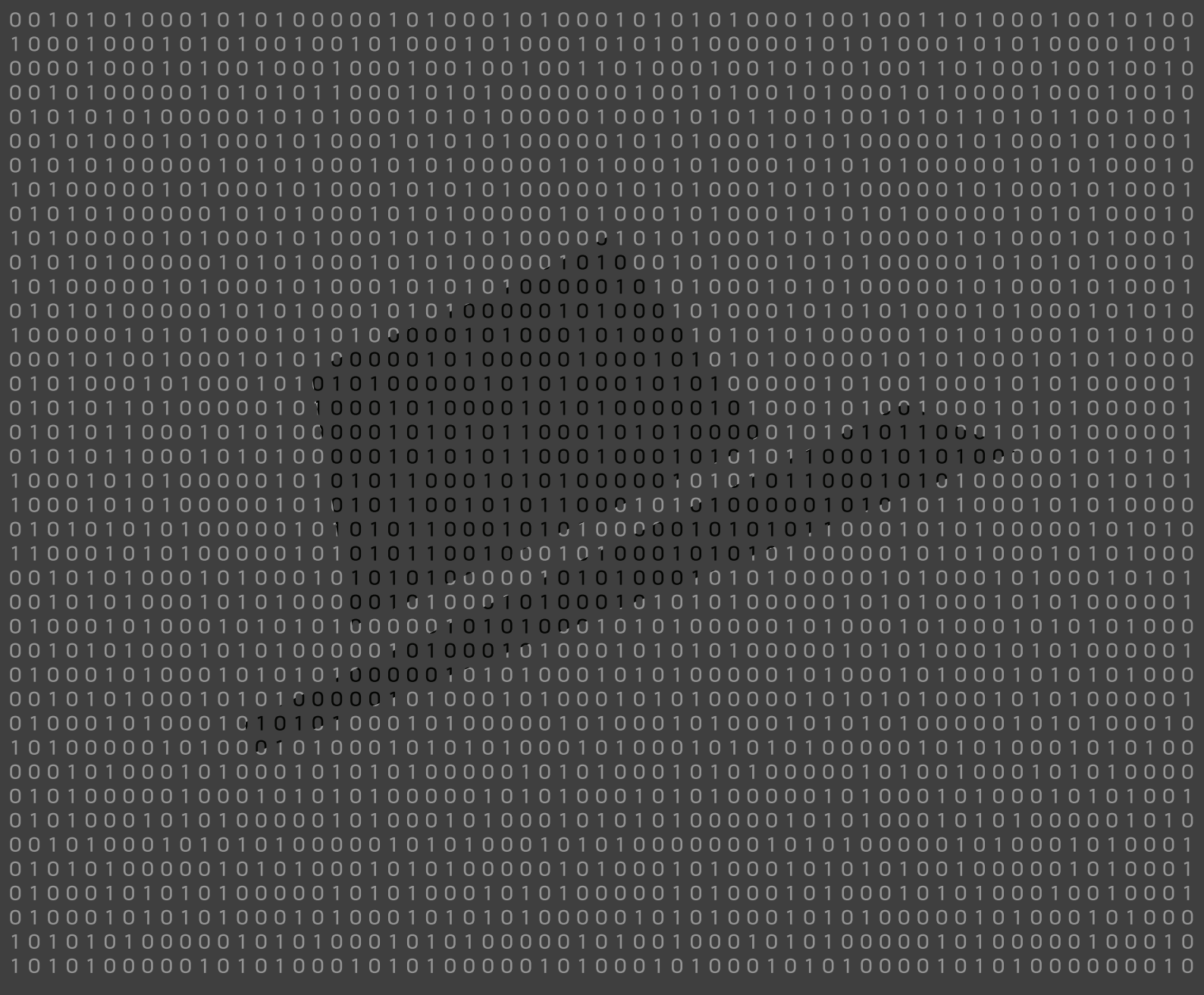
PEN TEST INSIGHT REPORT 2020



trillium Information Security Systems
Institutum de Excellentia

TSAS
Security Assessment Services

Trillium Insights

TABLE OF CONTENTS

INTRODUCTION

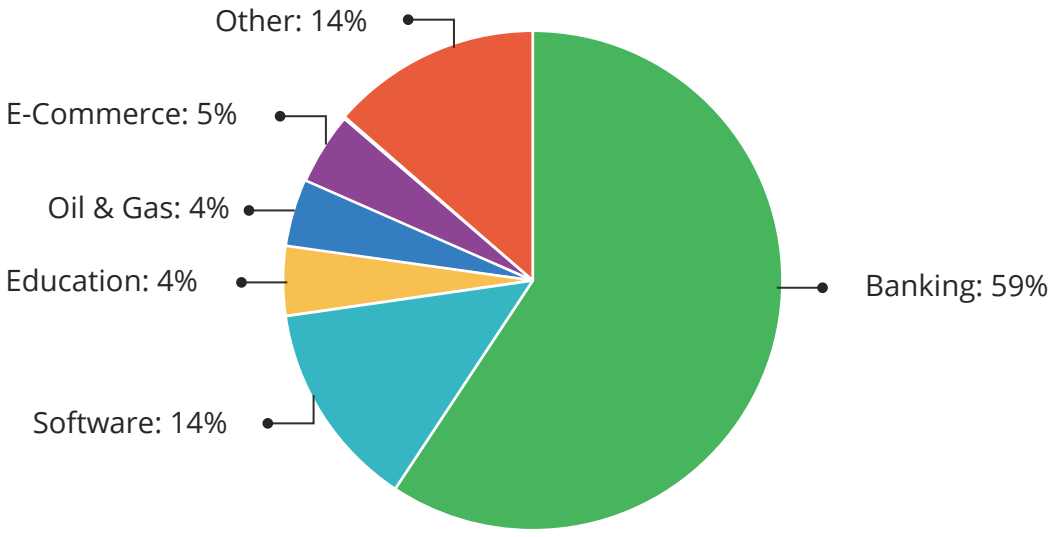
Cybersecurity is a complex landscape with rapidly evolving technologies, architectures, and policies. At the same time, there's an ever-motivated group of people out there seeking to exploit vulnerabilities for not-so-virtuous purposes: to gain access to information, take over networks, install malware, disrupt services, and more. Will your tools and configurations stand up to the test? Do they meet industry standards? Only a penetration test can tell.

However, penetration testing is an approach with a potential that is unrealized to its fullest and organizations are often unsure of what results to expect, ultimately making it difficult to get a clear picture of the overall Pen-testing landscape and its space in the cybersecurity realm. Understanding the challenges faced by Cybersecurity Leaders and Managers, we have utilized the findings of our penetration testing engagements, to share our experience and verdicts, for a better understanding of the penetration testing landscape.

This report presents the results of corporate information system penetration testing performed by TISS in the year 2019. Based on these engagements, the document describes the most common security concerns discovered, potential exploitation hazards, most at risk scope items, and recommendations for security improvements. This information is intended to promote a better understanding among cybersecurity specialists regarding the most relevant issues in a particular sector, as well as to assist in timely detection, and remediation, of vulnerabilities. We expect readers to come away from these pages with a baseline understanding of how penetration testers help organizations identify their own unique (and not-so-unique) IT risks.

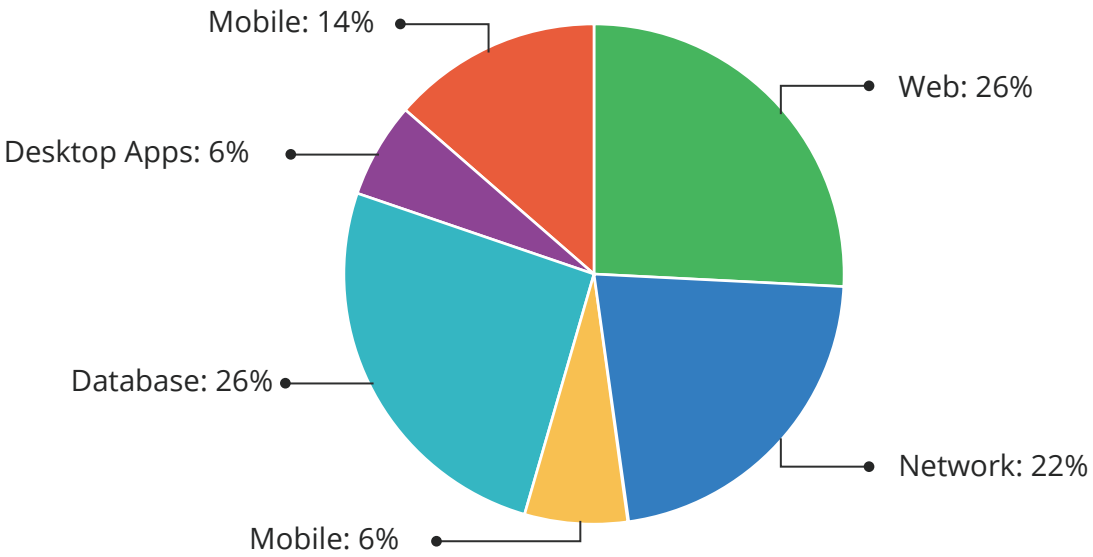
ENGAGEMENT DEMOGRAPHIC

The dataset, for the year 2019, consists of 24 engagements involving testing of corporate information systems. Engagements represented a wide range of industries, predominantly in the financial and digital sector. Banking makes up for more than half the total engagements, while software companies and other industries have been evolving their cybersecurity infrastructure and making such testing approaches a regular part of its overall strategy. This can be seen from their second space after the banking sector in our total demographic.



Engagement Demographic

In any penetration testing engagement, one of the most critical aspects is defining the scope: what networks, applications, databases, physical security controls and other assets are open for the penetration tester to attack. Each engagement in penetration testing has a predetermined scope of what is to be tested. Databases, network and web were the most famous scope items to be tested for most of these engagements taking up around 70% of the total engagements carried out. Desktop apps and systems took the least priority standing at 6% each of the total engagements done..



Engagement Scope Item

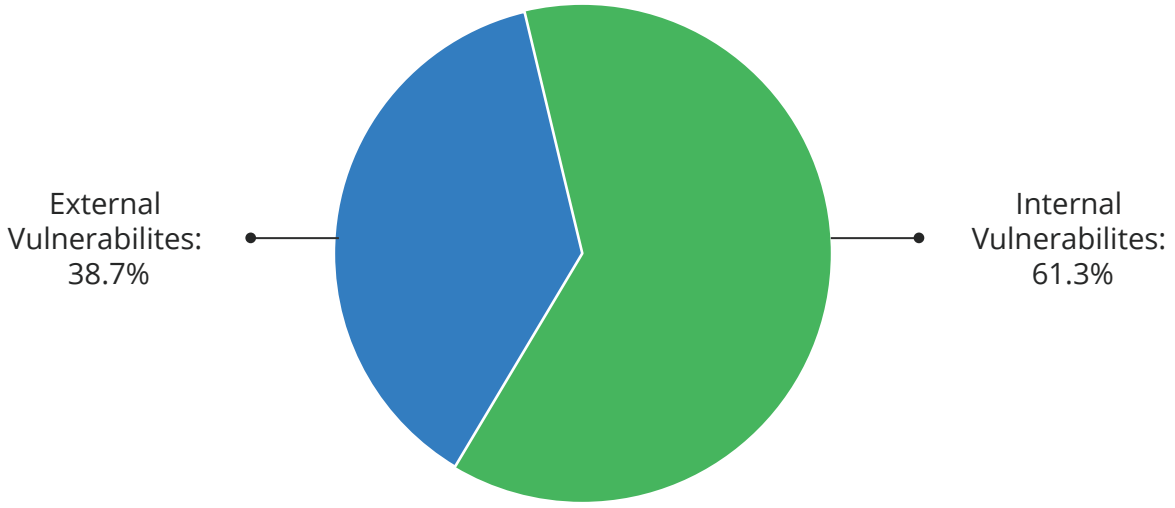
Along with the scope of what's to be tested, another factor penetration testers need to consider is the amount of time contracted to the client. Over the course of the year, we've seen a trend that edges up the average contracted hours for both internal and external to just about two weeks, or 80 contracted hours, with some significant outliers in external testing going on for several months.

Usually, automated attacks of the internet are time-bound, and are continuously trying to access your data. Such attacks pry commonly on the internet uninformed and follow a hit-or-miss strategy, and as such are not really targeted at system vulnerabilities, placing them outside the design scope of penetration testing. Such automated attacks can be dealt with relative ease by automated systems, whereas penetration testing is designed to uncover the limitations and weaknesses of automated solutions and their coverage of the infrastructure. Reconnaissance and planning take the bulk of time during penetration testing, allowing the testing to be disguised as a modern, and significantly more devastating threats faced by organizations and companies today.

VULNERABILITIES

Corporate information systems were subjected to external and/or internal penetration testing. External testers take on the role of a threat actor who has Internet access but no pre-existing privileges on the target system. Their goal is to breach the network perimeter and obtain access to resources on the local network. Meanwhile, internal pen testers work on a segment of the local network and attempt to obtain control over the system infrastructure or critical resources predetermined by the client.

By making conditions as close as possible to those of the real world, such testing provides a true measure of the overall state of security. Most engagements, whether internal or external assessment, saw at least one vulnerability exposed to attackers, with 61.3 % vulnerabilities being found in the internal scope while the rest laying in external scope.



Vulnerabilites Found (External vs. Internal Engagements)

In external engagements, our testers were able to gain internal access about 60% of the time. While not every engagement has a stated goal of achieving domain or enterprise administrative access, all internal engagements typically have a goal involving proving access to sensitive data. In such scenarios, we were able to gain access about 80% of the time. Cyber security is often seen as an afterthought when it comes to the overall management strategy of a business. Stats like these show how much work is needed to seriously prioritize security in order to ensure the confidentiality, integrity, and availability of information, products, and services. It is essential for organizations to position security at the heart of their culture, in order to mitigate the threat of operational, financial and reputational damage.

MOST FREQUENT VULNERABILITIES:

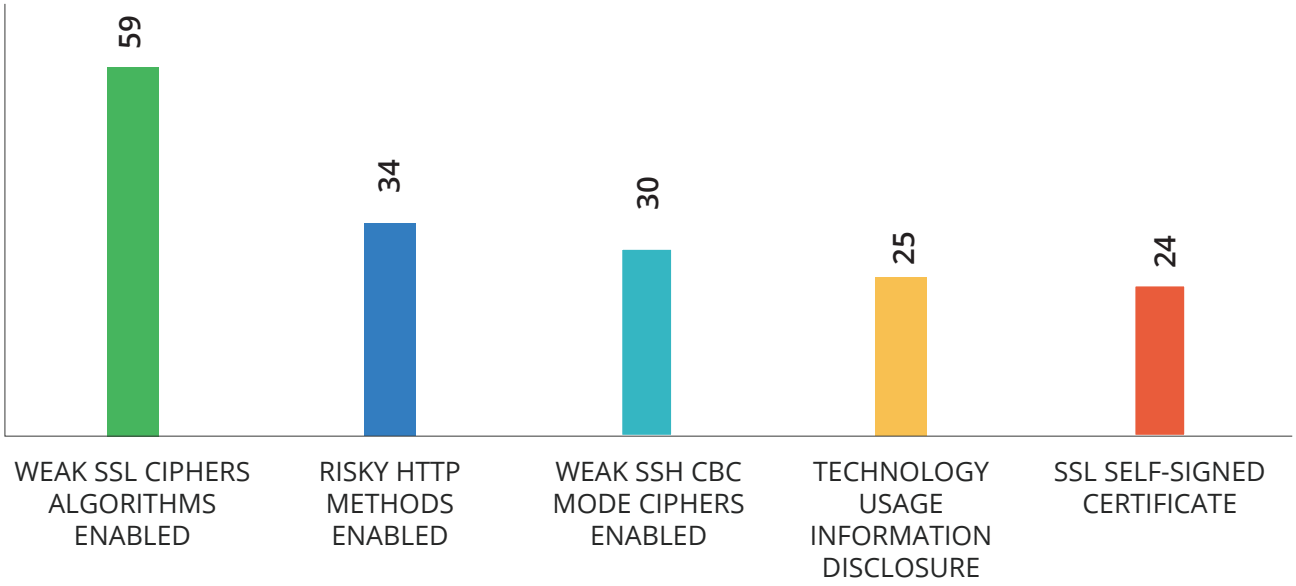
Each industry functions differently, and has a distinct set of features. Such is also the case with the cyberspace. Each industry has its own set of concerns when it comes to cybersecurity. Based on our vast engagement findings, we compiled and put together a list of vulnerabilities most encountered and found, unique for each industry.

Companies in the financial services will almost certainly remain a high profile target for cyber-criminals, hacktivists, and APT groups, making it essential to clear out potential vulnerabilities

that can be exploited. The most frequent vulnerability found in the banking sector was 'Weak SSL Ciphers Algorithms Enabled'.

BANKING

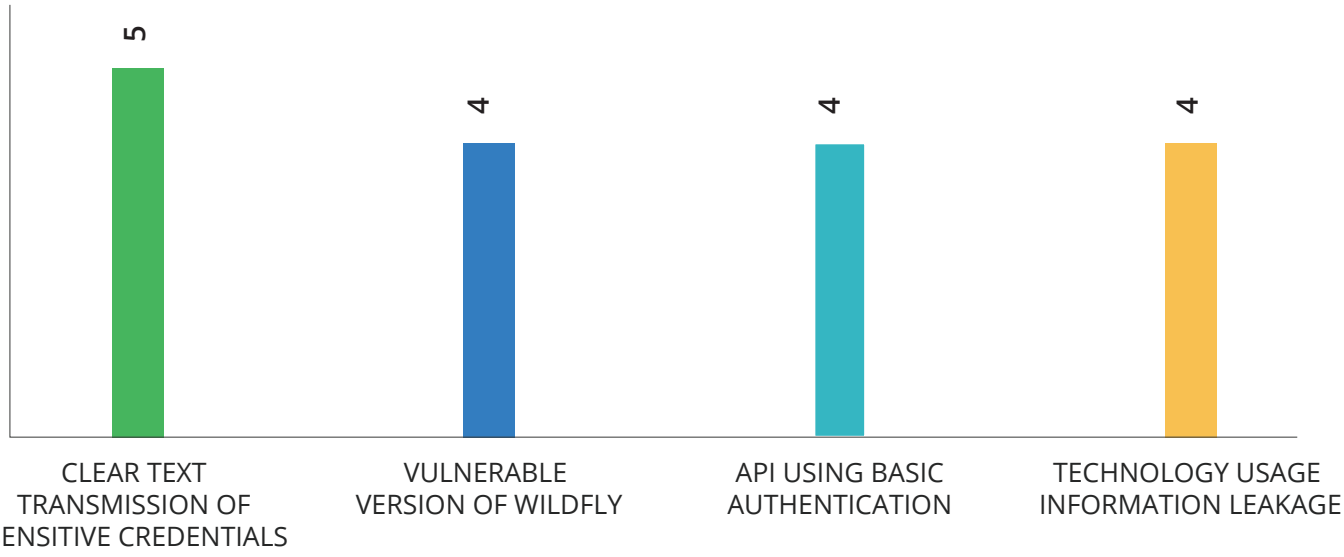
Most Frequent Vulnerabilities in Banking



Telecom service providers build, operate and manage the complex network infrastructures used for voice and data transmission – and they communicate and store huge amounts of sensitive data, making them a top target for cyber-attacks. Thus, it is of utmost importance to have resilient cyber defenses, leaving no gap to be exploited by attackers. Having tested major Telecom industries nationally, we analyzed some common patterns over the year, and the most seen vulnerabilities included; 'Clear Text Transmission of Sensitive Credentials', 'Vulnerable version of WildFly', 'API using Basic Authentication' and 'Technology Usage Information Leakage'.

TELECOM

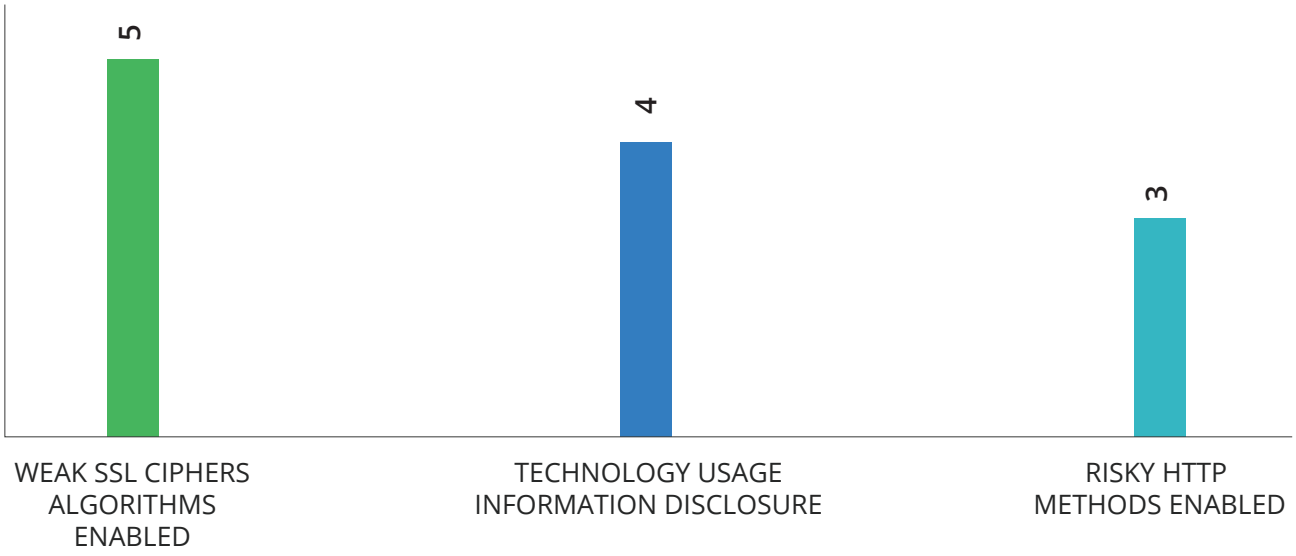
Most Frequent Vulnerabilities in Telecom



Online commerce is a massive business and only growing larger. After evaluating the most common cyber threats facing the E-Commerce industry in the year, common threats to the digital industries included 'Weak SSL Ciphers Algorithms Enabled', 'Technology Usage Information Disclosure', and 'Risky HTTP Methods Enabled'.

E-COMMERCE

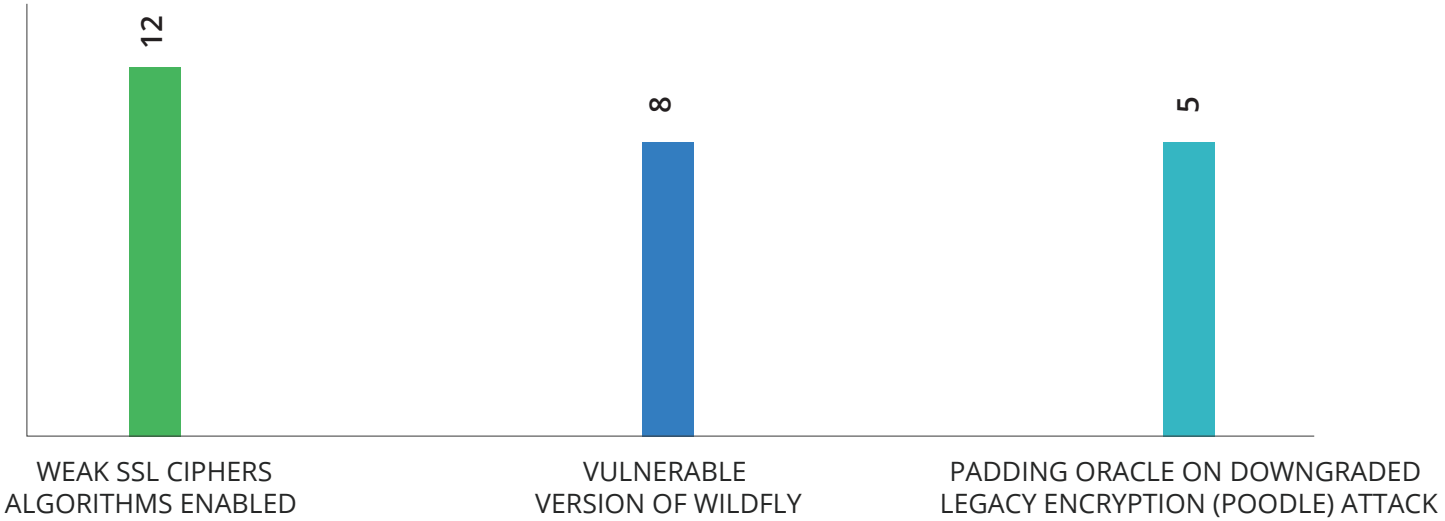
Most Frequent Vulnerabilities in E-Commerce



Any activity in the oil and gas sector is subject to risks caused by threats and vulnerabilities. This increasingly also applies to risks due to digital vulnerabilities. Similar to the E-Commerce sector, Oil and Gas industries also encountered 'Weak SSL Ciphers Algorithms Enabled' and 'Risky HTTP Methods Enabled'. However, 'Padding Oracle on Downgraded Legacy Encryption (Poodle) attack' seemed to be unique to this sector.

OIL & GAS

Most Frequent Vulnerabilities in Oil and Gas

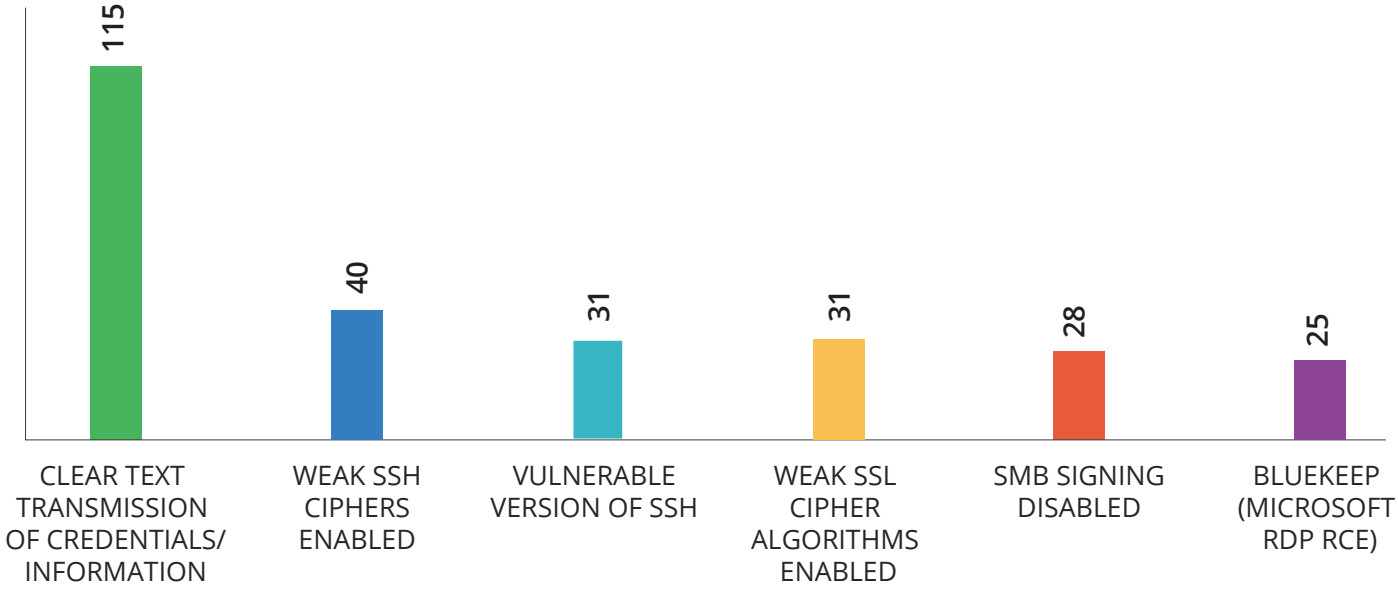


Likewise, the rest of the industries encountered some recurring vulnerabilities. 'Clear Text Transmission of Credentials/ Information' was found to be the top threat from all sectors combined. Weak SSH Ciphers Enabled', 'Vulnerable Version of SSH', 'Weak SSL Cipher

Algorithms Enabled, 'SMB Signing Disabled', 'BlueKeep (Microsoft RDP RCE)' were also periodic. Adding to this list, Weak SSH CBC Mode Ciphers Enabled was specific in the Education sector was 'Multiple CSRF Vulnerabilities' and 'Old Version of JQuery' was encountered in Software companies.

OTHER

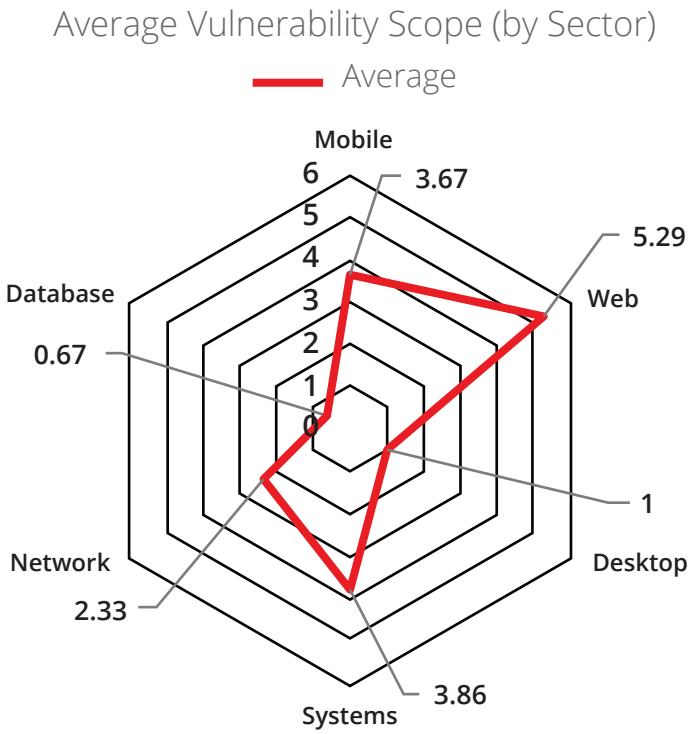
Most Frequent Vulnerabilities in Other



VULNERABILITY SCOPE

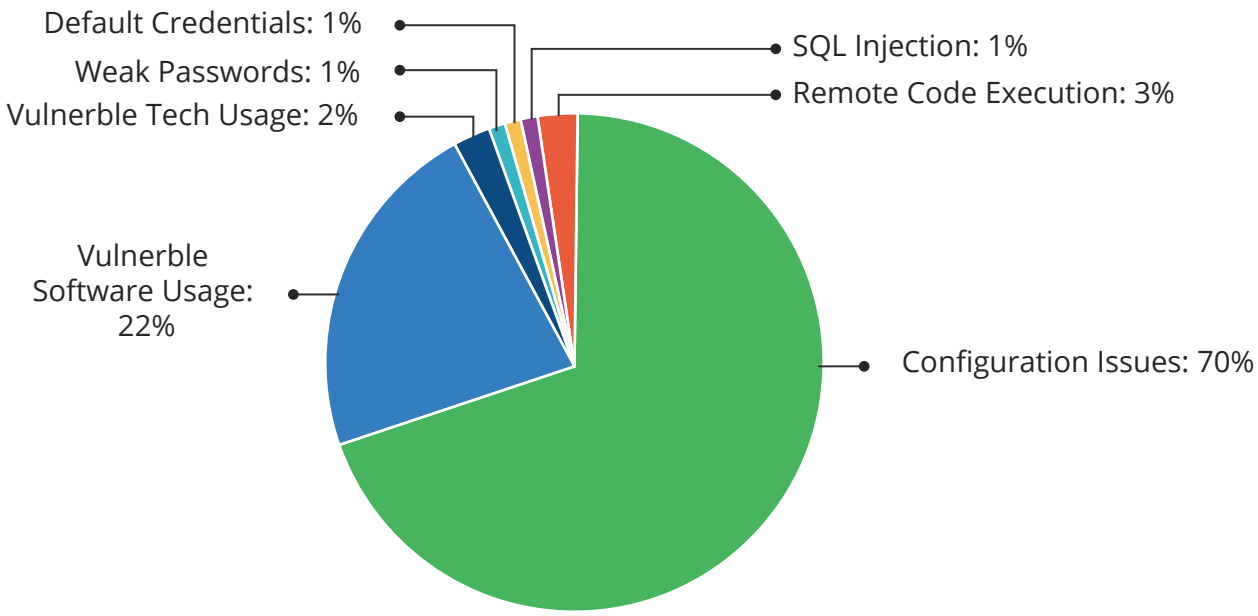
The radar chart represents average vulnerabilities in a single engagement for each scope item, with each radar ring representing a unit scale. Average vulnerabilities discovered during each engagement vary depending on the technology, with databases proving to be the least vulnerable at less than one average vulnerability per engagement. Meanwhile, web due to its inherent exposure, is the most vulnerable item, with the highest average vulnerabilities at more than 5 vulnerabilities per engagement.

Average Vulnerability Scope (by Sector)



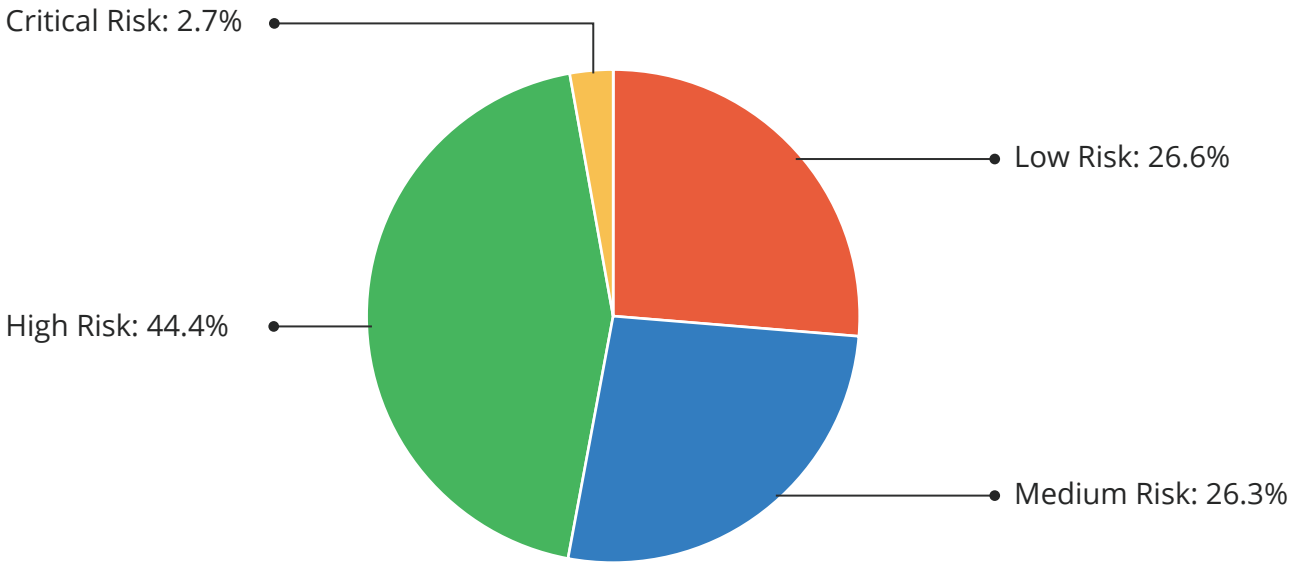
VULNERABILITY RISK AND CATEGORY

Most vulnerabilities found can be divided into different sets based on their types. The graph shows the division of the categories of vulnerabilities found in our engagements. A leading 70% of vulnerabilities featured were related to issues in configuration. This was followed by vulnerable software usage which accounted for 22% of the total vulnerabilities encountered. Other issues such as Sqlinjection, default credentials and weak passwords seem to be sparse. However, it does not mean that these issues are extinct.



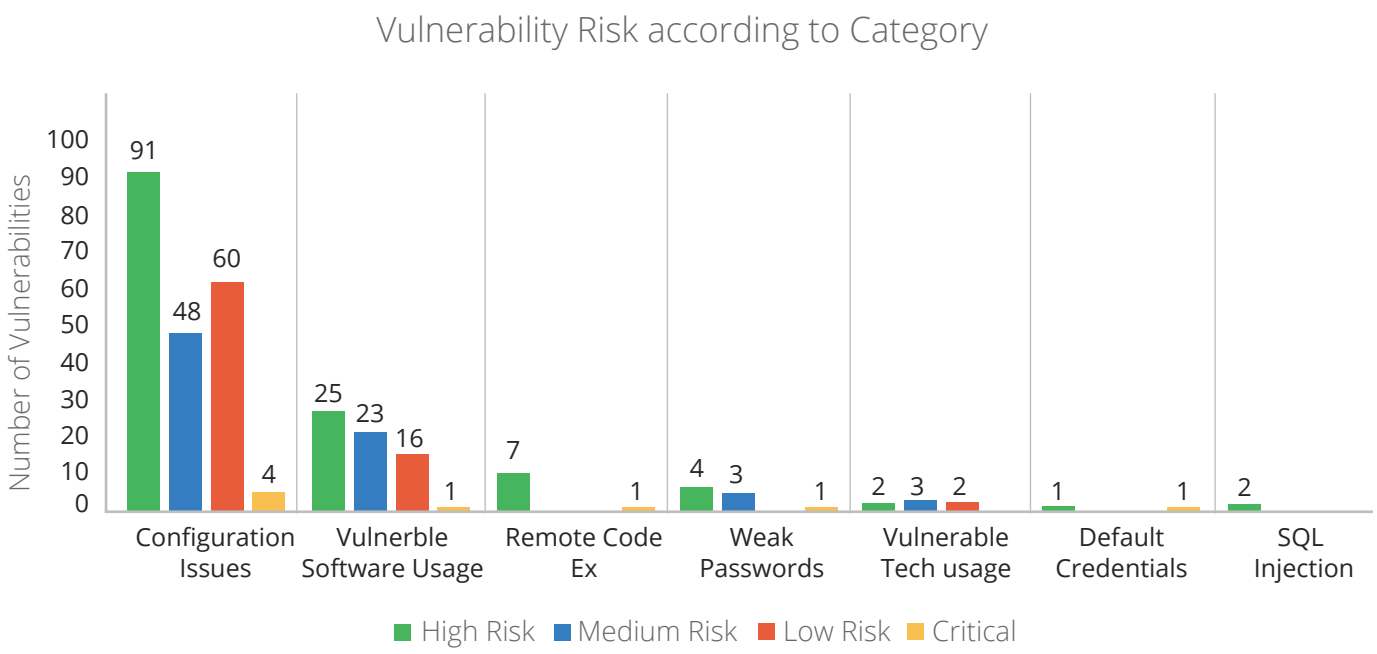
Vulnerability Category

Based on CVSSv3.0, each vulnerability is assigned a degree of risk: Critical, High, Medium, or Low. Almost all systems contained critical vulnerabilities, and vulnerabilities that rated out to be High Risk topped the chart at 44.4%, reiterating our stance regarding the essentiality of penetration testing as a component of a broad, all-encompassing vulnerability management strategy.

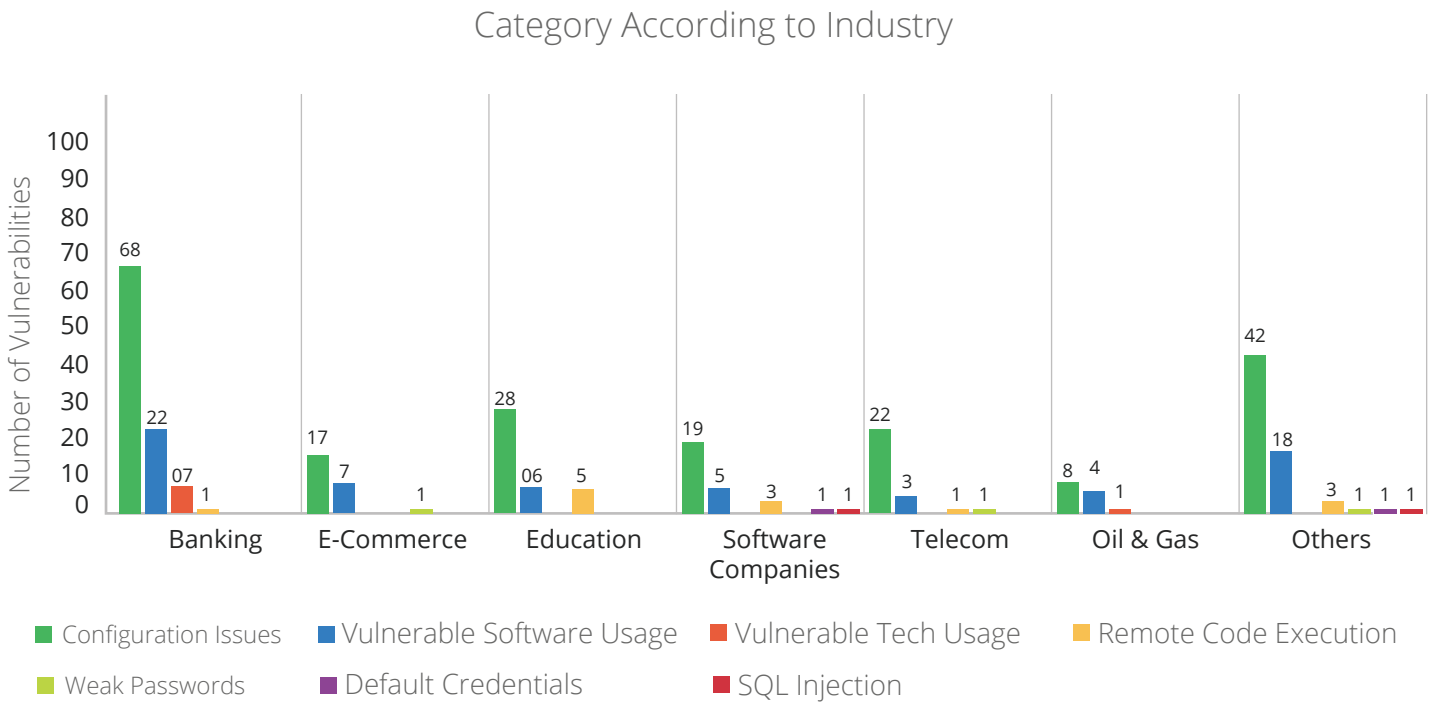


Vulnerability Severity Level

Most of these high-risk vulnerabilities related to Configuration Issues which is expected, given the expanse of vulnerabilities accounted for in configuration. 30% of high-risk vulnerabilities found were relating to configuration issues, and then followed by vulnerable software usage. However, the division of severity seems to be balanced when using vulnerable software at approximately the same ratio of high, medium and low risk vulnerabilities. On the contrary, configuration issues had a higher percentage of high risk vulnerabilities compared to medium and low risk. The most critical vulnerabilities were also seen in configurations.



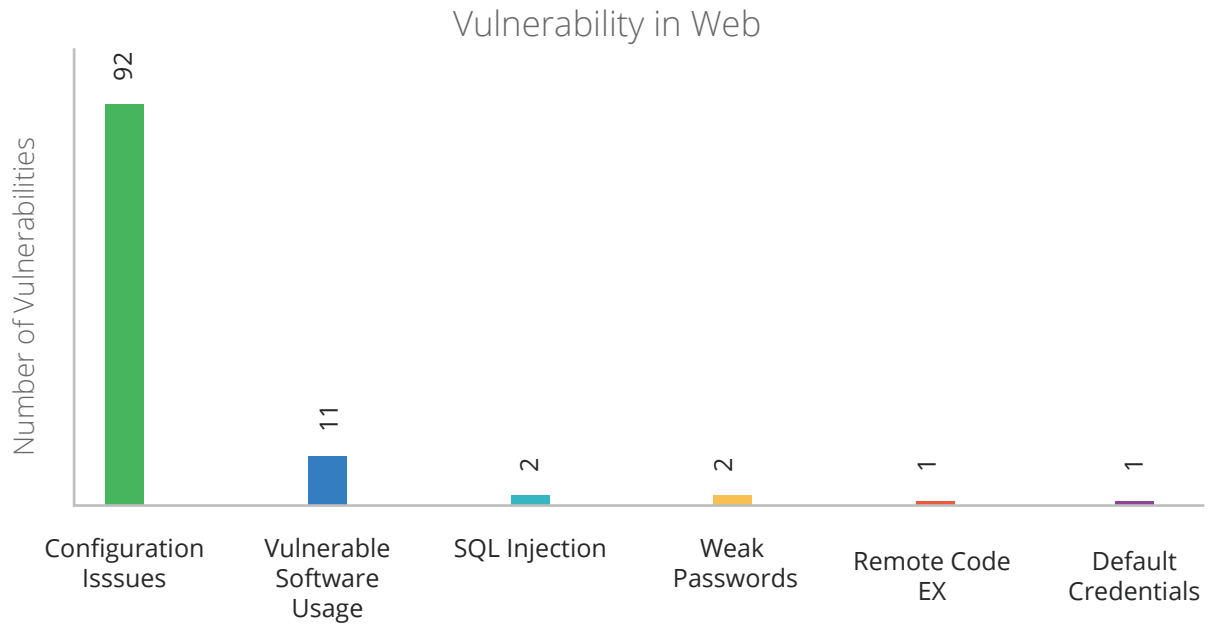
Following the pattern, configuration issues were the most common and prominent item followed by vulnerable software usage across each sector. Vulnerable Technology usage seemed to a bigger threat in the banking sector while remote code execution was dominant in the other sectors. Default credentials and Sqlinjection seemed to be an issue found in software companies and the other category.



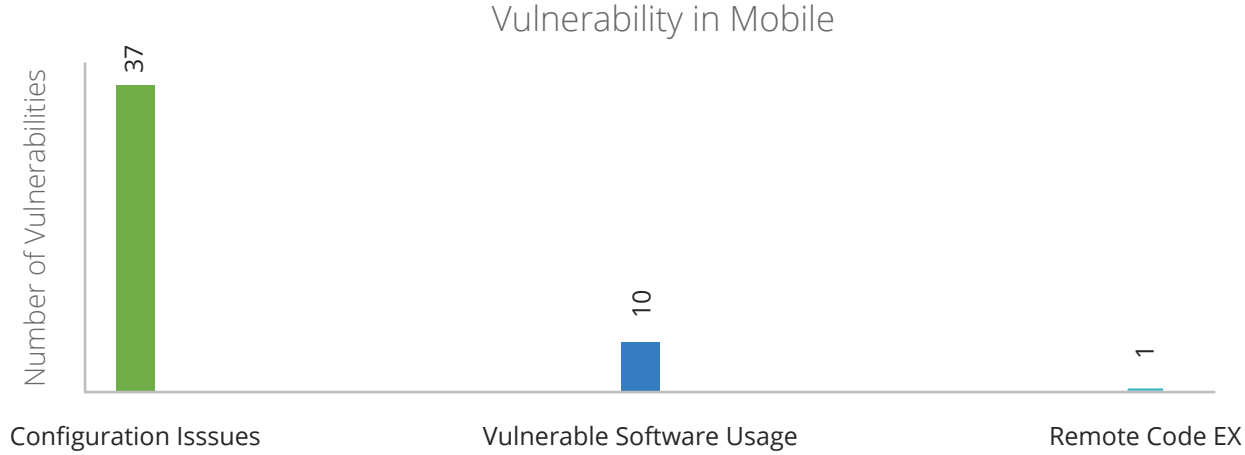
VULNERABILITIES CATEGORY IN SCOPE ITEMS

To prevent and reduce security breaches, it is vital to uncover security vulnerabilities in every part of our environment. As scope of each penetration test engagement is predetermined, it might prove fruitful to compare how vulnerabilities vary across the scopes and what sort of issues each entail. Configuration issues and vulnerable software usage seem be issues across every domain item including web, mobile, desktop applications, database, system and networks. However, some issues were more prominent in certain scope items such as vulnerable tech usage seems to be a colossal problem in systems and networks.

Web application vulnerabilities are a common and distinct source of vulnerabilities and tend to be featured prominently in findings during both internal and external engagements. The figure below shows the type of web vulnerabilities uncovered and their frequency in engagements where web apps were in scope

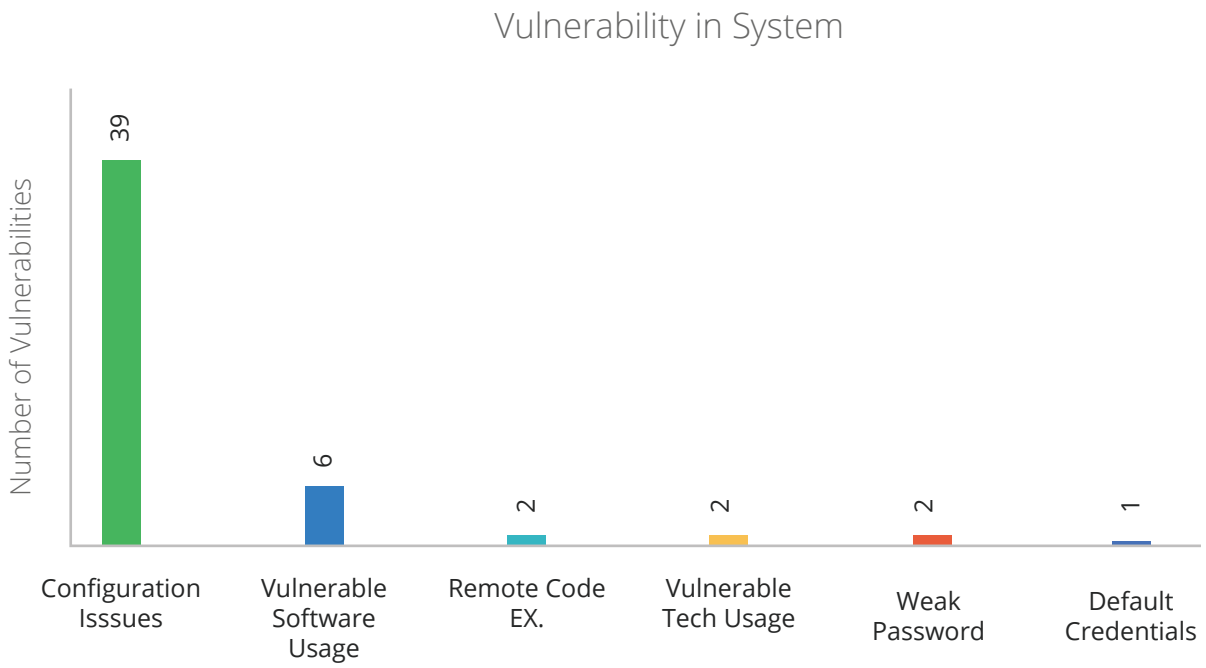


Mobile saw a constricted range of vulnerabilities with configuration issue being the main focus of vulnerabilities followed by vulnerable software usage and remote code execution.

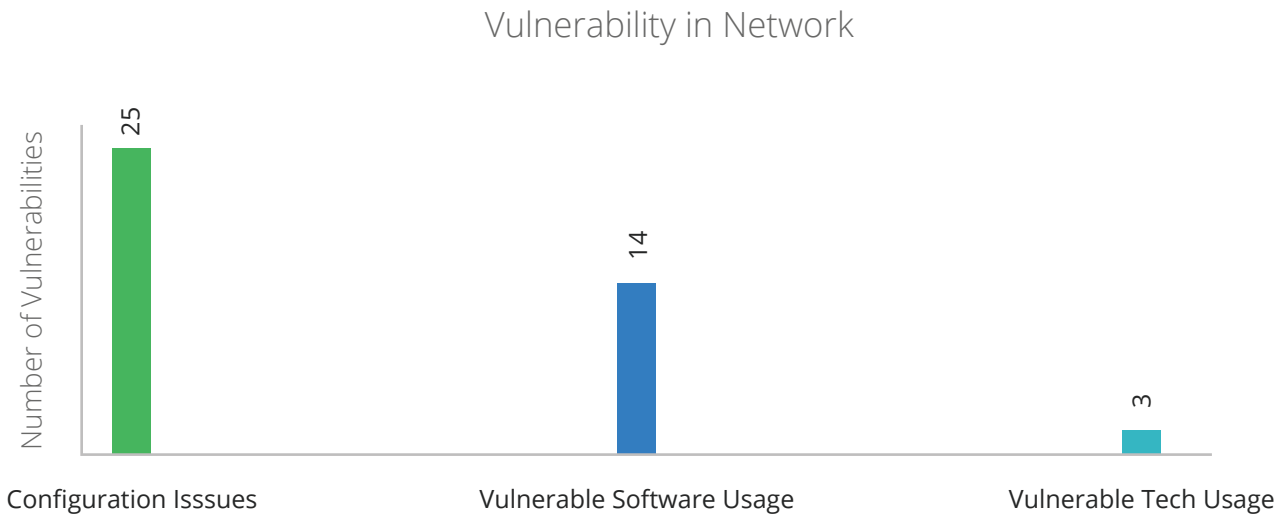


Systems encountered a varied range of issues making path for exploitable vulnerabilities. Configuration issues and vulnerable software usage were the most frequent type of

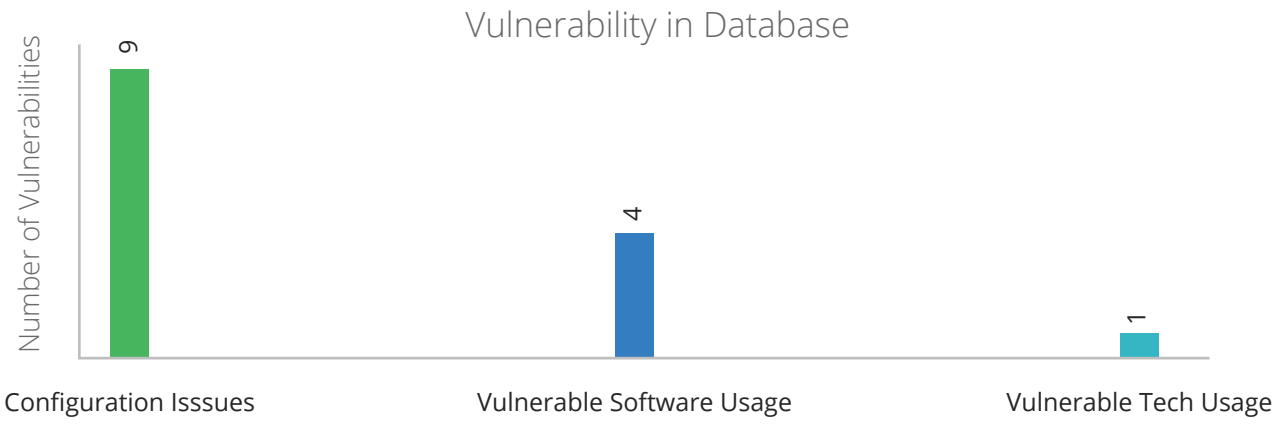
vulnerabilities found. Remote code execution, weak passwords, vulnerable tech usage and default credentials also made the list.



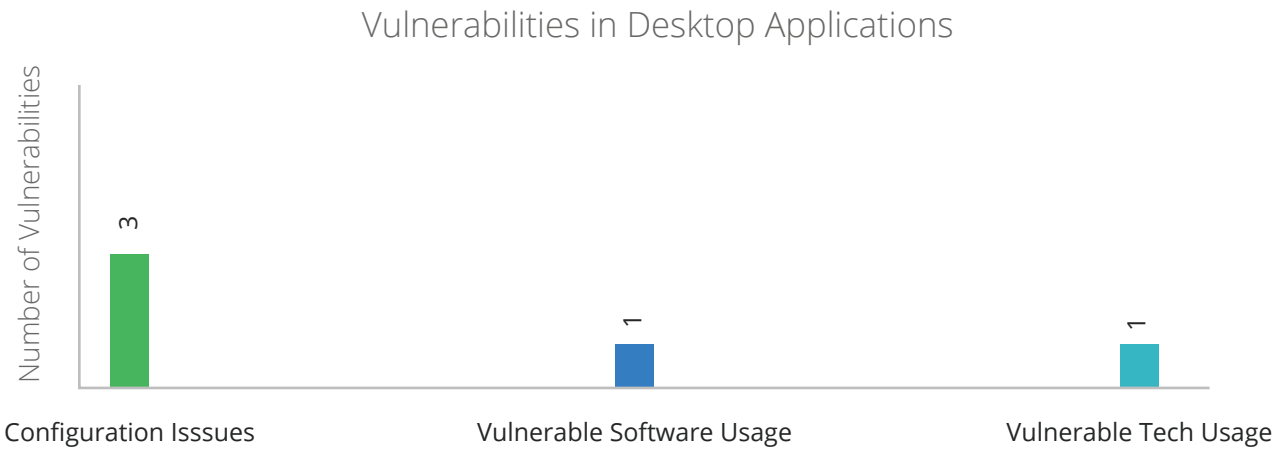
The network is often the nerve system of an organization — storing its information and driving its communication. Network infrastructure is always evolving, and not all changes are made with security being prioritized in mind. Issues in configuration and using vulnerable technology and software was the major source of exploitable vulnerabilities when testing organization networks..



Database security should provide controlled and secure access to the users and should also maintain the overall quality of the data. Following the pattern, databases saw the same sources of vulnerabilities as the networks, namely; configuration issues, vulnerable software usage and vulnerable tech usage



Lastly, Desktop applications saw issues in configurations, vulnerable software usage and weak passwords as being the most prominent source of vulnerabilities



CONCLUSION

Through this report, we hope to provide a comprehensive analysis of the common vulnerability patterns and the penetration testing landscape in Pakistan. In essence, a penetration test will not only hunt out vulnerabilities from every nook and dark corner of the infrastructure but also provides detailed guidance to resolve each issue as part of its reporting process.

As seen throughout in this report, improper configurations can cause vulnerabilities even in fully patched hardware and software components and was by far the most common factor in all cyber vulnerabilities encountered. However, these are relatively easy to fix; given that one is aware of the issue. Since, configuration changes and patching can impact system availability and therefore are often overlooked. Using Defective hardware and software was the second most common source of cyber vulnerabilities. Organizations should maintain an accurate asset inventory and establish secure configuration standards for each major device and software category to avoid creating unnecessary vulnerabilities.

Just like it is impossible to absolutely secure any network by eliminating all degrees of risk, no penetration test could ever provide a 100% guarantee that you're secure, as new vulnerabilities, techniques and technologies are surfacing constantly. However, a penetration test provides proof that you've made your systems as secure as you can, drastically reducing the chances of a successful attack. Thus, for organizations having secured all information security systems, regular testing should be made essential.