Vulnerability disclosure page

VTEX has a channel to receive communications about potential vulnerabilities in its systems and undertakes not to “sue” the users who report them, as long as the rules below are complied with:

1. Only VTEX systems are tested. We do not authorize testing on customer or supplier pages.
2. The pages availables to be tested are:
    a. Use securitystore.myvtex.com (and others e.g.) as an entry point
    b. Scoped domains mean the VTEX properties used to support the store:
    c. vtexassetsjj
    d. vtex.io
    e. vtexcommercesable
    f. vtexpayments

3. The security researcher performing the test must:
    a. create your own user accounts;
    b. prevent violations of the privacy of others, including other security researchers;
    c. report crashes as soon as you find them, and don’t use crashes to “scale out” access;
    d. make a good faith effort to avoid damage to the VTEX production environment (e.g. not attempt mass deletions, DoS attacks, etc. etc.);
    e. give VTEX reasonable time to investigate and resolve security issues before publishing the results of the iterations.

4. VTEX reserves the right to:
    a. distribute the content of the reports internally and share them with any third parties you deem necessary;
    b. publish interactions with researchers (including programs);
    c. publicly thank researchers who reported failures;
    d. investigate any activity that can be attributed to the person submitting the report on others;
    e. run any program sent as a PoC;
    f. change the rules of this program;

You can contact us via security at vtex.com