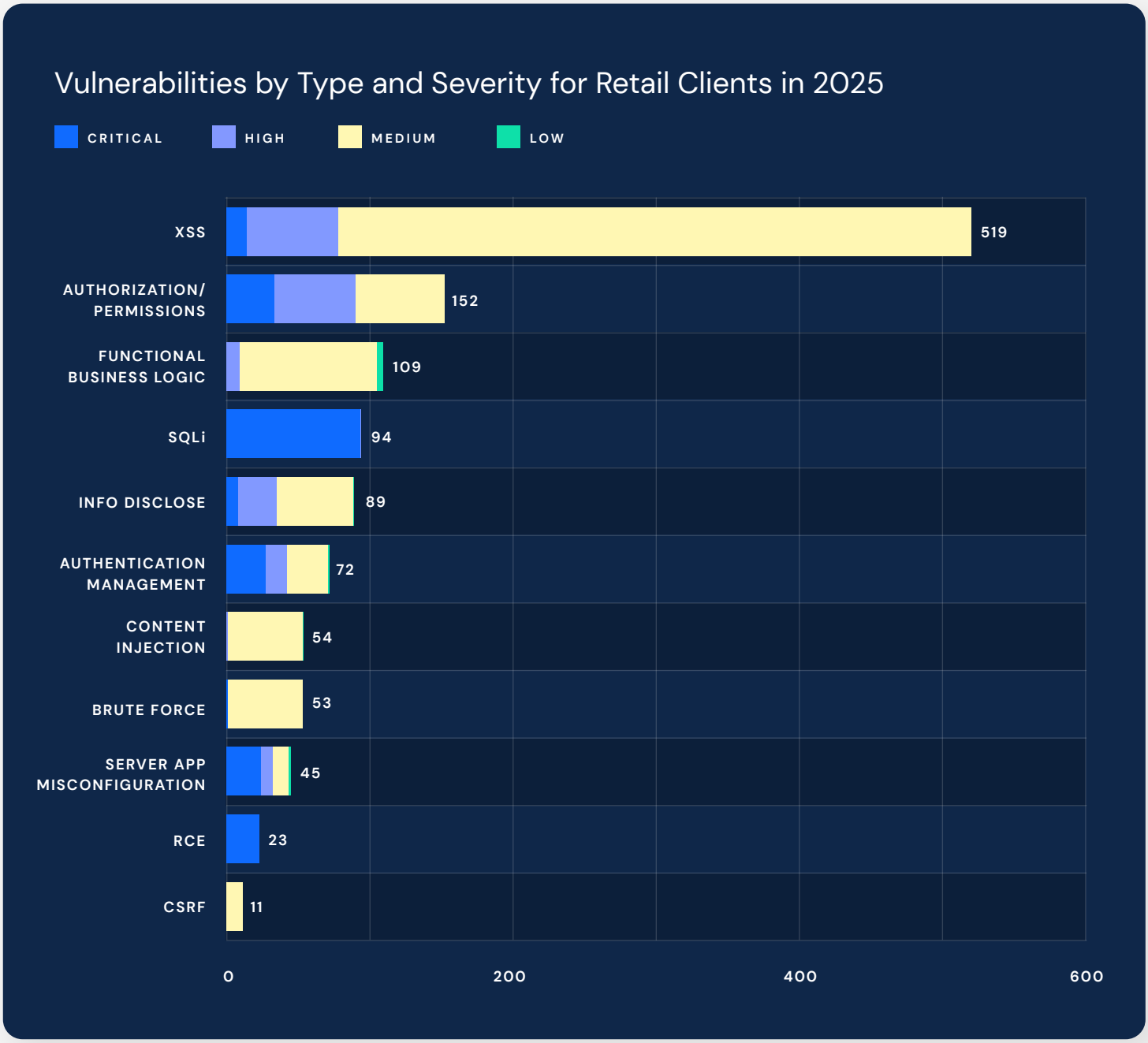
Percentage of Critical and High Vulnerabilities for Retail Clients in 2024 and 2025



Despite the volume drop, the share of critical and high findings climbed from 30.2% to 32.4%. Fewer findings at higher severity means the remaining vulnerabilities carry greater exploitation risk. For retail security teams navigating consumer data protection and PCI compliance obligations, the severity shift warrants attention.

XSS REMAINED THE DOMINANT FINDING CATEGORY, WITH THE LARGEST CLUSTERS IN MEDIUM AND HIGH SEVERITY.

SQL injection was the top critical finding with 93 critical-severity instances, illustrating a persistent gap in retail's complex e-commerce and payment processing environments. Brute force attacks and content injection both appeared at meaningful volume, consistent with the industry's exposure to high-traffic consumer-facing authentication systems.



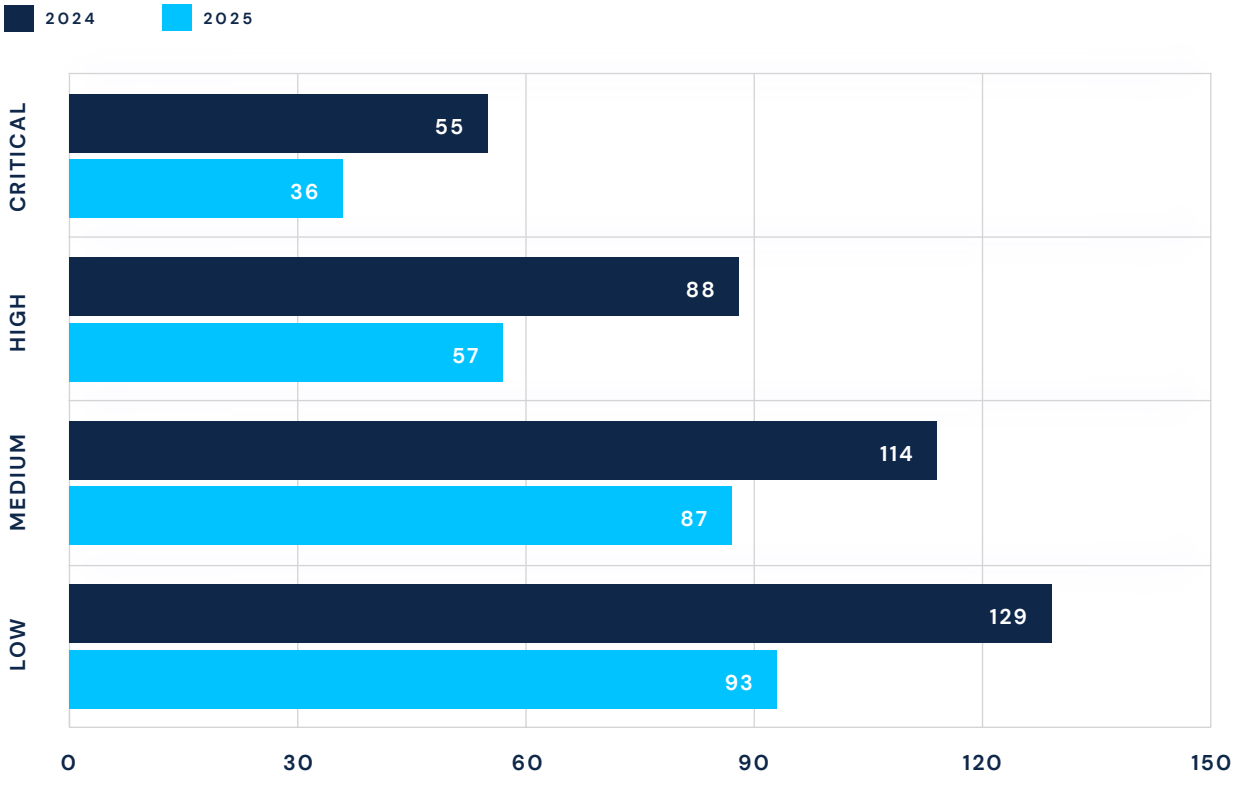
INDUSTRY OVERVIEW

Financial Services

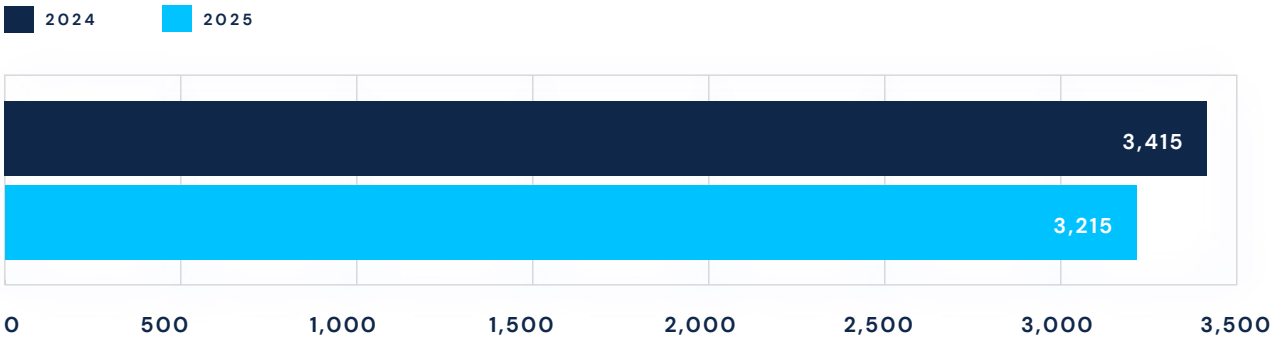
FINANCIAL SERVICES ORGANIZATIONS DELIVERED ONE OF THE STRONGEST REMEDIATION PERFORMANCES OF ANY SECTOR IN 2025.

Average time to remediate critical vulnerabilities fell 19 days—from 55 to 36 days—while high-severity remediation improved by 30 days, from 88 to 57 days. In a sector shaped by regulatory mandates and the high cost of breach events, this pace of improvement reflects meaningful investment in security operations.

Average Number of Days to Remediate Vulnerabilities by Severity for Financial Services Clients in 2024 and 2025

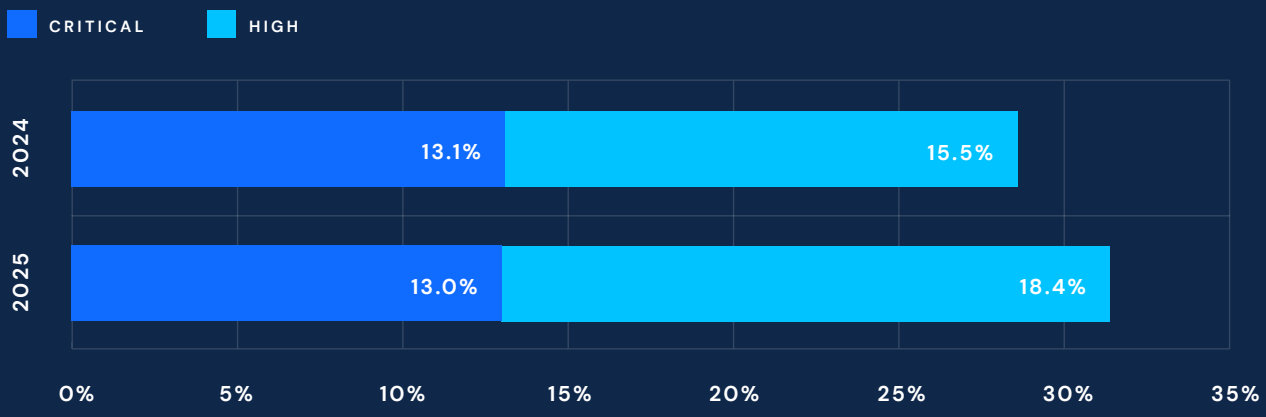


Total Vulnerabilities for Financial Services Clients in 2024 and 2025



Synack's financial services customers surfaced 3,215 total vulnerabilities in 2025, which is a modest 6% decrease from 3,415 in 2024.

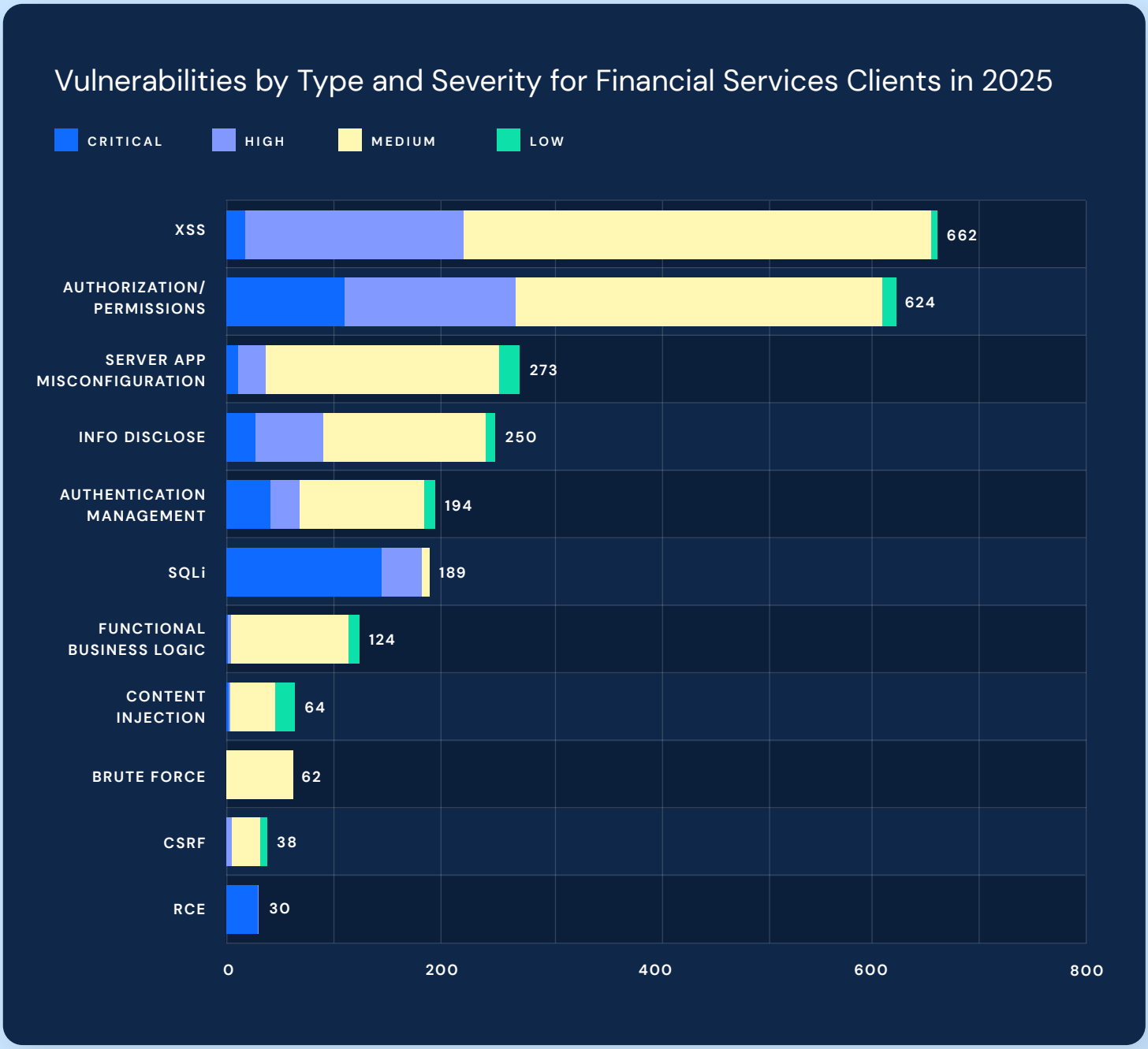
Percentage of Critical and High Vulnerabilities for Financial Services Clients in 2024 and 2025



The severity mix intensified, however, with critical and high findings climbing from 28.6% to 31.4% of total volume.

AUTHORIZATION AND PERMISSIONS VULNERABILITIES LED THE CATEGORY BREAKDOWN FOR FINANCIAL SERVICES, FOLLOWED BY XSS ACROSS MEDIUM AND HIGH SEVERITY BANDS.

SQL injection produced 144 critical-severity instances. Remote code execution appeared at 29 critical instances, highlighting continued exposure of API layers and backend services to high-impact exploits.



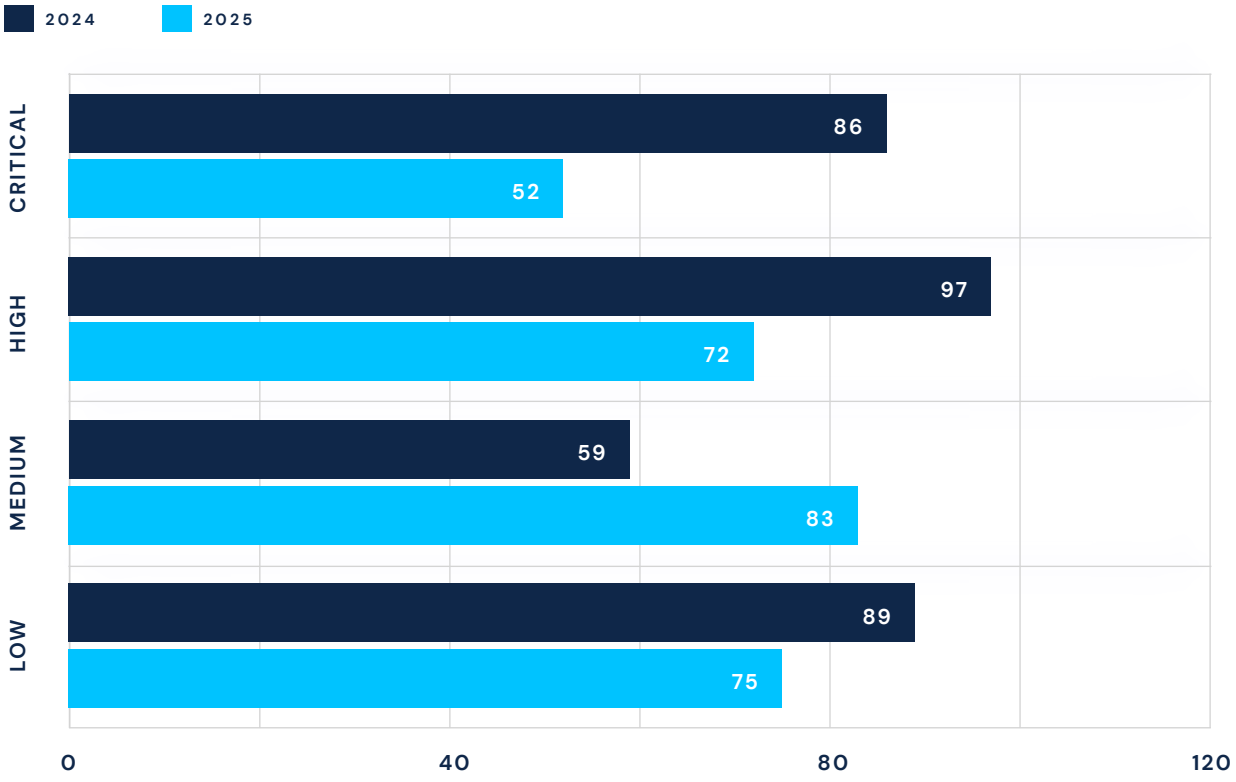
INDUSTRY OVERVIEW

Government

GOVERNMENT AGENCIES CUT THE AVERAGE TIME TO REMEDIATE CRITICAL VULNERABILITIES BY 34 DAYS—FROM 86 TO 52—AND HIGH-SEVERITY FINDINGS BY 25, FROM 97 TO 72 DAYS.

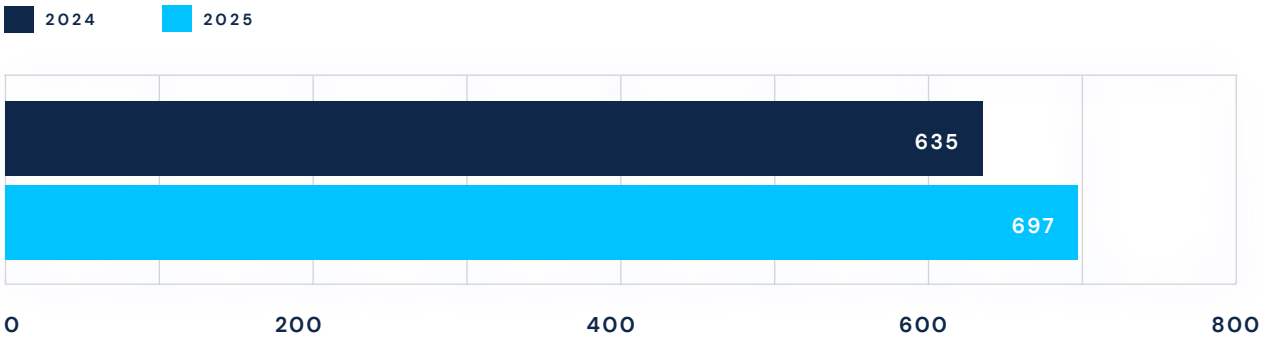
These improvements reflect both the continued maturation of federal security operations and the pressure of compliance mandates requiring faster, more comprehensive vulnerability response.

Average Number of Days to Remediate Vulnerabilities by Severity for Government Clients in 2024 and 2025



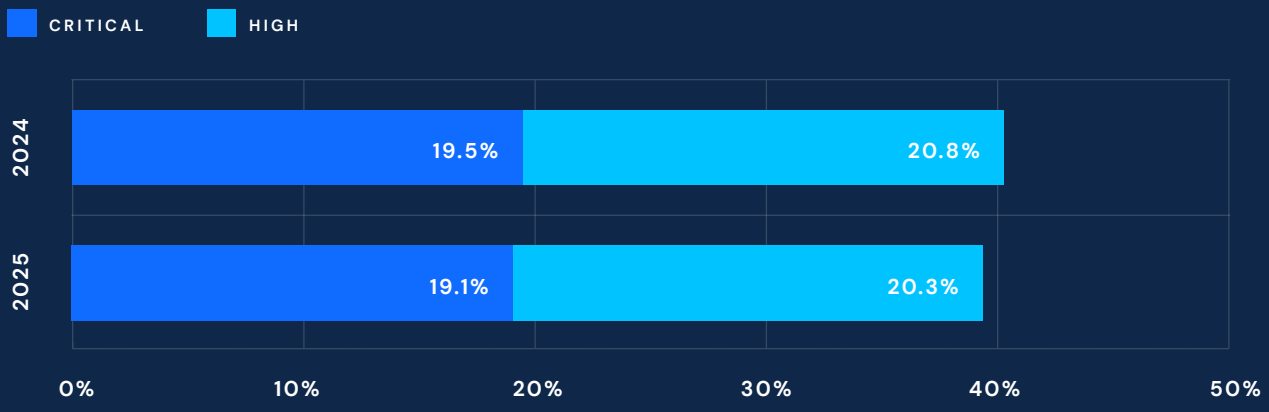
INDUSTRY: GOVERNMENT

Total Vulnerabilities for Government Clients in 2024 and 2025



Synack's public sector customers surfaced 697 total vulnerabilities in 2025—a 10% increase from 635 the prior year.

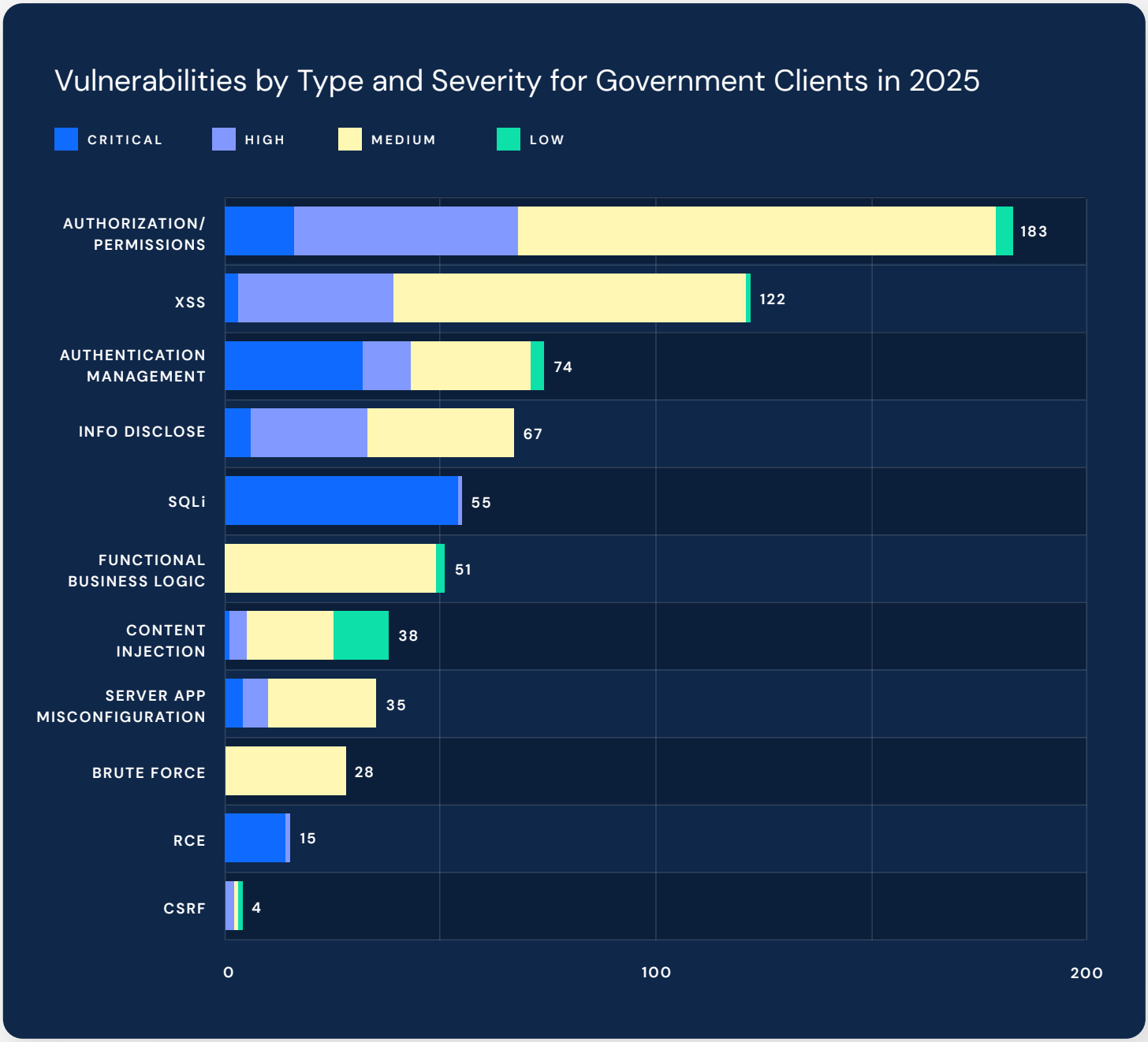
Percentage of Critical and High Vulnerabilities for Government Clients in 2024 and 2025



Critical and high findings represented 39.4% of total volume, a slight improvement from 40.3% in 2024. The volume increase reflects expanded attack surface testing as agencies bring more assets into scope. Staying near 40% critical and high means government environments remain a high-value target—but the remediation data shows agencies are responding with greater speed than before.

AUTHORIZATION AND PERMISSIONS VULNERABILITIES DOMINATED THE CATEGORY BREAKDOWN, WITH 111 MEDIUM AND 52 HIGH-SEVERITY INSTANCES REFLECTING THE INHERENT COMPLEXITY OF ACCESS CONTROL IN MULTI-AGENCY IT ENVIRONMENTS.

Authentication management appeared at 32 critical-severity instances, underscoring the risk profile of government identity systems as persistent targets for credential-based attacks. Remote code execution critical findings (14 instances) round out a sector navigating significant digital modernization risk.



Synack

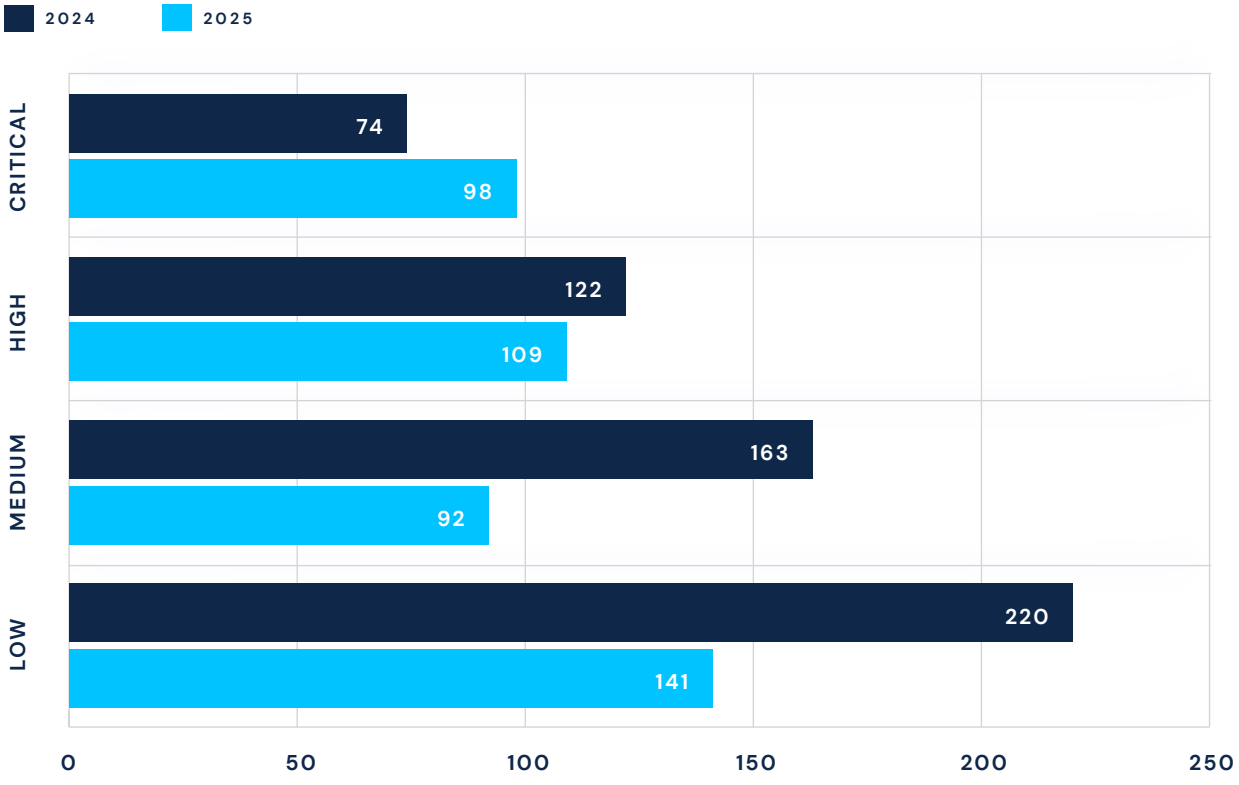
INDUSTRY OVERVIEW

Technology

TECHNOLOGY ORGANIZATIONS SAW MIXED REMEDIATION PERFORMANCE IN 2025.

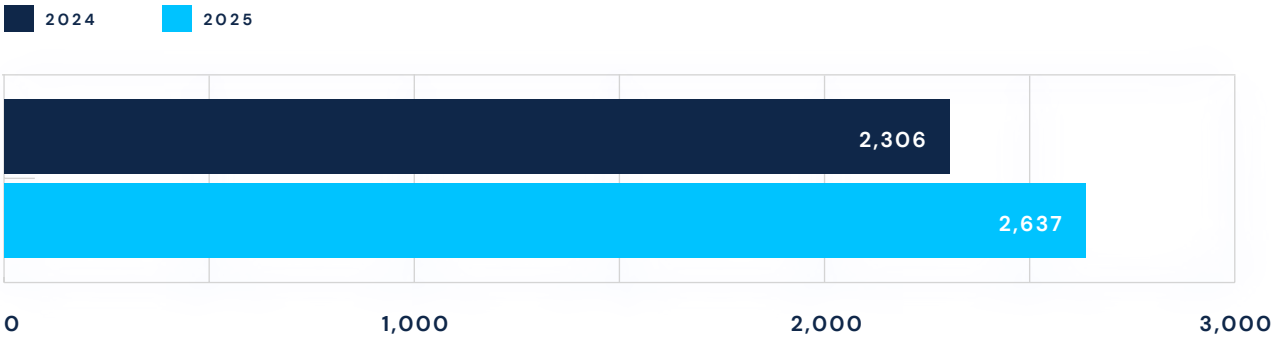
High-severity findings improved, with average remediation time falling from 122 to 109 days. At the same time, critical vulnerability remediation extended from 74 to 98 days, which could signal that the critical findings being surfaced are increasingly complex, requiring deeper architectural remediation.

Average Number of Days to Remediate Vulnerabilities by Severity for Technology Clients in 2024 and 2025



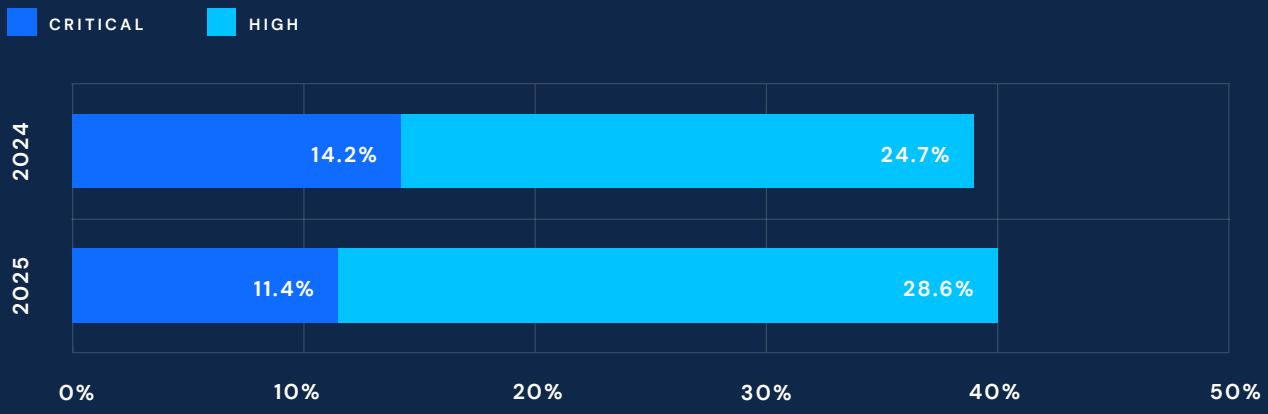
Synack

Total Vulnerabilities for Technology Clients in 2024 and 2025



Synack's technology customers registered 2,637 total vulnerabilities in 2025—a 14% increase from 2,306 in 2024.

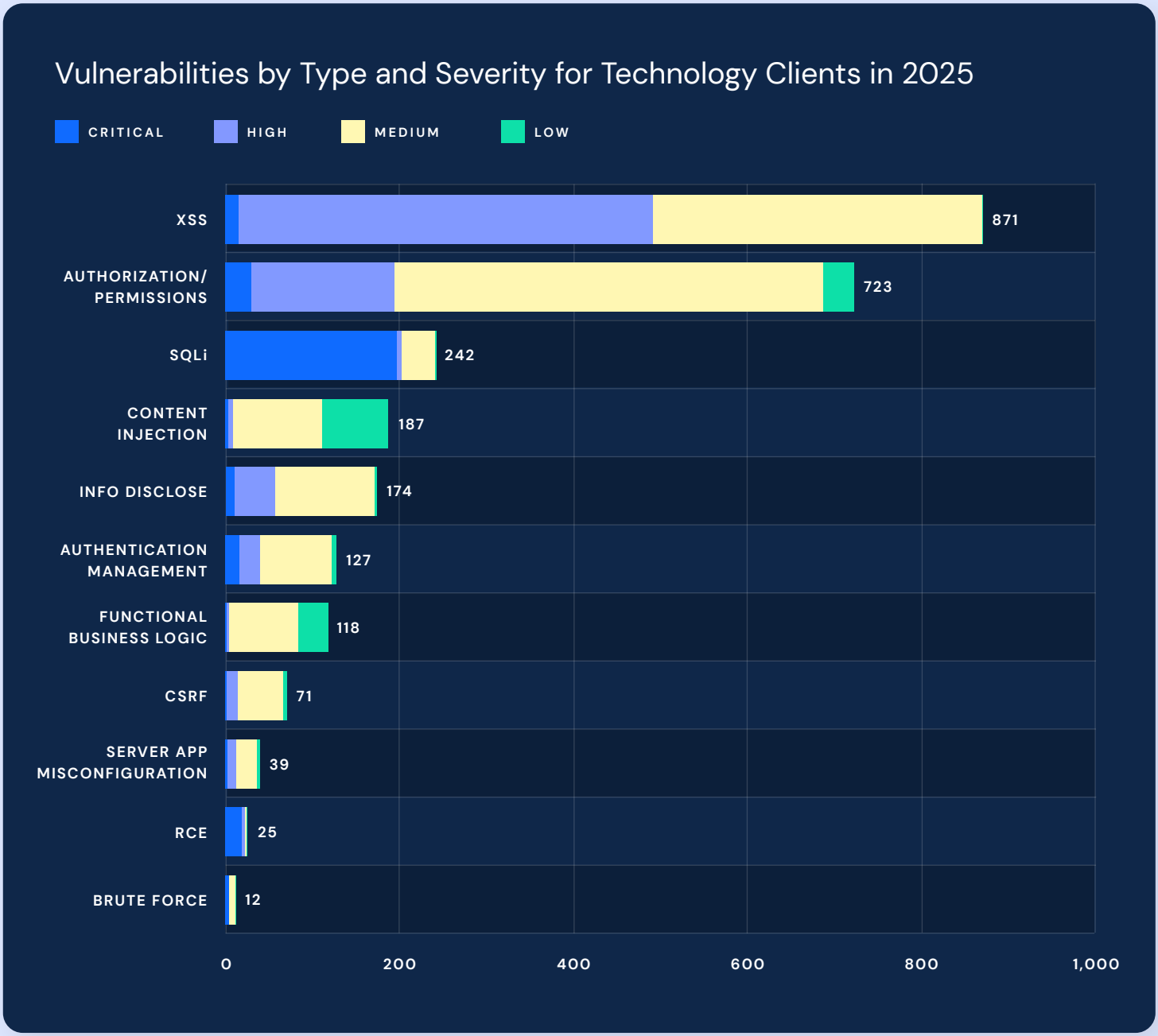
Percentage of Critical and High Vulnerabilities for Technology Clients in 2024 and 2025



Critical and high findings represented 40.0% of total volume, up from 38.9% the year prior. Volume growth in this sector often reflects expanding attack surfaces: more software, more APIs, more AI integration points, and the severity data shows that the findings being surfaced are increasingly impactful.

XSS IN TECHNOLOGY ORGANIZATIONS PRODUCED THE HIGHEST CONCENTRATION OF HIGH-SEVERITY FINDINGS OF ANY SECTOR COVERED IN THIS REPORT, WITH 476 HIGH-SEVERITY INSTANCES.

Authorization and permissions vulnerabilities were the second-most common category overall. SQL injection generated 197 critical-severity instances—the highest SQL injection critical volume of any sector in this report, consistent with the pace of software development and the complexity of modern API ecosystems. Content injection appeared at 103 medium-severity instances, pointing to emerging risks in AI-integrated frontend applications that process unstructured external inputs.



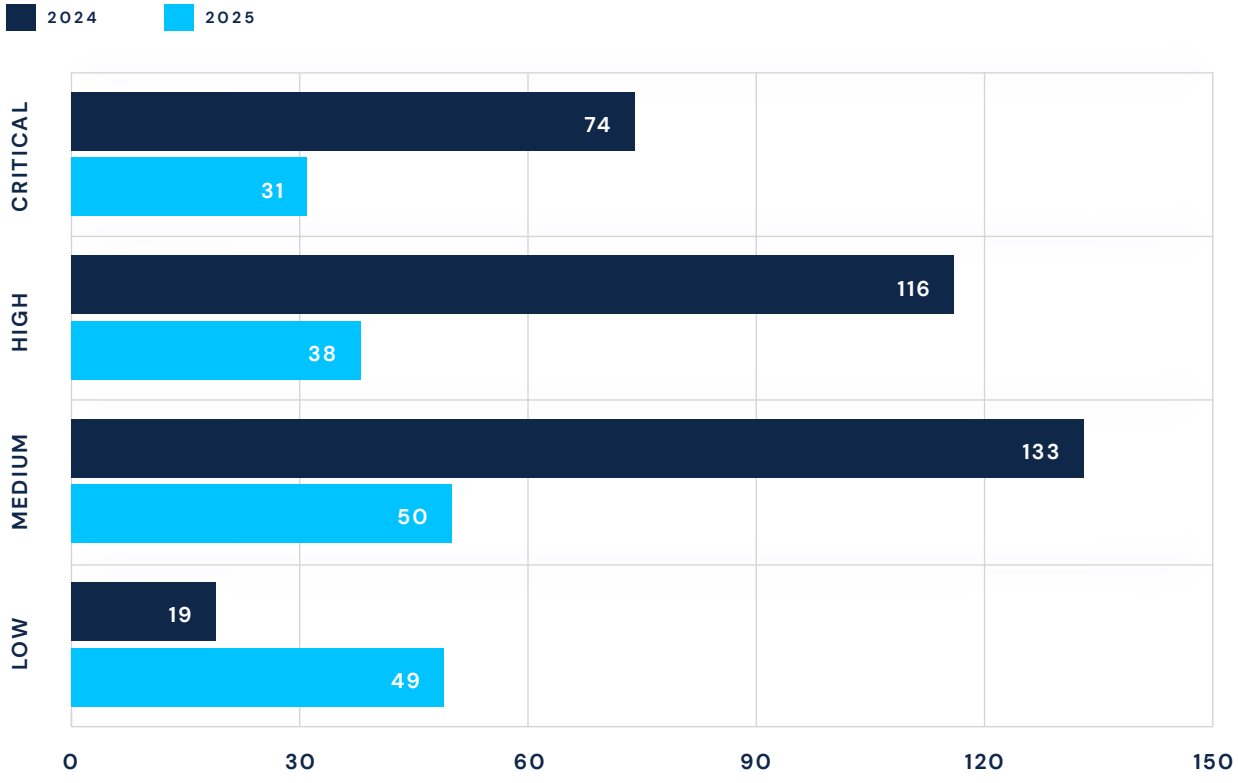
INDUSTRY OVERVIEW

Manufacturing

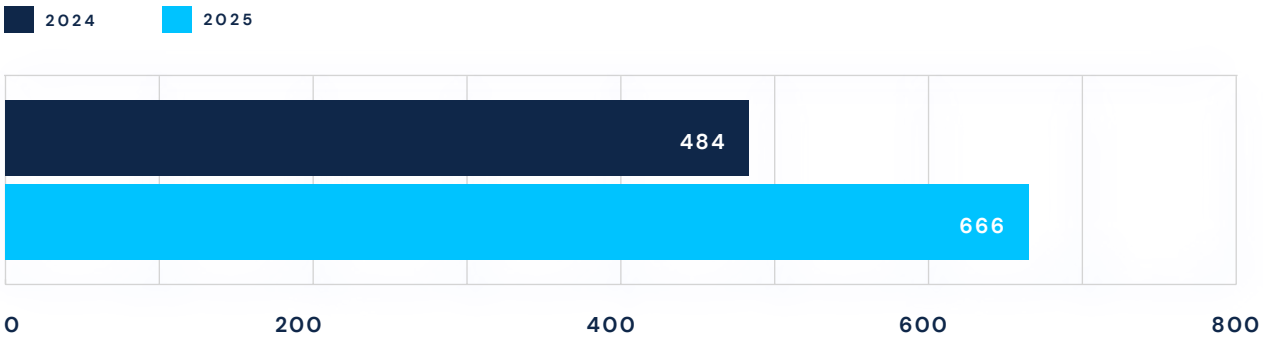
MANUFACTURING DELIVERED THE MOST DRAMATIC REMEDIATION IMPROVEMENT OF ANY SECTOR IN 2025, CUTTING THE AVERAGE TIME TO REMEDIATE CRITICAL VULNERABILITIES BY 43 DAYS, AND HIGH-SEVERITY FINDINGS BY 78 DAYS.

At a time when operational technology and IT convergence is accelerating, these gains signal that manufacturing security teams are treating software vulnerabilities with the same urgency as production uptime.

Average Number of Days to Remediate Vulnerabilities by Severity for Manufacturing Clients in 2024 and 2025

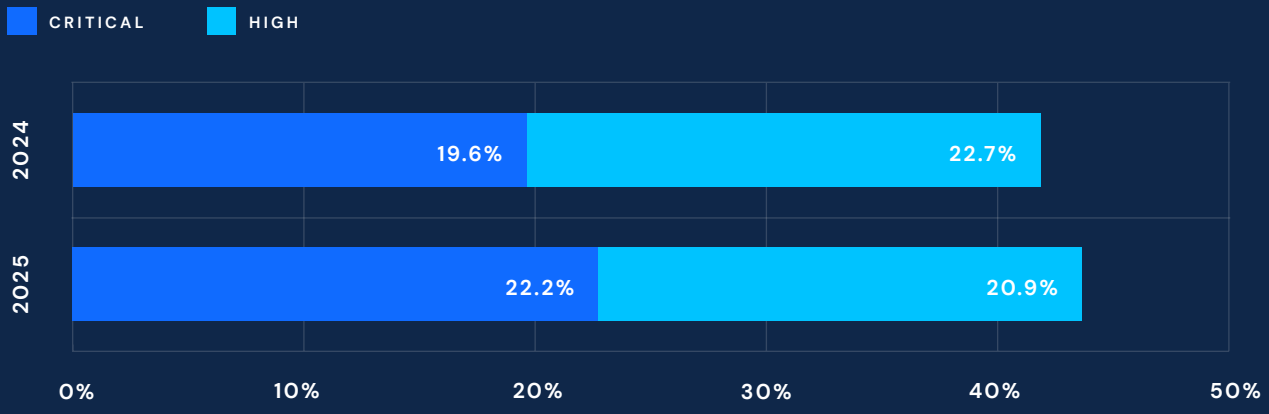


Total Vulnerabilities for Manufacturing Clients in 2024 and 2025



Manufacturing organizations surfaced 666 total vulnerabilities in 2025, which is a 37% increase from 484 in 2024.

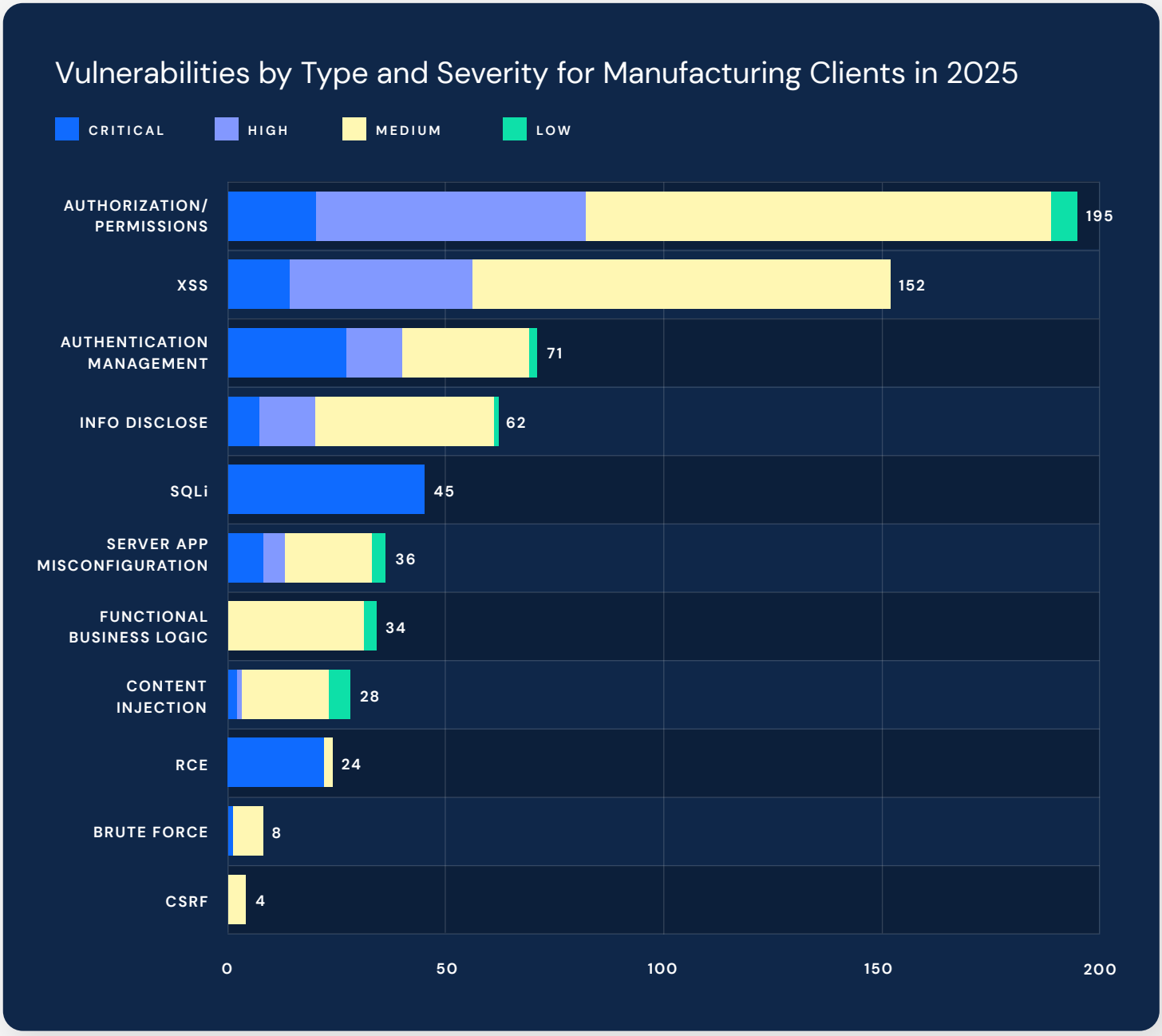
Percentage of Critical and High Vulnerabilities for Manufacturing Clients in 2024 and 2025



Critical and high findings represented 43.1% of total volume, up slightly from 42.3% the prior year. Volume growth alongside a high critical and high severity share makes manufacturing one of the more closely watched sectors from a risk perspective. The remediation data is the counterbalance: organizations in this sector are finding more but closing gaps faster.

AUTHORIZATION AND PERMISSIONS VULNERABILITIES LED THE CATEGORY BREAKDOWN FOR MANUFACTURING, FOLLOWED BY XSS.

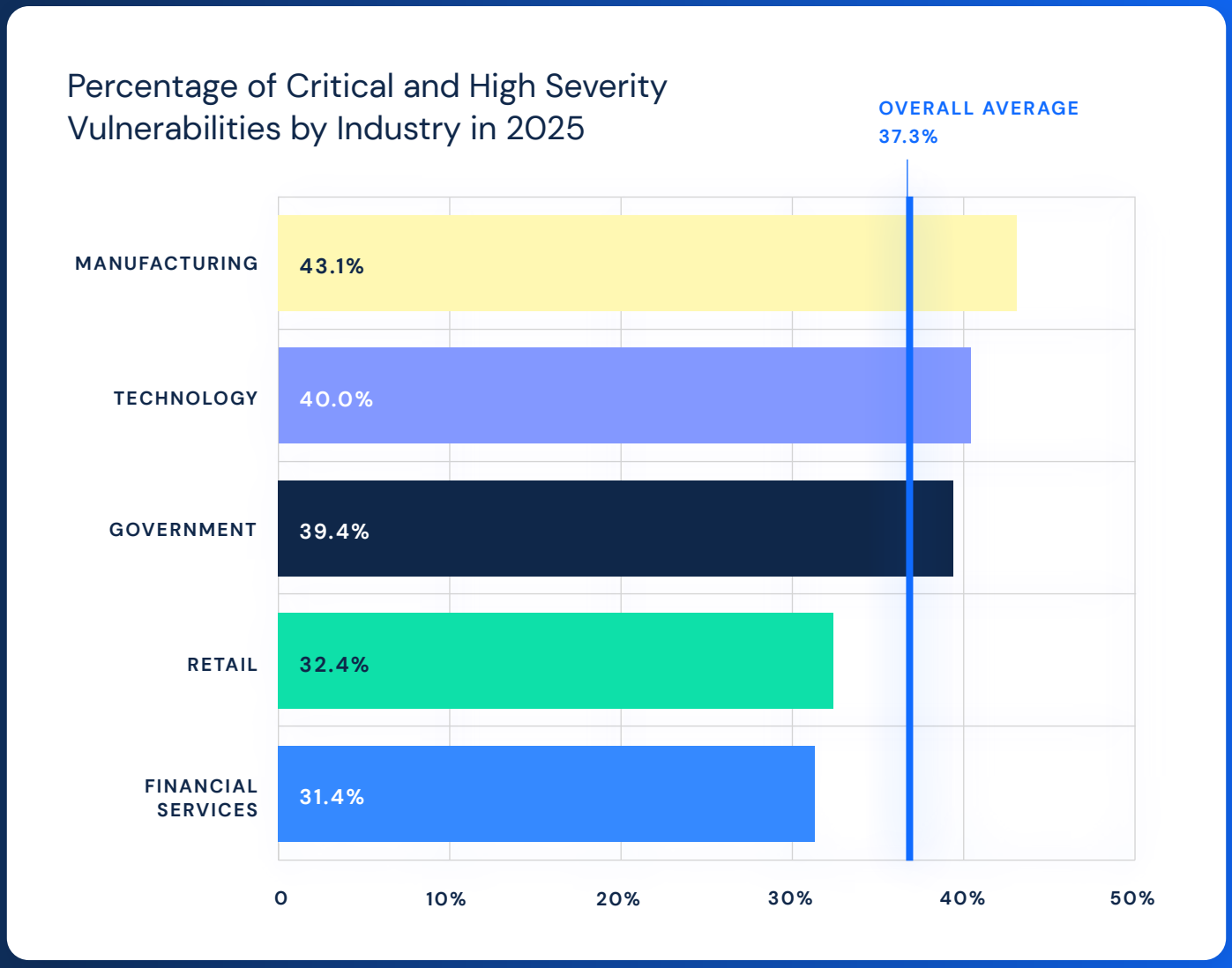
SQL injection produced 45 critical-severity instances, while remote code execution critical findings reached 22. This is among the higher RCE volumes of the sectors covered in this report. Authentication management critical findings (27 instances) reflect the identity risks that accompany rapid OT/IT integration. As manufacturing environments add more connected systems and IP-addressable devices, authentication and authorization controls remain a persistent pressure point.



HOW INDUSTRIES COMPARE

Critical and high vulnerability density

In 2025, 37% of vulnerabilities found across the Synack platform in these industries were critical or high severity. Manufacturing (43.1%) and technology (40.0%) carried the highest share among the five sectors highlighted in this report, followed closely by government (39.4%). Retail (32.4%) and financial services (31.4%) fell below the overall average.



Synack

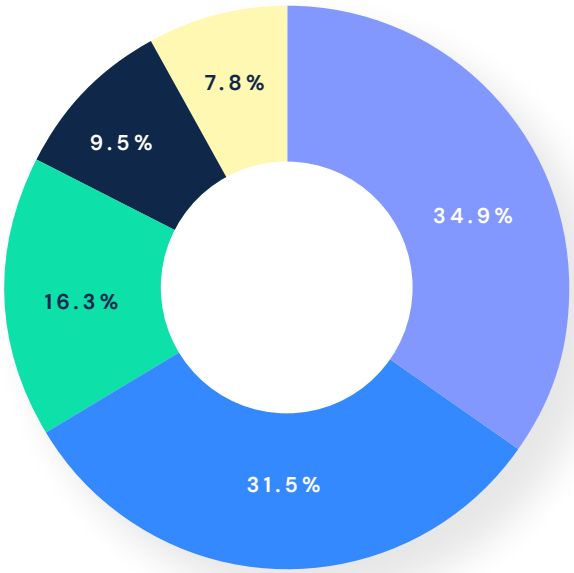
SQLi and RCE by industry

SQL injections and RCE vulnerabilities remain among the most impactful findings in any pentest engagement. The breakdown below shows each industry's contribution to the overall pool of critical and high-severity SQL injection and RCE findings.

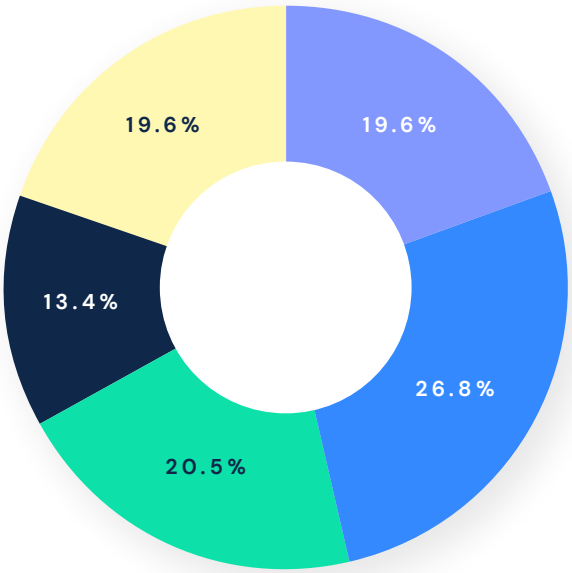
Critical and High Severity SQLi and RCE Findings by Industry in 2025

TECHNOLOGY FINANCIAL SERVICES RETAIL GOVERNMENT MANUFACTURING

SQLi VULNERABILITIES BY INDUSTRY



RCE VULNERABILITIES BY INDUSTRY



In 2025, the technology sector accounted for the largest share of SQL injection critical findings among the five industries at 34.9%, followed by financial services at 31.5%. Retail (16.3%), government (9.5%), and manufacturing (7.8%) accounted for the remainder. For RCE critical findings, the distribution was more even: financial services (26.8%), retail (20.5%), technology (19.6%), manufacturing (19.6%), and government (13.4%).

Synack

THE AI THREAT MULTIPLIER

Why stable vulnerability volume is a warning

Stable vulnerability volume is sometimes read as a positive signal, however, the data tells a broader story. An unchanged finding rate alongside a 20% annual increase in published CVEs and narrowing average time-to-exploit means the effective risk exposure is growing, even when the vulnerability count holds steady. The variables that determine actual risk aren't just how many vulnerabilities exist, but how quickly they can be found and exploited by an adversary operating with increasingly capable tools.

The combination of AI-driven tools and an exposed attack surface is creating a narrowing window for defenders. Models like Anthropic's Mythos are demonstrating that the timeline from exploit discovery to exploitation is now a matter of days. Using these kinds of tools, attackers are finding the forgotten legacy systems and chained exploit paths that human attackers would have missed.

The case for scaling pentesting

The answer to AI-enabled adversaries is broader coverage of the attack surface at higher frequency. As AI tools lower the cost of attack exploration, defenders need to match that scale. Pentesting needs to move from periodic to continuous, from sampled to comprehensive.

This is why the combination of the (Sara) and the Synack Red Team (SRT) creates a uniquely powerful offering: the scalability of agentic AI testing with the depth and creativity of vetted human researchers, applied continuously across the entire attack surface.

Meet Sara, Synack's AI pentesting solution

WITH STABLE VULNERABILITY VOLUME, FASTER ADVERSARIES, AND A BROADER ATTACK SURFACE, THE QUESTION IS WHAT DEFENDERS CAN DO TO MATCH THAT PACE.

SARA IS PART OF THE ANSWER.

Sara is purpose-built to scale coverage without sacrificing depth. As an agentic AI solution, Sara amplifies Synack's elite researchers, handling systematic surface mapping and automated testing so the SRT can focus on the creative, high-value exploit work that machines can't replicate.

SARA IN ACTION

3 high-severity exploits in a single session

Since it launched, Sara has demonstrated its value across multiple engagements. In a recent six-hour session, with no human intervention, Sara found and fully exploited multiple high-severity vulnerabilities across a live application including a SQLi, an admin account takeover, and stored cross-site scripting. In fact, 70% of Sara's findings on this target were rated high or critical.

3 high-severity exploits in a single session

1. Admin Account Takeover

Sara probed the “forgot password” flow and caught the API returning the reset token directly in the response body. Sara used it to change the admin password, confirmed the original credentials failed, and logged in with the new ones.

2. Two-Stage SQL Injection

Sara enumerated user-controlled parameters and surfaced a SQLi on a sort parameter that returned a timestamp instead of a result. Sara reasoned that this was a deferred job, queried a separate status endpoint to retrieve the output, and went on to extract emails and hashed passwords for every user, all max-privilege accounts.

3. Stored Cross-Site Scripting

Several user settings fields were displayed in the UI but had no visible form control. Sara inferred that the underlying API supported them anyway, sent an update request directly, and injected a payload that fires in every user’s browser on page load, exposing session tokens and creating a persistent foothold.

EACH FINDING IS DANGEROUS ALONE. CHAINED IT’S COMPLETE COMPROMISE:

Enumerate every user via SQLi, identify the admin accounts in that data, silently take them over using the reset token exploit, and seed a persistent payload through stored XSS. With basic automation behind it, that chain runs in minutes.

CONCLUSION

The attack surface doesn't wait, neither should your testing

THE 47% REDUCTION IN MTTR ACROSS SYNACK CUSTOMERS IS THE MOST ENCOURAGING DATA POINT IN THIS REPORT.

It reflects real operational improvement where security teams are processing and closing vulnerabilities faster than they were a year ago.

The challenge is that the benchmark for fast enough has shifted. Commercial exploit tooling and AI-assisted reconnaissance are compressing the window between CVE disclosure and active exploitation. Days-level MTTR was a reasonable target in 2023, but that's no longer true when working against AI-enabled adversaries.

Organizations that test continuously, across their full attack surface, close findings faster and surface higher-severity issues earlier in the exposure window. Organizations that test periodically are, by definition, operating with incomplete information about their current risk posture.

The combination of agentic AI and vetted human researchers addresses both sides of that problem—coverage at scale and depth on the findings that automated tools miss.

METHODOLOGY

We securely and confidentially analyzed proprietary vulnerability data to understand the top flaws for all organizations testing with Synack in 2025. We compared that to 2024 data, which includes vulnerabilities by industry vertical, the distribution of criticality and average time to remediation. Due to the dynamic nature of vulnerabilities and their remediation, they may take many months to close. Attack surface discovery statistics are pulled from a wider dataset that includes prospective as well as current customers.

For more on Synack's approach to continuous pentesting, visit www.synack.com.

About Synack

Synack is the leader in human-led and AI-powered Penetration Testing as a Service (PTaaS), transforming offensive security to help organizations proactively reduce risk, stay compliant, and defend against evolving cyber threats. We are committed to making the world more secure by harnessing agentic AI innovations and a talented, vetted community of security researchers to deliver continuous penetration testing and autonomous vulnerability management. Founded by former NSA operatives, Synack has enabled nearly 10 million hours of expert testing to protect critical assets, from global financial systems to U.S. Defense Department networks.

To learn more about Synack, visit www.synack.com.