CITADELO

Ethical Hacking Report

2,795 ways we hacked
our clients in 2023

www.citadelo.com

Management summary

2,795 **VULNERABILITIES**
found in total

384 **PROJECTS**
tested in 2023

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

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

2 **CRITICAL**
vulnerabilities found in projects analyzed

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 2023 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 2023.

How we got our numbers

This report analyzes the risks identified in projects tested by Citadelo during 2023. The statistics we gathered from our own first-hand testing of over 384 projects revealed a total of 2,795 vulnerabilities of varying criticality. We performed penetration tests on an average of 7 projects per week and found an average of 7 vulnerabilities in every project. The number of projects decreased since our last report due to increased level of MDs per projects as well as client demands of diversifiyng categories of testing, which were not as prioritized by clients in 2022.

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:

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 2023:

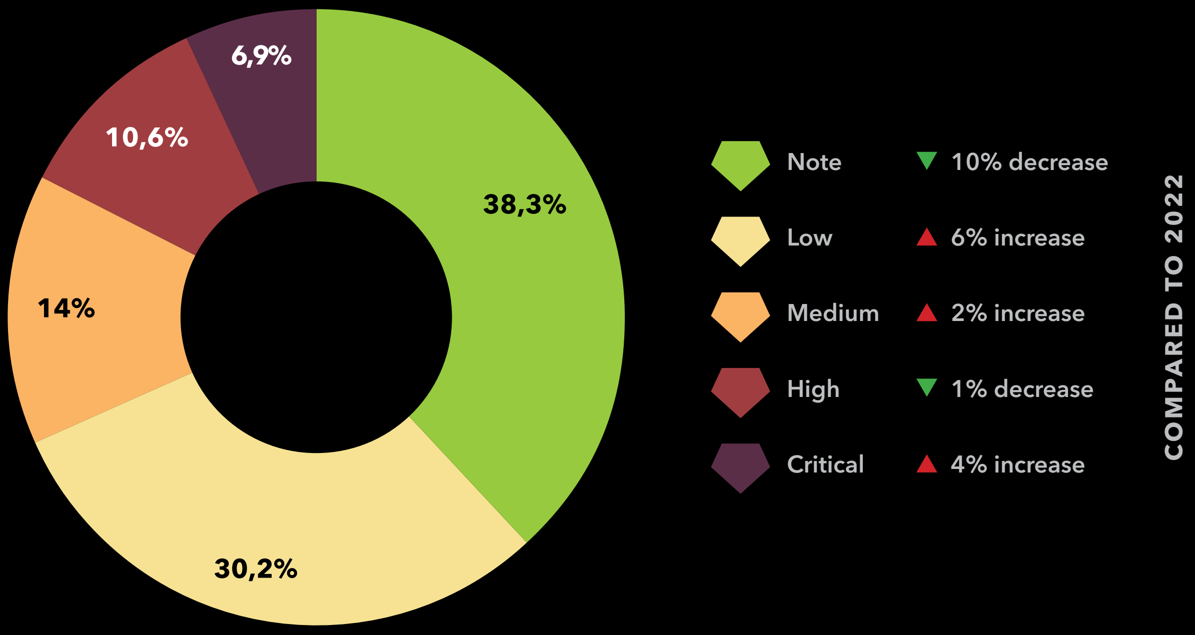
OVERALL RESULTS FOR 2023:

	Web	Application	Mobile	Combined	Custom/Other	API	Infra	Cloud	Social Engineering	Total
# of reports	210	20	20	7	9	30	25	39	24	384
Note	558	39	125	27	22	73	80	128	19	1071
Low	333	14	33	20	19	27	87	303	9	845
Medium	153	6	14	18	17	7	80	74	22	391
High	144	13	8	14	12	14	46	31	14	296
Critical	70	15	4	10	6	5	56	7	19	192
Total	1258	87	184	89	76	126	349	543	83	2795

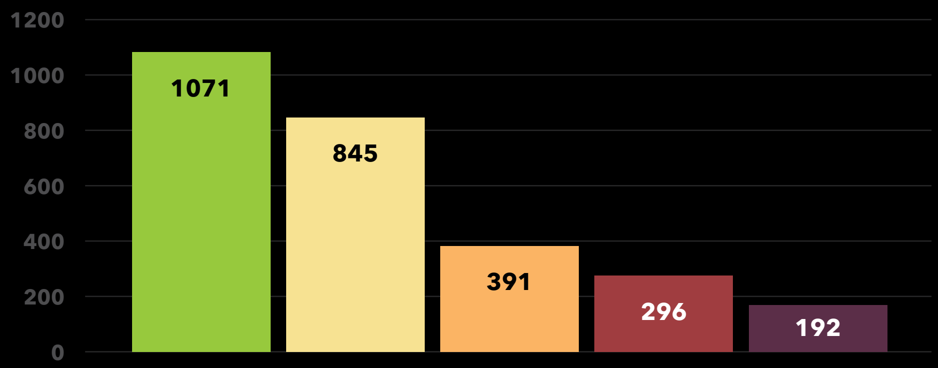
Prevalence of vulnerabilities

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

VULNERABILITY RISKS IN 2023:



NUMBER OF VULNERABILITIES FOUND BY TYPE IN 2023:



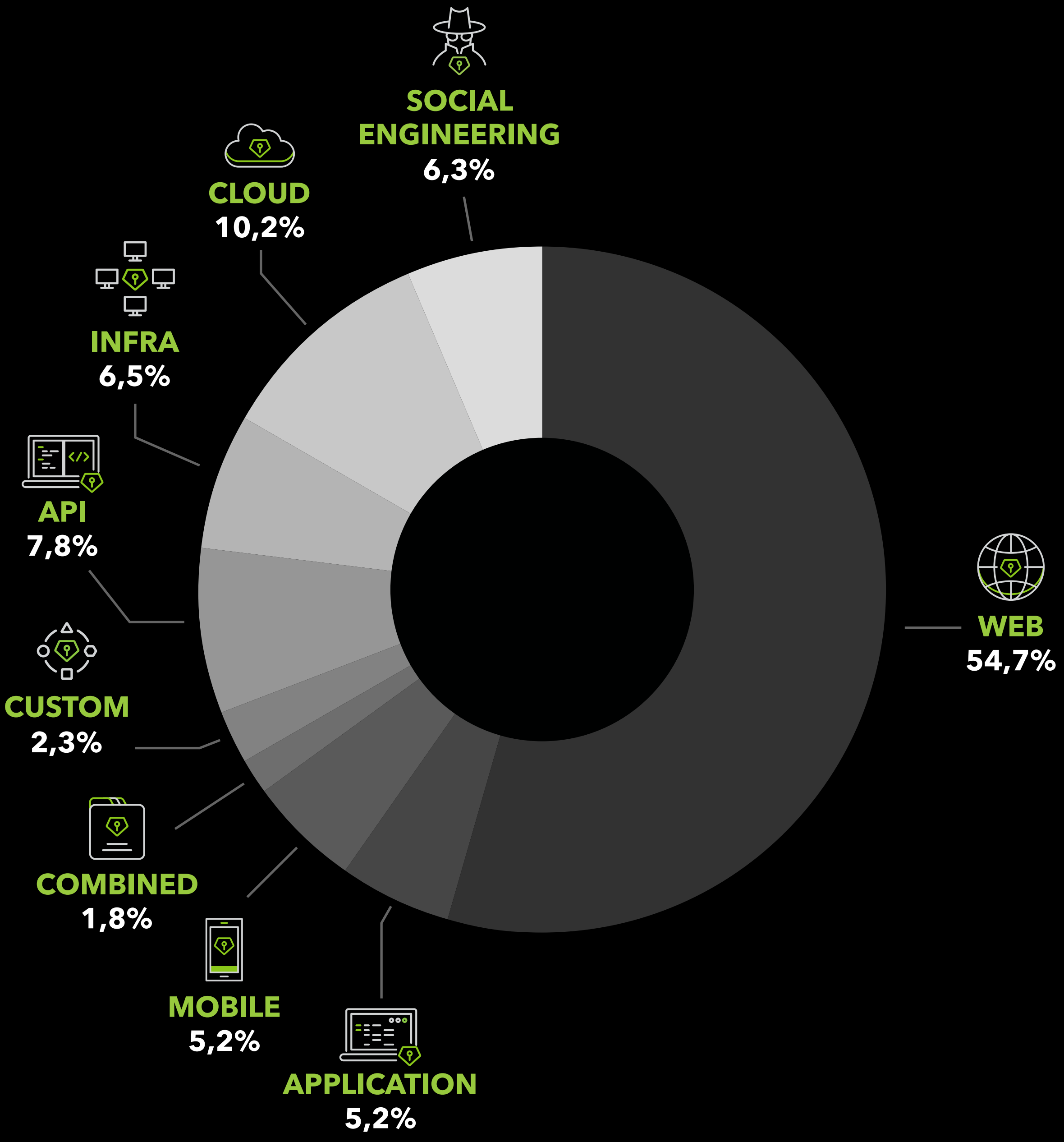
As a rule of thumb, the less critical the risk, the more frequently it is likely to be exposed in any given project type. On average, Note risks made up the highest proportion of vulnerabilities identified at 38%. These types of risks are still highly advisable to resolve but do not present an immediate threat to projects. Critical risks, on the other hand, made up 7% 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 were by far the most common, comprising over 55% of all projects. Cloud project (AWS, Azure and GCP) were the next most common types at 10 %, while API projects were close at 8%. Infrastructure was at 7%, closely followed by Social Engineering (Phishing,Vishing, OSINT and Red Teaming) at 6%, Mobile and Application (Windows apps) both at 5%. Lastly we've had Custom projects at 2% and Combined projects finishing at 2%.

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

PROJECT TYPES IN 2023:



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.

MOBILE AND APPLICATIONS

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, s 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. The variety of project types resulted in 2% of our projects done in 2023.

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.

INFRASTRUCTURE

Infrastructure projects power a wide range of industries, but made up just 7% 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.

SOCIAL ENGINEERING

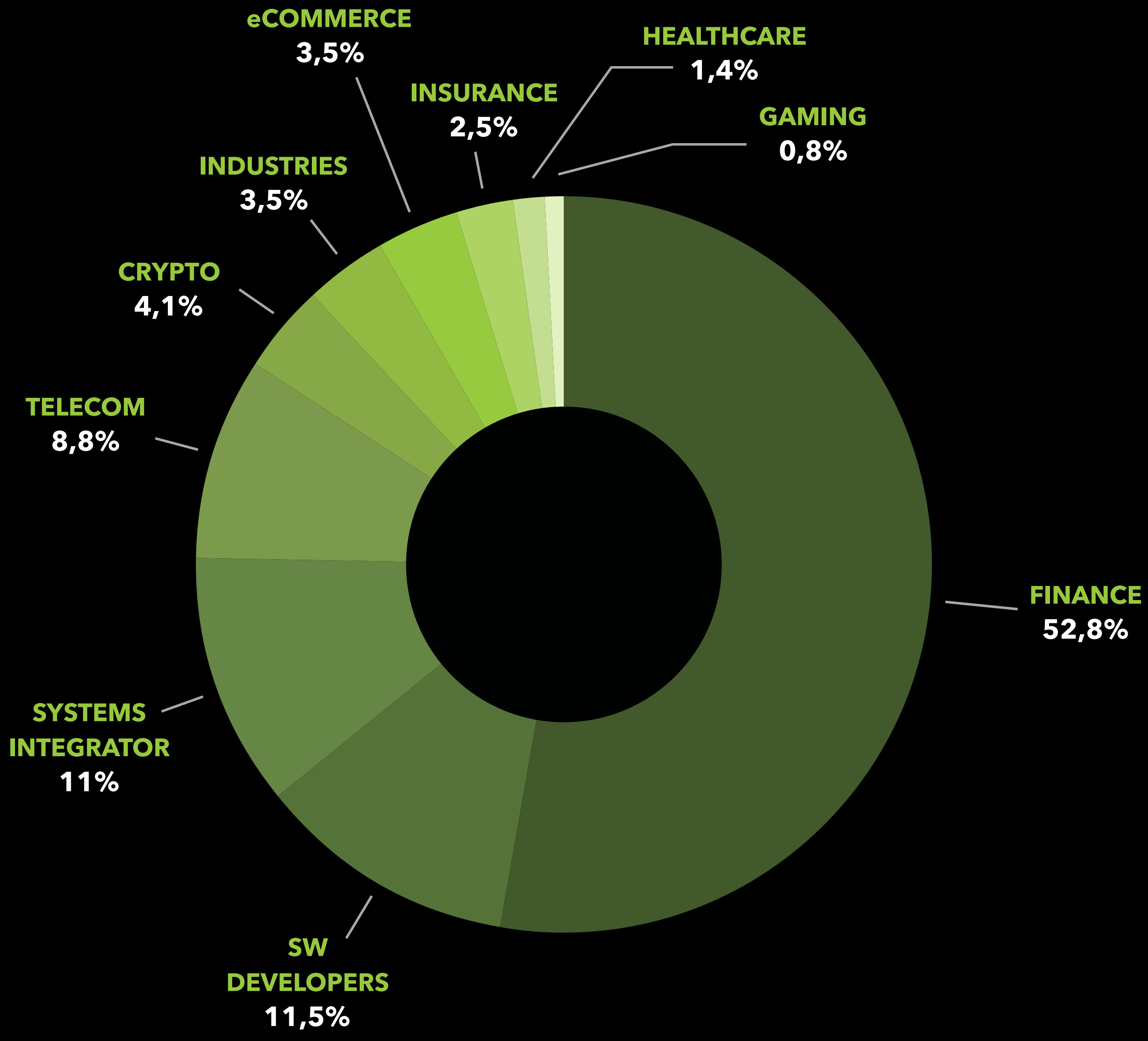
Social engineering, especially phishing (vishing), OSINT campaigns and Red-teaming exeprienced even bigger increase. We have been pleasantly suprised by the number of projects in comparison to year 2022. As social engineering is still leading as the most common type of cyber attack, we could not recommend enough to plan this type of testing of your organisation and your team, to keep the data of your clients and the data of your company safe.

Industries we tested

Citadelo provided penetration testing and security audits for a wide range of industries in 2023. While the vast majority of projects (53%%) fell under the broadly defined Finance sector, clients from the SW Developers were the second biggest field, making up 12% of all projects tested. The remaining sectors were fairly evenly distributed, each making up between 3 and 11% of all projects tested.

Please consult the table below for a full breakdown of the industries tested in 2023:

TYPES OF INDUSTRY SEGMENTS IN 2023:



Conclusion

The over 2,795 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 192 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 2,795 different ways hackers could attack our clients' systems, and protected their critical data from being tampered with or stolen.***

Tomáš ZAŤKO
CEO of CITADELO
Expert Division of Ethical Hacking at Boltonshield

Citadelo services

More information on our website **HERE.**

Cloud Security Testing

Elevate your cloud infrastructure security with our comprehensive Cloud Security Testing services. Tailored to identify and mitigate vulnerabilities, our approach ensures your cloud environment is secure and resilient. We cover:

- **Amazon Web Services (AWS) Security Testing** Identifying misconfigurations and vulnerabilities unique to AWS environments.
- **Google Cloud Security Enhancements:** Strengthening your Google Cloud configurations and access management.
- **Microsoft Azure Security Assessments:** Ensuring the security of Azure, Office 365, and Azure Active Directory.
- **Custom Cloud Penetration Testing:** Black-box penetration testing tailored to reveal hidden vulnerabilities in your cloud setup.

Internal Infrastructure Penetration Testing

Discover and mitigate internal threats with our penetration testing, designed to simulate attacks from within your network. This insider perspective helps identify vulnerabilities that could be exploited by employees, ensuring a secured internal defense mechanism.

Red Teaming

Strengthen your security with our Red Teaming exercise, combining OSINT, black-box penetration testing, and social engineering to assess system integrity, staff readiness, and overall resilience of your infrastructure against real-world attacks.

MAIN DIFFERENCES BETWEEN STANDARD PENETRATION TESTING AND RED TEAMING:

PENETRATION TESTING	RED TEAMING
Broad testing - Find as many vulnerabilities as possible	**In-depth testing - Find the one major vulnerability to get into the system and take full advantage of it to achieve the objective**
A short period of time	**A longer period of time**
The goal is to identify the vulnerabilities of a specific area (unit)	**The goal is to test the resilience of the entire company's defenses**
Clearly defined scope of the project (several systems or applications)	**The scope of the project is to test the entire company's security and vulnerabilities to achieve the objective and identify aspects that could be misused**
The IT department knows about the testing and closely cooperates with the security/pentesting company	**The IT department (blue team) has no idea about the ongoing exercise**
To test the system unit	**The goal is to test the IT department's ability to recognize and defends against any random cybersecurity attack**
–	**To test the employees' knowledge and capability of resisting the social engineering techniques that are used today**
–	**The company's physical security is also part of the test**
Applications are tested according to the OWASP methodology	**Is not possible to follow any methodology**

Contact our Sales Force Here!

Tomáš HORVÁTH
Sales Director

Jakub NOVÁK
Sales Manger

Tomáš KEBORT
Sales Manger

CITADELO

Hackers on your side

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

www.citadelo.com