TISS
CYBERSECURITY
INSIGHTS

TRILLIUM
INFORMATION SECURITY SYSTEMS

PEN TEST
INSIGHTS REPORT
2023

TABLE OF CONTENTS

INTRODUCTION

In today's digital age, cybersecurity is paramount for organizations across all sectors. With evolving technologies and sophisticated cyber threats, mitigation of vulnerabilities is crucial. Penetration Testing provides valuable insights into security tools and configurations, ensuring compliance with industry standards.

In 2023, Trillium Information Security Systems (TISS) conducted penetration testing across various sectors, including banking, pharmaceuticals, telecom, and more. It covered a wide range of assets, including web applications, mobile apps, networks, databases, servers, and AWS cloud instances. TISS identified more than 2,000 vulnerabilities, categorized by severity levels, highlighting critical, high, medium, and low risks.

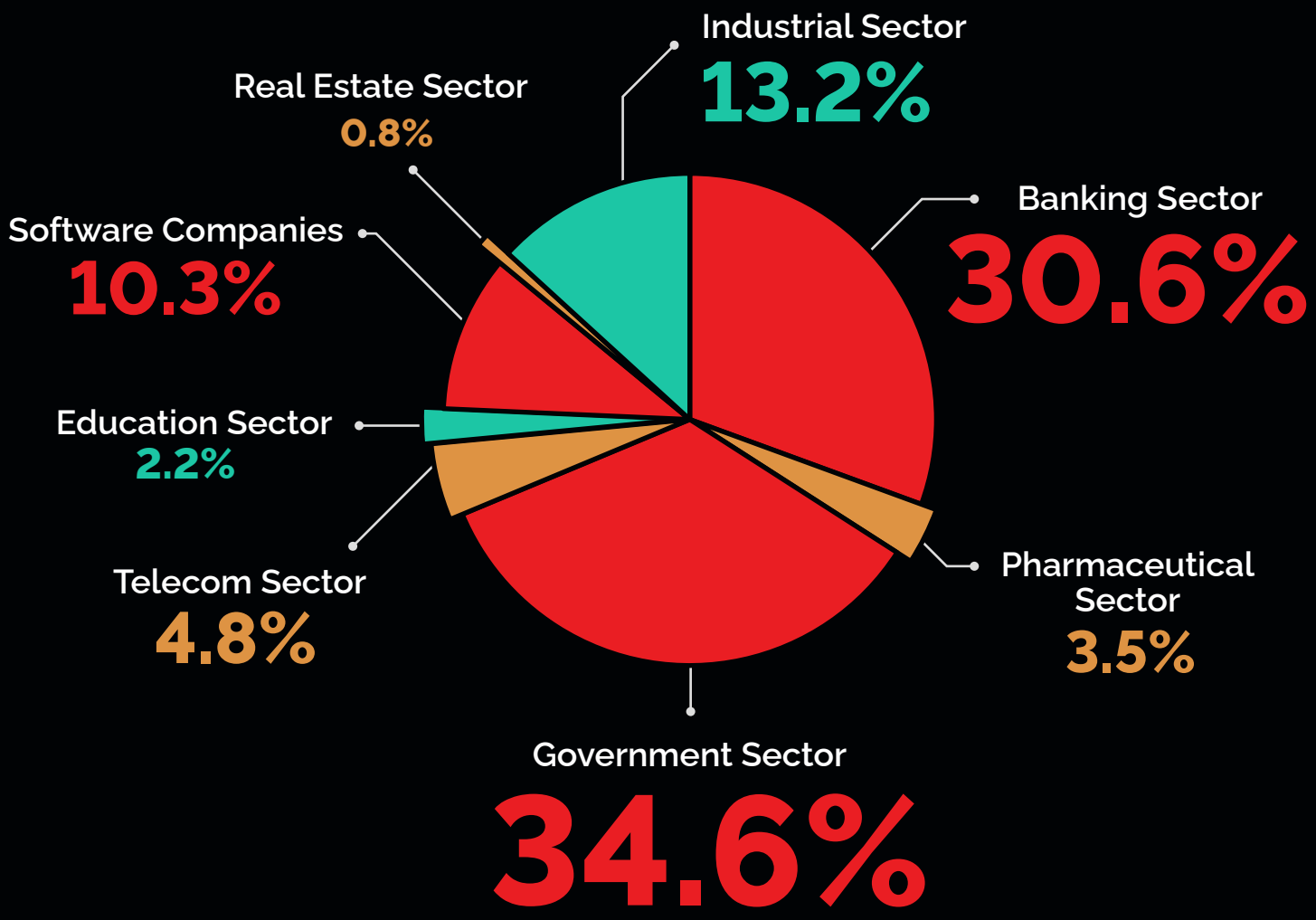
This report offers a comprehensive analysis of vulnerabilities across all sectors, shedding light on the cybersecurity landscapes. By detailing the count of assets tested and vulnerabilities identified, it provides insights into the most pressing cybersecurity challenges. These findings aim to help organizations understand their risks and develop targeted strategies to enhance their security posture.

By addressing vulnerabilities and implementing appropriate measures, organizations can safeguard their data, systems, and customers from cyber threats. This report serves as a valuable resource for organizations looking to strengthen their cybersecurity defenses.

ENGAGEMENT DEMOGRAPHIC

The dataset used in the analysis included several engagements focused on testing multiple organizations' information systems and networks. These engagements spanned across various industries, such as banking, real estate, education, and telecommunications to name a few. The government sector stood out with the highest number of assessments, representing roughly 34.6% of the total engagements, followed closely by the banking sector accounting for 30.6% of the total engagements. However, the importance of security assessment isn't lost on other sectors, though. For instance, sectors such as software, government, and telecommunications, are also actively adopting testing approaches to enhance their cybersecurity measures, demonstrating a growing commitment to their organization's cybersecurity. This trend is evident by their notable presence in the data of the total demographic.

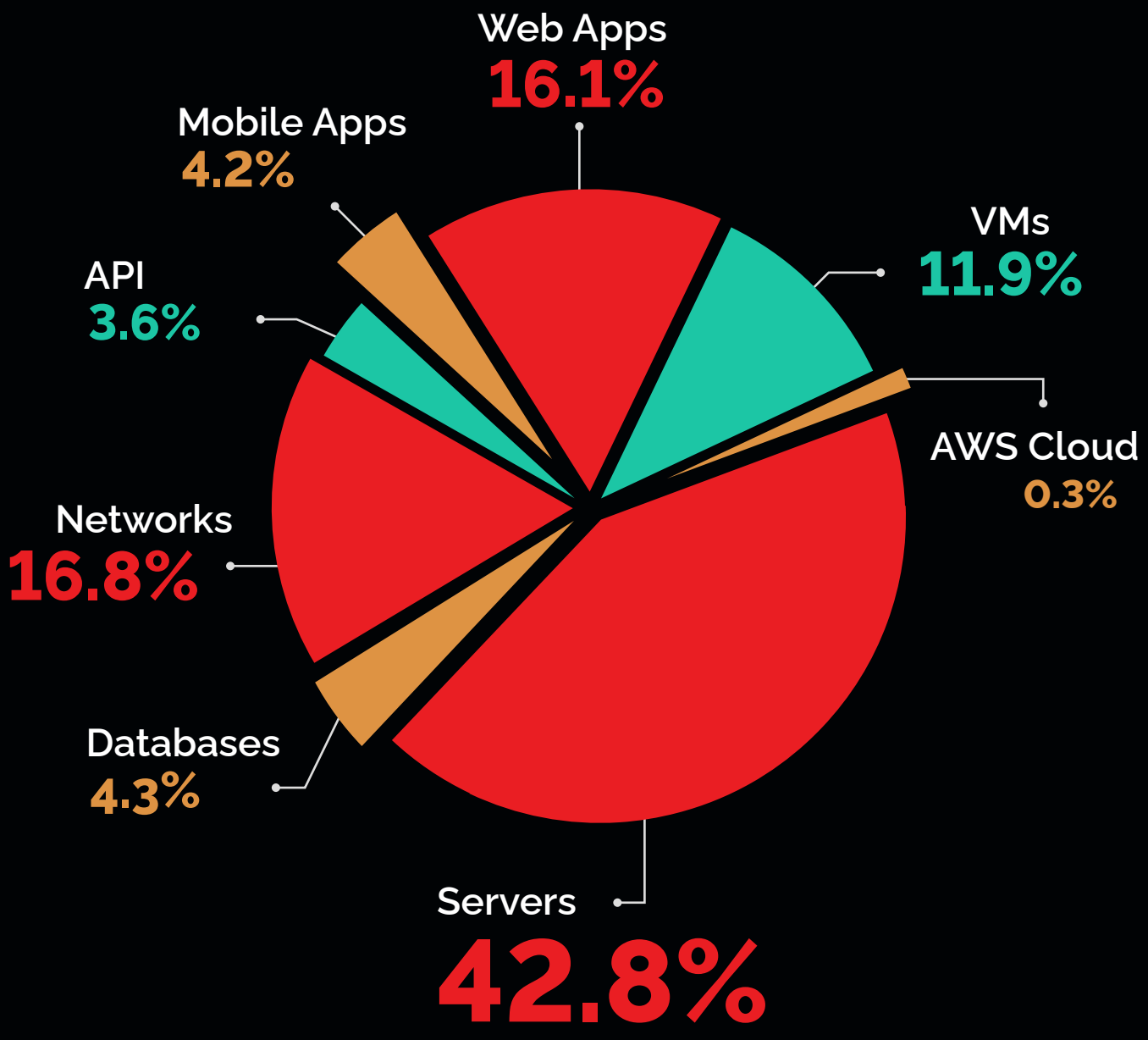
In total, TISS employees carried out and evaluated engagements involving 155 web applications, 40 mobile apps, 35 APIs, 161 networks, 42 databases, 411 servers, 3 AWS Cloud instances, and 114 VMs. These engagements identified 277 external vulnerabilities and 677 internal vulnerabilities across various sectors.



ENGAGEMENT SCOPE

In each penetration testing engagement, a crucial step is defining the scope, which involves identifying accessible networks, applications, databases, physical security controls, and other assets for the penetration tester to target. The predetermined scope outlines what will be assessed in each engagement. Servers, web applications, networks, and VMs were the most frequently tested items, accounting for about 87% of all engagements. API and AWS Cloud testing had the least engagement, each comprising only 5% and 0.4% of the total engagements conducted, respectively.

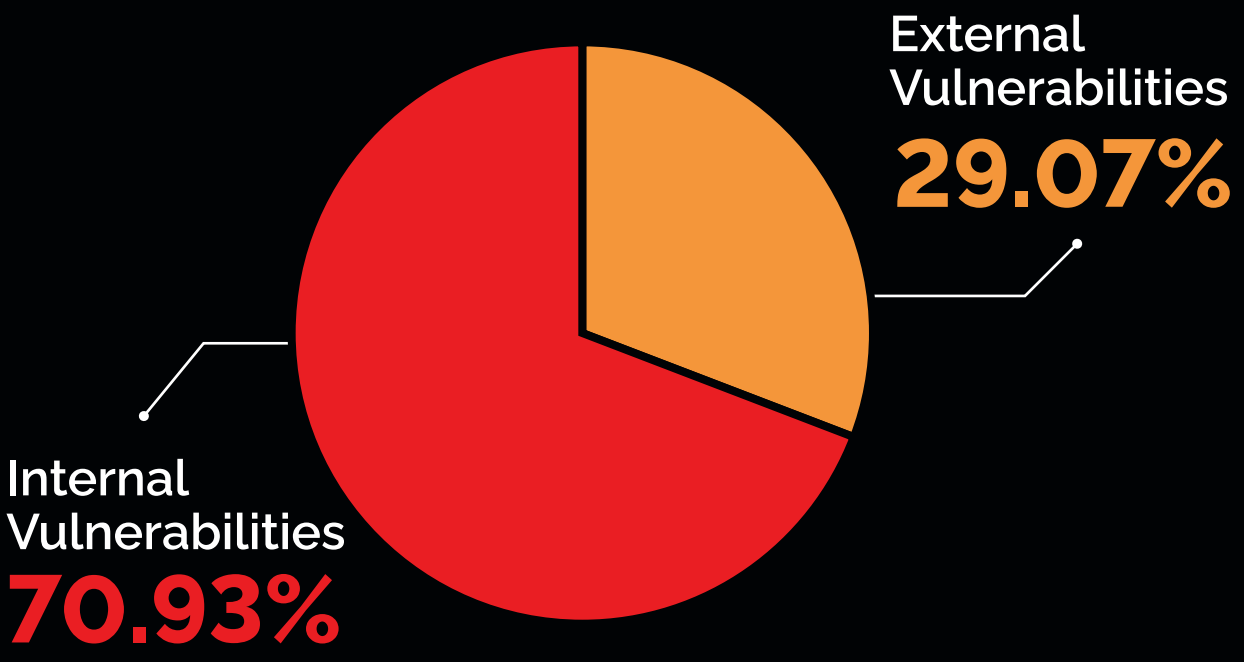
TOTAL ENGAGEMENTS



VULNERABILITIES IDENTIFIED

Our penetration testing included thorough assessments of both external and internal vulnerabilities in corporate information systems. External testers functioned as threat actors with internet access but lacked pre-existing privileges on the target system, allowing for a comprehensive evaluation from an external viewpoint. Their objective was to breach the network perimeter and gain access to resources on the local network. Internal penetration testers focused on a segment of the local network, aiming to gain control over the system infrastructure or critical resources as predetermined by the client.

By simulating realistic conditions, such testing provides an accurate assessment of the overall security posture. Most engagements, whether internal or external assessments, revealed at least one vulnerability exposed to potential attackers. Approximately 70.93% of vulnerabilities were identified in the internal scope, with the remainder in the external scope.



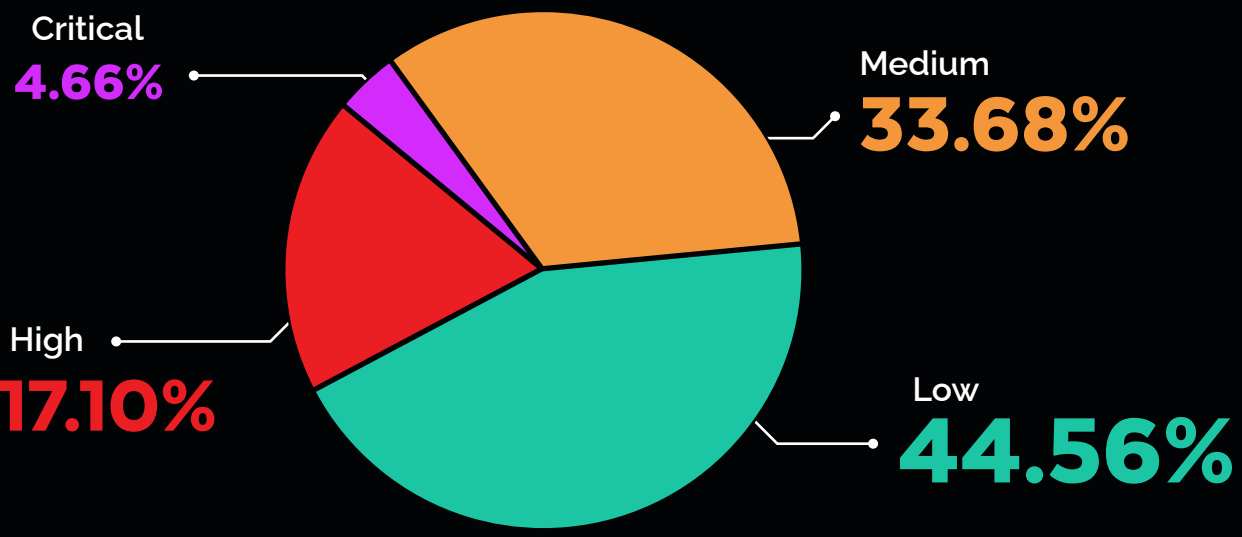
In external engagements, our testers often achieved internal access relatively easily, accomplishing this almost every time. While not every engagement aims for domain or enterprise administrative access, all internal assessments typically seek to prove access to sensitive data, a goal we often achieved. These statistics highlight the need for organizations to prioritize cybersecurity as a fundamental aspect of their management strategy. Without such prioritization, businesses risk operational, financial, and reputational damage due to potential breaches of confidentiality, integrity, and availability of information, products, and services. It is essential for organizations to position security at the heart of their culture to mitigate the threat of operational, financial, and reputational damage.

SECTOR-WISE VULNERABILITIES

Our analysis identifies sector-specific vulnerabilities, ensuring cybersecurity measures align effectively with each industry's distinct characteristics. This approach allows for targeted cybersecurity plans, enhancing overall security posture.

VULNERABILITIES IN THE BANKING SECTOR

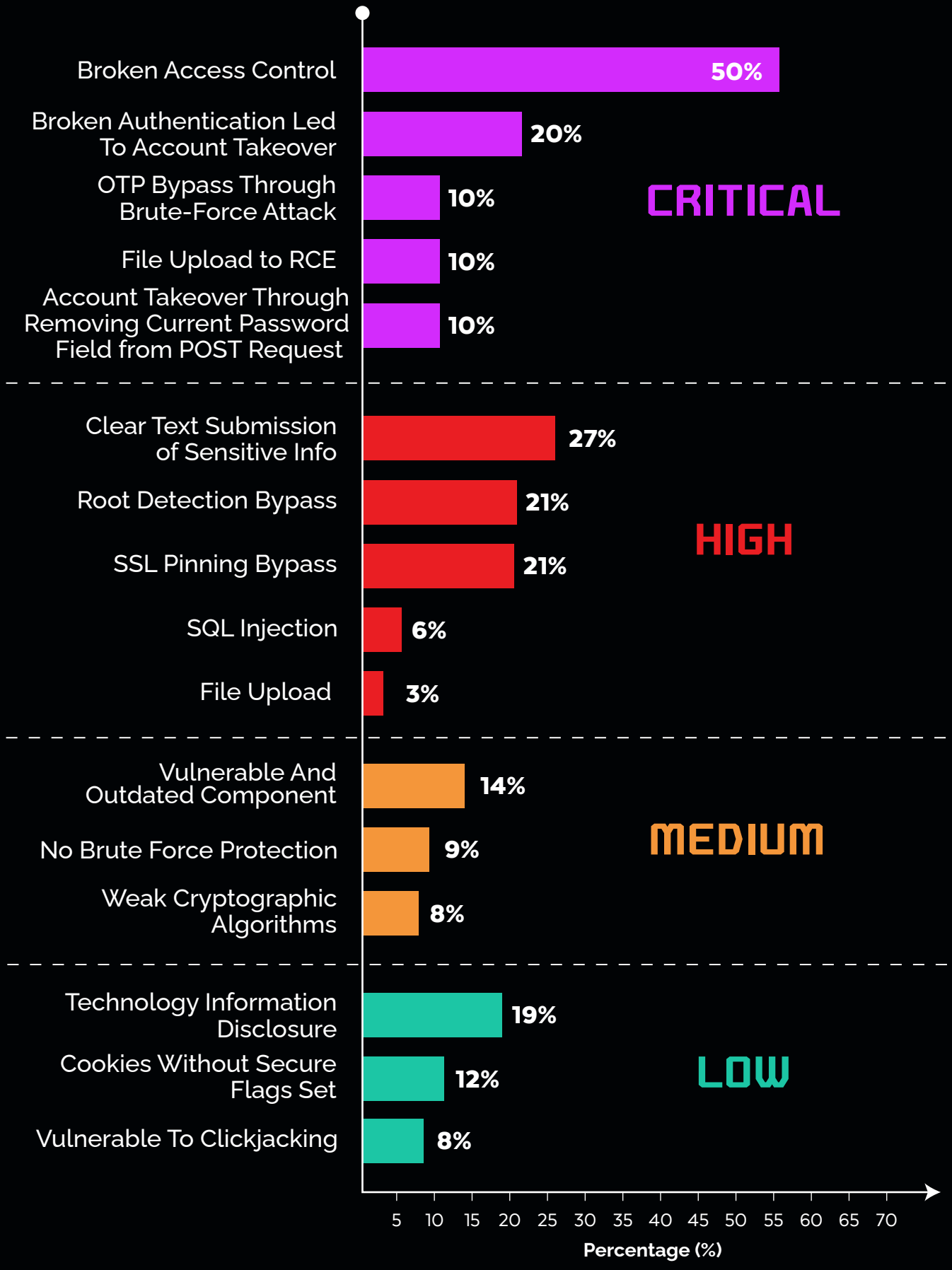
The banking sector plays a pivotal role in the economy, managing financial transactions and storing sensitive customer information. This sector is a prime target for cyber-attacks due to the potential for financial gain and access to valuable data. As such, it is imperative for banks to have robust cybersecurity measures in place to protect against threats.



Our testers found 4.66% critical vulnerabilities, along with 17.1% high, 33.68% medium, and 44.56% low vulnerabilities. These vulnerabilities ranged from issues with access control to vulnerabilities allowing for the uploading of files that could lead to remote code execution.

Specifically, in the web applications of these banks, vulnerabilities such as SQL injection, Insecure Direct Object References (IDOR), stored cross-site scripting (XSS), and disclosure of technology information were discovered. The mobile applications exhibited vulnerabilities, including broken authentication that could lead to account takeover, insecure handling of tokens, and methods to bypass jailbreak detection. Additionally, APIs were found to have vulnerabilities such as business logic vulnerabilities, disclosure of error messages, and insecure enforcement of authorization. The most frequent vulnerability found in the banking sector was 'Technology Information Disclosure.'

MOST PREVALENT VULNERABILITIES - BANKING SECTOR

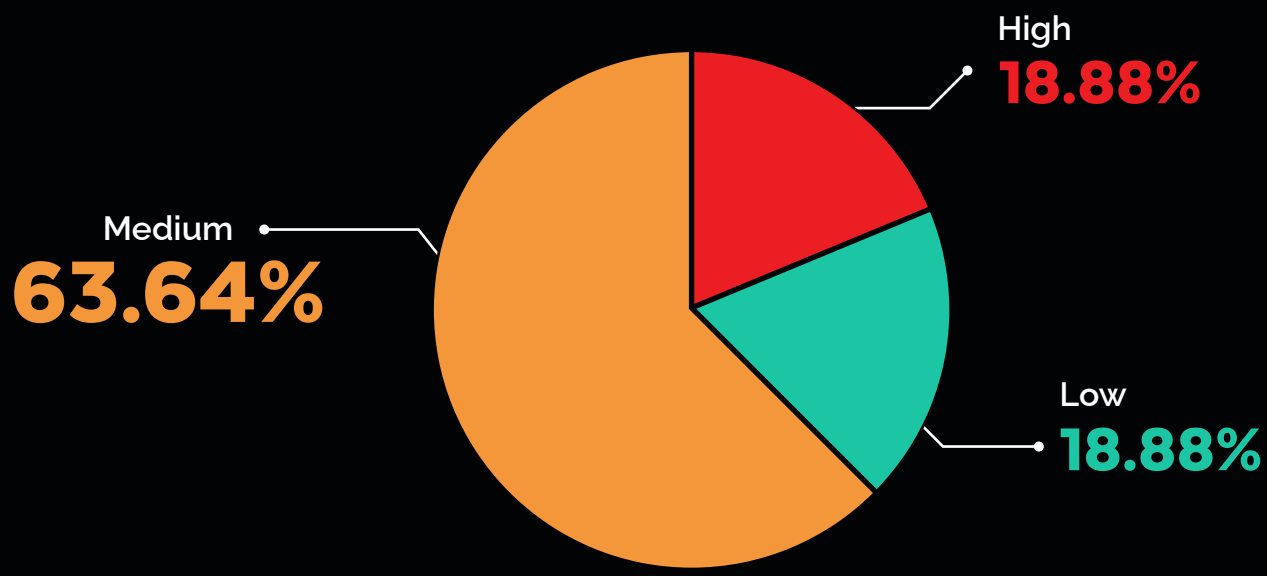


*Disclaimer: The graph displays the top 5 critical & high vulnerabilities, and top 3 medium & low vulnerabilities, or fewer if less were identified.

VULNERABILITIES IN THE PHARMACEUTICAL SECTOR

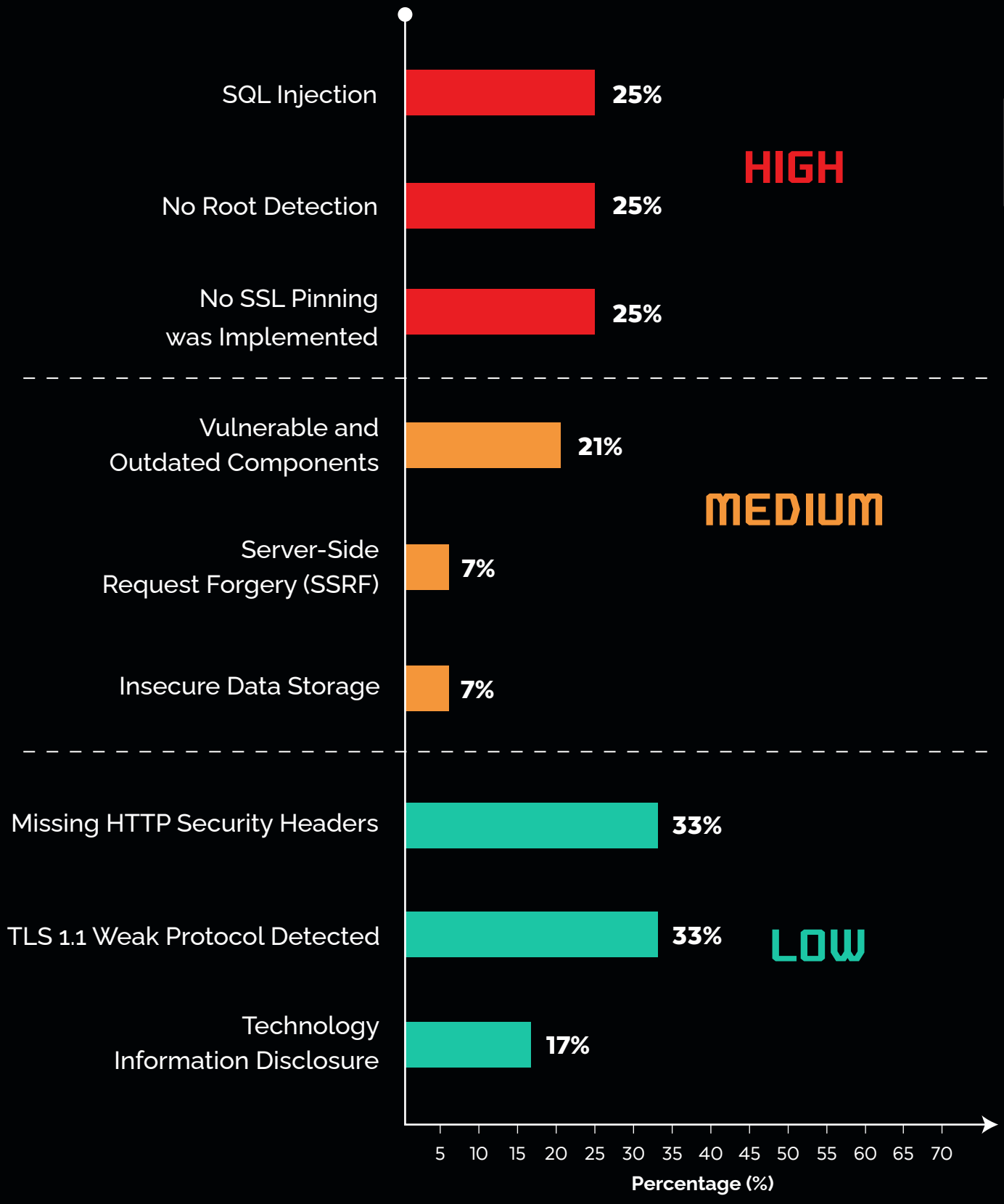
The pharmaceutical sector plays a critical role in researching, developing, and producing medications to treat and prevent diseases, contributing significantly to improving and saving lives globally. However, the pharmaceutical industry is increasingly vulnerable to cyber threats due to the sensitive nature of its research data, intellectual property, and patient information. Cybercriminals often target pharmaceutical companies to steal valuable research data, disrupt operations, or even tamper with drug development processes.

Our assessment revealed vulnerabilities across different parts of the digital infrastructure of the pharmaceutical sector. While no critical vulnerabilities were detected, we identified 18.88% high-risk vulnerabilities, 63.64% medium-risk vulnerabilities, and 18.88% low-risk vulnerabilities. These vulnerabilities include issues such as SQL injection, authentication brute force, WordPress XML-RPC interface server-side request forgery, and missing security headers.



The absence of critical vulnerabilities was a positive finding, indicating a baseline level of security. However, the presence of high and medium vulnerabilities highlights the need for improved security measures. These included risks like SQL injection and weak authentication methods, as well as missing security headers and outdated TLS protocols. Low-risk vulnerabilities like clickjacking and WordPress username disclosure were also discovered.

MOST PREVALENT VULNERABILITIES - PHARMACEUTICAL SECTOR

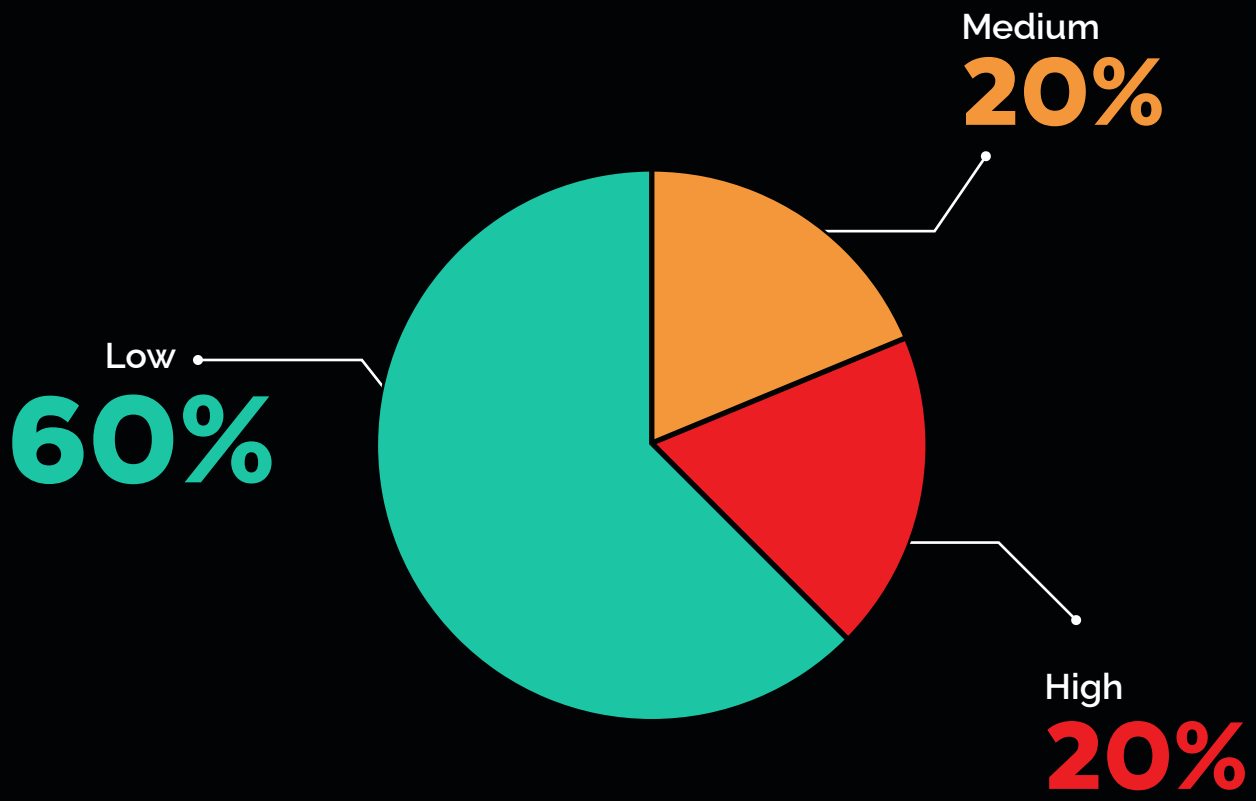


*Disclaimer: The graph displays the top 5 critical & high vulnerabilities, and top 3 medium & low vulnerabilities, or fewer if less were identified.

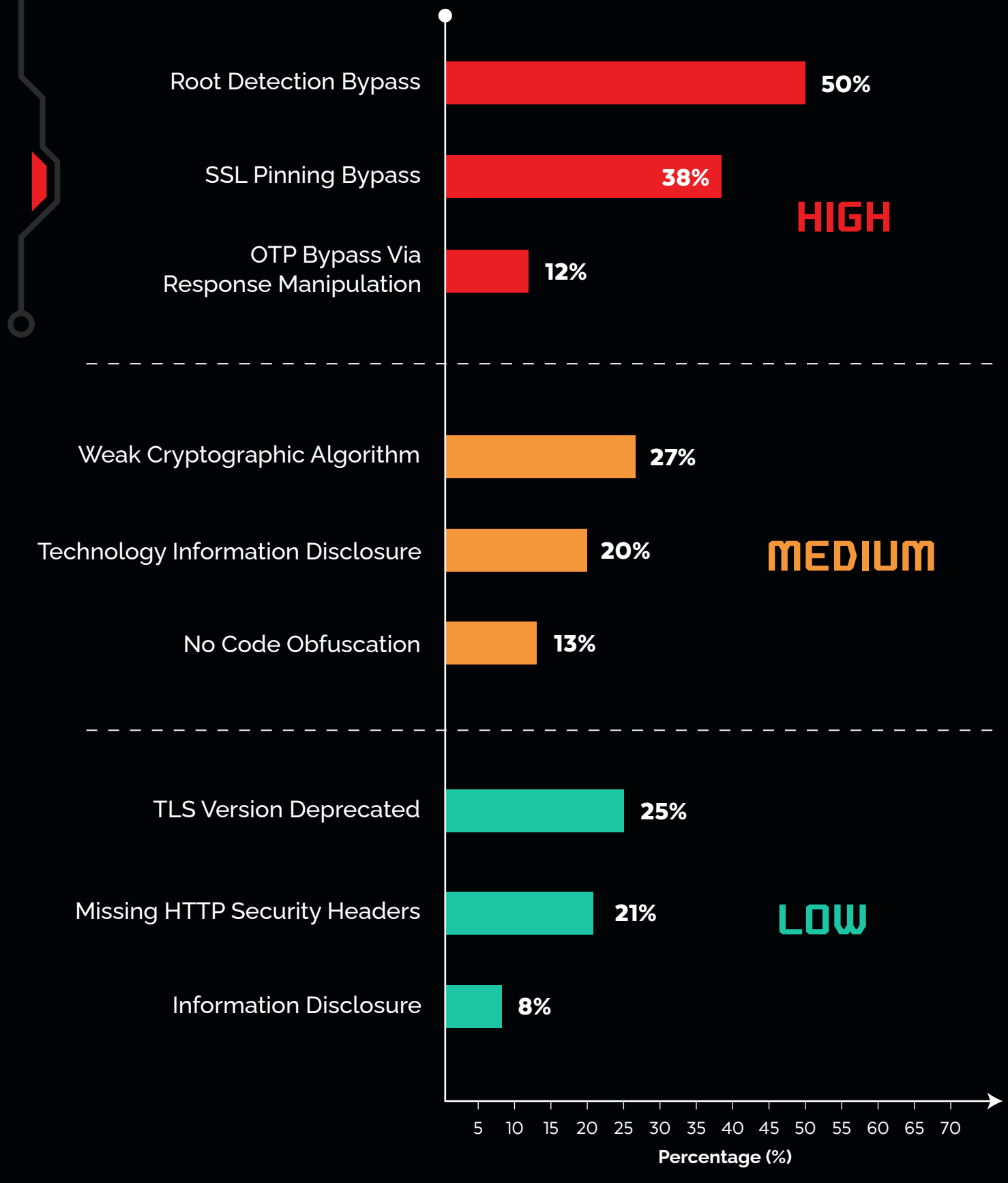
VULNERABILITIES IN THE TELECOM SECTOR

Telecom service providers construct, oversee, and maintain intricate network infrastructures for voice and data transmission. They manage vast amounts of sensitive information, rendering them prime targets for cyber-attacks. After conducting comprehensive tests on major national Telecom industries, we identified common patterns and the most prevalent vulnerabilities observed over the year.

While no critical vulnerabilities were found in the telecom sector, high vulnerabilities were identified in 20% areas, medium vulnerabilities in another 20% areas, and low vulnerabilities in the remaining 60% areas. These vulnerabilities encompass a range of issues, such as technology information disclosure, autocomplete enabled, forgot password CAPTCHA bypass, missing HTTP security headers, and detected deprecated TLS versions. After our teams conducted comprehensive tests, we identified common patterns and the most prevalent vulnerabilities observed over the year, which include Missing HTTP Security Headers, Root Detection Bypass, and Weak Cryptography Algorithms.



MOST PREVALENT VULNERABILITIES - TELECOM SECTOR

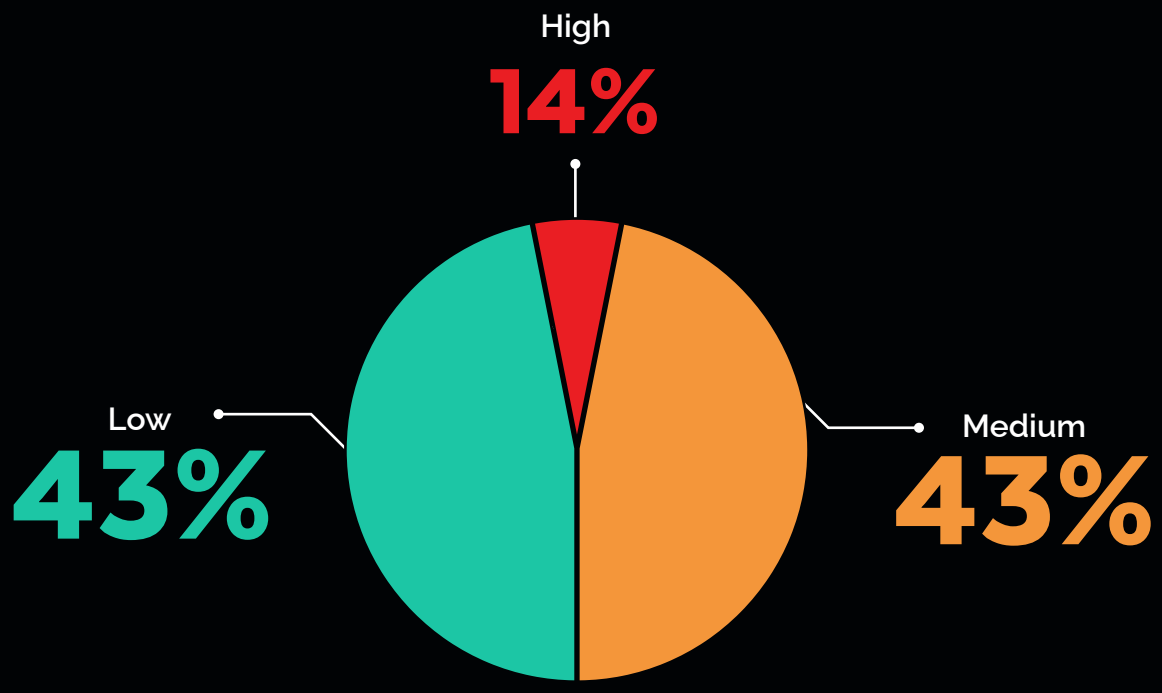


*Disclaimer: The graph displays the top 5 critical & high vulnerabilities, and top 3 medium & low vulnerabilities, or fewer if less were identified.

VULNERABILITIES IN THE EDUCATION SECTOR

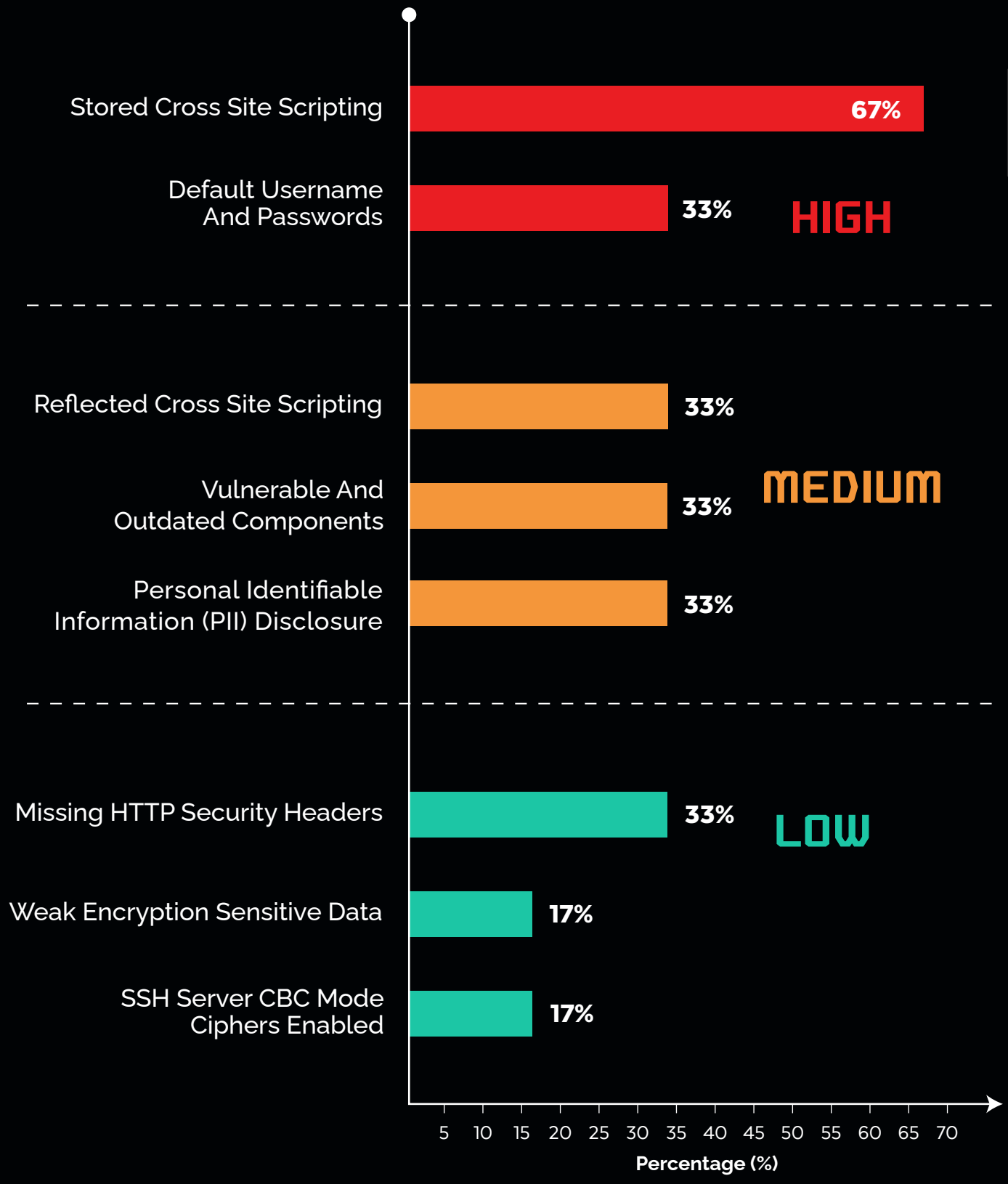
The education sector plays a vital role in society, overseeing a wide range of sensitive information about students, faculty, and administrative operations. This sector faces increasing cybersecurity challenges, given the digital transformation in education. Educational institutions are often targeted by cybercriminals seeking to access valuable data or disrupt operations.

Through our analysis of the education sector, we have identified no critical vulnerabilities, 14% high vulnerabilities, 43% medium vulnerabilities, and 43% low vulnerabilities. These vulnerabilities included source code and sensitive information disclosure through an exposed git directory, stored cross-site scripting, reflected cross-site scripting, vulnerable and outdated components, HTML injection, secure and HTTP Only flags not set, missing security headers, weak encoding scheme, cross-site request forgery (CSRF), file upload, and personal identifiable information (PII) disclosure.



The education sector assessment identified critical vulnerabilities that need immediate attention, including default usernames and passwords, weak encryption for sensitive data, and inadequate password policies. These issues could lead to unauthorized access and compromise system integrity. Additionally, outdated software versions and weak key exchange algorithms in SSH servers were found, posing security risks.

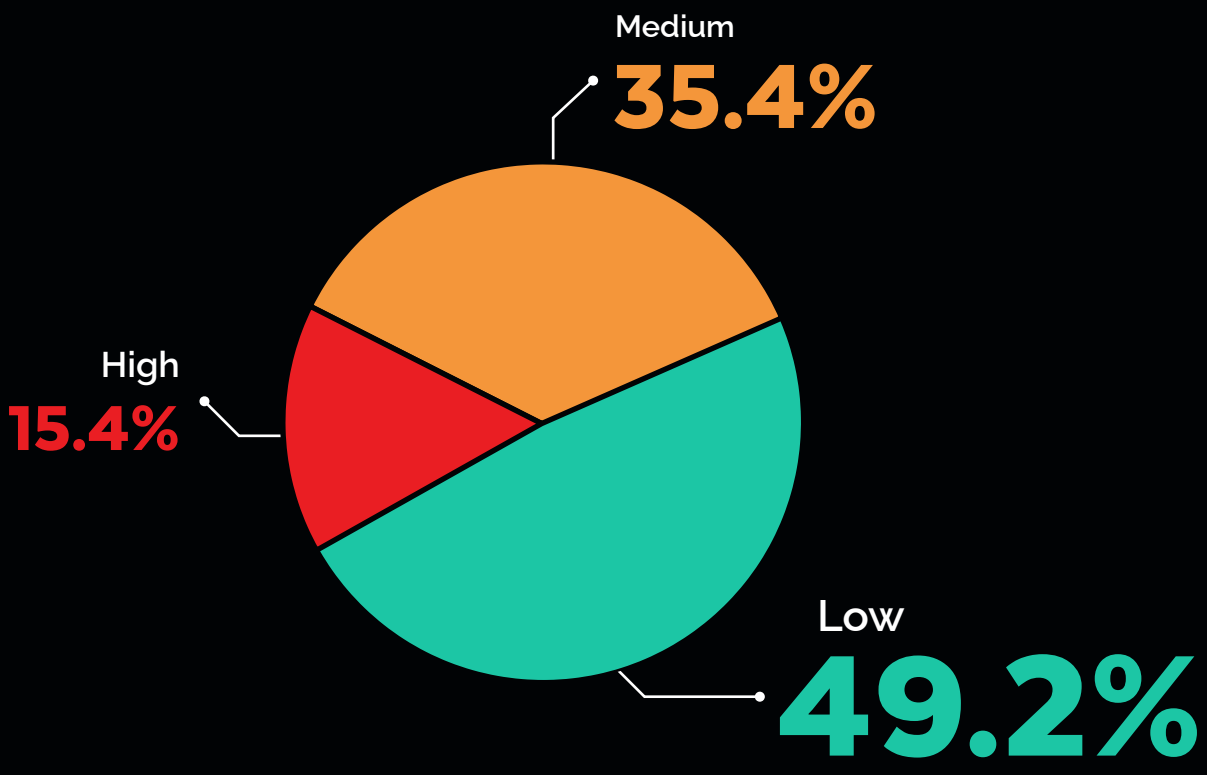
MOST PREVALENT VULNERABILITIES – EDUCATION SECTOR



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

VULNERABILITIES IN THE SOFTWARE COMPANIES

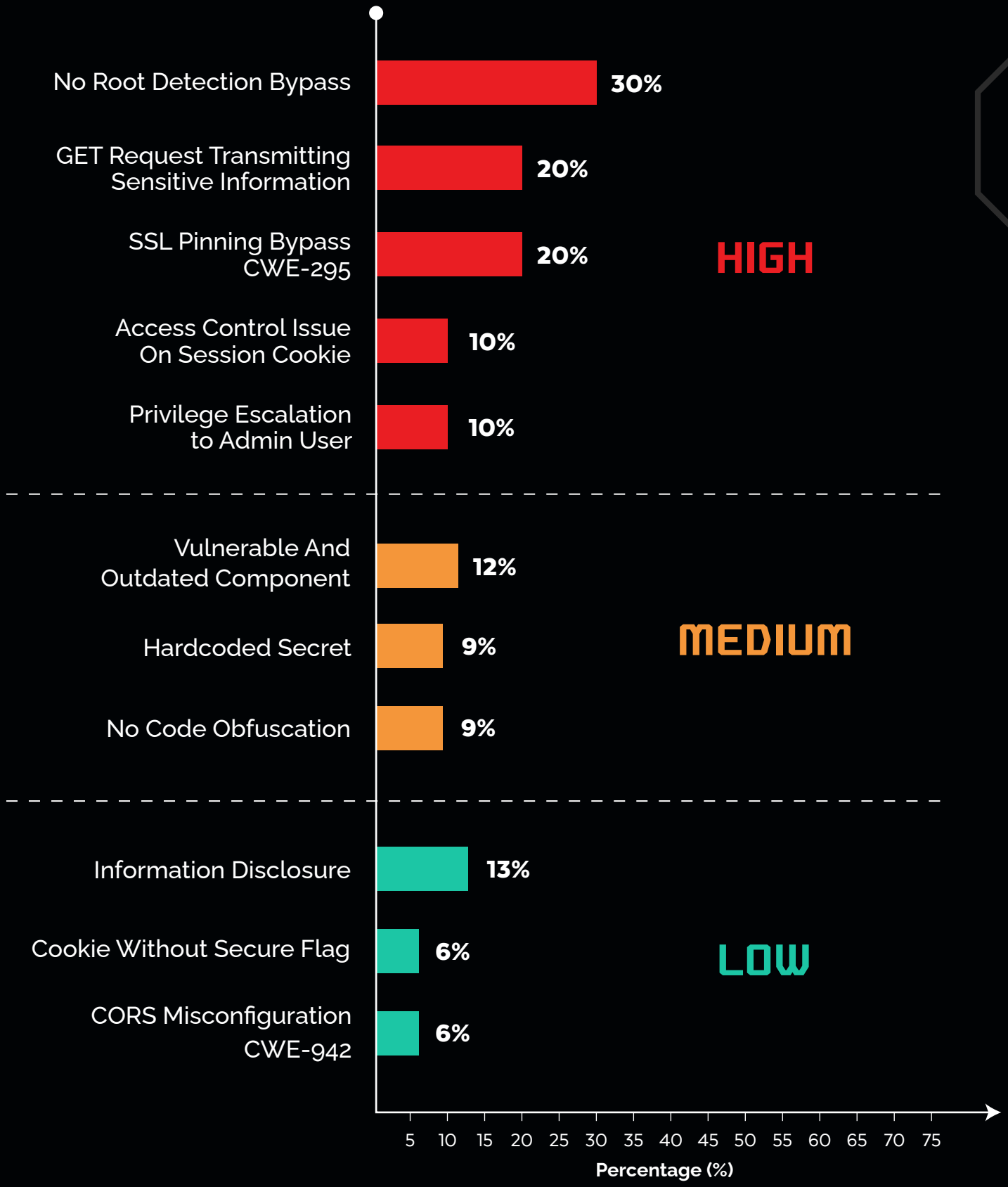
In software companies, vulnerabilities were identified across web applications, mobile apps, and APIs. Critical vulnerabilities were not found, but high vulnerabilities were identified in 15.4% areas, medium vulnerabilities in 35.4% areas, and low vulnerabilities in 49.2% areas. These vulnerabilities include privilege escalation to admin user, access control issue on session cookie, vulnerable and outdated versions, and smart contract vulnerabilities.



Beyond the critical, high, medium, and low vulnerabilities already mentioned, additional issues were discovered. These included vulnerabilities related to weak encoding schemes, which could expose sensitive data to unauthorized access. Furthermore, certain applications were found to lack proper security headers, leaving them more susceptible to attacks like cross-site scripting (XSS) and clickjacking. In some cases, the absence of secure and HTTP-only flags on cookies was noted, increasing the risk of session hijacking and other related attacks.

Furthermore, the assessment identified vulnerabilities in file upload mechanisms, which could enable malicious actors to upload and execute arbitrary files on the system. Additionally, instances of personal identifiable information (PII) disclosure were discovered, indicating weaknesses in data protection practices.

MOST PREVALENT VULNERABILITIES - SOFTWARE COMPANIES

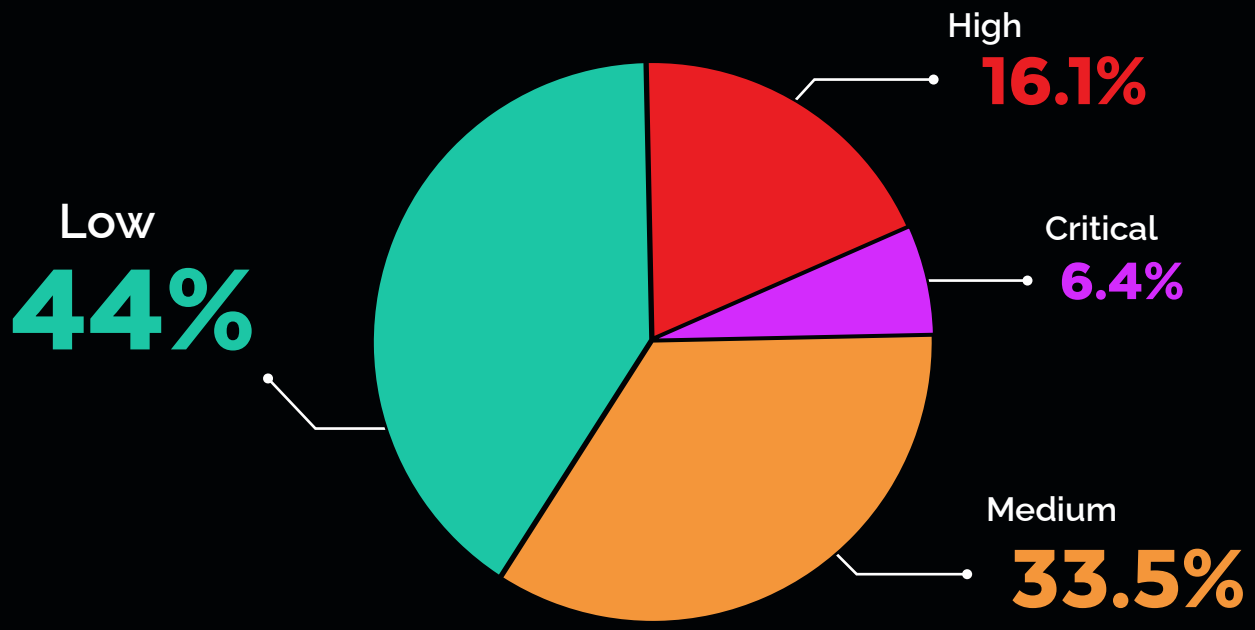


*Disclaimer: The graph displays the top 5 critical & high vulnerabilities, and top 3 medium & low vulnerabilities, or fewer if less were identified.

VULNERABILITIES IN THE GOVERNMENT SECTOR

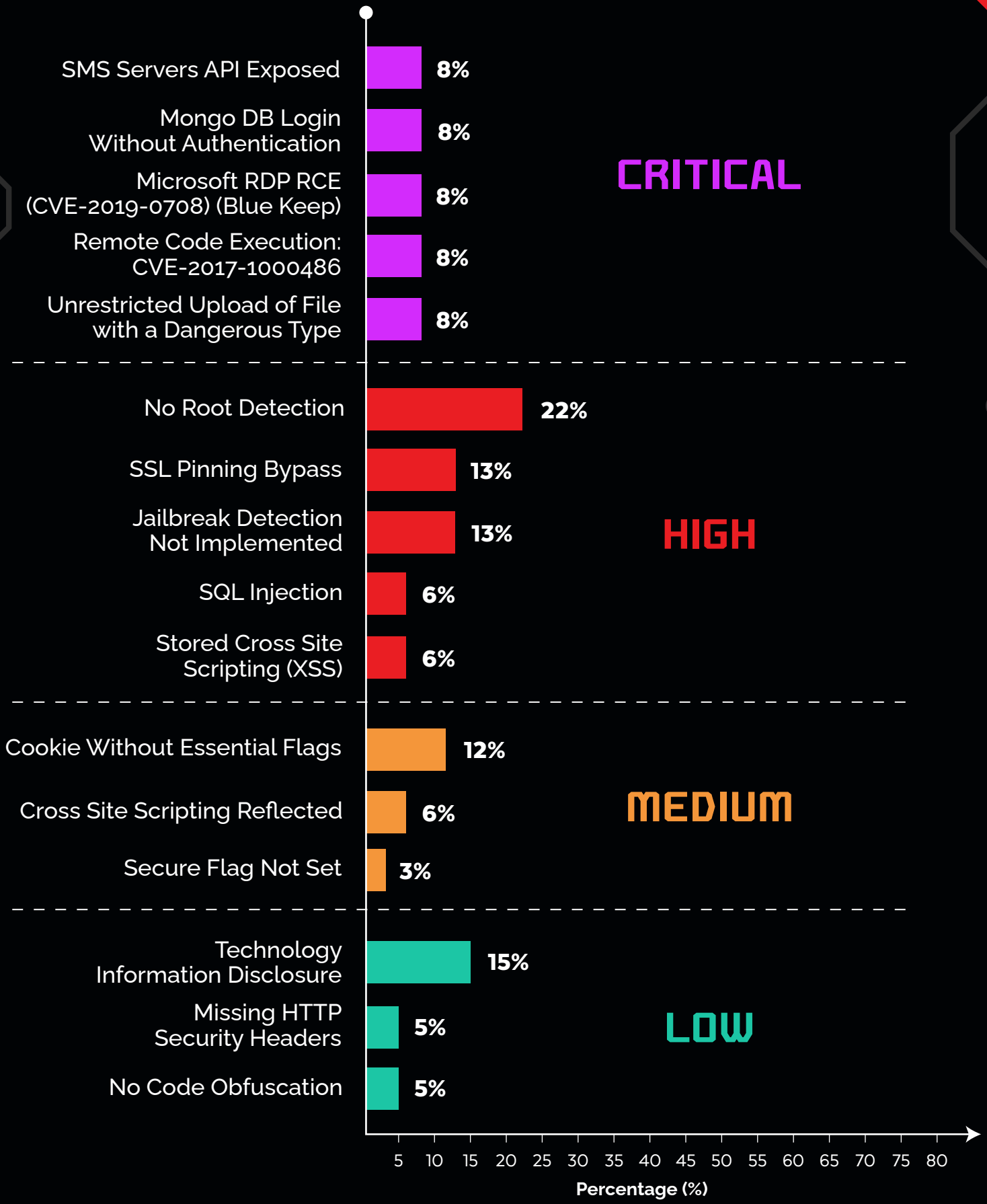
As central authority, government entities collect and store vast amounts of sensitive information, making them attractive targets for cybercriminals and anti-state-sponsored actors. Government systems are often interconnected, creating a broad attack surface that can be exploited. Moreover, the political nature of government operations can make them targets for cyberattacks seeking to disrupt operations or steal sensitive information for political gain. The importance of securing government systems against cyber threats cannot be overstated, as a breach can have far-reaching consequences on national security, economic stability, and public trust.

In the government sector, critical vulnerabilities, such as default credentials and SQL injection, were identified, which could potentially allow malicious actors to gain unauthorized access to sensitive government systems. High and medium vulnerabilities, including response manipulation and file upload restrictions bypass, were also discovered, highlighting the need for improved security measures within government agencies.



In the world of cybersecurity, the numbers paint a vivid picture: a comprehensive audit of the government sector revealed 6.4% critical, 16.1% high, 33.5% medium, and 44% low vulnerabilities across a range of applications and systems, including web and mobile apps, APIs, networks, databases, and servers.

MOST PREVALENT VULNERABILITIES - GOVERNEMNT SECTOR

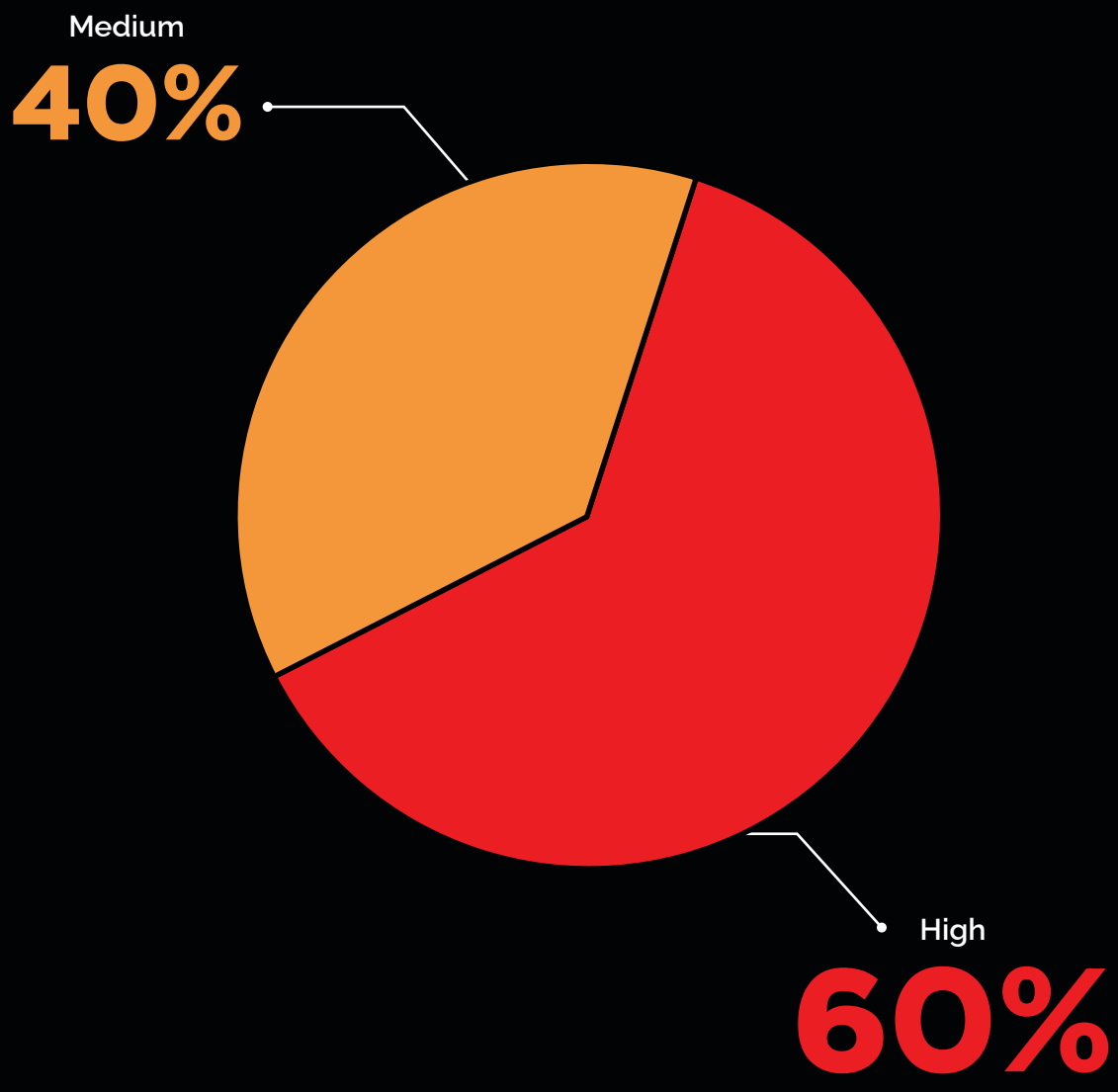


*Disclaimer: The graph displays the top 5 critical & high vulnerabilities, and top 3 medium & low vulnerabilities, or fewer if less were identified.

VULNERABILITIES IN THE REAL ESTATE SECTOR

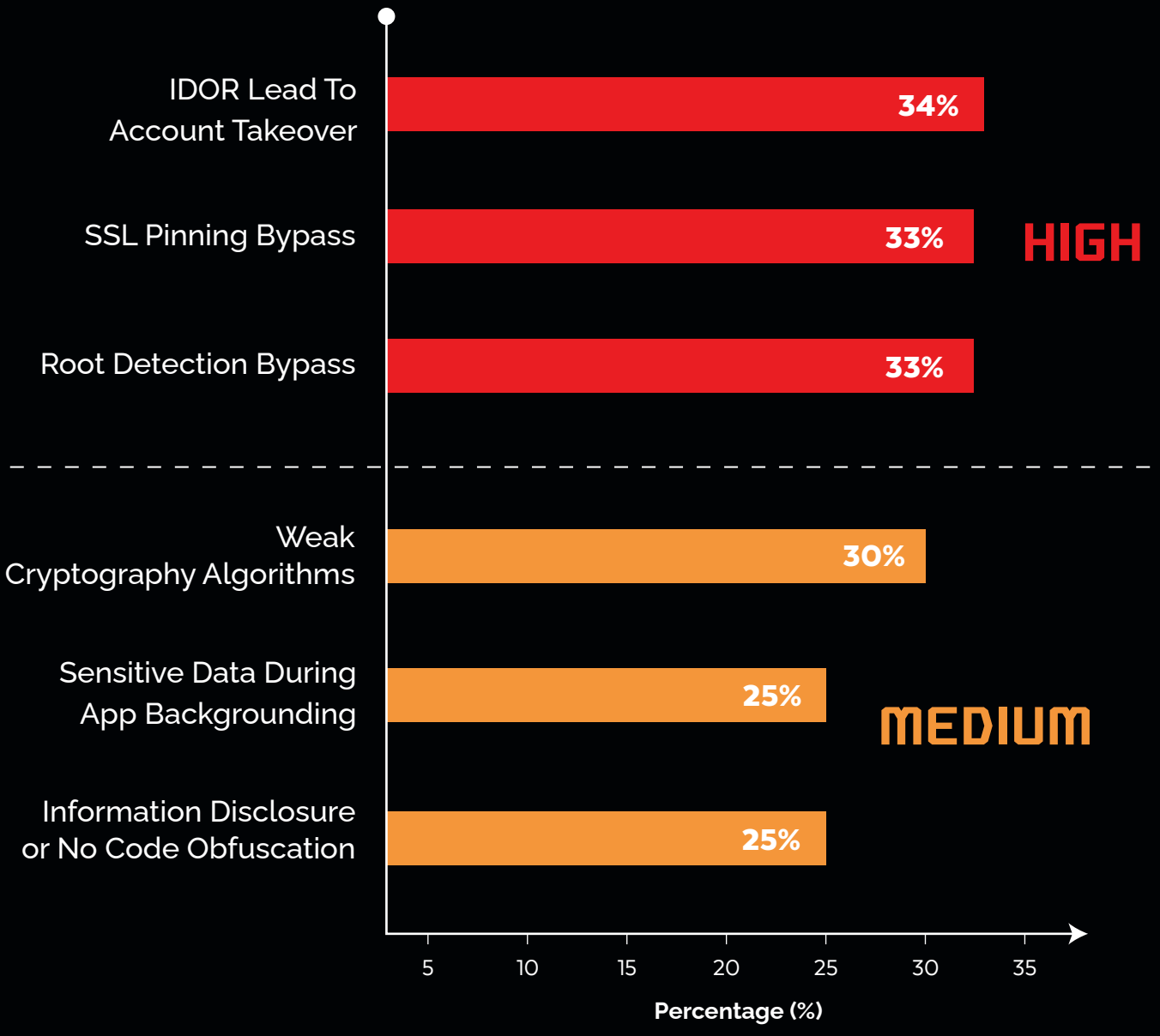
The real estate sector facilitates the buying, selling, and renting of property. It is increasingly susceptible to cyber threats due to its reliance on digital technologies. Real estate transactions involve the exchange of sensitive financial and personal information, making them attractive targets for cybercriminals. Not only that, but the sector's use of Internet of Things (IoT) devices in smart buildings and property management systems increases the potential attack surface.

The vulnerability assessment identified 60% high-risk vulnerabilities and 40% medium-risk vulnerabilities across the real estate sector. These vulnerabilities range from root detection bypasses and SSL pinning bypasses to insecure storage, insecure pasteboard, information disclosure, and exposure of sensitive data during app backgrounding.



Among the vulnerabilities discovered, the most prevalent ones were root detection and SSL pinning bypasses that could lead to unauthorized access and data breaches. Additionally, insecure storage and pasteboard usage highlighted the sector's need for improved data protection. Other significant vulnerabilities included information disclosure and sensitive data exposure during app backgrounding.

MOST PREVALENT VULNERABILITIES – REAL ESTATE SECTOR

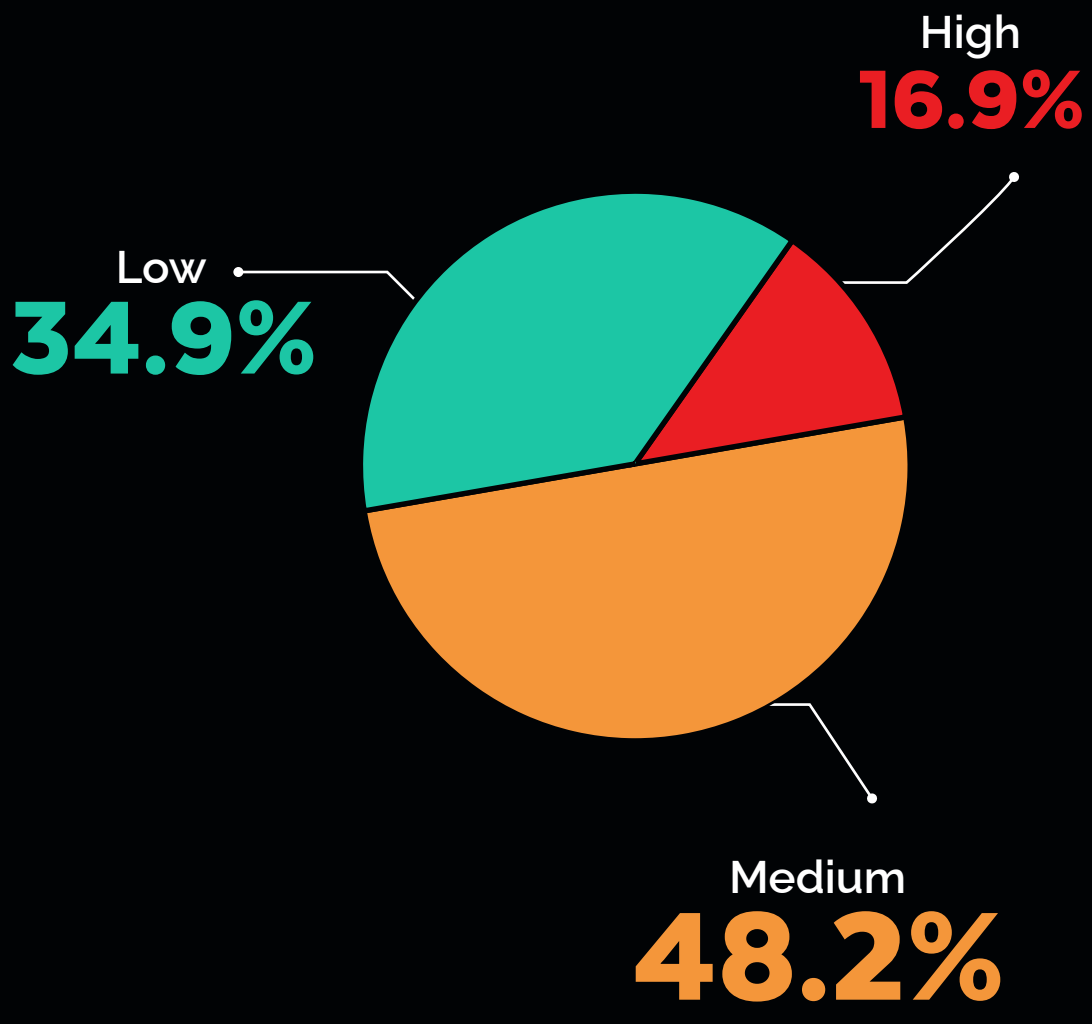


*Disclaimer: The graph displays the top 5 critical & high vulnerabilities, and top 3 medium & low vulnerabilities, or fewer if less were identified.

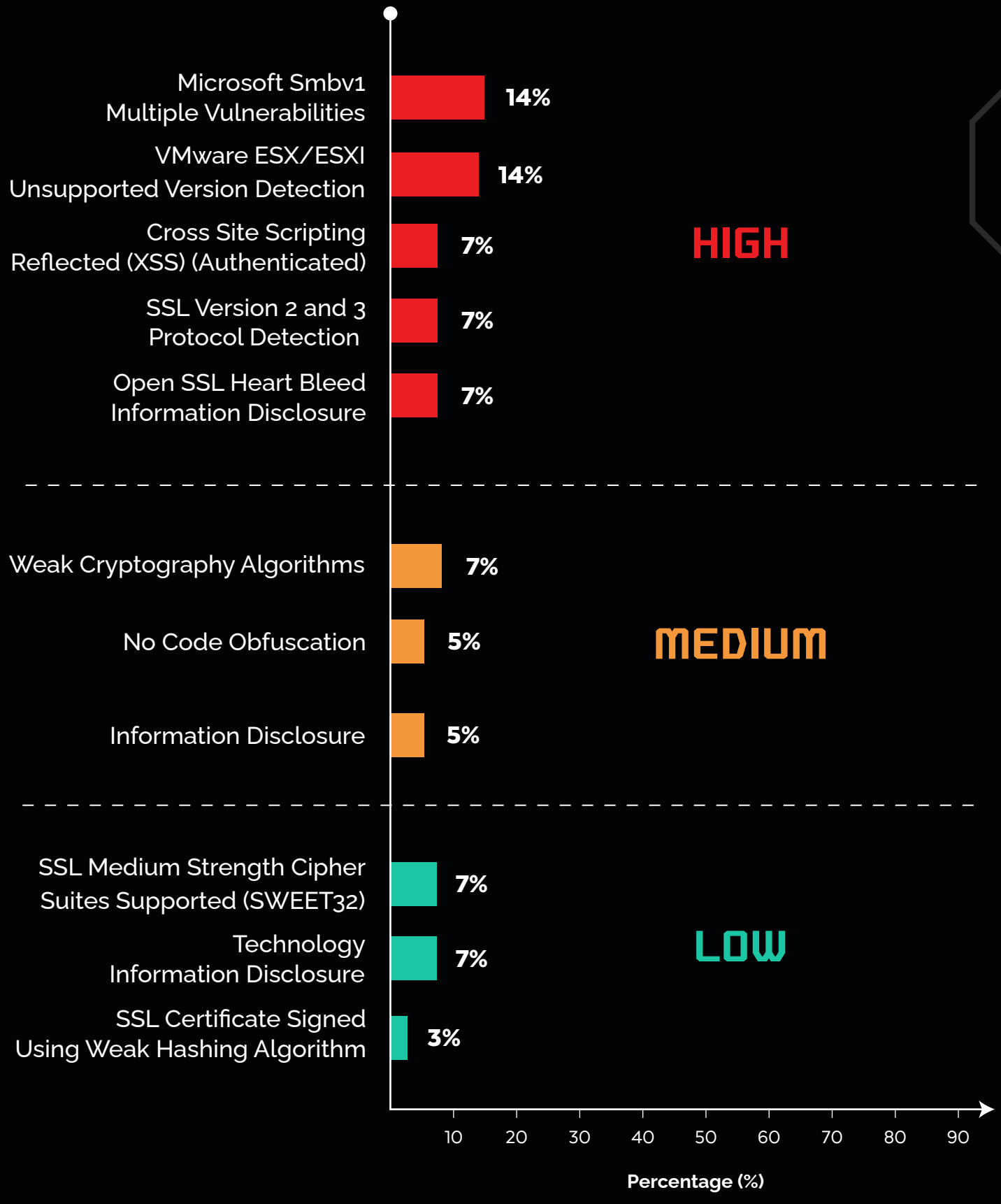
VULNERABILITIES IN THE INDUSTRIAL SECTOR

The industrial sector is key to economic growth and infrastructure development, providing essential goods and services that drive economies worldwide. Cyberattacks targeting the industrial sector can result in significant disruptions to operations, leading to production delays, financial losses, and potentially compromising safety and environmental integrity. The reliance on legacy systems and the lack of cybersecurity awareness in some industrial organizations further exacerbate these risks.

In the industrial sector, vulnerabilities were identified in both private and industrial companies, revealing a total of 16.9% high, 48.2% medium, and 34.9% low vulnerabilities. These vulnerabilities encompassed a range of issues, including file path manipulation, insecure direct object reference (IDOR), vulnerable web applications susceptible to clickjacking, session cookies without secure flags set, and browsable web directories. Additionally, vulnerabilities were found in workstations, such as SMB signing not being required, support for SSL medium-strength cipher suites (SWEET32), and deprecated TLS versions 1.0 and 1.1 protocols.



MOST PREVALENT VULNERABILITIES – INDUSTRIAL SECTOR



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

CONCLUSION

Through this report, we have provided a comprehensive overview of the cybersecurity landscape in Pakistan, as revealed through the 2023 penetration testing activities conducted by our organization. Our findings highlight opportunities for improvement across various sectors, including banking, pharmaceuticals, education, and government. Each sector has the potential to enhance its security posture and mitigate cyber threats.

We identified significant vulnerabilities, such as outdated components and insecure storage practices, across multiple sectors. Addressing these challenges requires a multifaceted approach that includes regular security updates, secure coding practices, and comprehensive employee training. By prioritizing cybersecurity and integrating it into their business strategies, organizations can better protect their data, systems, and customers.

Implementing robust security measures and conducting regular assessments can significantly enhance the protection of sensitive information and customer data. For example, addressing vulnerabilities like weak hashing algorithms, improper authentication, and insufficient brute-force protection enables organizations to navigate the diverse range of cybersecurity threats they face regularly.

This report sheds light on common vulnerability patterns and the critical role of penetration testing in identifying and mitigating them. It emphasizes the importance of maintaining secure configurations and accurate asset inventories. Regular security assessments are vital in reducing the risk of cyber-attacks and by embracing a proactive cybersecurity approach, organizations can improve their security posture and minimize the risk of successful cyber-attacks.

Trillium Information Security Systems (TISS) is dedicated to sharing this data and information to support app developers, security teams, and organizations. By equipping them with the insights from our findings, we aim to empower them to build more secure applications and systems, fostering a safer digital environment for everyone.

TECHNOLOGY INFORMATION DISCLOSURE

OCCURRENCES: 39

SECTORS AFFECTED: BANKING, PHARMACEUTICAL, TELECOMMUNICATION, GOVERNMENT, INDUSTRIAL, FINANCIAL

VULNERABLE AND OUTDATED COMPONENTS

OCCURRENCES: 22

SECTORS AFFECTED: BANKING, PHARMACEUTICAL, DEFENSE, TELECOMMUNICATION, EDUCATION, INDUSTRIAL, FINANCIAL

SSL PINNING BYPASSED

OCCURRENCES: 12

SECTORS AFFECTED: BANKING, REAL ESTATE, GOVERNMENT

COOKIES WITHOUT ESSENTIAL FLAGS

OCCURRENCES: 18

SECTORS AFFECTED: BANKING, GOVERNMENT