Responsible Disclosure Policy

JSC “TBC Insurance” takes the security and privacy of our users, products, and staff very seriously. If you discover a vulnerability in our websites, we encourage you to help us mitigate it by disclosing it responsibly. Should you find any issues on our web presence, we'd appreciate it if you reported them to us. Our security team reviews all vulnerability reports and takes action in line with responsible disclosure practices and the issue's criticality. We aim to respond to all reports within 10 business days. We will keep you updated as we work through the reports and strive to resolve them as quickly as possible.

Guidelines for Responsible Disclosure

- Conduct research only within the "In Scope" defined in this Policy.
- You MUST add the following string to the HTTP header User-Agent: "pentester - [your full name here]";
- If the vulnerability could be used to obtain sensitive information about our company's customers, please include a complete list of requests you sent during testing in your report;
- Email your findings ONLY to our security team at websecurity@tbcinsurance.ge . Include comprehensive information about the vulnerability, its impact (specific to your case), POC video and detailed steps to reproduce it including used tools and commands.
- Disclosure of any vulnerability is prohibited without written consent from JSC “TBC Insurance”. This rule applies to all vulnerability details and information obtained during penetration testing, even for resolved issues;
- Maintain open communication channels to enable effective collaboration;
- Make every effort to avoid privacy violations, degradation of user experience, disruption to production systems, and destruction of data during security testing;
- If your report involves a "qualifying vulnerability" (described below) and you'd like to be included in our "Hall of Fame," please provide your full name or nickname;
- Automated scanning tools MUST be limited to a maximum of 10 requests per second to a single target host, considering all tools and threads running concurrently;
- Submit one vulnerability per report, unless you need to chain vulnerabilities to demonstrate impact;

What you can expect from us

- We will work with you to understand and resolve the issue to enhance the protection of our customers and systems;
- If you adhere to the guidelines outlined above, we will not pursue or support any legal action related to your research;
- We will respond to your report within 10 business days of submission;
- If you are the first to responsibly disclose a "qualifying vulnerability" according to this Policy, and we implement a code or configuration change based on your report, we will recognize your contribution on our "Hall of Fame" list;

In Scope

- *.tbcinsurance.ge

Out of Scope

Any services hosted by third-party providers and anything not explicitly mentioned in the "In Scope" section are excluded.

What constitutes a “Qualifying Vulnerability”?

A qualifying vulnerability must meet the following criteria:

- It affects a service or domain listed in the "In Scope" section above;
- It is included in the "Qualifying Vulnerabilities" list below;
- You are the first researcher to responsibly disclose the vulnerability;
- You adhere to the responsible disclosure guidelines set out in this Policy, including allowing us a reasonable time to address the vulnerability. We will confirm this timeframe with you after you disclose the vulnerability;

In general, in-scope submissions should involve vulnerabilities that could realistically pose a risk to the online security of JSC “TBC Insurance” or its customers.

Qualifying vulnerabilities typically exhibit these characteristics:

- Directly or indirectly impact the confidentiality or integrity of user sensitive data or privacy;
- Compromise the system's integrity;
- Enable unauthorized access to sensitive data or resources;
- Allow the execution of unauthorized code with privileged user rights;
- Interfere with or bypass security controls or mechanisms;
- Are exploitable (not just theoretical);

Qualifying Vulnerabilities

We are particularly interested in vulnerabilities in the following areas:

Cross-Site Scripting (XSS)

XML External Entity Injection (XXE)

Cross-Site Request Forgery (CSRF)

Server-Side Request Forgery (SSRF)

Injection (SQLi, CRLF, etc.)

Local/Remote File Inclusion (LFI/RFI)

Remote Code Execution (RCE)

Authentication Issues

Authorization Issues

Privilege Escalation

Account Takeover

Sensitive Data Disclosure and/or Manipulation

Out of Scope

Please note that we do not accept reports on the following categories:

- Any activity that could disrupt our service (DDoS/DoS, etc.);
- Attacks requiring MITM or physical access to a user's device;
- Clickjacking on pages without sensitive actions;
- Use of automated tools that could generate significant traffic and potentially impair our application's functionality;
- Disclosure of non-sensitive information (e.g., product version, file path on a server, stack trace);
- Disclosure of private IP addresses or domains pointing to private IP addresses;
- Leakage of sensitive tokens (e.g., password reset tokens) to trusted third parties over a secure connection (HTTPS);
- Missing best practices in SSL/TLS or DNS configuration (DKIM/DMARC/SPF/TXT)
- Missing best practices in headers without demonstrating a vulnerability;
- Missing notifications about important actions;
- Missing protection mechanisms or best practices without demonstrating a real security impact;
- Previously known vulnerable libraries without a working proof of concept;

- Automated tool output without a working proof of concept;
- Unauthenticated/login/logout CSRF;
- User enumeration;
- Vectors requiring browser versions released 6 or more months before the report submission;
- Comma Separated Values (CSV) injection without demonstrating a vulnerability
- Content spoofing and text injection issues without showing an attack vector/without being able to modify HTML/CSS;
- Issues experienced in end-of-life and no longer supported web browser;

JSC "TBC Insurance" reserves all legal rights in the event of any non-compliance with the following guidelines:

- Do not disclose or discuss any bug or vulnerability (even if resolved) anywhere or with anyone without written consent from JSC "TBC Insurance";
- If you discover a vulnerability, you are not authorized to exploit it to compromise or expose any data. Furthermore, you are not authorized to access, view, modify, delete, copy, capture, or share any data exposed by the vulnerability;
- Do not perform DDoS/DoS or Brute Force attacks or degrade services in any way;
- Do not install programs, scripts, or malware on any JSC "TBC Insurance" resource, nor use these resources to control or distribute such malicious software;
- Never engage in phishing, social engineering, or physical attacks against our users, employees, or infrastructure;

Bug Bounty

JSC "TBC Insurance" does not offer monetary bug bounty payments. Instead, in the case of an original and valid vulnerability discovery, we will recognize security researchers by adding them to our "Hall of Fame" list.

Hall of Fame

Dachi Ketiladze