

Vulnerability Disclosure Policy

Table of Contents

I. Introduction 3
II. Scope 3
III. Reporting a Vulnerability 3
IV. Our Commitment 3
V. Eligibility for Acknowledgements 4
VI. Third-Party Services 4
VII. Underlying Vulnerabilities 4
VIII. Good Faith Effort 4
IX. Conclusion 5
Appendix 1: Example of vulnerability disclosure report 6

I. Introduction

At 365.bank, a.s., we prioritize the security of our systems and the protection of our customers' data. We value the contributions of the security community who take time and effort in identifying vulnerabilities and helping us improve our security posture by reporting it according to this policy. This policy outlines the process for reporting vulnerabilities and how we acknowledge the efforts of security researchers. We do not offer monetary rewards.

II. Scope

Main website https://365.bank and any subdomain *.365.bank

III. Reporting a Vulnerability

If you have identified a potential security vulnerability in our systems, we encourage you to report it to us responsibly. Please follow these steps:

1. Contact Information: Send an email to security365@365.bank with the subject line "Vulnerability Disclosure". Emails can be encrypted with the PGP key https://365.bank/security/gpg-key.txt
2. Report: Include detailed information about vulnerability, including:
    a. Description of the vulnerability
    b. Asset where you found it (IP address, URL, etc.)
    c. Steps to reproduce
    d. Any relevant screenshots or proof-of-concept code
    e. Optionally:
        i. Potential impact
        ii. Any mitigations or recommendations
        iii. Your contact details (name, link to your LinkedIn or other public profile), if you want mention on the acknowledgment page
3. Confidentiality: Do not publicly disclose the vulnerability until we have had a reasonable amount of time to address it.

Low-quality reports, such as those which only contain automated output, will be rejected. In addition, reports generated solely by AI are not acceptable.

IV. Our Commitment

- Acknowledgment: We will acknowledge receipt of your report within 5 business days.
- Investigation: We will investigate the reported vulnerability and provide you with an estimated timeline for remediation.
- Updates: We will keep you informed of our progress throughout the remediation process.
- Recognition: If you are the first to report a vulnerability that leads to a code or configuration change, and you follow this policy, we will acknowledge your contribution on our Acknowledgements page: https://365.bank/security/acknowledgements.html

V. Eligibility for Acknowledgements

We will refuse credits where researchers breach the rules below or do not otherwise behave responsibly and ethically. Reports we do not class as security issues are not eligible for an acknowledgement on this page; these include but are not limited to:

- Directory Listings and FTP sites: Our products are based on open source components and we make certain content available using directory listings and via anonymous FTP. Please only report these if you find (what can reasonably be assessed as) non-public content being exposed.
- Version Numbers: We do not hide the version numbers of online service components and you should expect these will not be the latest upstream versions.
- Secure Certificate Issues: Mismatched host names, expired certificates, support for older protocols such as SSLv3.
- Reports from automated tools or scanners without manual verification and analysis.
- Theoretical attacks without proof of exploitability.
- Brute force attacks (e.g., on passwords or tokens).
- Attacks involving any user accounts not created by you.
- Attacks involving physical access to a user's device or involving a device or network that is already compromised.
- Missing security headers that do not lead directly to a vulnerability.
- Clickjacking.
- Cookies missing Secure or HttpOnly flags.
- Bugs that rely on an unlikely user interaction.
- Issues that are the result of a user deliberately performing an insecure action (like sharing their password or API tokens publicly).
- Social engineering of 365.bank staff or users.
- Issues related to password and account recovery processes.
- Sender Policy Framework (SPF), DKIM and DMARC configuration suggestions

VI. Third-Party Services

Some 365.bank branded services are operated by third parties. If you notify us about security issues on such sites, we will coordinate fixes with the affected vendors and acknowledgements may be given by those vendors or under their rules.

VII. Underlying Vulnerabilities

Some security issues may be due to underlying vulnerabilities in third-party applications that we use. In these cases, we will coordinate fixes with the application vendor and acknowledgements may be given by those vendors or on our CVE dictionary pages.

VIII. Good Faith Effort

We expect you to make a good faith effort to avoid privacy violations, destruction of data, or degradation to our service during your research. Please avoid using tools that are likely to automatically generate significant volumes of traffic or otherwise cause operational problems for our sites.

IX. Conclusion

We appreciate the efforts of the security community in helping us maintain the security and integrity of our systems. Thank you for your contributions.

Appendix 1: Example of vulnerability disclosure report

Report Section	Description/Example
Description (M)	When submitting a crafted JavaScript payload via the "username" parameter, the input is reflected unsanitized, enabling malicious script execution in users' browsers. See attached screenshot and proof-of-concept payload below.
Asset (M)	https://www.example.com/login
Steps to Reproduce (M)	1. Open https://www.example.com/login 2. Input <script>alert('xss')</script> in the "username" field 3. Submit the form 4. Observe alert popup in the browser due to reflected payload.
Supporting Files	Attached screenshot and proof-of-concept code.
Impact	Successful exploitation allows attackers to execute arbitrary JavaScript in victim's browser, leading to potential credential theft, session hijacking, and further compromise of user accounts.
Mitigations or recommendations	Input validation, consider all potentially relevant properties, including length, type of input, the full range of acceptable values, missing or extra inputs, syntax, consistency across related fields, and conformance to business rules. As an example of business rule logic, "boat" may be syntactically valid because it only contains alphanumeric characters, but it is not valid if the input is only expected to contain colors such as "red" or "blue."
Weakness	CWE-79: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')
Contact Details	Name: Kevin Mitnick Email: kevin@mitnick.com LinkedIn: https://www.linkedin.com/in/kevinmitnick/

(M) mandatory field