CITADELO

Ethical Hacking Report

2,677 WAYS WE HACKED
OUR CLIENTS

MANAGEMENT SUMMARY

275 PROJECTS

tested in 2021

5 NEW PROJECTS

tested per week on average

10 VULNERABILITIES

found in every project on average

2,677

vulnerabilities found in total

1 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 2021 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 2021. The statistics we gathered from our own first-hand testing of over 275 projects revealed a total of 2,677 vulnerabilities of varying criticality. We performed penetration tests on an average of 5 projects per week and found an average of 10 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 project risks, from suggested best practices to critical vulnerabilities. We use the following risk types to categorize the vulnerabilities we identify:

NOTE	Deviation from best practices that should be corrected to ensure optimal security (missing headers, verbose errors)
LOW	Vulnerabilities that present low technical impact or have very low likelihood but should not be left exposed
MEDIUM	Vulnerabilities that present a considerable technical risk to projects and should be dealt with asap (SSRF, 2FA bypass)
HIGH	Vulnerabilities that present a very serious technical risk to projects and require swift resolution (e.g. XSS, XXE)
CRITICAL	Vulnerabilities that present immediate and potentially disastrous technical risks to projects (e.g. SQL injection, RCE, code/command injection, authentication bypass)

The following chart gives a full overview of the tests performed by Citadelo in 2021:

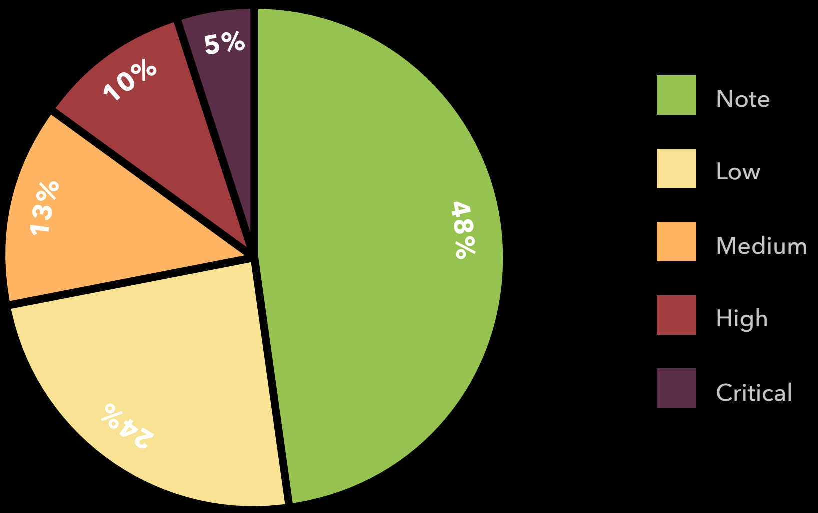
OVERALL RESULTS

	Web	API	Mobile	Infra	Cloud	Combined	Other	Total
No. of projects	118	22	24	32	18	41	20	**275**
Note	631	67	196	115	55	174	44	**1282**
Low	232	24	43	62	118	120	36	**635**
Medium	125	13	22	32	50	58	20	**346**
High	89	10	15	19	55	58	20	**266**
Critical	54	4	3	21	14	42	10	**148**
Total	1131	118	279	249	292	478	130	**2677**

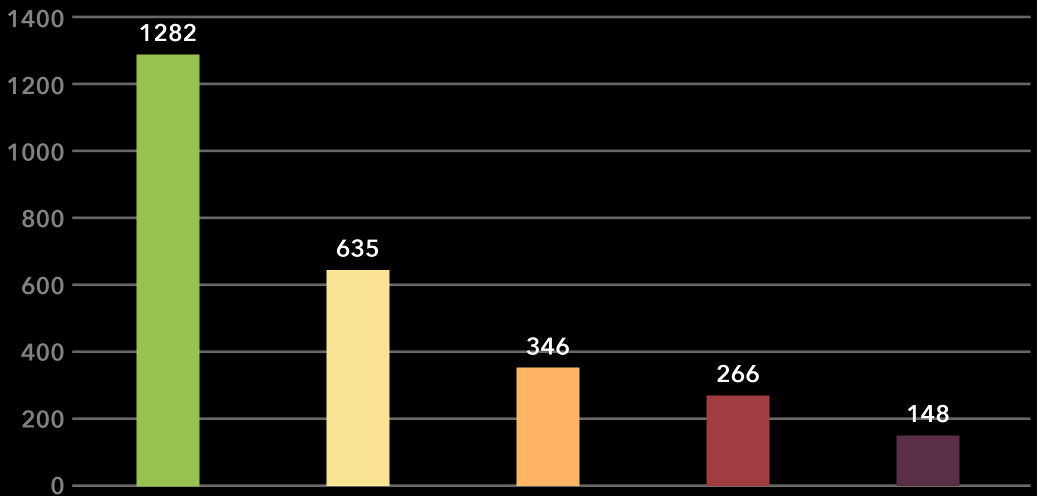
PREVALENCE OF VULNERABILITIES

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

VULNERABILITY RISKS IN 2021:



NUMBER OF VULNERABILITIES FOUND BY TYPE IN 2021



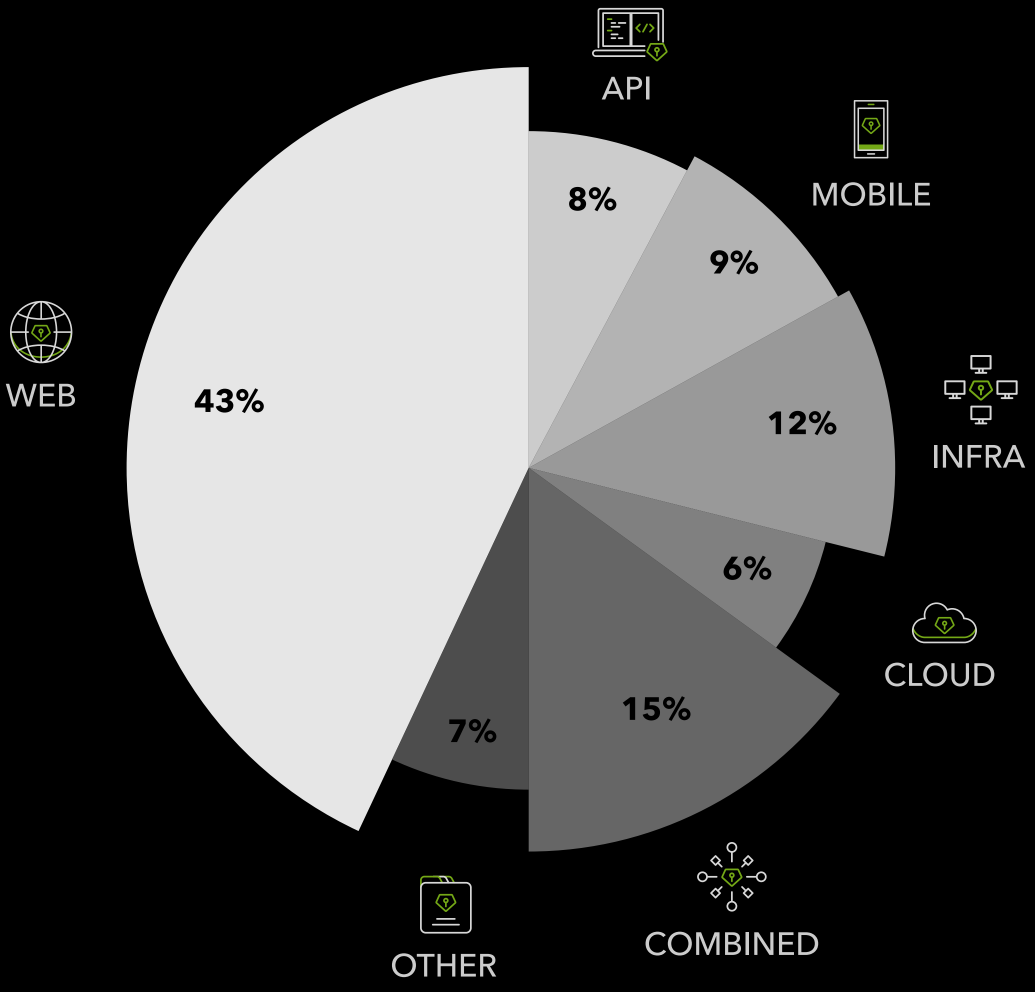
As a rule of thumb, the less critical the risk, the more frequently it is likely to be exposed in any given project type. On average, Note risks made up the highest proportion of vulnerabilities identified at 48%. These types of risks are still highly advisable to resolve but do not present an immediate threat to projects. Critical risks, on the other hand, made up just 5% 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 50% of all projects. Infrastructure and combined projects were the next most common types, at 12% and 15%, respectively, followed closely by mobile apps at 9%. The number of cloud projects tested continued to rise in 2021 to 6%, also making up a significant portion of the combined project types in our study. The remaining portion of projects tested was largely made up of desktop apps, ATMs, and social engineering projects.

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

PROJECT TYPES IN 2021:



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.

COMBINED

Combined projects consist of several different types of sub-projects, and thus, logically, contained the highest average number of vulnerabilities. The variety of project types results in a higher potential for more widespread vulnerabilities, as all common vulnerabilities of every previously mentioned project type can arise in combined projects.

INFRASTRUCTURE

Infrastructure projects power a wide range of industries, but made up just 12% 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.

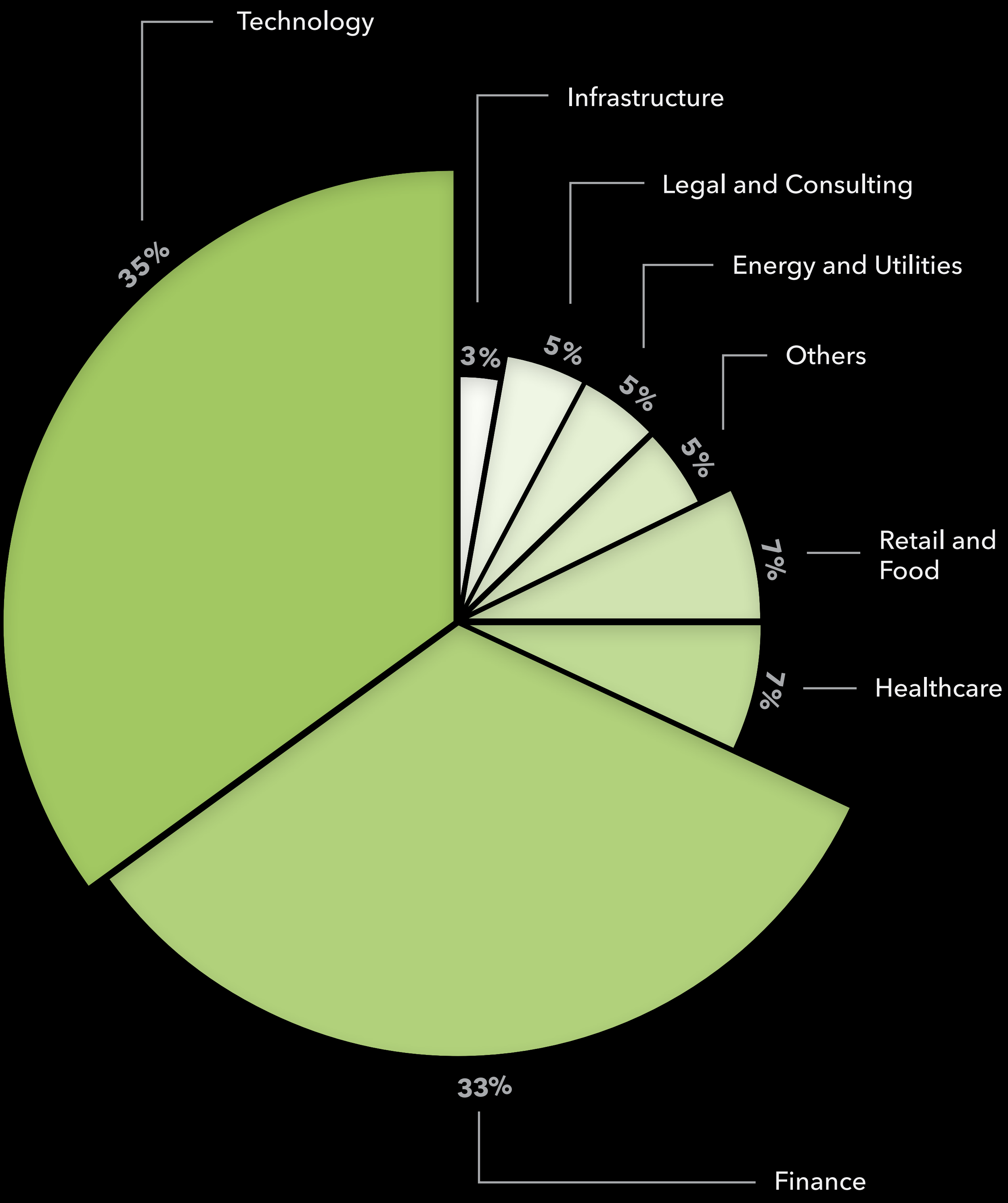
OTHER

The "other" project type encompasses any project that does not fall under the previous categories, and represents a very small statistical sample. Since these projects are not closely related by any common parameters and are widely dispersed across different industries and product verticals, it is difficult to draw any statistically meaningful conclusions from within this subset.

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:



CONCLUSION

The over 2,677 vulnerabilities we found present a snapshot of the current state of cybersecurity and the importance of penetration testing in 2022. While less serious errors made up the vast majority of vulnerabilities, the 148 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.

> *"Upon first glance, it may seem alarming that our team managed to find so many vulnerabilities last year. But I think it's fantastic: we eliminated 2,677 different ways hackers could attack our clients' systems, and protected their critical data from being tampered with or stolen."*

Tomáš **ZAŤKO**
CEO CITADELO

CITADELO

Hackers on your side

Contact sales@citadelo.com

www.citadelo.com