

Ethical Hacking Report

2,859 ways we hacked
our clients in 2022

Management summary

2,859 **VULNERABILITIES**
found in total

388 **PROJECTS**
tested in 2022

8 **VULNERABILITIES**
found in every project on average

5 **NEW PROJECTS**
tested per week on average

2,5 **CRITICAL**
vulnerability found in 50% of projects analyzed

1 **HIGH**
vulnerability found in every project on average

1 **MEDIUM**
vulnerability found in every project on average

Introduction

Over the years, Citadelo has performed thousands of security assessments and penetration tests globally. This first-hand testing experience and the extensive sample size have allowed us to gain unique insights into the current state of cyber security and the prevalence of various vulnerabilities across different types of IT projects.

While different project types experienced varying levels of vulnerabilities due to a variety of factors, on average 50% of projects tested in 2022 suffered from at least

one critical vulnerability, and medium - to high-level vulnerabilities were found in nearly every project tested.

These results confirm the absolute necessity for comprehensive penetration testing for any IT project, regardless of vertical. The frequency and sophistication of cyber-attacks are constantly on the rise and penetration testing and full-stack security assessments are more crucial than ever in 2022.



How we got our numbers

This report analyzes the risks identified in projects tested by Citadelo during 2022. The statistics we gathered from our own first-hand testing of over 388 projects revealed a total of 2,859 vulnerabilities of varying criticality. We performed penetration tests on an average of 8 projects per week and found an average of 7 vulnerabilities in every project.

All figures are directly taken from our own testing procedures, without any information from external sources. Retests were not included in the figures, as they would influence the results and decrease the perceived prevalence of certain risks.

Types of vulnerabilities

In Citadelo's penetration testing and full-stack security analysis, we identify a full range of risks, from suggested best practices to critical vulnerabilities. We use the following risk types to categorize the vulnerabilities we identify:



The following chart gives a full overview of the tests performed by Citadelo in 2022:

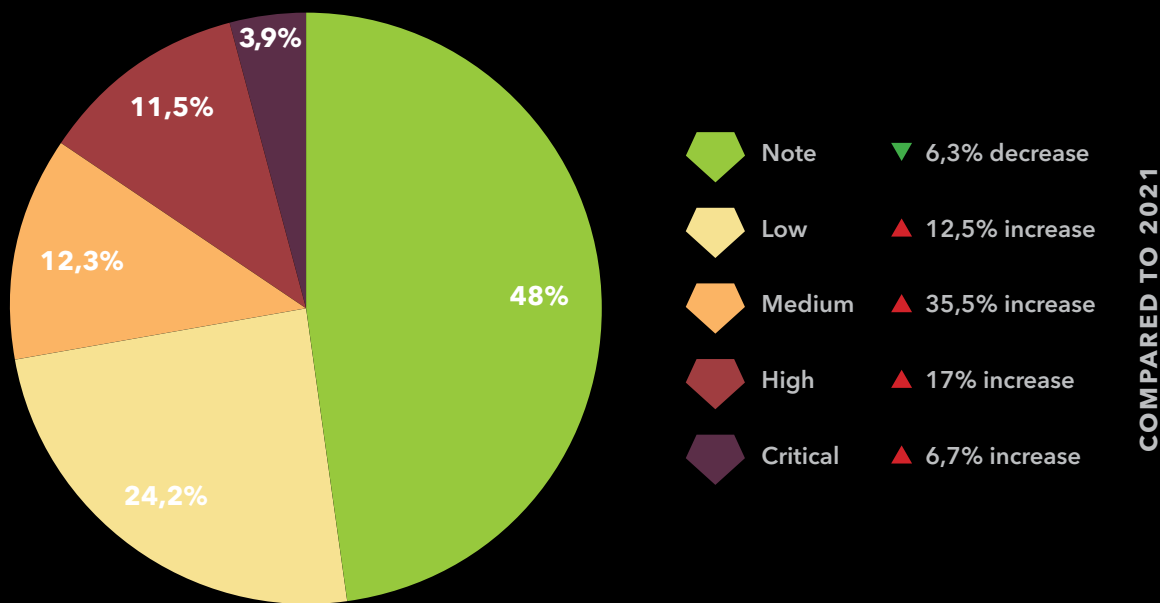
OVERALL RESULTS FOR 2022:

	Web	API	Mobile	Infra	Cloud	Social Engineering	Other	Total
No. of projects	202	36	36	45	46	8	15	388
Note	592	80	185	144	175	2	28	1260
Low	299	50	67	108	179	0	12	715
Medium	152	25	39	67	175	2	9	469
High	142	11	14	49	89	1	5	311
Critical	48	4	10	19	27	16	4	158
Total	1233	170	315	417	645	21	58	2859

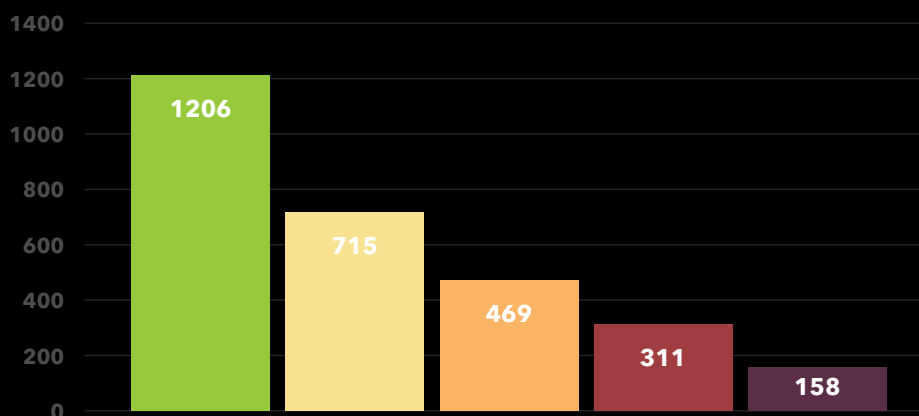
Prevalence of vulnerabilities

The following is a breakdown of the prevalence of the different types of vulnerabilities identified throughout our testing:

VULNERABILITY RISKS IN 2022:



NUMBER OF VULNERABILITIES FOUND BY TYPE IN 2022:



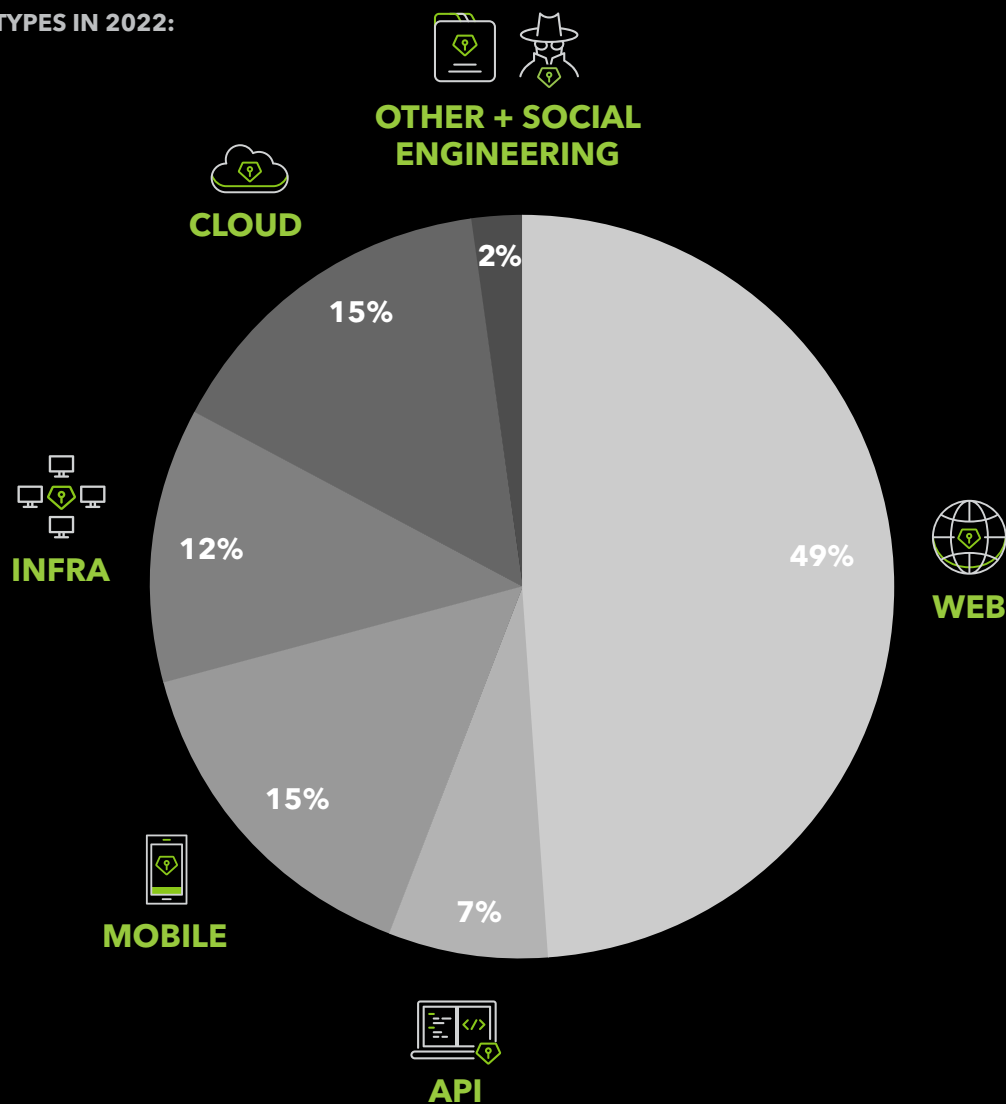
As a rule of thumb, the less critical the risk, the more frequently it is likely to be exposed in any given project type. On average, Note risks made up the highest proportion of vulnerabilities identified at 48%. These types of risks are still highly advisable to resolve but do not present an immediate threat to projects. Critical risks, on the other hand, made up just 4% of the vulnerabilities identified. However, these types of risks represent immediate threats to projects and must be remedied as quickly as possible.

Common risks by project type

Of the projects we tested, web-based projects (websites or APIs) were by far the most common, comprising over 49,1% of all projects. Mobile app projects were the next most common types, at 15,3%, **followed closely by continuously rising Cloud at 14,5%**. While **Infrastructure projects were at 11,9%, the API stayed low at 6,6%**. Social engineering together with other projects tested was largely made up of desktop apps, ATMs, and **social engineering projects and rounded up to approximately 2,5%**.

The following is a breakdown of the different types of projects and vulnerabilities most commonly associated with each type of project:

PROJECT TYPES IN 2022:





WEB

In the modern, digital age, websites and web projects are by far the most common, and suffer the most vulnerabilities of any other project type.



API

We tested significantly fewer solely API-based projects, as APIs are nearly always tested with a web interface, and thus most projects that included an API were grouped in with the "Web" project category. Since the subset of API vulnerabilities does not include client-side vulnerabilities and consists of less common vulnerabilities like (e.g. XSS or JSON), the average number of vulnerabilities identified was much lower than with web projects.



MOBILE

With the continued rise in popularity of mobile apps, a marked increase in verified vulnerabilities was identified in our data. A much higher number of "note" vulnerabilities was found, as analysis of mobile apps also includes client-side layers (i.e. APK/AAB and IPA itself) where these types of vulnerabilities are most prevalent.

However, fewer binding vulnerabilities were found, as these are most commonly associated with APIs, and are rarely found on the client-side in intents, URL schemes, etc.



INFRASTRUCTURE

Infrastructure projects power a wide range of industries, but made up just 11,9% of our sample. Interestingly, we found more critical vulnerabilities (medium and higher) than any other type in this segment. This is likely due to the fact that many projects tested were internal infrastructure (i.e. not connected to the Internet), which led clients to be less cautious than with external infrastructure projects (i.e. connected to the Internet). This false sense of security is a troubling trend that makes internal infrastructure projects prime targets for

cyber-attacks. Clients undertaking internal infrastructure projects must be aware of the risks involved and continue to test the security of their infrastructure to avoid exposing critical vulnerabilities, even without a direct connection to the Internet.



CLOUD

Similarly to internal infrastructure projects, clients undertaking cloud projects suffer from a false sense of security that led to a higher number of critical vulnerabilities. The misguided beliefs that the audits and penetration testing commonly provided alongside cloud services are sufficient, and that the lack of exposure of services to the Internet guarantees higher security, led clients to overlook critical vulnerabilities that were subsequently revealed in our testing.



OTHER AND SOCIAL ENGINEERING

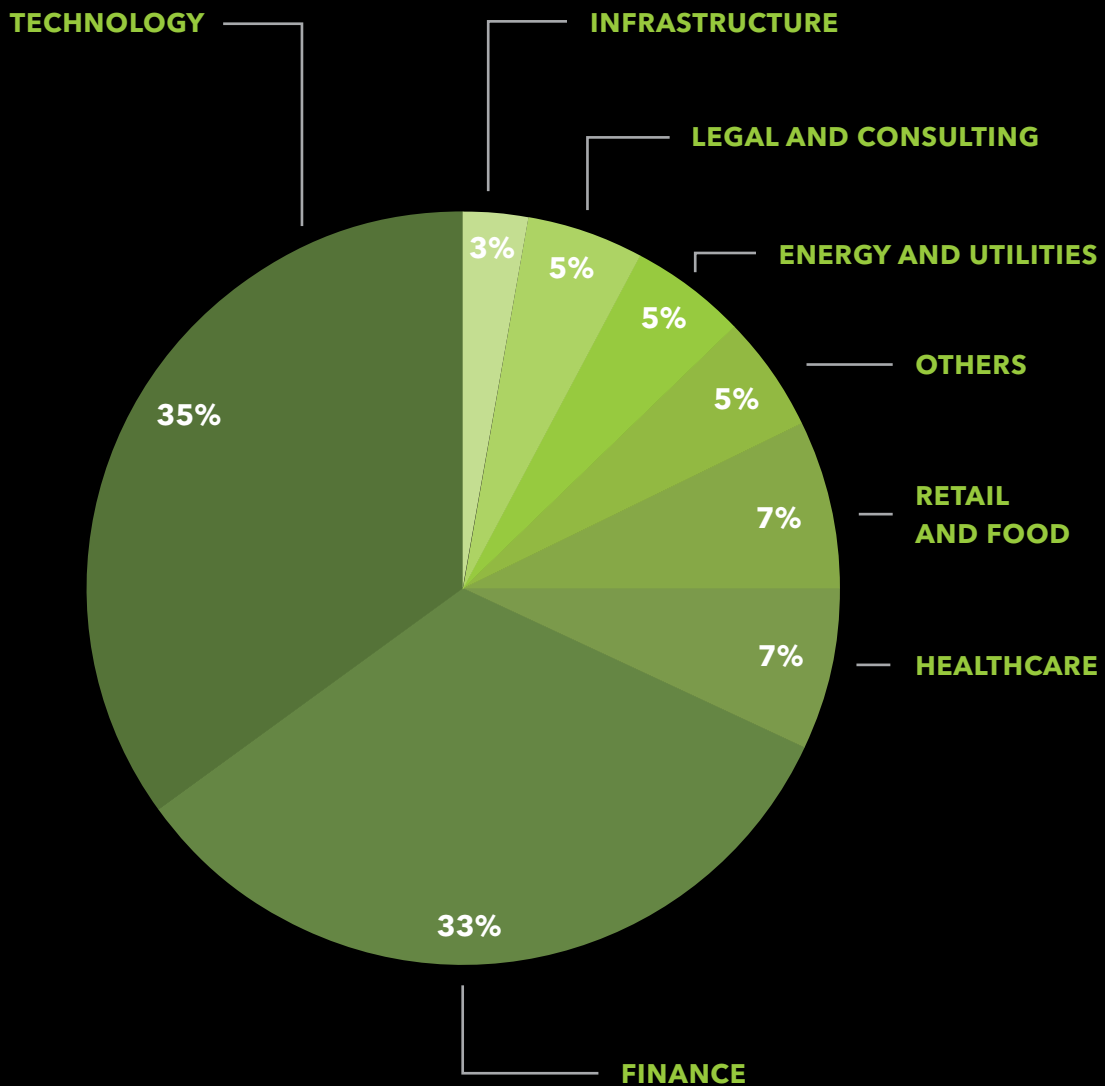
As social engineering, especially phishing is on the rise, we came across a small sample of projects that included phishing, smishing, vishing and even though the number we were able to test was small, we could not highlight more the importance and awareness this topic needs to have, thus we are including it in our report.

Industries we tested

Citadelo provided penetration testing and security audits for a wide range of industries in 2021. While the vast majority of projects (35%) fell under the broadly defined Technology sector, clients from the field of Finance were not far behind, making up 33% of all projects tested. The remaining sectors were fairly evenly distributed, each making up between 3 and 7% of all projects tested.

Please consult the table below for a full breakdown of the industries tested in 2021:

TYPES OF INDUSTRY SEGMENTS IN 2022:



Conclusion

The over 2,859 vulnerabilities we found present a snapshot of the current state of cybersecurity and the importance of penetration testing in 2023. While less serious errors made up the vast majority of vulnerabilities, the 158 critical vulnerabilities discovered could have resulted in catastrophic consequences had they not been immediately remedied.

Above all, an important common theme was highlighted by our data: whenever the importance of security or penetration testing is overlooked or underestimated,

more vulnerabilities inevitably emerge. Whether it be internal infrastructure applications assuming they are safe because they are not connected to the Internet, or cloud service applications that assume the internal audits of their providers are sufficient, the overarching lesson from this data is that you can never be too careful. Comprehensive penetration testing from experienced agencies like Citadelo is an essential component of any security solution, and its importance will only increase in the years to come.



I believe in the power of ethical hacking to uncover vulnerabilities before the bad guys do. So, when we saw a 20% increase in critical vulnerabilities compared to last year, we didn't panic - and got to work to execute the 2,859 vulnerabilities that we detected, to ensure our clients' security.



Tomáš **ZAŤKO**
CITADELO CEO



Hackers on your side

Feeling vulnerable?
Let's hack-proof your business.
Contact us at: sales@citadelo.com