Vulnerability Disclosure Policy

Trustpage takes the security of our systems seriously, and we value the security community. The disclosure of security vulnerabilities helps us ensure the security and privacy of our users.

Guidelines

We require that all researchers:

- Make every effort to avoid privacy violations, degradation of user experience, disruption to production systems, and destruction of data during security testing
- Perform research only within the scope set out below
- Use the identified communication channels to report vulnerability information to us
- Keep information about any vulnerabilities you've discovered confidential between yourself and Trustpage until we've had 90 days to resolve the issue.

If you follow these guidelines when reporting an issue to us, we commit to:

- Not pursue or support any legal action related to your research
- Work with you to understand and resolve the issue quickly (including an initial confirmation of your report within 72 hours of submission)
- Recognize your contribution on our Security Researcher Hall of Fame, if you are the first to report the issue and we make a code or configuration change based on the issue
- Consider paying a cash reward if the vulnerability is determined to be of high impact and probability

📌 The impact assessment is based on the attack's potential for causing privacy violations, financial loss, and other user harm, as well as the user-base reached.

The probability assessment takes into account the technical skill set needed to conduct the attack, the potential motivators of such an attack, and the likelihood of the vulnerability being discovered by an attacker.

In Scope

Services

In principle, any Trustpage-owned web service that handles reasonably sensitive user data is intended to be in scope. This includes virtually all the content in the following domains:

- *.trustpage.com
- *.preview.trustpage.app

Qualifying vulnerabilities

Any design or implementation issue that substantially affects the confidentiality or integrity of user data is likely to be in scope for the program. Common examples include:

- Cross-site scripting
- Cross-site request forgery
- Mixed-content scripts
- Authentication or authorization flaws
- Server-side code execution bugs

Out of scope

Services

Any services hosted by third-party providers and services are excluded from scope. These services include any services listed in our Trust Center as a subprocessor.

Non-qualifying vulnerabilities

In the interest of the safety of our users, staff, the Internet at large and you as a security researcher, the following test types are excluded from scope:

- Findings from physical testing such as office access (e.g. open doors, tailgating)
- Findings derived primarily from social engineering (e.g. phishing, vishing)
- Findings from applications or systems not listed in the ‘Scope’ section
- UI and UX bugs and spelling mistakes
- Network level Denial of Service (DoS/DDoS) vulnerabilities
- Cross-site scripting vulnerabilities in “sandbox” domains
- URL redirection
- Legitimate content proxying and framing
- Bugs requiring exceedingly unlikely user interaction
- Flaws affecting the users of out-of-date browsers and plugins
- Logout cross-site request forgery
- User enumeration

Things we do not want to receive:

- Personally identifiable information (PII)
- Credit card holder data

How to report a security vulnerability?

If you believe you’ve found a security vulnerability in one of our products or platforms please send it to us by emailing security@trustpage.com. Please include the following details with your report:

- Description of the location and potential impact of the vulnerability;
- A detailed description of the steps required to reproduce the vulnerability (POC scripts, screenshots, and compressed screen captures are all helpful to us); and
- Your name/handle and a link for recognition in our Hall of Fame.