Stcoins Potential Vulnerability Reward Program ("PVR Program")

Stable Universal is dedicated to providing our users with safe and reliable services. We recognize the important role that security researchers and our user community play in helping us to keep our products, our customers and websites secure We will evaluate submitted issues and will reward qualifying issues up to $1,000 USD. Rewards will be Amazon or JD.com Gift Card. Rewards are determined at the discretion of Stable Universal.

Program Terms

Please note that your participation in Stable Universal's PVR Program is voluntary and subject to the terms and conditions set forth on this page ("Program Terms"). By submitting a site or product vulnerability to Stable Universal Limited ("Stable Universal"), you acknowledge that you have read and agreed to these Program Terms.

These Program Terms supplement the terms of Stable Universal User Agreement, and any other agreement in which you have entered with Stable Universal (collectively "SU Agreements"). The terms of those SU Agreements will apply to your use of, and participation in, the PVR Program as if fully set forth herein. If any inconsistency exists between the terms of the SU Agreements and these Program Terms, these Program Terms will control, but only with regard to the PVR Program.

To encourage responsible disclosures, Stable Universal commits that, if we conclude, in our sole discretion, that a disclosure respects and meets all the guidelines of these Program Terms and the SU Agreements, Stable Universal will not bring a private action against you or refer a matter for public inquiry.

As part of your research, do not modify any files or data, including permissions, and do not intentionally view or access any data beyond what is needed to prove the vulnerability. Do not access any personal information that is not your own, including by exploiting the vulnerability which will result in disqualification from the PVR Program.

The PVR Program is only applicable to vulnerabilities submitted with regard to the stcoins.com website and servers.

Eligibility Requirements

To be eligible for the PVR Program, you must not:

- Be a resident of, or make your Submission from, a country against which the United States has issued export sanctions or other trade restrictions (e.g., Cuba, Iran, North Korea, Sudan and Syria);
- Be in violation of any national, state, or local law or regulation;
- Be employed by or under contract to Stable Universal, its subsidiaries or affiliates or have been employed or under contract with Stable Universal within a 1 year period prior to your submission;
- Be an immediate family member of a person employed by , or under contract with, Stable Universal or its subsidiaries or affiliates; or
- Be less than 18 years of age. If you are at least 18 years old, but are considered a minor in your place of residence, you must get your parent's or legal guardian's permission prior to participating in the program.

If Stable Universal discovers that you meet any of the criteria above, Stable Universal will remove you from the PVR Program and disqualify you from receiving any PV Reward Payments.

Disclosure Guidelines

By providing a Submission or agreeing to the Program Terms, you agree that you may not publicly disclose your findings or the contents of your Submission to any third parties in any way without Stable Universal's prior written approval.

Failure to comply with the Program Terms will result in immediate disqualification from the PVR Program and ineligibility for receiving any VR Reward Payments.

How to Submit a Vulnerability

1. Vulnerability reports can be submitted via the form on the "Submit a Vulnerability" page or via email to sec@stcoins.com.
2. Stable Universal will review and verify each vulnerability report submitted, and a member of the Customer Service Team may contact you regarding the submission.
3. A reward may be offered to you as outlined by the "Rewarding Criteria" below. The amount of PV Reward Payment will be determined by Stable Universal in accordance with the Rewarding Criteria, based on the risk level posed by the vulnerability.

PV Reward Payments

You may be eligible to receive a monetary reward ("PV Reward Payment") 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 Stable Universal's security team; and (iii) you have complied with all Program Terms. PV Reward Payments, if any, will be determined by Stable Universal, in its sole discretion. In no event shall Stable Universal be obligated to pay you a reward for any Submission. All PV Reward Payments shall be considered gratuitous.

All PV Reward Payments will be made in United States dollars (USD). You will be responsible for any tax implications related to PV Reward Payments you receive, as determined by the laws of your jurisdiction of residence or citizenship.

Stable Universal will determine all PV Reward Payments based on the risk and impact of the vulnerability. The maximum bounty for a validated bug submission is $1,000 USD.

Stable Universal retains the right to determine if the bug submitted to the PVR Program is eligible. All determinations as to the amount of a PV Reward Payment made by Stable Universal are final. PV Reward Payments (and applicable ranges) are based on Rewarding Criteria stated below and determined to be a valid security issue by Stable Universal.

If multiple vulnerabilities are generated by the same vulnerability submitted, these will be treated as one vulnerability for the purpose of determining the relevant PV Reward Payment after Stable Universal has deemed the submission as a valid security issue.

If the same vulnerability is submitted by multiple researchers, Stable Universal will reward the researcher who first submitted the vulnerability;

Rewarding Criteria for Submissions

[Critical Risk] Rewards: $500 - $1,000 USD

- Access to a large amount of sensitive user info, such as accounts, passwords and identity info;
- Access to key server control permissions;
- Direct access to key system permissions, including but not limited to remote command execution, arbitrary code execution and uploading Web shell;
- Critical leaks of sensitive info, including but not limited to SQL injection into core DB (related to assets, user identity or trades) or access to a large amount of key user identity info caused by socket-related problems;

- Serious flaws in logic or process design, including but not limited to sending fake messages in batches through sockets, consumption with random accounts, changing random accounts and passwords in batches.

[High Risk] Rewards: $200 - $300 USD

- High-risk info leaks, including but not limited to directly exploitable sensitive data;
- Unauthorized access to sensitive info, including but not limited to bypassing authentication to access admin backstage, weak backstage password, access to a large amount of sensitive internal data with the SSRF;
- Direct access to system permissions for general businesses, including but not limited to remote command execution, arbitrary code execution and uploading Web shell;
- Local arbitrary code execution, including but not limited to locally exploitable stack overflow, UAF, double free, format string, LPE and other vulnerability resulting from logic-related problems;
- Directly obtaining permissions on clients, including but not limited to remote arbitrary command execution, remote buffer overflow, and other remote code execution vulnerability due to logic-related problems;
- Other vulnerability affecting users on a large scale, including but not limited to self-propagating storage-type XSS (including storage-type DOM-XSS) on key pages and the CSRF related to trades, assets and passwords.

[Moderate Risk] Rewards: $30 - $80 USD

- Vulnerability that users can be affected by the demand interaction. Including but not limited to storage-type XSS for general business, reflective XSS (including reflective DOM-XSS), and important operational CSRF vulnerability;
- Common logic design defects and process defects, including but not limited to SMS bomb attack and email bomb attack;
- Vulnerability with limited scope, including but not limited to unauthorized modification of user information;
- Remote application denial of service, sensitive information disclosure, kernel denial of service, XSS vulnerability of client products that can obtain sensitive information or perform sensitive operations.

[Low Risk] Rewards: $10 - $20 USD

- Slight information leakage. Including but not limited to path information leakage, SVN information leakage, PHPinfo, abnormal information leakage, and client application local SQL injection (leak only database name, field name, cache content), log printing, configuration information, abnormal information, etc.;
- Vulnerability that are difficult to exploit but have potential security risks. Including but not limited to SQL injection points that are difficult to use, SelfXSS that can cause propagation and utilization, URL redirection, CSRF that needs to construct some parameters and has some influence;
- Local denial of service vulnerability in PC and mobile apps. This includes, but is not limited to, local denial of service vulnerability caused by component permissions.

While some issues may fall out of the scope of the reward program, Stable Universal encourages submission of these issues and will evaluate to determine whether they may qualify for rewards. Such issues may include:

- Vulnerabilities that do not involve security issues. Including but not limited to product defects, garbled web pages, confusing styles, static file directory traversal, and application compatibility issues;
- Unexploitable vulnerability. Including but not limited to CSRF without sensitive operations, meaningless leakage of abnormal information, lower SSL version, Clickjacking, internal network IP address / domain name leakage;
- The vulnerability cannot directly reflect other problems, including but not limited to problems purely guessed by users;
- Mail forgery in non-core business; Scanner vulnerability reports with no practical meaning, including but not limited to XSS vulnerability in WEB service versions that are too low or in browsers with lower versions (IE9 and below);
- Non-Stcoins business related vulnerability.

Ownership of Submissions

As a condition of participation in the PVR Program, you hereby grant Stable Universal, 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 Stable Universal in

connection therewith, for any purpose. You should not send us any Submission that you do not wish to license to us.
You hereby represent and warrant that the Submission is original to you and you own all right, title and interest in and to the Submission. Further, you hereby waive all other claims of any nature, including express contract, implied-in-fact contract, or quasi-contract, arising out of any disclosure of the Submission to Stable Universal. In no event shall Stable Universal be precluded from discussing, reviewing, developing for itself, having developed, or developing for third parties, materials which are competitive with those set forth in the Submission irrespective of their similarity to the information in the Submission, so long as Stable Universal complies with the terms of participation stated herein.

Termination

In the event (i) you breach any of these Program Terms or the terms and conditions of the SU Agreements; or (ii) Stable Universal determines, in its sole discretion that your continued participation in the PVR Program could adversely impact Stable Universal (including, but not limited to, presenting any threat to Stable Universal's systems, security, finances and/or reputation) Stable Universal may immediately terminate your participation in the PVR Program and disqualify you from receiving any PV Reward Payments..

Confidentiality

Any information you receive or collect about Stable Universal or any user or customer through the PVR Program ("Confidential Information") must be kept confidential and only used in connection with the PVR Program. You may not use, disclose or distribute any such Confidential Information, including, but not limited to, any information regarding your Submission and information you obtain when researching Stable Universal sites, without Stable Universal's prior written consent.

Indemnification

In addition to any indemnification obligations you may have under the SU Agreements, you agree to defend, indemnify and hold Stable Universal, its subsidiaries, affiliates and the officers, directors, agents, joint ventures, employees and suppliers of Stable Universal, its subsidiaries, or our affiliates, harmless from any claim or demand (including attorneys' fees) made or incurred by any third party due to or arising out of your Submissions, your breach of these Program Terms and/or your improper use of the PVR Program.

Changes to Program Terms

The PVR Program, including its policies, is subject to change or cancellation by Stable Universal at any time, without notice. Stable Universal may amend these Program Terms and/or its policies at any time by posting a revised version on our website. By continuing to participate in the PVR Program after Stable Universal posts any such changes, you accept the Program Terms, as modified.