PGi Bug Bounty Program

January 2021

Overview

PGi encourages security researchers to contact us with their findings. Findings should be truly novel (not previously reported), not passed on from reports output from vulnerability scanners *and* must show some demonstrable risk to PGi's assets, customers or reputation. If you discover a site or product vulnerability that you believe may qualify, please notify us using the guidelines below.

By submitting a vulnerability, you acknowledge that you are agreeing to the terms and conditions of PGi's program below.

Please submit all bug bounty reports to: globalsecurity@pgi.com

Reports sent to other email addresses including marketing may not get responses, or delayed response.

Services in Scope

Domains:

- *.Globalmeet.com
- Pgi.com
- Pgi.hub.globalmeet.com
- *.Imeetcentral.com
- *.webcasts.com
- PGI Official Partner Sites – partners.pgi.com/*

APIs: Any public API associated with one of the above domains.

Besides these domains, PGi has ties to several third-party marketing sites that are hosted by our vendors, acquisitions or partners. We cannot authorize you to test these systems on behalf of their owners and will not reward any such reports.

Vulnerabilities in Scope

While we don't spell out specifically what is in scope, in general any design or implementation issue that substantially affects the confidentiality or integrity of PGi or user data is likely to be in scope for the program. Common examples include:

- Stored XSS

- Authentication bypasses or weaknesses that could allow impersonation or account hijacking
- Injection vulnerabilities that can be leveraged into server-side execution or file system tampering
- Data exposure, of a sensitive nature

Vulnerabilities out of Scope

Certain vulnerabilities are considered out-of-scope for the Bug Bounty Program. Those out-of-scope vulnerabilities include, but are not limited to:

- Vulnerabilities dependent upon social engineering techniques (e.g. shoulder attack, stealing devices, phishing, fraud, stolen credentials)
- Host Header
- Version disclosure in headers - disclosures like versions of software running will only be accepted with a PoC showing how that may be exploitable.
- Missing Security headers such as X-XSS-protection, Content-Security-Policy, as these are easily bypassed and only valid to the extent that the browser enforces them.
- Denial of service (DOS)
- Self-XSS (User defined payload) – XSS attacks should show more than a single user affecting their own account or trivial client-side rendering of HTML/JavaScript
- Login/logout CSRF
- Content spoofing without embedded links/HTML
- Vulnerabilities which require a jailbroken mobile device
- Clickjacking or iframe based attacks.
- Infrastructure vulnerabilities, including:
    - Certificates/TLS/SSL related issues
    - DNS issues (i.e. MX records, SPF records, etc.)
    - Server configuration issues (i.e., open ports, TLS, etc.)
    - Weak SSL Ciphers without a PoC on how that could be leveraged into a loss of confidentiality or sensitive data
- Most vulnerabilities within our sandbox, lab, QA or staging environments.
- Outdated web browsers: vulnerabilities contingent upon outdated or unpatched browsers will not be honored, including Internet Explorer versions prior to version 8
- Vulnerabilities involving active content such as web browser add-ons

Code of Conduct

Please submit all vulnerabilities found during testing, at once. Submitting findings one by one, in a sequential fashion, is **not permitted** and will result in no bounty payment, or reduced payment for only the first submission.

Please include:

- Full description of the vulnerability being reported including the exploitability and impact
- Document all steps required to reproduce the exploit of the vulnerability
- Provide all:

- URL(s)/application(s) affected in the submission (even if you provided us a code snippet\video as well)
- IPs that were used while testing
- Always include the user ID that is used for the Proof-of-concept (PoC)
- Always include all the files that you attempted to upload
- Provide the complete PoC for your submission (e.g. For RCE's do not change files, upload only "hello world" test files, etc.)
- Please save all the attack logs and attach them to the submission.

When investigating a vulnerability, please, only ever target your own accounts. Never attempt to access anyone else's data and do not engage in any activity that would be disruptive or damaging to your fellow users or to PGi.

Bounty Payments

You may be eligible to receive a monetary reward, or "bounty," if: (i) you are the first person to submit a site or product vulnerability; (ii) that vulnerability is determined to by a valid security issue by PGi's security team; and (iii) you have complied with all Program Terms.

Bounty payments, if any, will be determined by PGi, at PGi's sole discretion. In no event shall PGi be obligated to pay you a bounty for any Submission. All bounty payments shall be considered gratuitous.

Legal Stuff

You may not publicly disclose your findings or the contents of your Submission in any way without PGi's prior written approval.

By providing your Submission, you hereby grant PGi, its subsidiaries, affiliates and customers a perpetual, irrevocable, worldwide, royalty-free, transferrable, sublicensable (through multiple tiers) and non-exclusive license to use, reproduce, adapt, modify, publish, distribute, publicly perform, create derivative work from, make, use, sell, offer for sale and import the Submission, as well as any materials submitted to PGi in connection therewith, for any purpose.

The Bug Bounty program, including its policies and code of conduct, is subject to change or cancellation by PGI at any time, without notice. As such, PGI may amend these Program Terms and/or Code of Conduct at any time. By continuing to participate you accept the Program Terms, as modified.

Your testing must not violate any state, federal or other law, and must not disrupt PGi's operations. You are responsible for any and all consequences if you fail to comply with any law and ignorance of the law is not a valid reason.

Participation in this program is voluntary and can be ended at any time, at PGi's discretion.