TISS
CYBERSECURITY
INSIGHTS

TRILLIUM
INFORMATION SECURITY SYSTEMS

PEN TEST
INSIGHTS REPORT
2025

TABLE OF CONTENTS

INTRODUCTION

Cybersecurity continues to be a defining risk area for organizations operating in increasingly digital and interconnected environments. As business processes, customer interactions, and critical services rely more heavily on technology, the potential impact of security failures has grown significantly. Cyber threats are no longer isolated or opportunistic; they are targeted, persistent, and capable of causing operational disruption, financial loss, and reputational damage. In this context, proactive security assessment is essential. Penetration testing enables organizations to evaluate real-world attack scenarios, identify exploitable weaknesses, and validate the effectiveness of existing security controls.

Trillium Information Security Systems (TISS) has been conducting structured penetration testing engagements across key industries for several years. This annual Pen Test Insights Report captures real world security findings, tracks how vulnerability trends shift year over year, and gives organizations the kind of grounded intelligence they need to make smarter security decisions.

In 2023, TISS assessed organizations across multiple sectors including Banking, Pharmaceuticals, Telecommunications, Education, Software Companies, Government, Real Estate, and Industrial. Over 2,000 vulnerabilities were identified in total, with 70.93% traced to internal environments. The findings that year pointed to recurring weaknesses in authentication, insecure data storage, and insufficient brute-force protection.

The 2024 cycle expanded into multiple sectors with internal vulnerabilities, climbing to 80% of all findings. The most frequently detected issues included Technology Information Disclosure, Vulnerable and Outdated Components, SSL Pinning Bypass, and deprecated TLS 1.0 & 1.1 protocols, reinforcing a familiar pattern of foundational gaps.

During 2025, Trillium Information Security Systems (TISS) carried out penetration testing engagements across a broad set of industries, including Banking, Education, FinTech, Government, Insurance, IT and Technology, Manufacturing, and Telecommunications. These engagements reflect the expanding digital footprint of organizations and the increasing exposure of critical systems to external and internal threat actors.

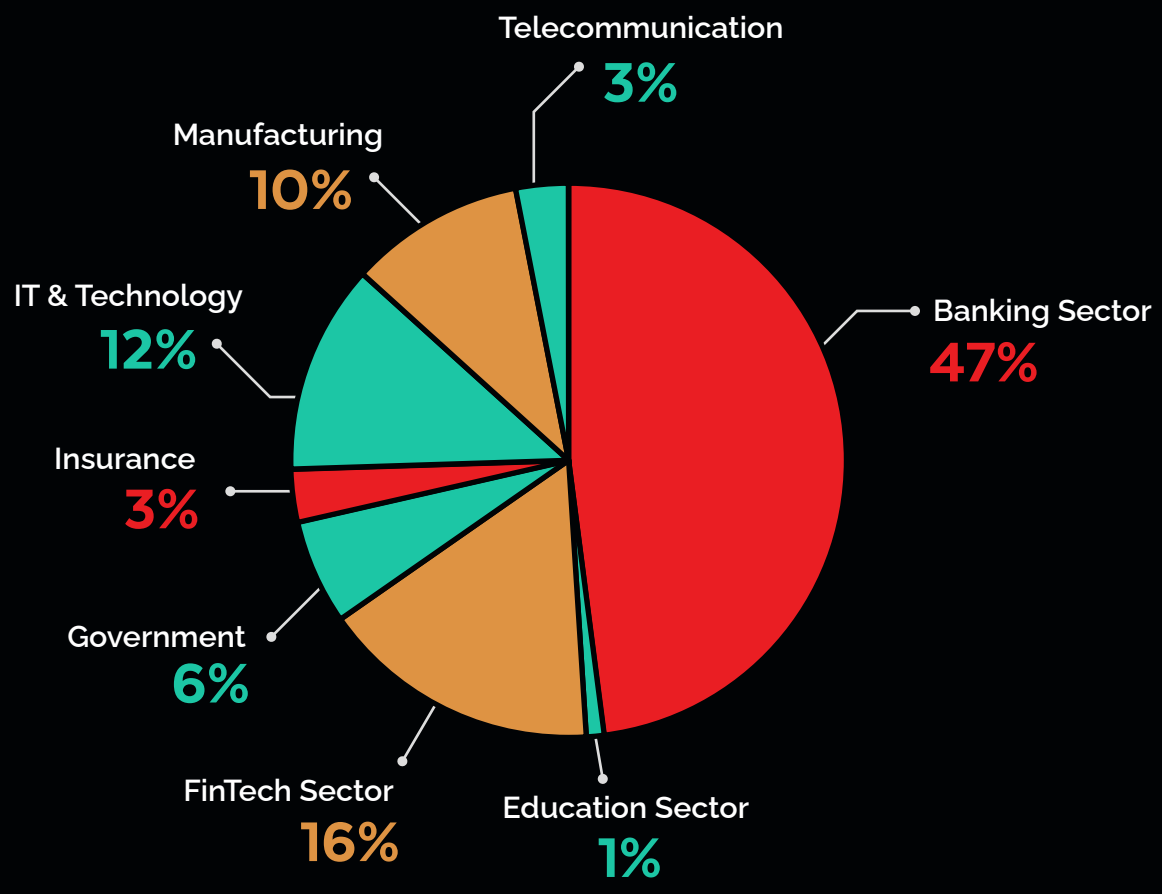
These assessments spanned a broad spectrum of digital environments, testing web applications, mobile apps, networks, active directory environments, databases, servers, virtual machines, and cloud infrastructures.

The results indicate that many organizations continue to face challenges in addressing foundational security weaknesses. Recurrent issues such as inadequate access controls, insecure configurations, and delayed remediation efforts remain prevalent across multiple sectors. Although organizations in regulated and data-sensitive industries demonstrate comparatively stronger security practices, gaps in visibility, detection, and response capabilities persist and contribute to ongoing exposure to emerging threats.

This report adopts a data-driven approach to examine vulnerability trends, severity distribution, and sector-specific risk patterns observed during 2025. By focusing on the most frequently identified vulnerabilities and their relative impact, the report aims to support informed decision-making and more effective prioritization of security improvements.

ENGAGEMENT DEMOGRAPHIC

This section provides an overview of penetration testing engagements conducted during 2025, categorized by industry sector. The distribution highlights sectors with higher testing activity and reflects varying levels of cybersecurity focus across industries.



Banking sector accounted for the largest share of engagements at 47%, reflecting the sector's exposure to cyber risk and the critical nature of financial systems and data. FinTech followed with 16%, driven by the continued growth of digital financial services and associated security challenges.

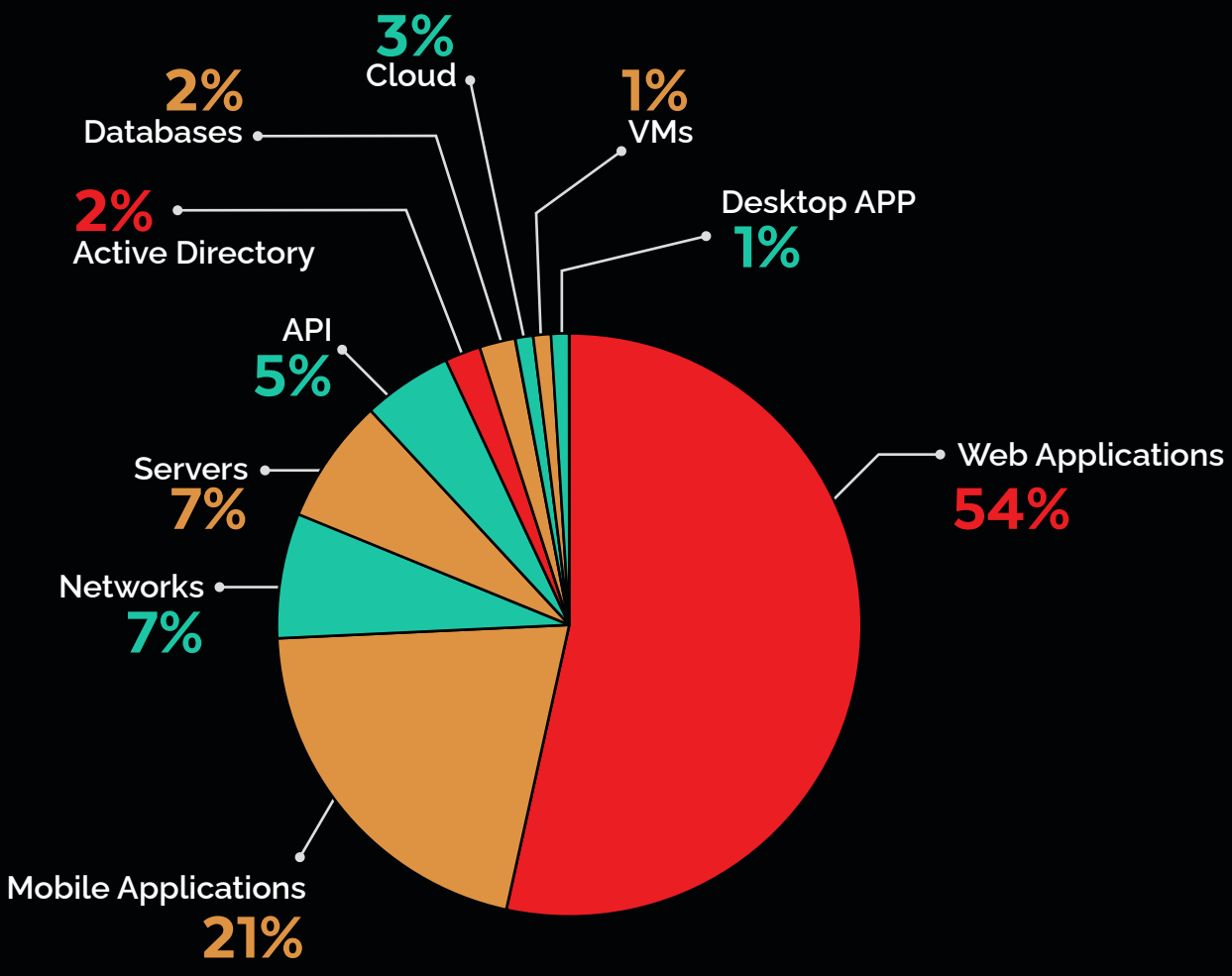
The IT and Technology sector represented 12% of engagements, while Manufacturing accounted for 10%, indicating increased attention toward securing technology-enabled operational environments. Government engagements comprised 6% of the total, showing moderate testing activity within the public sector.

Insurance and Telecommunications each accounted for 3% of engagements, while Education represented 1%. The lower proportion of assessments in these sectors may indicate differences in security prioritization or resource allocation.

Overall, the engagement distribution shows a strong concentration of testing within financially and technologically driven sectors, with several industries remaining comparatively underrepresented.

ENGAGEMENT FOCUS AREAS

Security assessments consistently focused on the systems that support day-to-day digital operations. The most frequently tested assets included web applications, mobile applications, and networks, collectively making up 82% of all assessments. Web applications led at 54%, reflecting their critical role in digital operations.

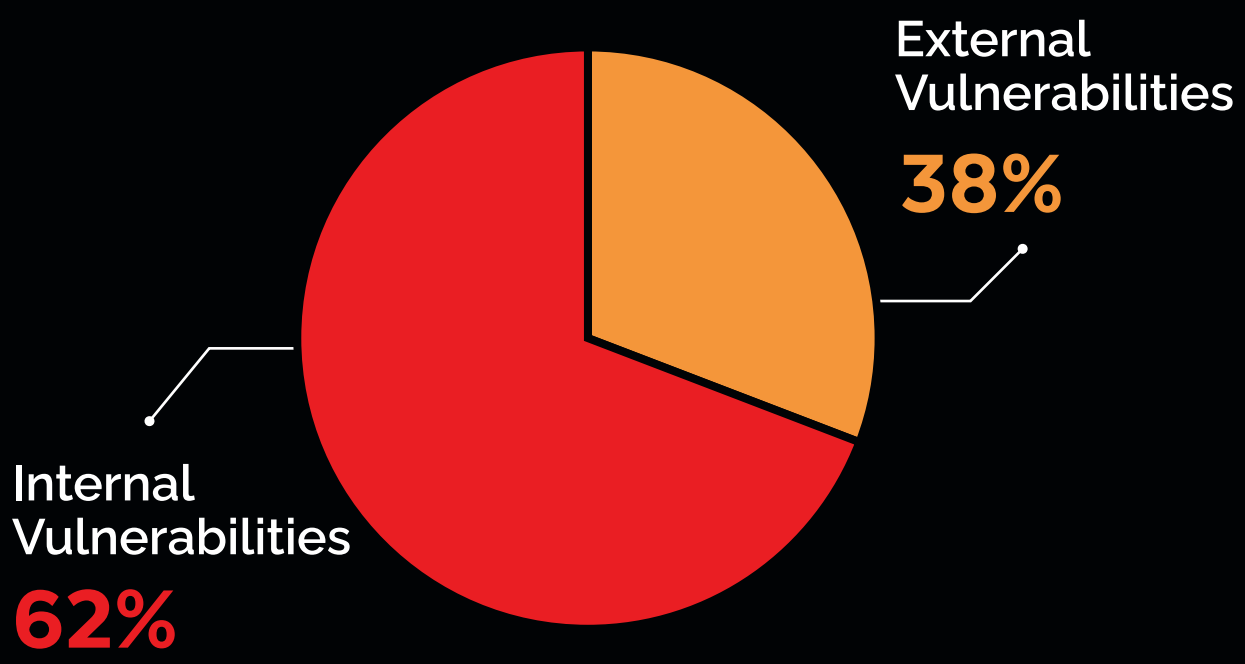


Mobile applications followed at 21%, a share that continues to grow in line with the expansion of mobile-first services across financial and technology sectors. Networks and servers each accounted for 7%, covering the infrastructure layer that underpins most digital operations. APIs, databases, Active Directory, and cloud environments collectively represented less than 11% of total engagements.

Given how central these assets are to modern operations handling authentication, sensitive data, and increasingly, core business logic, the relatively low testing activity in these areas is worth noting. As cloud adoption accelerates, ensuring these environments receive adequate security coverage will be just as important as securing the applications that sit on top of them.

VULNERABILITIES IDENTIFIED

Assessments covered both external and internal environments, from internet-facing applications and perimeter devices to domain infrastructure, internal servers, and segmented network zones.



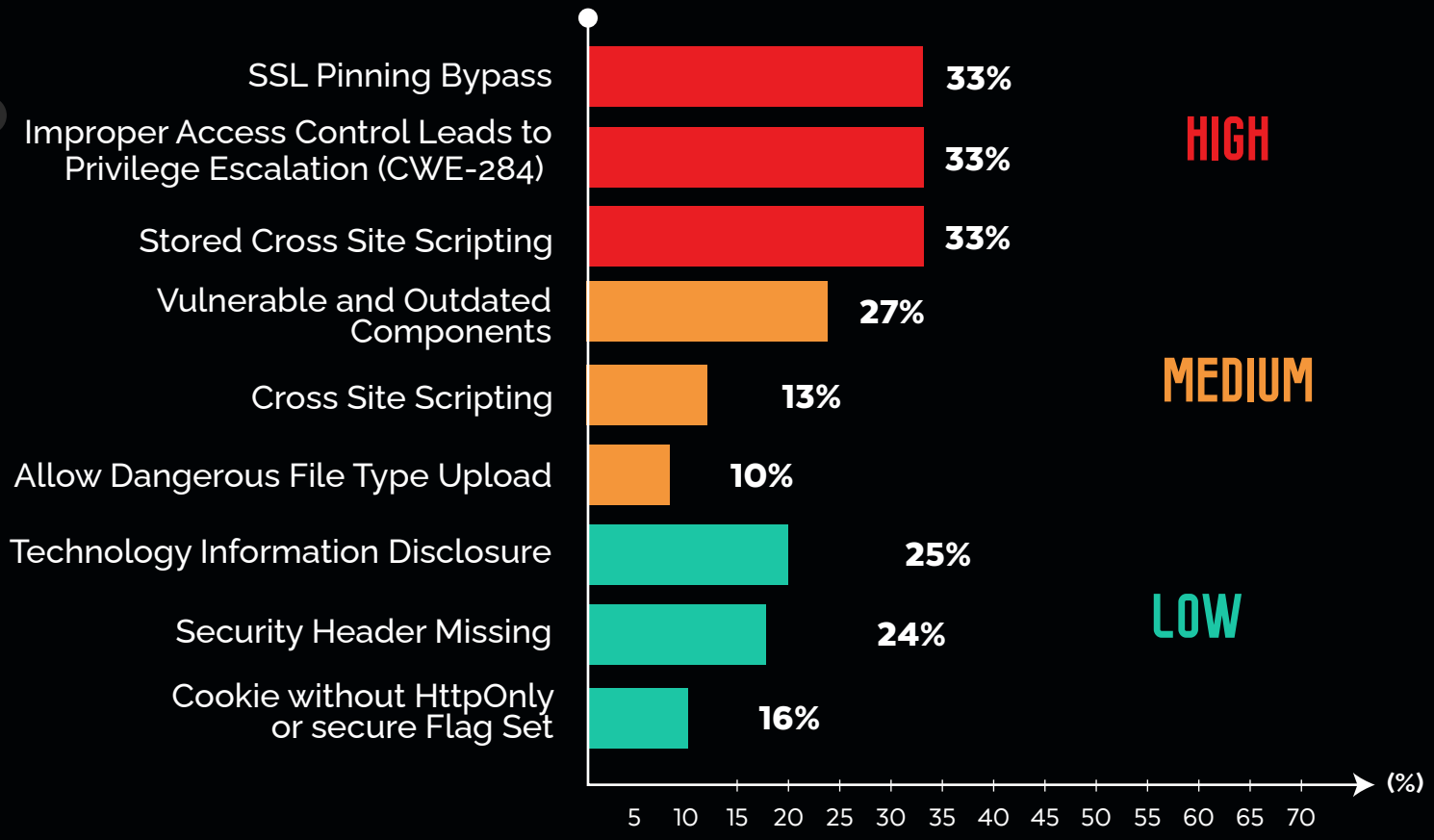
External testing focused on identifying entry points an attacker could exploit from outside the network, including exposed services, weak authentication, and application-level flaws. Internal testing simulated scenarios where an attacker had already gained a foothold, examining how far they could move and how much damage they could do once inside.

Across all engagements, 62% of vulnerabilities were found within internal environments. This is a meaningful improvement from 80% in 2024, but it still signals that once past the perimeter, attackers would find no shortage of opportunities to escalate privileges and access sensitive data.

VULNERABILITY TRENDS ACROSS ASSET TYPES

This section summarizes the most common security vulnerabilities identified across various asset types, categorized by severity: Critical, High, Medium, and Low. The subsections below highlight key findings for web applications, mobile applications, servers, cloud environments, network devices, active directory, and virtual machines.

WEB APPLICATIONS

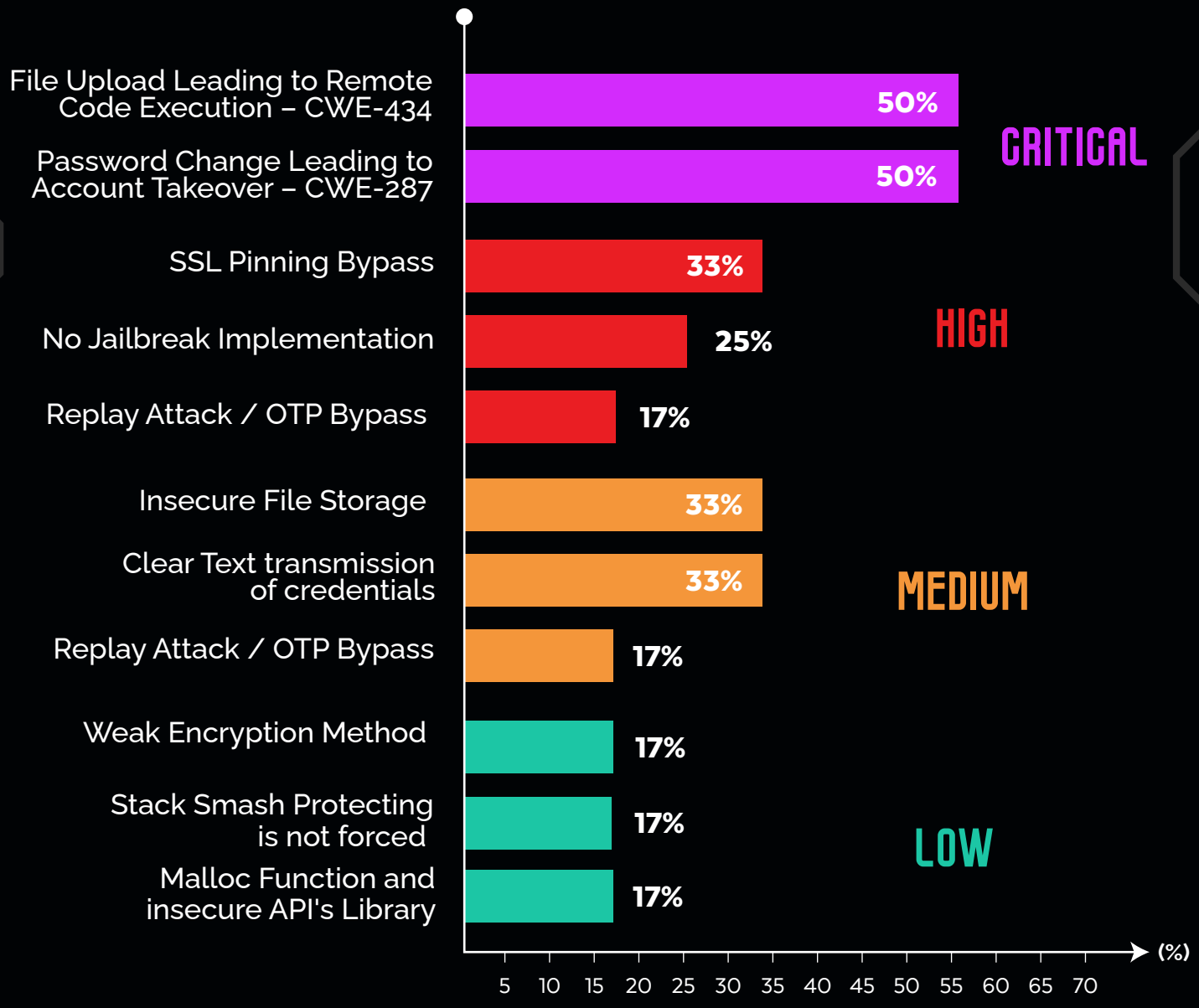


The assessment of web applications highlighted several high-severity vulnerabilities, including SSL pinning bypass, stored cross-site scripting (XSS), and improper access control leading to privilege escalation (CWE-284). These issues increase the risk of data breaches and enable attackers to gain elevated privileges, facilitating lateral movement within networks.

Medium-severity findings included outdated components, cross-site scripting, and dangerous file type uploads, reflecting gaps in secure development practices. Low-severity issues, such as technology information disclosure, missing security headers, and cookies without HttpOnly or Secure flags further expanded the attack surface.

Mitigation should focus on access controls, timely patching, secure coding practices, and strengthening authentication mechanisms to reduce potential attack vectors.

MOBILE APPLICATIONS (ANDROID)

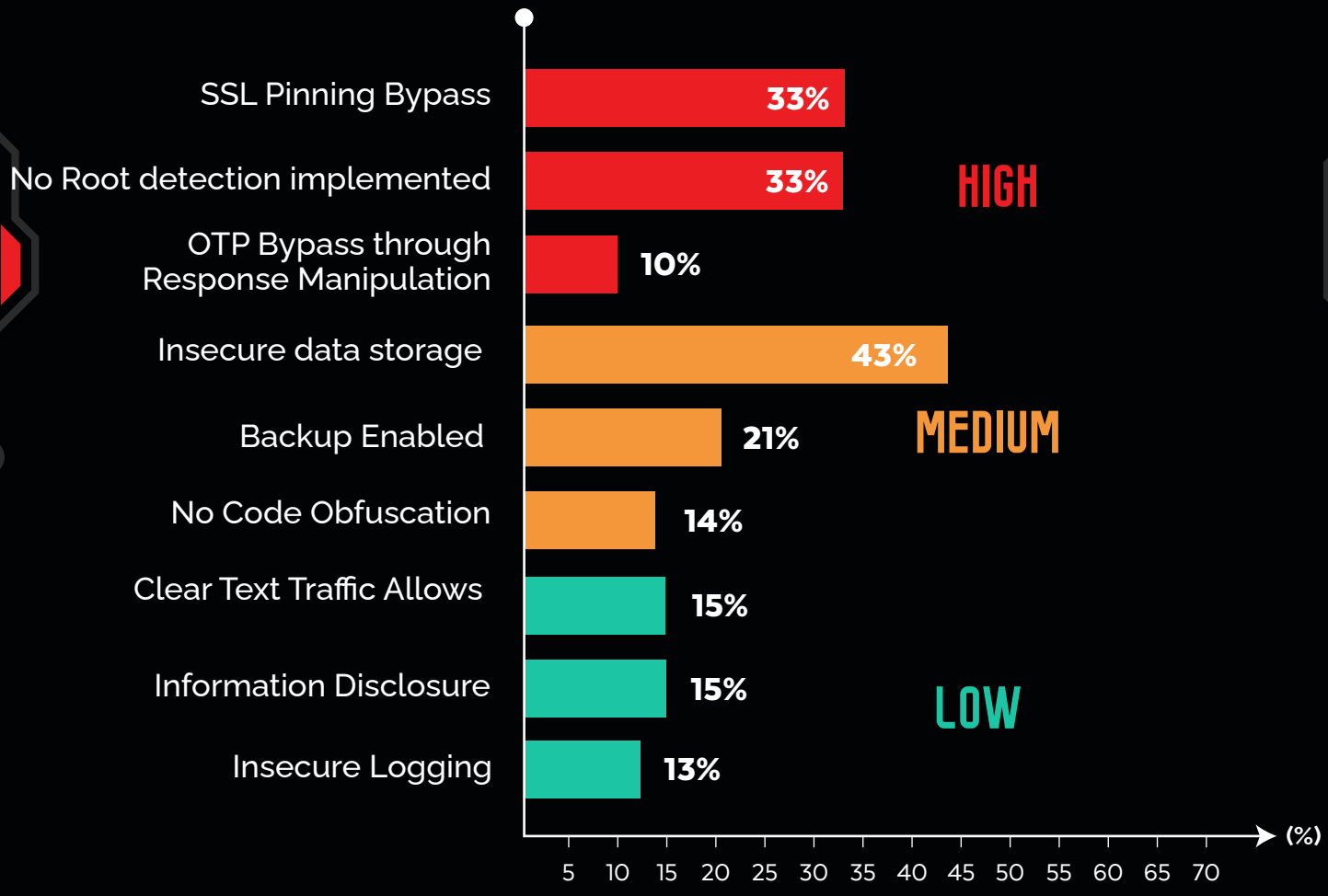


Security testing of Android mobile applications revealed critical and high-severity vulnerabilities, exposing users to remote code execution, account takeover, SSL pinning bypass, and missing jailbreak detection controls.

High-severity issues included SSL pinning bypass and OTP bypass, leaving users exposed to man in-the-middle attacks and unauthorized access. Medium-severity findings covered insecure file storage and cleartext transmission of credentials, increasing the risk of data leaks. Low-severity issues such as disabled stack smash protection and use of insecure API libraries further reflected gaps in secure coding practices.

Mitigation should focus on enforcing strong authentication, implementing SSL pinning and jailbreak detection, securing local data storage, and maintaining timely patching to reduce the attack surface across Android platforms.

(iOS)



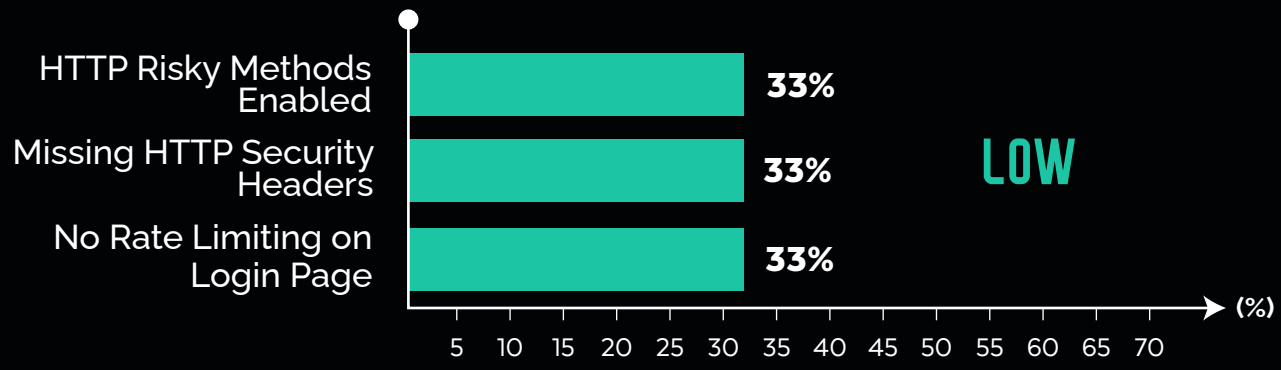
Security testing of mobile applications across Android and iOS platforms revealed critical and high-severity vulnerabilities, exposing users to remote code execution, account takeover, SSL pinning bypass, and missing root/jailbreak detection controls.

High-severity issues were prevalent on both platforms, including SSL pinning bypass, absence of root/jailbreak detection, and OTP bypass, exposing users to man-in-the-middle attacks, unauthorized access, and compromised runtime environments.

Medium-severity vulnerabilities included insecure data storage, cleartext transmission of credentials, and code obfuscation gaps, which increase the likelihood of data leaks and reverse engineering attacks. Low-severity issues, such as weak encryption, insecure logging, and unsafe API usage, further highlighted gaps in secure coding practices.

Mitigation recommendations include enforcing strong authentication, implementing SSL pinning and root/jailbreak detection, securing sensitive data storage, applying code obfuscation, and maintaining timely patching to reduce attack surfaces across mobile platforms

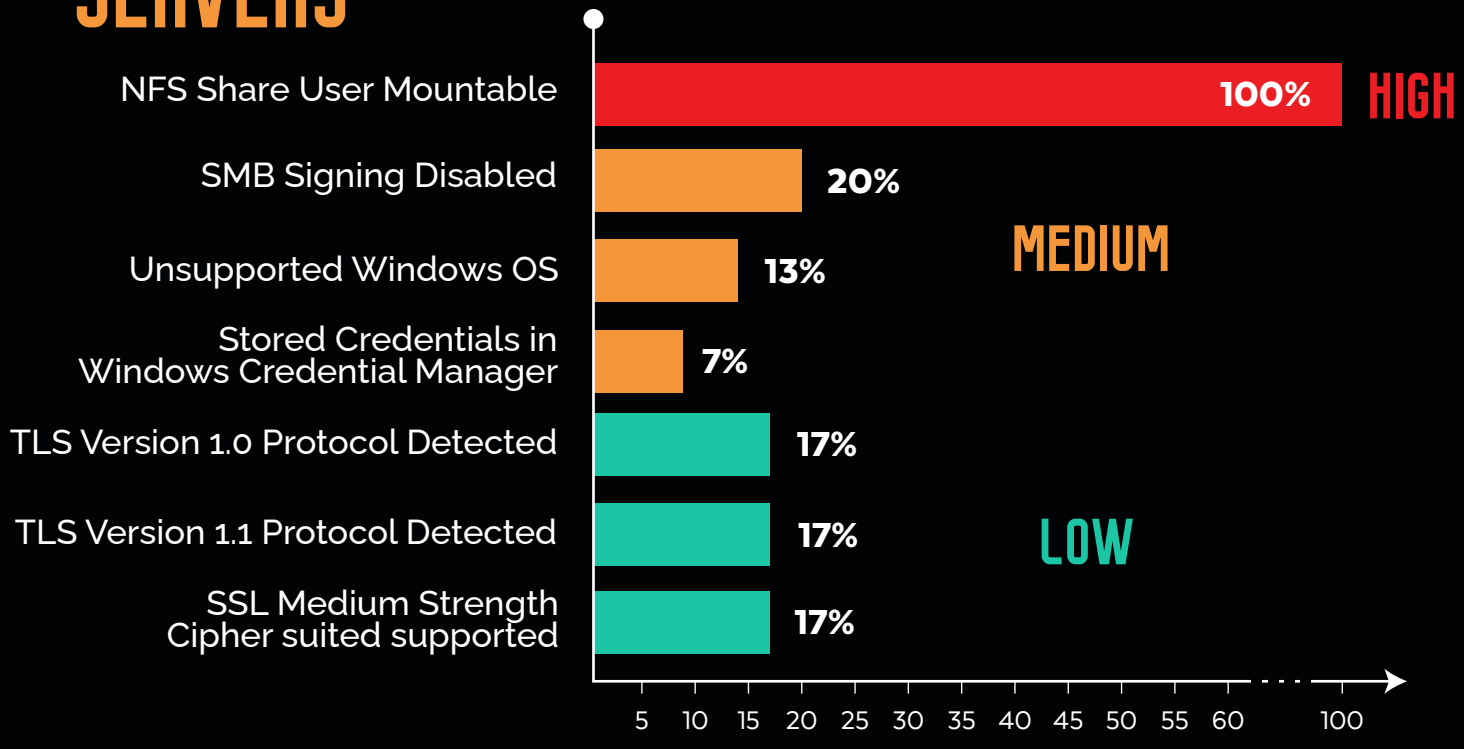
CLOUD ENVIRONMENTS



Assessments of cloud infrastructure did not uncover critical, high, or medium-severity vulnerabilities, indicating that fundamental security controls are largely effective.

Low-severity issues, including risky HTTP methods, missing security headers, and lack of rate limiting on login pages, highlight configuration weaknesses requiring hardening. Organizations should continue enforcing strict access policies, encryption, and continuous monitoring to maintain secure cloud environments as adoption grows.

SERVERS

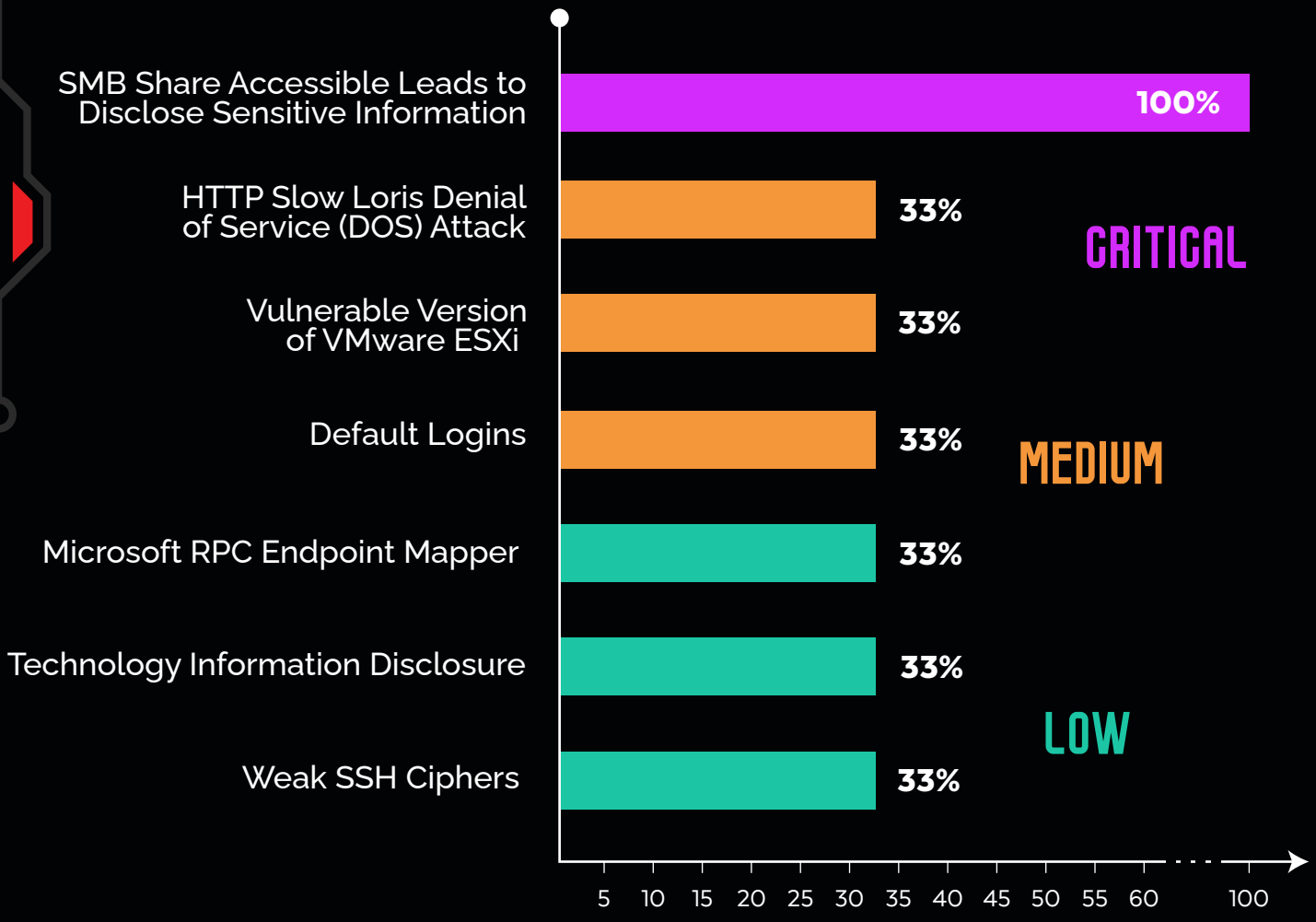


Server security assessments did not reveal any critical vulnerabilities; however, misconfigurations such as NFS shares being user-mountable posed high-risk exposure.

Medium-severity findings included SMB signing disabled, unsupported operating systems, and stored credentials, reflecting gaps in patch management and credential security. Low-severity concerns, such as outdated TLS versions and medium-strength cipher suites, indicate areas for improvement.

Mitigation involves regular updates, access restrictions, and enforcement of secure encryption practices.

NETWORK DEVICES

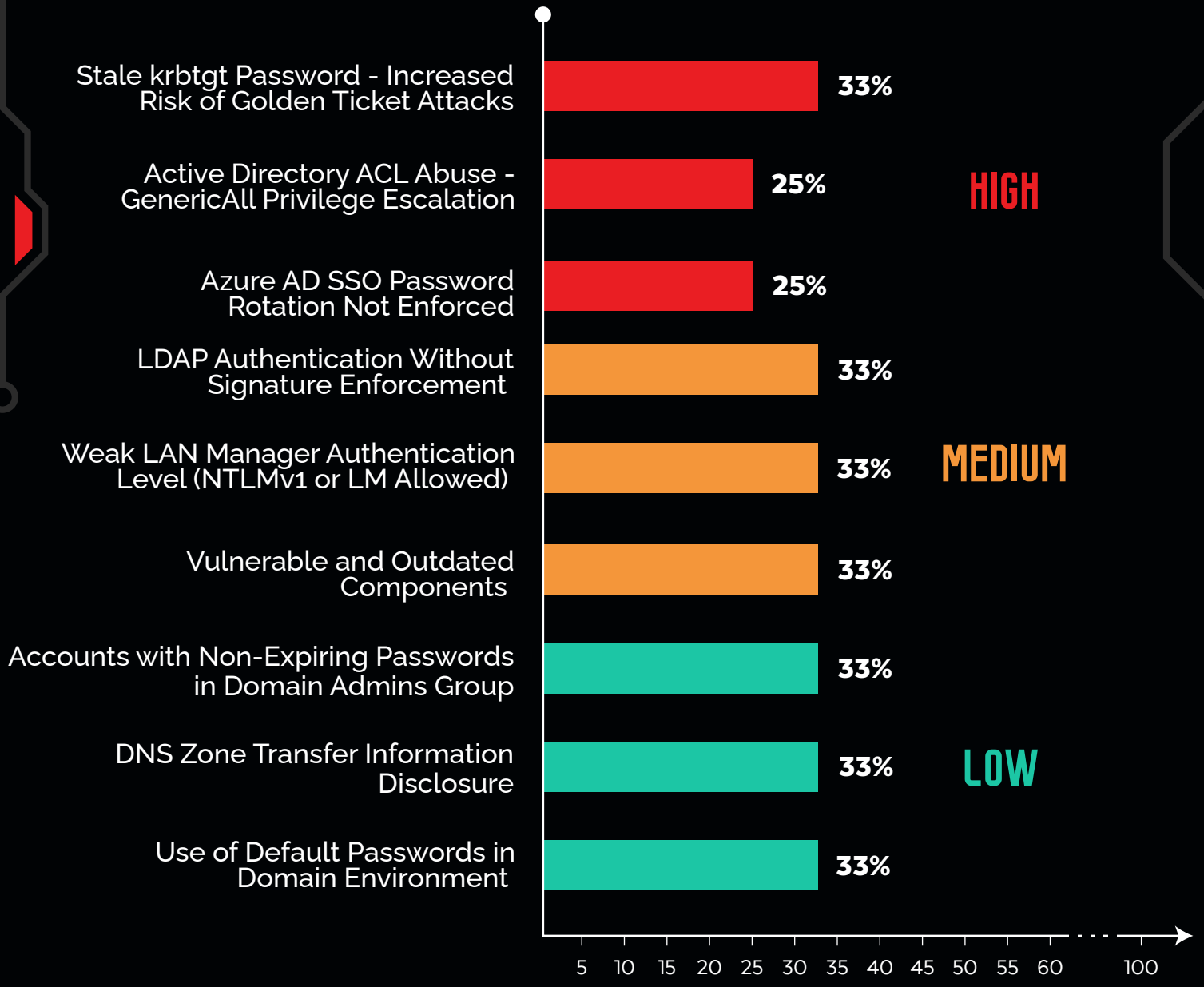


Network device assessments identified a critical vulnerability where an SMB share could expose sensitive information.

Medium-severity issues included HTTP Slow Loris DoS attacks, vulnerable VMware ESXi versions, and default logins. Low-severity findings, such as RPC endpoint mapper exposure, technology information disclosure, and weak SSH ciphers highlight further areas for improvement.

Organizations should implement prompt patching, enforce strict authentication policies, and upgrade encryption practices to strengthen network security.

ACTIVE DIRECTORY

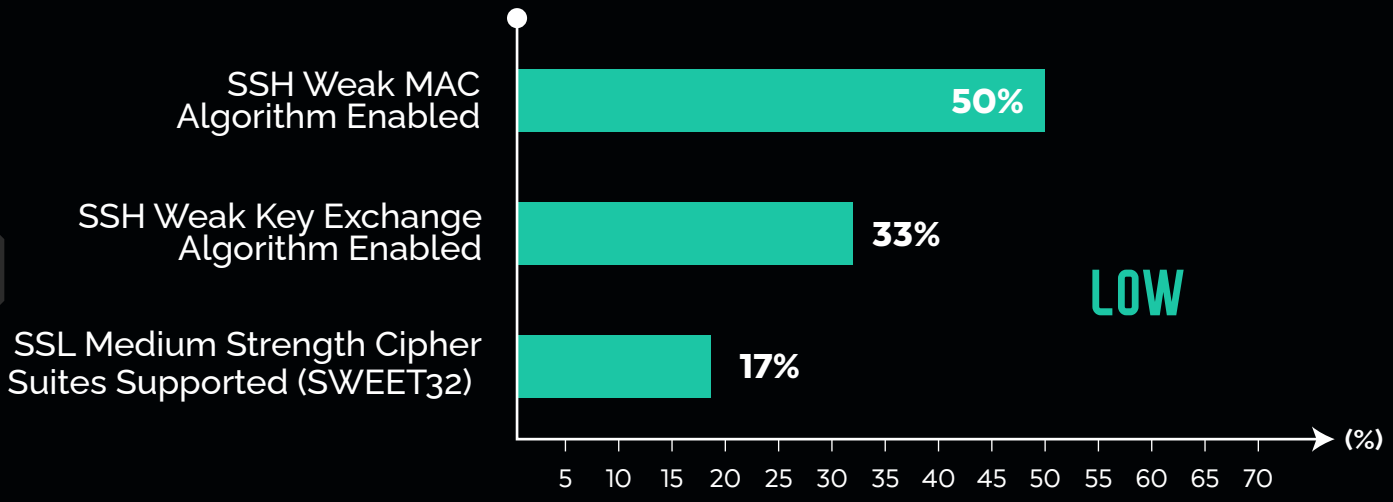


Assessments of Active Directory revealed high-severity vulnerabilities, including stale Kerberos passwords, ACL abuse, and lack of Azure AD SSO password rotation enforcement, which could allow privilege escalation.

Medium-severity concerns, weak LDAP authentication, outdated components, and insecure protocols, further weakened defenses. Low-severity findings included non-expiring passwords in the Domain Admins group, DNS zone transfer disclosure, and use of default passwords.

Mitigation should prioritize credential management, enforcing secure authentication protocols, and auditing ACLs to maintain a resilient Active Directory environment.

VIRTUAL MACHINES / DATABASES



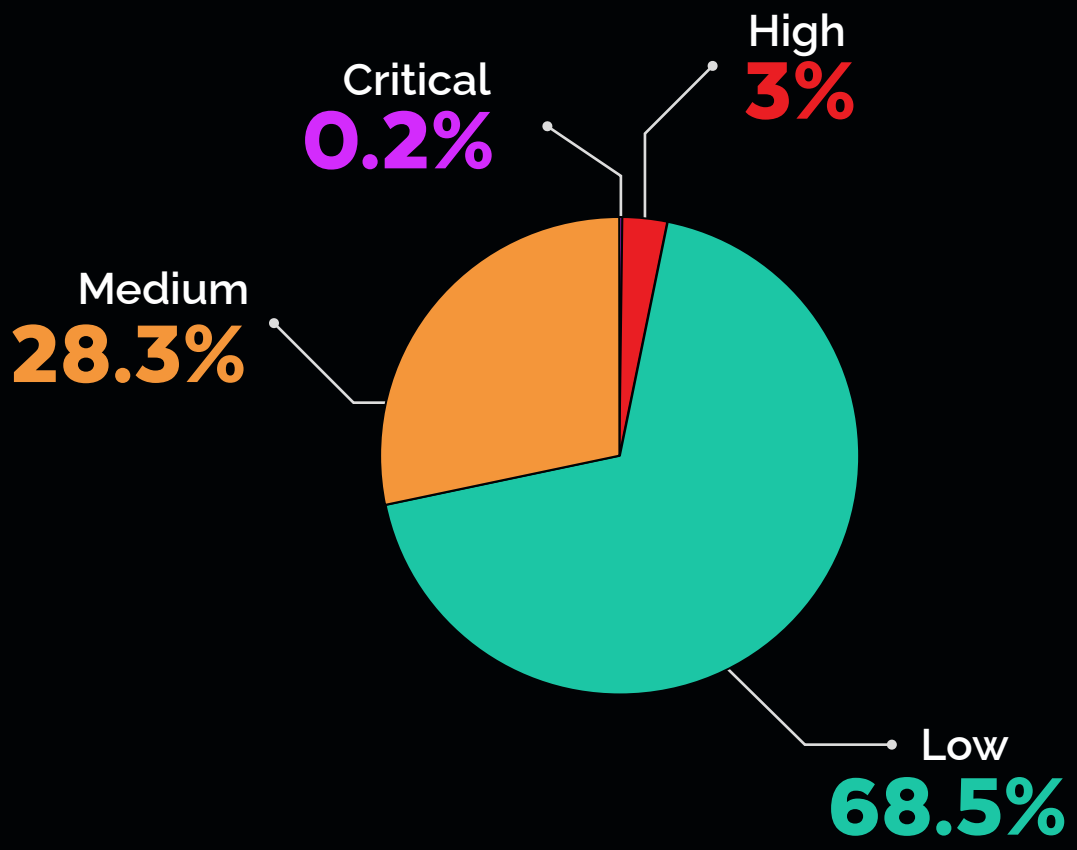
Security assessments of virtual machines and databases did not reveal critical, high, or medium-severity vulnerabilities.

Low-severity findings included weak SSH MAC algorithms, weak SSH key exchange algorithms, and medium-strength cipher suites, which could be mitigated through configuration updates and hardening practices.

SECTOR-WISE VULNERABILITIES

1. BANKING SECTOR

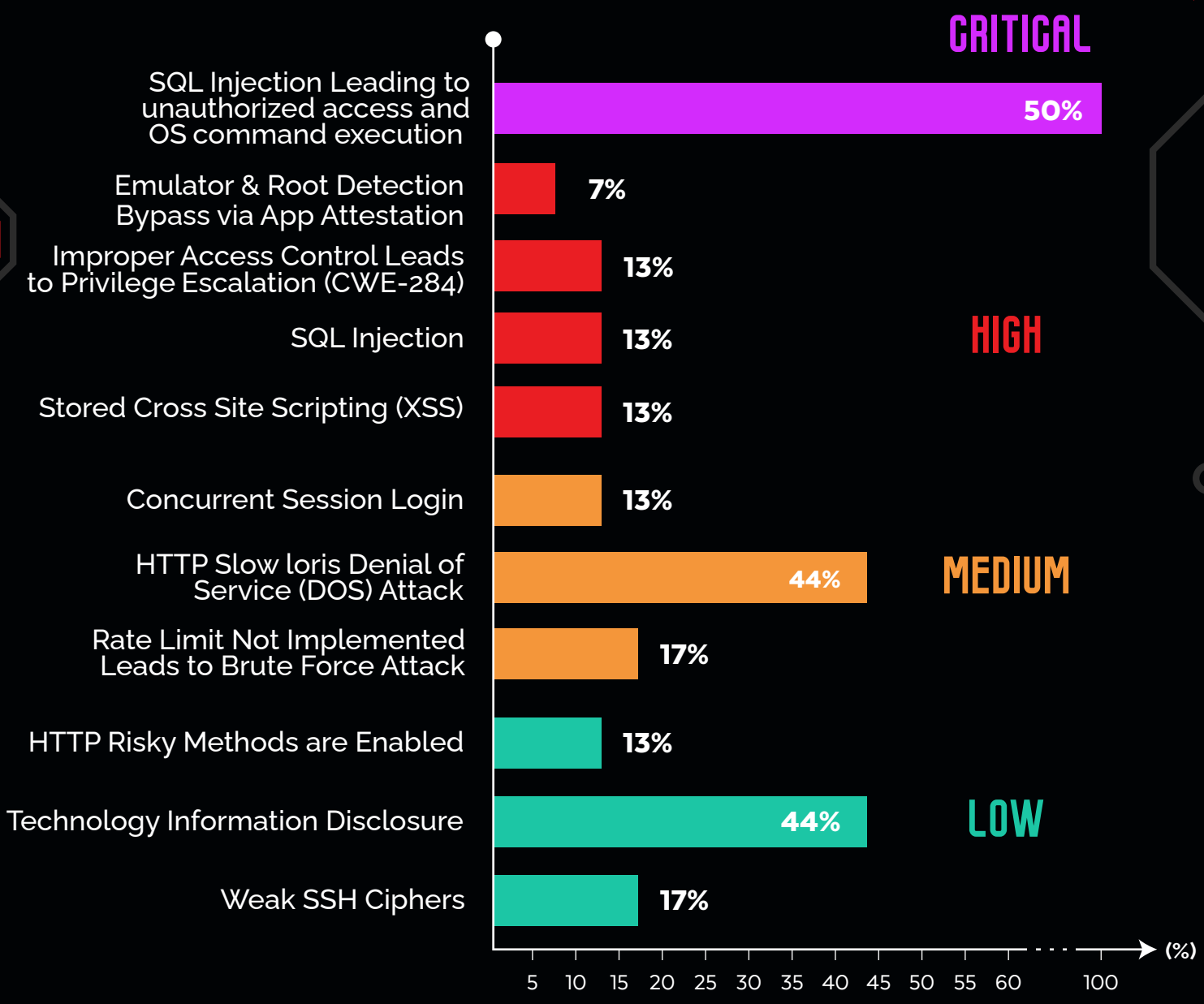
Banks and financial institutions remain high-value targets due to their role in managing financial transactions and sensitive customer information. The continued expansion of digital banking services has increased system complexity and exposure, making effective vulnerability management essential to maintaining operational integrity and customer trust.



In 2025, the majority of Banking sector findings fell within the Low (68.5%) and Medium (28.3%) severity categories, indicating widespread issues related to configuration weaknesses and control gaps. Common low-risk findings included technology information disclosure and weak cryptographic configurations, which may support reconnaissance activities if not addressed.

High severity vulnerabilities accounted for 3.0% of findings, including access control weaknesses, privilege escalation, SQL injection, and stored cross-site scripting. In addition, one Critical vulnerability involving SQL injection leading to unauthorized access and operating system command execution was identified. While limited in number, these issues highlight the potential impact of exploitable flaws and emphasize the importance of continuous testing, timely remediation, and strong access control enforcement.

MOST PREVALENT VULNERABILITIES IN BANKING SECTOR



At the critical level, SQL Injection leading to unauthorized access and OS command execution appeared in 50% of engagements, a serious concern for a sector managing sensitive financial data at scale, as successful exploitation extends well beyond data theft to direct control over underlying systems. High-severity findings further highlighted persistent access control weaknesses, with improper privilege escalation, SQL injection, and stored XSS each appearing in 13% of assessments.

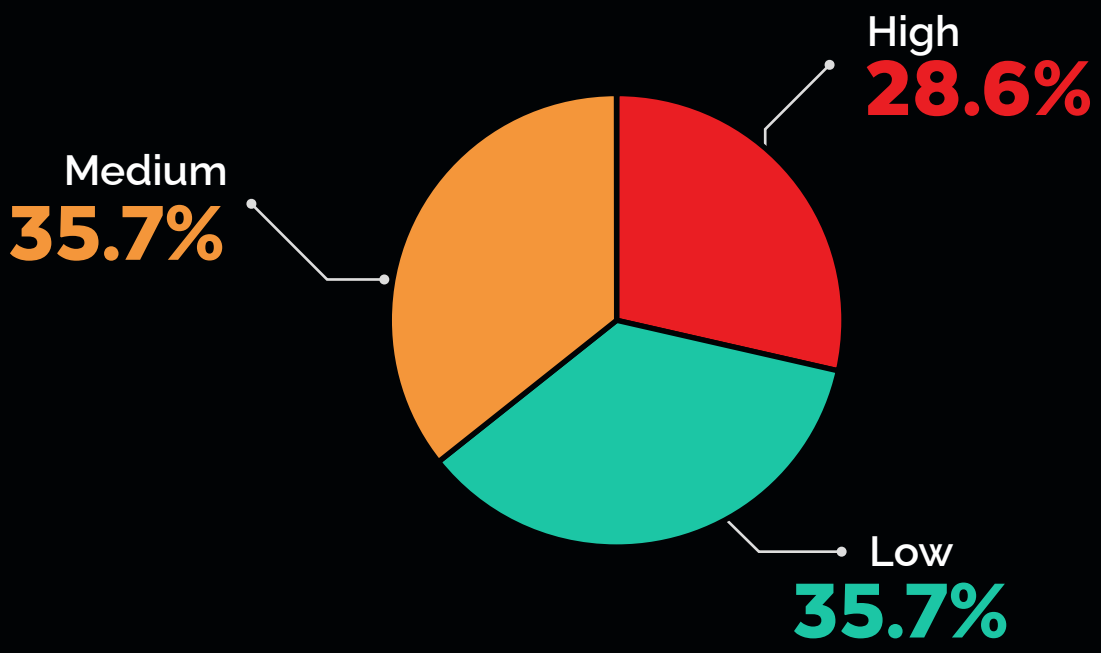
Medium-severity findings were dominated by HTTP Slow Loris DoS attacks at 44%, followed by missing rate limiting at 17% and concurrent session login issues at 13%. These gaps collectively increase exposure to service disruption and brute-force attacks, risks that are largely avoidable with consistent configuration controls.

At the low end, technology information disclosure was the most frequently recorded finding at 44%, alongside weak SSH ciphers and enabled HTTP risky methods. While these carry limited direct impact on their own, they hand attackers a useful starting point for deeper reconnaissance.

2. EDUCATION SECTOR

Educational institutions continue to expand their use of digital systems to support academic, administrative, and financial operations, introducing new security considerations across a diverse user base.

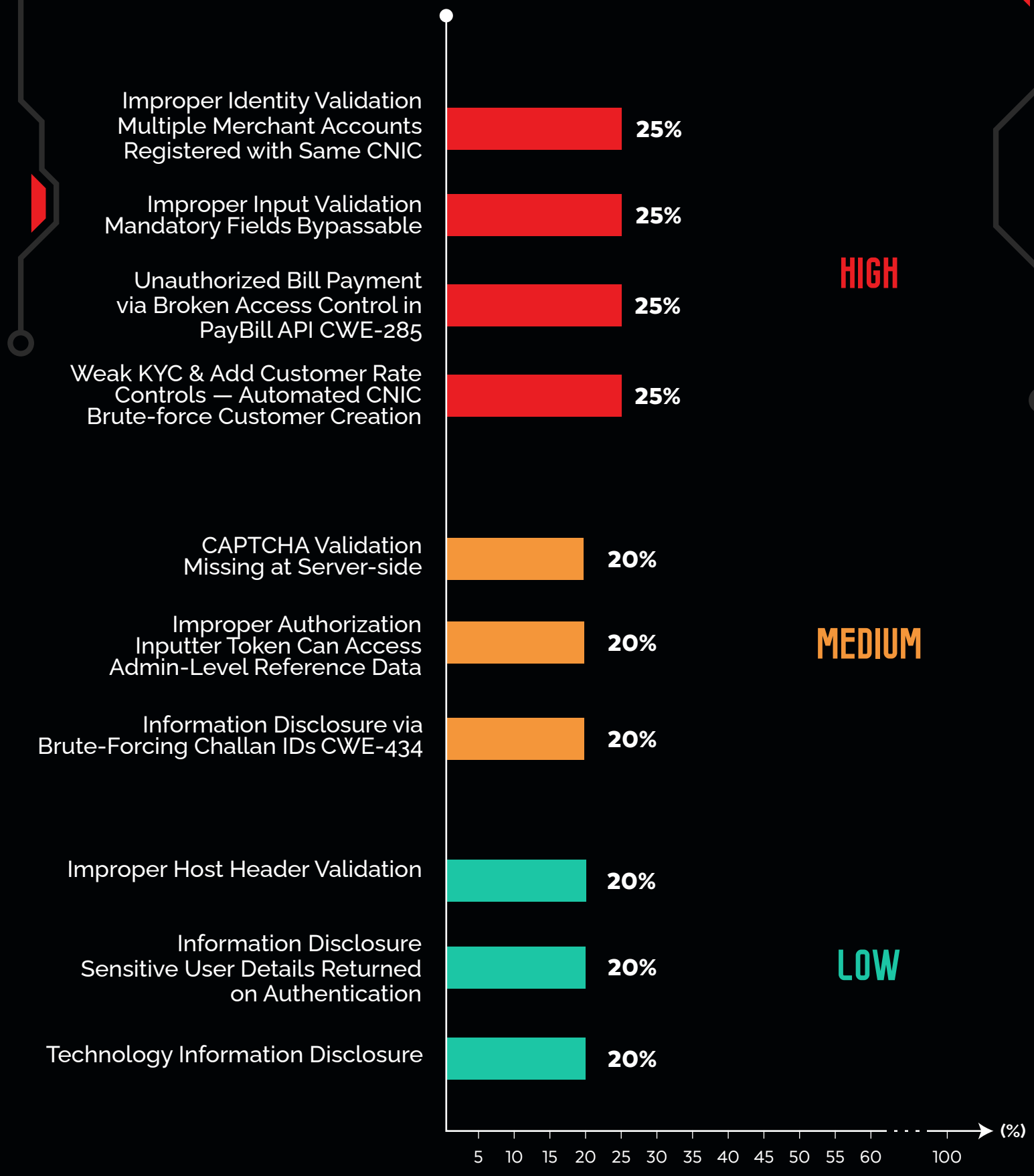
In 2025, the Education sector recorded a limited number of engagements; however, the findings show a balanced distribution of Low (35.7%) and Medium (35.7%) severity vulnerabilities, with High severity issues accounting for 28.6%. No Critical vulnerabilities were identified.



High severity findings were primarily associated with broken access control and validation weaknesses, including improper identity verification, weak KYC and rate controls, and unauthorized actions through exposed application interfaces. Medium and Low severity issues largely involved information disclosure and missing server-side security controls, such as inadequate input validation and CAPTCHA enforcement.

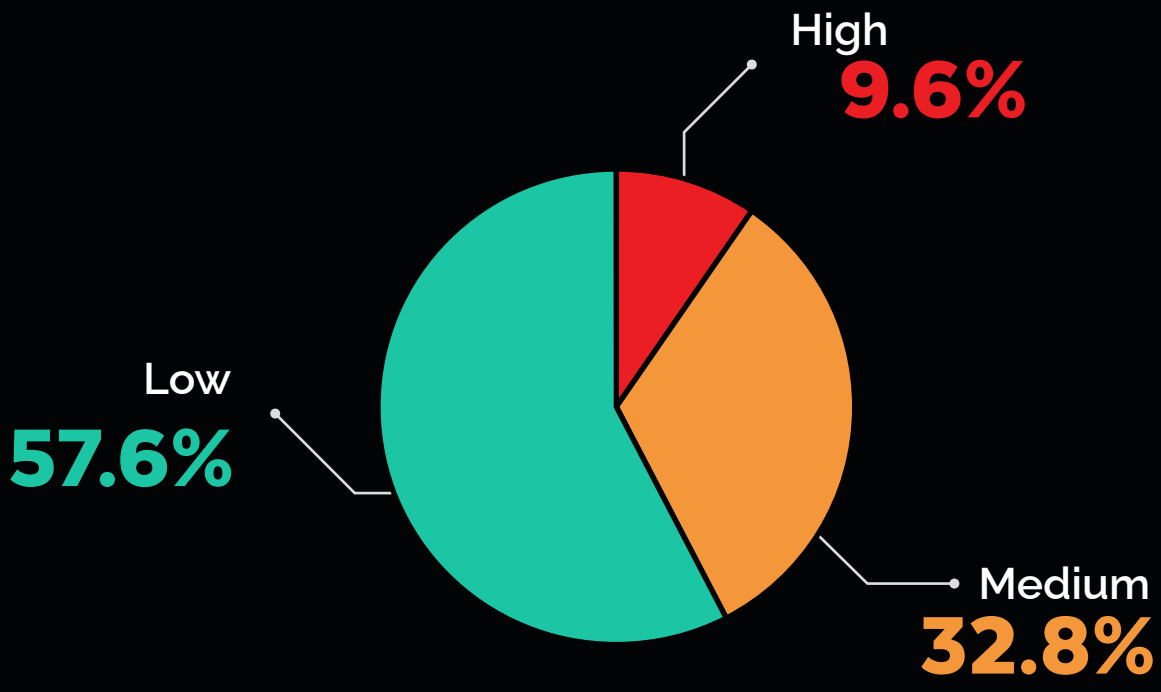
Although the overall volume of findings was low, the presence of high-risk vulnerabilities highlights the importance of strengthening access controls, validation mechanisms, and secure development practices to protect sensitive institutional and user data.

MOST PREVALENT VULNERABILITIES IN EDUCATION SECTOR



3. FINTECH SECTOR

The FinTech sector continues to expand rapidly, driven by digital payment systems, mobile applications, and API-based financial services. This reliance on interconnected platforms and real-time transactions increases exposure to security risks, particularly where authentication, encryption, and rate-limiting controls are insufficient.

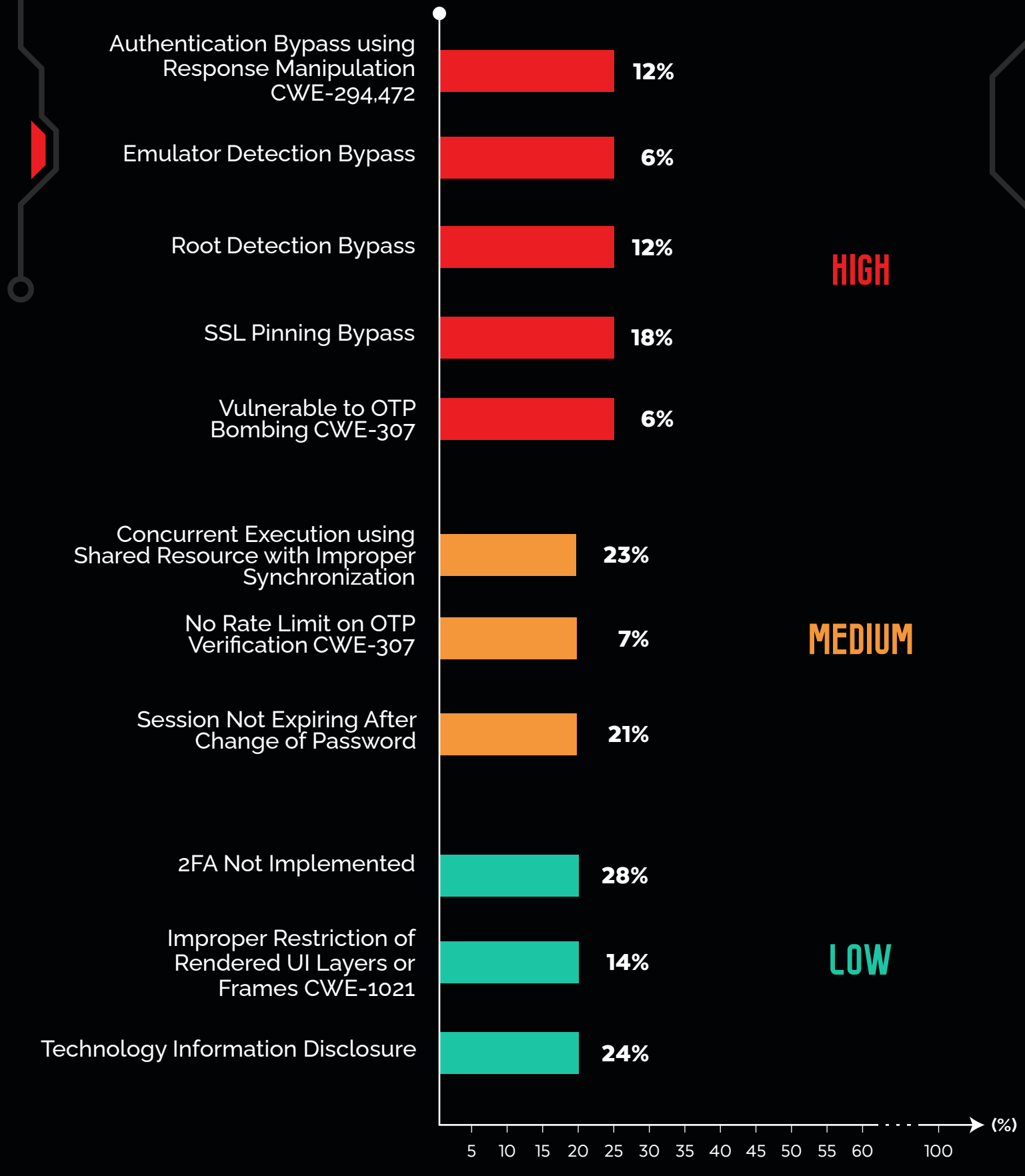


In 2025, FinTech findings were primarily concentrated in the Low (57.6%) and Medium (32.8%) severity categories, indicating recurring gaps in baseline security controls and session management. Common low severity issues included the absence of two-factor authentication, technology information disclosure, and UI-related security weaknesses.

High severity vulnerabilities accounted for 9.6% of findings, with critical weaknesses identified in mobile application and authentication security. These included SSL pinning bypass, root and emulator detection bypass, authentication manipulation, and exposure to OTP abuse scenarios. Medium severity issues further highlighted weaknesses in rate limiting, session handling, and synchronization controls, increasing the risk of account compromise and service abuse.

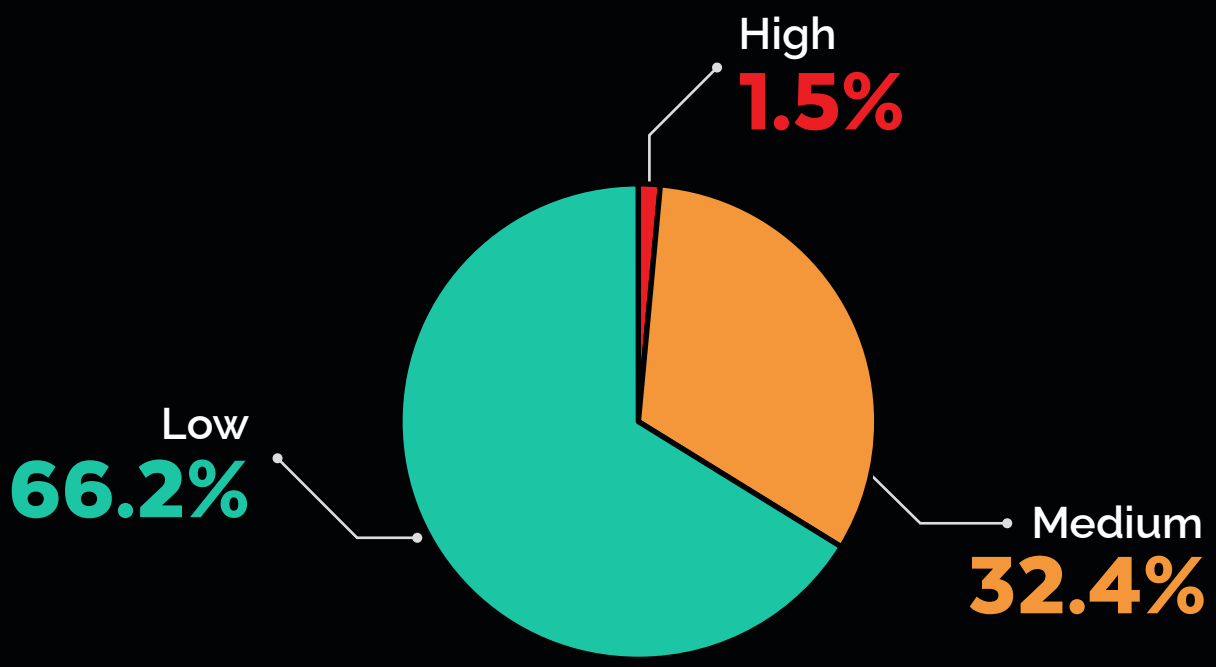
Although the majority of findings were not critical, the presence of high-risk vulnerabilities within transactional workflows underscores the importance of strengthening authentication mechanisms, enforcing robust encryption standards, and implementing effective rate-limiting and monitoring controls to reduce the risk of fraud and data exposure.

MOST PREVALENT VULNERABILITIES IN FINTECH SECTOR



4. GOVERNMENT SECTOR

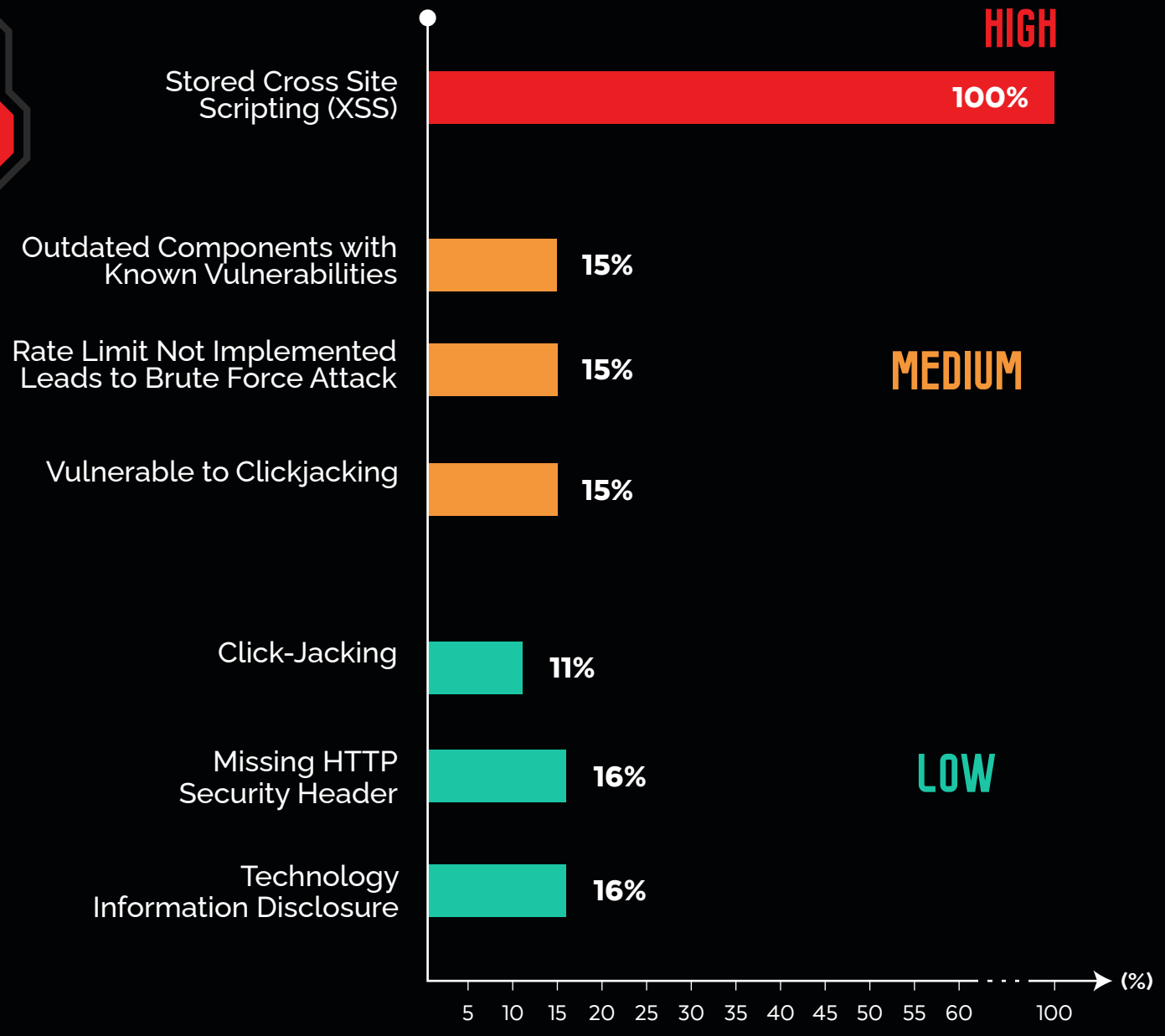
Government institutions manage critical public services and sensitive citizen data, making them prime targets for cyber threats. Robust security measures remain essential to protect national infrastructure and maintain public trust.



Majority of findings were Low (66.2%) and Medium (32.4%) severity, reflecting configuration gaps, outdated components, and missing security controls. High severity vulnerabilities accounted for 1.5% of findings, including a stored cross-site scripting (XSS) issue, highlighting potential risks to application security and data integrity.

Common medium and low severity issues involved rate-limiting gaps, clickjacking, missing HTTP security headers, and technology information disclosure. While most findings were not critical, the results emphasize the need for consistent patching, access control enforcement, and secure development practices to reduce exposure and strengthen defenses against evolving cyber threats.

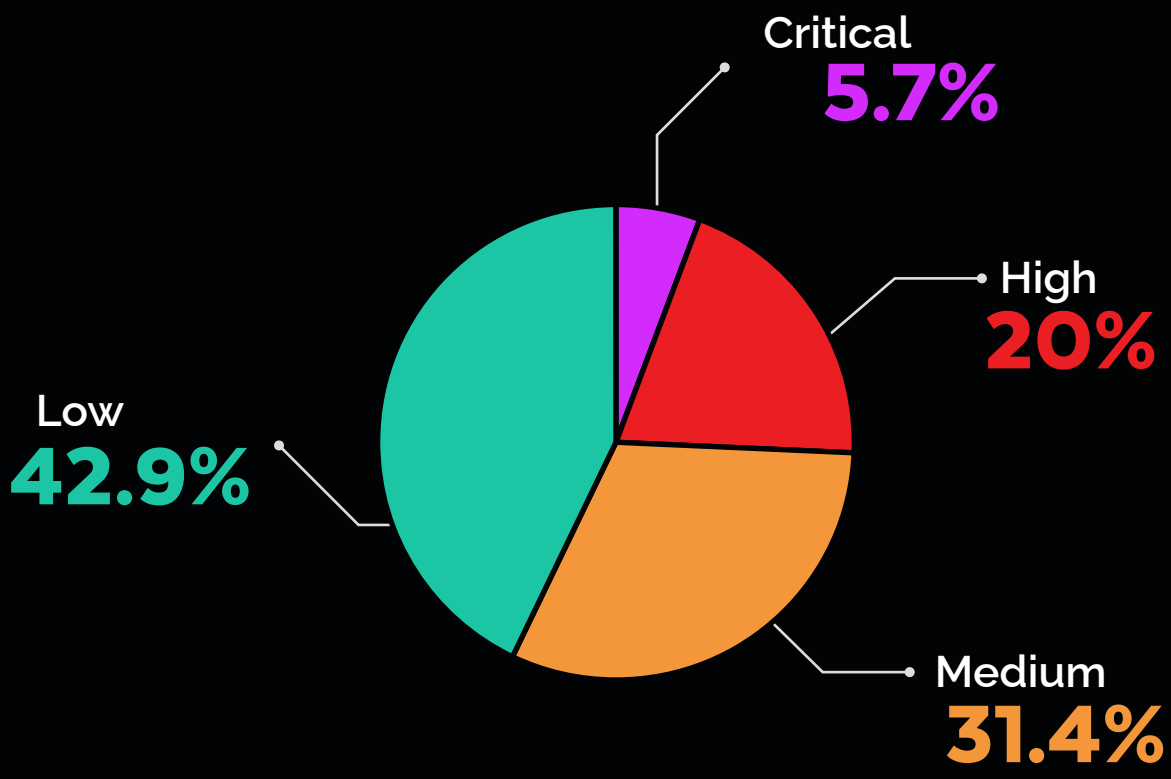
MOST PREVALENT VULNERABILITIES IN GOVERNMENT SECTOR



*Disclaimer: The graph displays the top 5 critical & high vulnerabilities, and top 3 medium & low vulnerabilities, or fewer if less were identified.

5. INSURANCE SECTOR

Insurance organizations handle highly sensitive personal and financial data, making them attractive targets for cyberattacks. The sector's reliance on digital platforms for policy management, claims processing, and customer interactions increases exposure to security risks, including account compromise and data leakage.

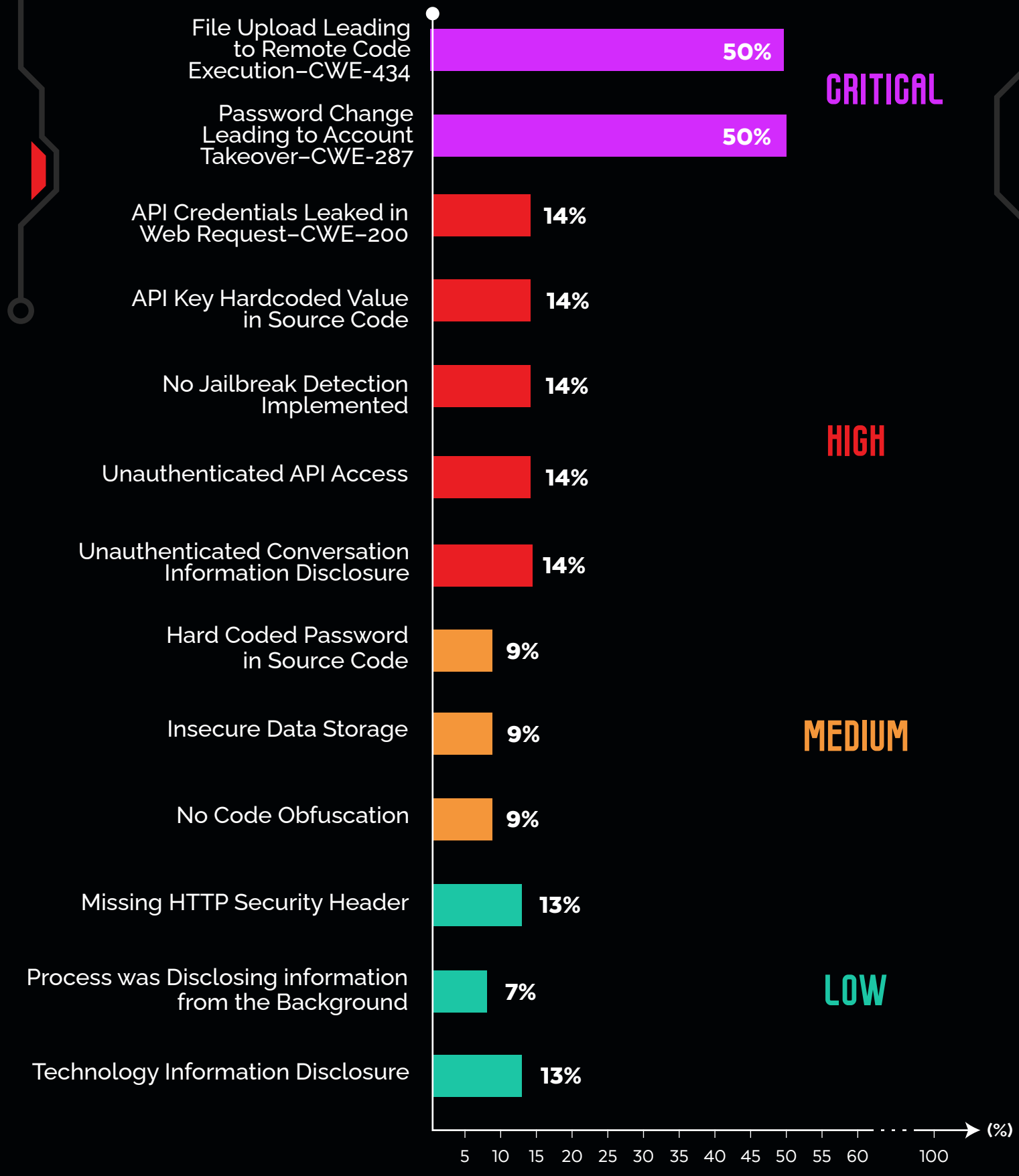


In 2025, the Insurance sector recorded a mix of findings across severity levels. Low severity issues accounted for 42.9%, primarily involving missing HTTP security headers, background process disclosures, and technology information leakage. Medium severity findings (31.4%) included hard-coded passwords, insecure data storage, and lack of code obfuscation.

Notably, High severity vulnerabilities represented 20% of findings, including exposed API credentials, hardcoded API keys, missing jailbreak detection, and unauthenticated access risks. Critical issues (5.7%) were identified as a file upload vulnerability leading to remote code execution and a password change flaw enabling account takeover.

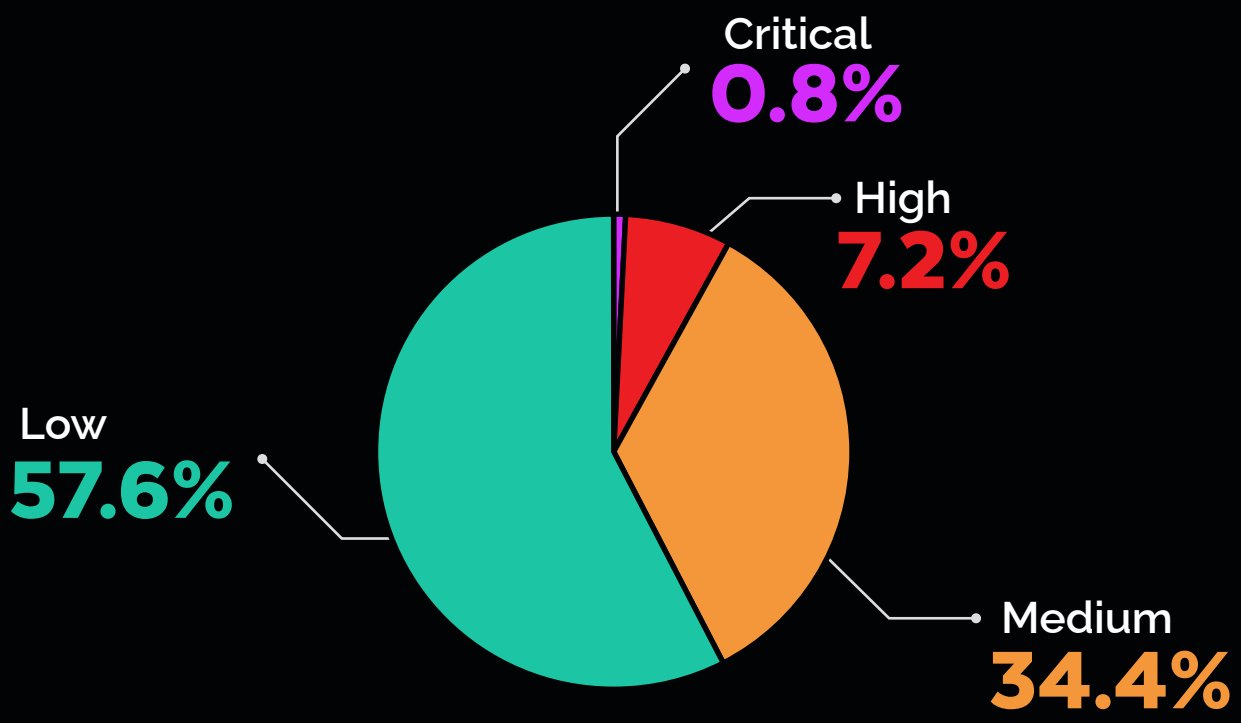
Although most findings were lower risk, the presence of high and critical vulnerabilities underscores the importance of secure coding practices, proper authentication controls, and proactive monitoring to protect sensitive customer data and maintain trust.

MOST PREVALENT VULNERABILITIES IN INSURANCE SECTOR



6. IT & TECHNOLOGY SECTOR

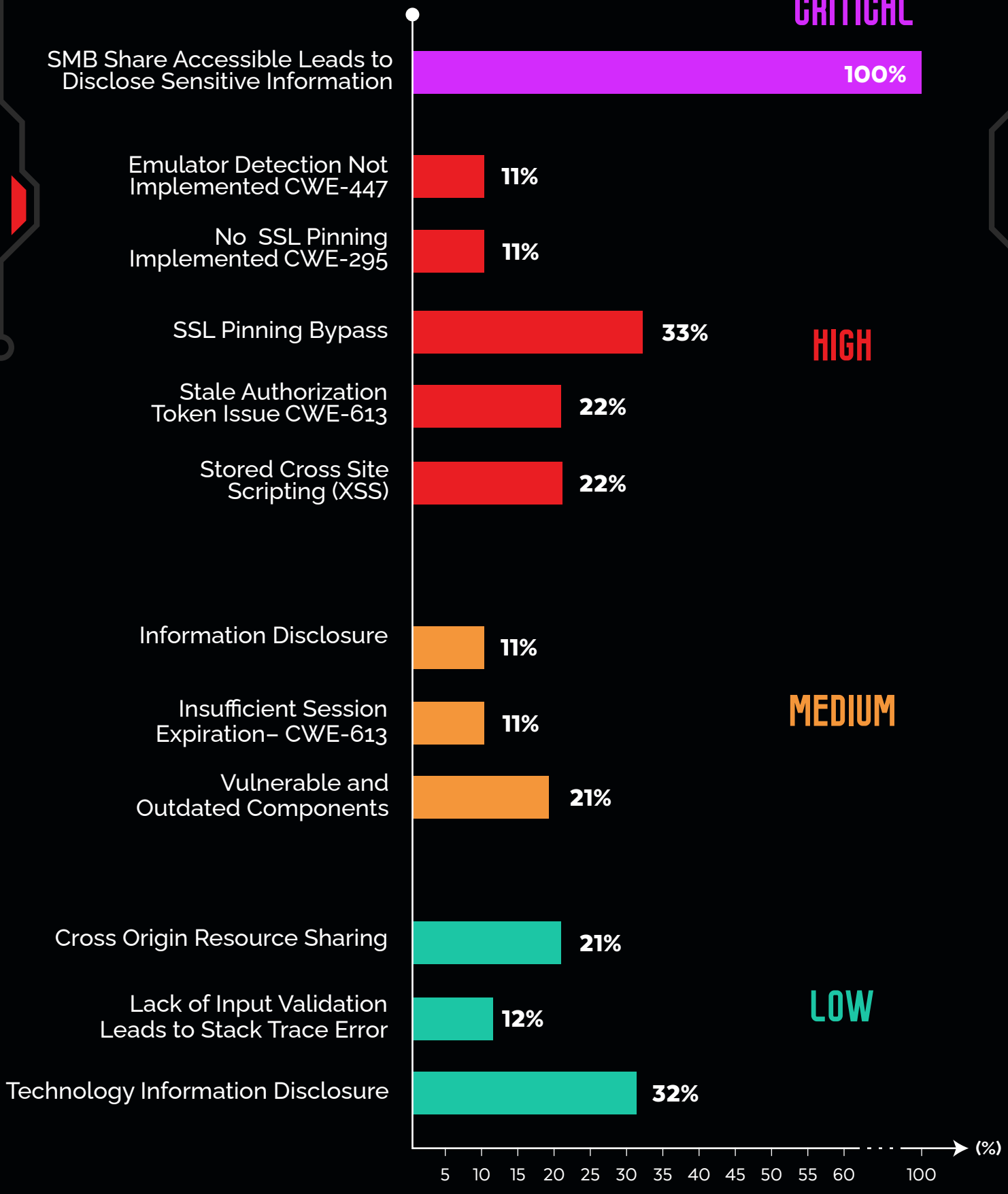
IT & Technology organizations develop and maintain the platforms, applications, and infrastructure that underpin modern business operations. Their central role in the digital ecosystem makes them prime targets for cyber threats, from data breaches to intellectual property theft and supply chain attacks.



In 2025, findings were mostly Low (57.6%) and Medium (34.4%) severity, reflecting recurring issues such as technology information disclosure, lack of input validation, insufficient session expiration, and outdated components. High severity vulnerabilities accounted for 7.2%, including SSL pinning bypass, stale authorization tokens, stored XSS, and missing emulator detection. One Critical vulnerability (0.8%) was identified, where an accessible SMB share could expose sensitive information.

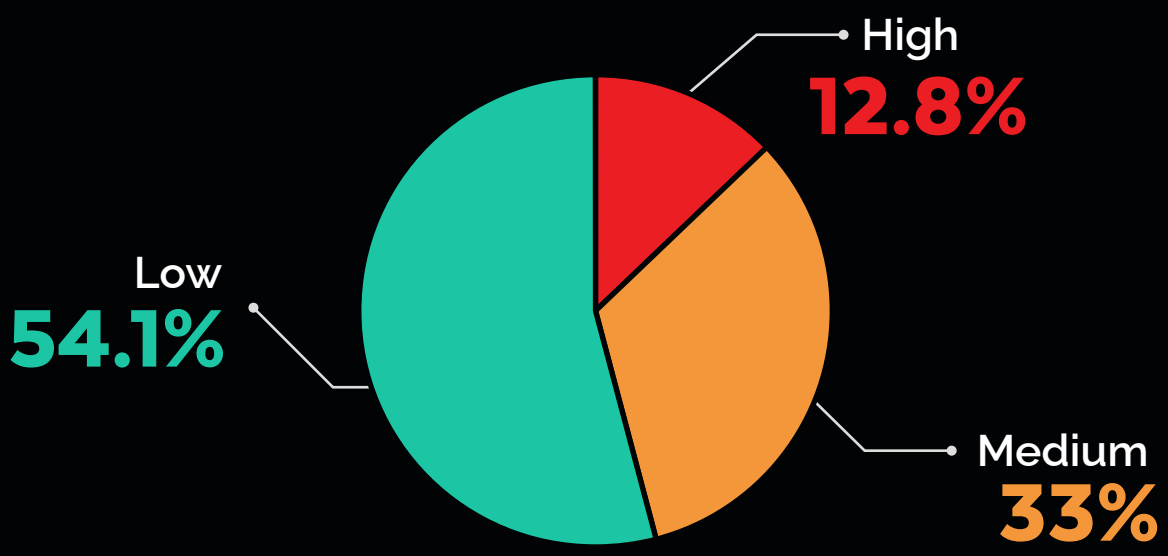
While most vulnerabilities were not critical, the presence of high-risk issues underscores the importance of secure coding, robust authentication controls, and continuous monitoring to reduce exposure and maintain trust across digital ecosystems.

MOST PREVALENT VULNERABILITIES IN IT & TECHNOLOGY SECTOR



7. MANUFACTURING SECTOR

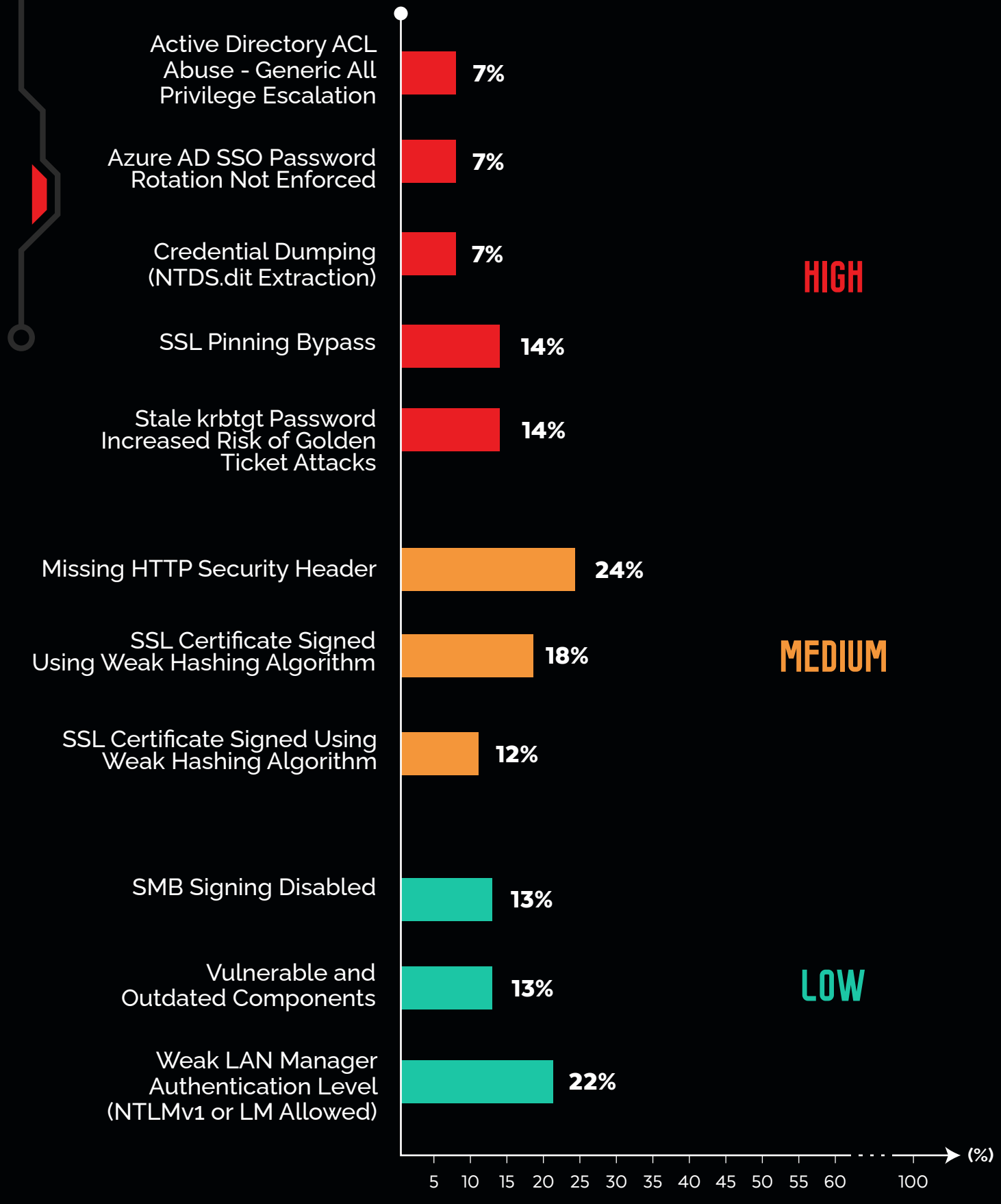
The manufacturing sector continues to modernize through automation and interconnected networks, increasing efficiency while expanding the attack surface. Protecting operational technology, proprietary designs, and sensitive business data remains critical to preventing financial losses, production disruptions, and intellectual property theft.



In 2025, most findings were Low (54.1%) and Medium (33.0%) severity, including technology information disclosure, vulnerable or outdated components, disabled SMB signing, and weak LAN manager authentication. High severity vulnerabilities accounted for 12.8%, with notable issues such as SSL pinning bypass, stale krbtgt passwords increasing golden ticket attack risk, credential dumping, Azure AD SSO password rotation gaps, and Active Directory ACL abuse.

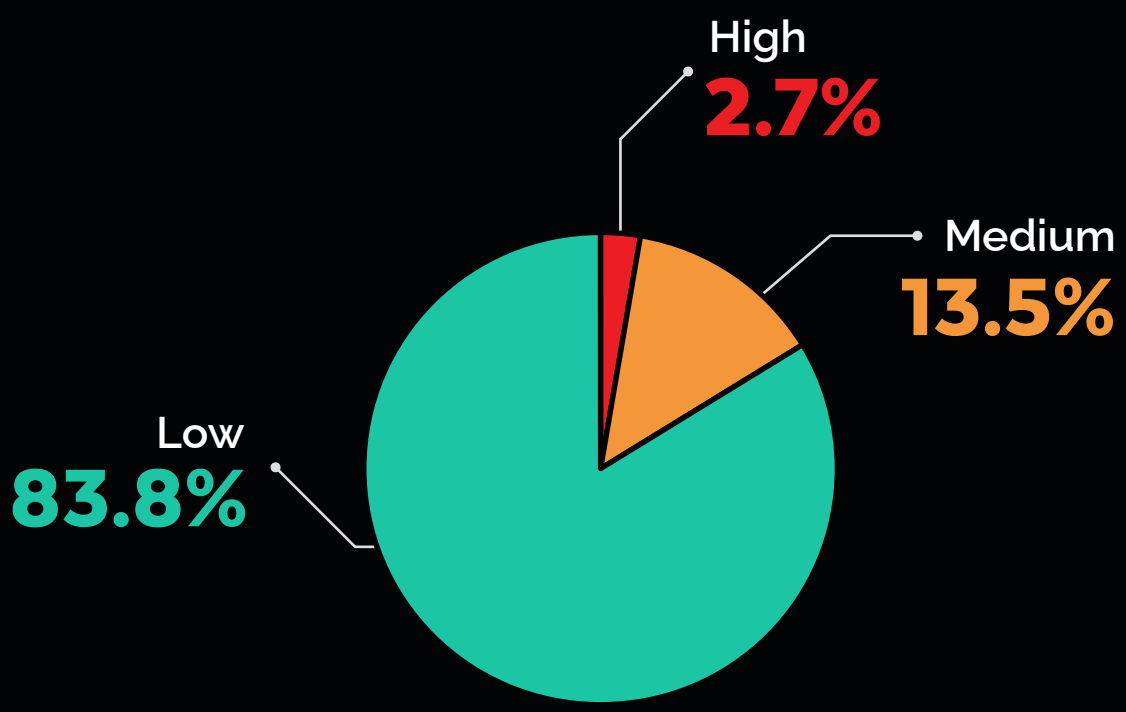
While no Critical vulnerabilities were reported, the presence of high-risk issues underscores the importance of enforcing secure authentication, strong access controls, and continuous monitoring to reduce exposure and strengthen overall cybersecurity posture in the sector.

MOST PREVALENT VULNERABILITIES IN MANUFACTURING SECTOR



8. TELECOMMUNICATIONS SECTOR

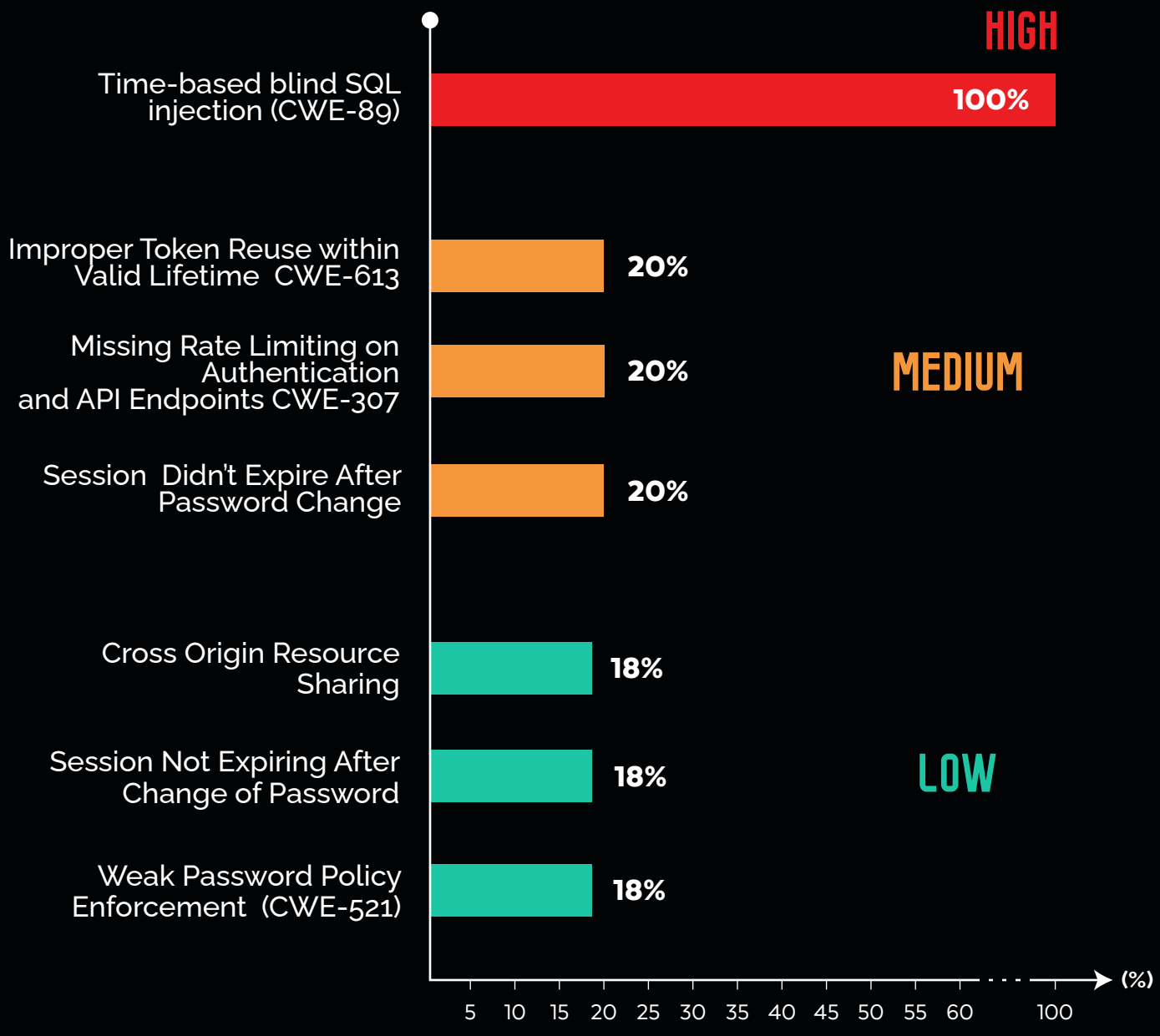
Telecommunications provide critical infrastructure for global connectivity, handling large volumes of sensitive user data such as call records, location information, and personal details. As networks become more software-driven, exposure to cyber threats, including financial fraud, espionage, and service disruption, continues to grow.



In 2025, the majority of findings were Low (83.8%), including weak password policies, session management issues, and CORS misconfigurations. Medium severity vulnerabilities accounted for 13.5%, such as improper token reuse, mssing rate limiting on authentication and API endpoints, and session expiration flaws. High severity findings were limited (2.7%), with a single time-based blind SQL injection identified.

While most vulnerabilities were lower risk, these findings highlight the importance of robust authentication, continuous monitoring, and proactive patch management to safeguard networks and maintain trust in telecommunications services.

MOST PREVALENT VULNERABILITIES IN TELECOMMUNICATIONS SECTOR



VULNERABILITY TRENDS YEAR-OVER-YEAR ANALYSIS (2024 - 2025)

The following analysis presents a comparative view of vulnerability trends observed between 2024 and 2025 across key industry sectors. By examining changes in the distribution of vulnerabilities by severity, this section highlights how organizational security postures have evolved over time.

The data reflects the impact of remediation efforts, improvements in security controls, and shifting threat patterns. While reductions in high and critical vulnerabilities may indicate stronger defensive measures, increases or persistence in medium and low severity findings point to ongoing gaps in foundational security practices.

Sector	Category	2023 (%)	2024 (%)	2025 (%)	Change (%)
Banking	Critical	4.6	0	0.2	0.2%
Banking	High	33.6	9	3	-97.0%
Banking	Medium	1.1	21	28.3	-71.7%
Banking	Low	44.5	64	68.5	-31.5%
Telecom	Critical	0	0	0	0%
Telecom	High	20	33	2.7	-97.3%
Telecom	Medium	20	0	13.5	13.5%
Telecom	Low	60	12	83.8	-16.2%
Education	Critical	0	0	0	0%
Education	High	24	1	28.6	-71.4%
Education	Medium	43	41	35.7	-64.3%
Education	Low	43	35	83.8	-64.3%

Sector	Category	2023 (%)	2024 (%)	2025 (%)	Change (%)
Government	Critical	6.4	6	0.0	-100.0%
Government	High	16.1	12	1.5	-98.5%
Government	Medium	33.5	26	32.4	-67.6%
Government	Low	4	50	66.2	-33.8%
Manufacturing	Critical	0	0	0	0%
Manufacturing	High	16.9	12	12.8	-87.2%
Manufacturing	Medium	48.2	31	33.0	-67.0%
Manufacturing	Low	34.9	63	54.1	-45.9%
Insurance	Critical	0	0	5.7	5.7%
Insurance	High	0	0	20.0	20.0%
Insurance	Medium	0	0	31.4	31.4%
Insurance	Low	0	0	42.9	42.9%
IT & Technology	Critical	0	0	0.8	0.8%
IT & Technology	High	15	20	7.2	-92.8%
IT & Technology	Medium	35.1	23	34.4	-65.6%
IT & Technology	Low	49.2	16	57.6	-42.4%

***Disclaimer:** In the % Change column, green indicates a decline in vulnerabilities (improved security), while red signals a rise in vulnerabilities since last year, pointing to worsened security.

The data reveals notable shifts in cybersecurity vulnerabilities across sectors from 2024 to 2025. While many sectors show marked improvements, some areas continue to face challenges.

- **Banking:** High-risk vulnerabilities dropped sharply by 97%, and medium-risk declined by 72%, indicating substantial improvements in core defenses. Low-risk issues also fell by 32%, showing attackers are finding fewer minor gaps. Critical vulnerabilities remained stable at 0.2%.

- **Telecom:** High-risk vulnerabilities decreased dramatically by 97 %, though medium-risk increased slightly by 14%, suggesting a minor shift in attack focus. Low-risk issues declined by 16%.

- **Education:** High-risk vulnerabilities fell by 71%, while medium and low risks dropped by 64%, reflecting a strengthened security posture.

- **IT & Technology:** High-risk issues dropped by 93%, and medium-risk declined by 66%, with low-risk vulnerabilities reducing by 42%, highlighting effective remediation of the sector's key attack surfaces. Critical vulnerabilities rose slightly by 0.8%, warranting ongoing monitoring.

- **Government:** High-risk issues decreased by 99%, medium by 68%, and low by 34%, though critical vulnerabilities fell entirely by 100%, reflecting a major focus on eliminating the most severe threats.

- **Manufacturing:** High and medium vulnerabilities fell by 87% and 67%, respectively, while low-risk issues decreased by 46%, showing strong mitigation efforts across the sector.

- **Healthcare:** Data for 2025 is not yet available.

- **Insurance:** High-risk vulnerabilities increased by 20%, medium by 31%, and low by 43%, while critical vulnerabilities rose by 5.7%, highlighting areas that require immediate attention.

These trends highlight the evolving threat landscape and reinforce the importance of continuous monitoring, targeted remediation, and adaptive security strategies to address both high-severity risks and recurring lower-severity vulnerabilities.

MOST COMMONLY DETECTED VULNERABILITIES

Across the assessed sectors, several vulnerability types appeared repeatedly, highlighting systemic gaps in security practices:

HIGH AND CRITICAL SEVERITY FINDINGS

- **SQL Injection & Stored XSS:** Found in Banking, Government, and IT/FinTech applications, exposing systems to unauthorized access and data manipulation.
- **Authentication & Access Control Weaknesses:** Including privilege escalation, broken access controls, and bypass of emulator/root detection in Banking, FinTech, Insurance, and IT sectors.
- **Remote Code Execution / Account Takeover Risks:** Critical issues observed in Insurance and IT/Technology environments, emphasizng the importance of secure input handling and file upload controls.

MEDIUM SEVERITY FINDINGS

- **Session and Token Management Issues:** Including improper session expiration and token reuse, affecting Banking, IT, Telecommunications, and FinTech applications.
- **Rate Limiting Gaps:** Leading to potential brute-force attacks, observed in Banking, Government, and FinTech platforms.
- **Outdated Components / Vulnerable Dependencies:** Common in IT, Manufacturing, and Government, increasing the likelihood of exploitation through known vulnerabilities.

LOW SEVERITY FINDINGS

- **Information Disclosure:** Technology information and configuration details exposed in Banking, IT, Manufacturing, and Education.
- **Missing Security Headers & Weak Cryptography:** Across multiple sectors, indicating gaps in basic hardening and secure communication practices.
- **Input Validation and CORS Issues:** Recurring in IT, Telecommunications, and Education systems, creating opportunities for recon and minor exploits.

This overview highlights that while the majority of vulnerabilities are low or medium severity, high and critical issues, though less frequently, the greatest risk. Organizations should focus on both remediating severe findings and addressing recurring lower-severity gaps to strengthen their overall security posture.

CONCLUSION

Cyber threats continue to evolve in both scale and sophistication, and organizational responses must keep pace. Recurring issues such as authentication weaknesses, gaps in access control, session management vulnerabilities, and unintended technology exposure remain prevalent, indicating that foundational security challenges are yet to be fully addressed.

High and critical severity findings, while less frequent, carry disproportionate risk. In sectors like Banking, Insurance, IT, and Manufacturing, a single exploited vulnerability can cascade into operational disruption, regulatory exposure, or lasting reputational damage. Meanwhile, the widespread prevalence of low and medium severity issues is a reminder that resilience is built through discipline, consistent patch management, secure coding standards, and rigorous configuration hygiene are not optional enhancements; they are baseline requirements.

Sector-specific patterns further reinforce why one-size-fits-all security approaches fall short. Financial and digital service platforms contend with sophisticated application-layer threats, while industrial and government environments face deeper exposure at the infrastructure and access control level. Effective security strategy must reflect these distinctions, not paper over them.

The path forward is not reactive, it is deliberate. Organizations that invest in continuous testing, enforce least-privilege access, embed security into the development lifecycle, and cultivate a security-aware culture are not just reducing risk; they are building competitive resilience. Every vulnerability addressed is an attack surface closed, and every proactive measure taken is a step ahead of adversaries who are constantly probing the next opening.