THG

IDEAS WITH MOMENTUM®

THG Security Issues

If you believe you have found a potential security vulnerability on any of our domains, we encourage you to report it to us responsibly by emailing us at **SecurityBugs@thehutgroup.com**. We will investigate all legitimate reports and take the appropriate actions. Before reporting though, please review this page.

Bug Bounty Programme:

The programme is at our discretion. We will try to investigate the issue in timely manner, however we may need time to investigate issues that are not straightforward.
To qualify for a bounty, you must comply with the following:

- Identify a vulnerability in our system that creates a security or privacy risk.
- Any inadvertent privacy violation, or disruption of service during testing must be disclosed immediately.
- Produce enough information for us to recreate the issue (see reporting section below for more details on producing a good quality report).
- If we cannot recreate the issue, the bounty will not be eligible for reward.
- Make sure your testing is in our Scope (see below).
- Physical access to our premises or interaction with our employees outside of the reporting email address is strictly prohibited.

We Will:

- Determine the bounty amount of a successful report based on several factors. These factors include likelihood of the issue being exploited and the impact such an event would have.
- We aim to be consistent with our bounty amounts, however bounty amounts may change over time. Past amounts may not guarantee the same amount in the future.
- If the same vulnerability is reported more than once, the person who first reported the vulnerability will receive the reward.
- We may cancel the bug bounty program without notice at any time.
- The time to respond will depend on our workload.

Rules:

- Use your own account for testing purposes.
- Automated testing should be limited to a sensible rate, one request per second is considered an acceptable rate.
- Do not cause any destruction of data on the services.

- Do not cause disruption or interruption to our services.
- We encourage responsible disclosure. Please speak to us before disclosing an issue publicly to allow us time to resolve the issue.
- Do not exploit a security issue you discover.
- Do not conduct any social engineering.
- Do not physically attack our premises or employees.
- Do not attempt to gain access to another user's account or confidential information.
- Your testing must not violate any law or disrupt or compromise any data that is not your own.
- If you accidentally access another user's data, please disclose this to us immediately so that we can ensure we remain compliant with data protection laws.
- We reserve the right to modify the rules for this program or deem any submissions invalid at any time.

Scope of the Programme:

In Scope THG Brands

The information on this page pertains to the THG brands found at https://www.thg.com/brands/

Not Eligible For Bounty:

- Brute Force attacks.
- You may not contact our support team over chat, email or phone.
- Denial-of-service attacks.
- Missing security headers.
- Version number information disclosure.
- Bugs that do not represent any security risk.
- Vulnerabilities only affecting users of outdated or unpatched browsers and platforms.
- When doing automated testing, make sure sensible rates are used. 1 request per second is considered an acceptable rate.
- SSL/TLS scan reports (For example, output from sites such as SSL Labs).
- Reports taken directly from automated scanners.

Reporting:

Email your report to: SecurityBugs@TheHutGroup.com.

Please include the following in your report:

- A clear description of the issue.
- Where the issue can be exploited.
- Well defined steps to reproduce the issue including browser, tools, account.
- A clearly written explanation of the impact on how an attacker could abuse the flaw.