PRüF Bug Bounty Program Details

The PRüF foundation will be giving the following rewards for bugs or security issues found in the PRüF infrastructure and web-application. All bounties will be paid in PRüF utility tokens. All submissions must comply with the rules and responsible disclosure guidelines given below to be considered for a reward.

BUG BOUNTIES

	Severity				
The exploit is…	**Very low**	**Low**	**Moderate**	**High**	**Critical**
Almost Certain	20000	50000	160000	400000	1000000
Likely	10000	20000	50000	160000	400000
Possible	4000	10000	20000	50000	160000
Unlikely	4000	4000	10000	20000	50000
Almost Possible	2000	4000	4000	10000	20000

Only bugs or exploits in the contract infrastructure will be given “High” or “Critical” status, except in extraordinary cases where a malfunction of the web-app causes an exposure of personally identifiable information. Malicious versions of the web-app that misrepresent data to the client or fail to properly preprocess data before publication will not be considered as an exploit or bug if the exploit cannot be replicated in the published web-app.

Within the contract infrastructure, we are especially interested in:

- Loss of collateral or stealing of funds or tokens from the PRüF infrastructure or ecosystem.
- Ineffective or error prone validation mechanisms for any operation
- Any call that is re-playable or front-runnable from a different address that results in an unintended change of state
- Any manipulation of the contracts that can cause unintended operation of any kind except that which only results in a complete revert of the transaction

- Unfair actions of any kind, especially through any mint or burn function, purchaseACtoken, createAssetClass, trustedAgentBurn, trustedAgentTransfer, payForService, and increaseShare.
- Locking or freezing or any of any contracts or inability to upgrade contracts
- Incorrect or error prone data retrieval from any contract

Almost all exploits in these categories will be classified as “CRITICAL”. Any exploit or bug in the contract infrastructure will be rated as “HIGH” severity or better, and the probability of exploit, if an exploit is possible to demonstrate, will be rated as “Likely” or higher.

Within the web-app, we are especially interested in anything that can leak information to another site or domain, or any way the web-app can be manipulated by XSS or other vectors outside the users control. Any new bug that significantly impacts the user experience will be rewarded.

Rules

- Public disclosure of any vulnerability, before explicit consent from PRüF to do so, will make the vulnerability ineligible for a bounty
- Attempting to exploit the vulnerability in any public (non test-net) Ethereum network will also make it ineligible for a bounty
- Only unknown vulnerabilities will be awarded a bounty; in case of duplicate reports, the first report will be awarded the bounty
- Rewards will be decided on a case by case basis and the bug bounty program, terms, and conditions are at the sole discretion of PRüF.
- Submissions out of the Bounty Scope may not be be eligible for a reward
- Any interference with the PRüF protocol, client or platform services, on purpose or not during the process of investigating a vulnerability will make the submission invalid. If you require a private test-net deployment of the PRüF infrastructure to safely test your vulnerability, contact us.
- Terms and conditions of the bug bounty process may vary over time
- Submissions not following the disclosure policy will not be eligible for a reward
- While researching, we'd like to ask you to refrain from:
    - Denial of service
    - Spamming
    - Social engineering (including phishing) of PRüF staff or contractors

Responsible disclosure

In case you discover a vulnerability, we would like to know about it immediately so we can take steps to address it as quickly as possible.

If you discover a vulnerability, please do the following:

- E-mail your findings to security@pruf.io with the subject line “bounty"
- Do not take advantage of or exploit the vulnerability or problem you have discovered
- Do not reveal the bug to anyone but the PRüF team, via email only, until it has been resolved
- Do not use attacks on physical security, social engineering, or distributed denial of service against the network or PRüF infrastructure.
- Please provide sufficient information to reproduce the problem, so we will be able to resolve it as quickly as possible. Complex vulnerabilities will probably require further explanation, so we may ask you for additional information

If you follow the responsible disclosure guidelines, we promise you the following:

- We will respond to your report with a confirmation of receipt, followed by our evaluation of the report and an expected resolution date within 5 business days
- If you have followed the responsible disclosure guide provided above, we will not take any legal action against you in regard to the report
- We will handle your report with strict confidentiality, and not pass on your personal details to third parties without your permission
- If you indicate that you would like us to, we will keep you informed of the progress towards resolving the problem
- With your permission, we will give your name as the discoverer of the problem in the public disclosure of the bug.
- We offer a reward for every report of a security problem that was not yet known to us. The amount of the reward will be determined based on the severity of the leak, the quality of the report and any additional assistance you provide