Beanstalk

Source: *https://immunefi.com/bounty/beanstalk/*

Beanstalk

10/11/2022	**No**	**$1,100,000**
Live since	**KYC Required**	**Max Bounty**

Program Overview

Beanstalk Farms is a decentralized development organization working on Beanstalk, Basin and Pipeline.

This bug bounty program is focused on securing all 3 projects:

- Beanstalk is a permissionless fiat stablecoin protocol;
- Basin is a composable EVM-native decentralized exchange protocol; and
- Pipeline is a sandbox contract that can execute an arbitrary number of actions within the EVM from an EOA in a single transaction.

There is a list of resources (docs, repositories, etc.) under the Assets in Scope section. You can also check out past bug reports and past bounty payouts for this bug bounty program.

Bounties are paid in BEAN via the Beanstalk Immunefi Community Multisig (BICM). For more details about the payment process, please view the Rewards by Threat Level section further below.

Eligibility Criteria

Security researchers who wish to participate must adhere to the rules of engagement set forth in this program and cannot be:

- A member of the Beanstalk Immunefi Committee (BIC); or
- A private auditor that has been paid by Beanstalk Farms or a related party to review the code that is reported to be vulnerable.

Responsible Publication

The Beanstalk bug bounty program adheres to category 1 - Transparent. This Policy determines that researchers can make public any information from their submitted bug reports. For more information about the category selected, please refer to our Responsible Publication page.

Primacy of Impact vs Primacy of Rules

The Beanstalk bug bounty program adheres to the Primacy of Rules, which means that the bug bounty program is run strictly under the terms stated on this page.

Previous Audits

Audit reports of the various in-scope assets can be found at https://github.com/BeanstalkFarms/Beanstalk-Audits. Any unfixed vulnerabilities mentioned in these reports (or otherwise known by the BIC or BCM) are not eligible for a reward.

Feasibility Limitations

The program may be receiving reports that are valid (the vulnerability is legitimate) and cite assets and impacts that are in scope, but there may be obstacles or barriers to executing any sort of attack in the real world. Conversely, there may also be mitigation measures that may be taken to prevent the impact of the bug, which are not feasible or would require unconventional action and hence, should not be used as reasons for downgrading a bug's severity.

Therefore, Immunefi has developed a set of feasibility limitation standards which by default states what security researchers, as well as projects, can or cannot cite when reviewing a bug report.

Immunefi Standard Badge

By adhering to Immunefi's best practice recommendations, the Beanstalk bug bounty program has satisfied the requirements for the Immunefi Standard Badge.

Rewards by Threat Level

Rewards are distributed according to the impact of the vulnerability based on the Immunefi Vulnerability Severity Classification System V2.3. The following is a simplified 3-level scale, focusing on the impact of the vulnerability reported. The complete scope can be found below.

In order to be considered for the maximum potential reward, bug reports must come with a Proof of Concept (PoC). Explanations and statements are not accepted in lieu of a PoC. Bug reports that do not come with a PoC may qualify for a maximum of up to 30% of the potential reward outlined below, as determined by the Beanstalk Immunefi Committee.

Funds at Risk for a given bug report are defined as follows:

- Funds at Risk are determined based on the token amounts and USD values at time of the bug report submission;
- For Beans, Funds at Risk are determined based on the liquidatable USD value of the Beans at risk;
- For non-Beans (ETH, WETH, 3CRV, USDC, DAI, USDT, etc.) in any in-scope assets, the Funds at Risk are determined based on their respective USD values;
- For Circulating non-Beans (i.e., outside of any in-scope assets), the Funds at Risk are determined to be 50% of their respective USD values; and
- If the smart contract where the vulnerability exists can be upgraded or paused, only the Funds at Risk in initial attacks that can be executed within the first hour will be considered for a reward.

Reward Calculation for Critical Smart Contract Reports

Rewards for Critical smart contract vulnerabilities are capped at the **lower** of (a) 10% of practicable economic damage, or (b) **USD 1 100 000**, primarily taking into consideration the Funds at Risk. However, there is a minimum reward of **USD 100 000** for Critical severity smart contract bug reports.

Reward Calculation for High Smart Contract Reports

Rewards for High smart contract vulnerabilities are capped at the **lower** of (a) 10% of practicable economic damage, or (b) **USD 100 000**, primarily taking into consideration the Funds at Risk. However, there is a minimum reward of **USD 10 000** for High severity smart contract bug reports.

Reward Calculation for Medium Smart Contract and All Website and Applications Reports

Rewards for Medium severity smart contract vulnerabilities and all website and applications vulnerabilities are scaled based on a set of internal criteria established by the BIC. However, there is a minimum reward of **USD 1 000** for Medium smart contract bug reports, **USD 5 000** for Critical website and applications bug reports and **USD 1 000** for High website and applications bug reports. The BIC will primarily take into account:

- The exploitability of the bug;
- The impact it causes; and
- The likelihood of the vulnerability presenting itself.

Reward Payment Terms

Payouts are handled by the Beanstalk Immunefi Committee Multisig (BICM) directly and are done in BEAN at the rate of 1 BEAN to 1 USD (i.e., amounts listed above are actually in BEAN) independent of liquidity (see BEAN liquidity here). Note that due to the decentralized governance process for rewarding bug bounties, rewards can take several days to be paid out after a report is confirmed to be valid.

BIC Determination

The BIC shall determine whether a submitting party is entitled to a bug bounty/reward, and if so, the amount of such bounty/reward (and specifically, whether such submission qualifies for a Critical, High or Medium Impact bounty/reward, what is the potential practicable economic damage of such bug based on the Funds at Risk, and what the appropriate bounty/reward should be within each Impact range). The BIC's determination of (i) whether such submission qualifies for a Critical, High or Medium Impact bounty/reward, (ii) what is the potential practicable economic damage of such bug based on the Funds at Risk, and (iii) whether such submission came with a PoC, thereby enabling it to be considered for the maximum potential applicable reward (vs. a submission that did not come with a PoC, thereby limiting such submission to a maximum of up to 30% of the applicable reward), shall be made in the BIC's sole and absolute discretion absolute and shall be final, and not be subject to any appeal or challenge.

A submitting party may only dispute the BIC's determination (a) that a submitting party is not entitled to any bug bounty/reward, or (b) what the appropriate bounty/reward should be within each Impact range. In such disputes, Immunefi will conduct a binding mediation. If the submitting party disputes the BIC's decision that a submitting party is not entitled to any bug bounty/reward, Immunefi will mediate, and shall determine, in its sole and absolute discretion, which is non-appealable, whether the submitting party is entitled to any bug bounty/reward, and if so, the amount of such bug bounty/reward, up to **USD 10 000** in the case of a smart contract bug reports (i.e., as if it were a Medium Impact fix), and up to **USD 1 000** in the case of a website and applications bug report (i..e, as if it were a High Impact fix). If the submitting party disputes the BIC's determination what the appropriate bounty/reward should be within a specific Impact range, Immunefi will mediate, and shall determine, in its sole and absolute discretion, which is non-appealable, the amount of such bug bounty/reward in the relevant Impact category; however, Immunefi may not modify or change (i) the practicable economic damage determination made by the BIC, or (b) the BIC's determination whether such submission came with a PoC, thereby enabling it to be considered it for the maximum potential applicable reward (vs. a submission that did not come with a PoC, thereby limiting such submission to a maximum of up to 30% of the applicable reward).

Category	Severity	Reward Amount	PoC Required
Smart Contract	Critical	USD 100 000 - 1 100 000	Yes
Smart Contract	High	USD 10 000 - 100 000	Yes
Smart Contract	Medium	USD 1 000 - 10 000	Yes
Website & Application	Critical	USD 5 000 - 50 000	Yes
Website & Application	High	USD 1 000 - 5 000	Yes

Assets in Scope

Target	Type
https://etherscan.io/address/0xC1E088fC1323b20BCBee9bd1B9fC9546db5624C5	Smart Contract - Beanstalk
https://etherscan.io/address/0xBEA0000029AD1c77D3d5D23Ba2D8893dB9d1Efab	Smart Contract - Bean ERC-20 token
https://etherscan.io/address/0x1BEA0050E63e05FBb5D8BA2f10cf5800B6224449	Smart Contract - Unripe Bean ERC-20 token
https://etherscan.io/address/0x1BEA3CcD22F4EBd3d37d731BA31Eeca95713716D	Smart Contract - Unripe BEAN:ETH LP ERC-20 token
https://etherscan.io/address/0x402c84de2ce49af88f5e2ef3710ff89bfed36cb6	Smart Contract - Fertilizer ERC-1155 token
https://etherscan.io/address/0x39cdAf9Dc6057Fd7Ae81Aaed64D7A062aAf452fD	Smart Contract - Fertilizer Implementation
https://etherscan.io/address/0xBA51AAAA95aeEFc1292515b36D86C51dC7877773	Smart Contract - Aquifer
https://etherscan.io/address/0xBA510C20FD2c52E4cb0d23CFC3cCD092F9165a6E	Smart Contract - Constant Product 2 Well Function
https://etherscan.io/address/0xBA510f10E3095B83a0F33aa9ad2544E22570a87C	Smart Contract - Multi Flow Pump
https://etherscan.io/address/0xBA510e11eEb3	Smart Contract - Well Implementation

87fad877812108a3406CA3f43a4B	
https://etherscan.io/address/0xBEA0e11282e2bB5893bEcE110cF199501e872bAd	Smart Contract - BEAN:ETH Well
https://etherscan.io/address/0xb1bE0000C6B3C62749b5F0c92480146452D15423	Smart Contract - Pipeline
https://etherscan.io/address/0xDEb0f00071497a5cc9b4A6B96068277e57A82Ae2	Smart Contract - Depot
https://app.bean.money	Website and Applications - Beanstalk UI
https://basin.exchange	Website and Applications - Basin UI

If an impact can be caused to any other asset related to Beanstalk, Basin, etc. that isn't on this section but for which the impact is in the Impacts in Scope section below, bug bounty hunters are encouraged to submit it for consideration by the BIC.

Note that unexpected outcomes (like loss of funds) due to misuse of Pipeline and/or Depot do not qualify as valid bug reports. Read more here.

Also note that the various ecosystem subgraphs (Beanstalk, Bean, Basin, etc.) are not included as Assets in Scope.

Undeployed Code in Scope

The BIC also maintains a list of pull requests/repositories whose code is considered in-scope but has not yet been deployed on-chain. This code has been audited. The following code is also in-scope of the bug bounty program:

- None at this time.

Additional Resources

All Beanstalk smart contracts and the Beanstalk UI can be found at https://github.com/BeanstalkFarms/Beanstalk. However, only those in the Assets in Scope section are considered as in-scope of the bug bounty program. The following links may also be helpful:

Beanstalk

- Beanstalk Whitepaper

- Beanstalk Docs
- Beanstalk Technical Docs
- Beanstalk GitHub
- Beanstalk Discord
- Beanstalk on Louper

Basin

- Basin Whitepaper
- Multi Flow Pump Whitepaper
- Basin Docs
- Basin GitHub
- Basin Discord

Pipeline

- Pipeline Whitepaper
- Pipeline GitHub

Impacts in Scope

Only the following impacts are accepted within this bug bounty program. All other impacts are not considered as in-scope, even if they affect something in the assets in scope table.

Smart Contract

Impact	Severity level
Direct theft of any user funds, whether at-rest or in-motion, other than unclaimed yield	Critical
Permanent freezing of funds	Critical
Theft of unclaimed yield	High
Permanent freezing of unclaimed yield	High
Temporary freezing of funds for at least 1 hour	High
Illegitimate minting of protocol native assets	High
Smart contract unable to operate due to lack of token funds	Medium

Block stuffing for profit	Medium
Griefing (e.g. no profit motive for an attacker, but damage to the users or the protocol)	Medium
Theft of gas	Medium
Unbounded gas consumption	Medium
Contract fails to deliver promised returns, but doesn't lose value	Medium

Web/Apps

Impact	**Severity level**
Taking down the application/website requiring manual restoration	Critical
Redirecting users to malicious websites	Critical
Direct theft of user funds	Critical
Ability to execute arbitrary system commands	Critical
Injecting code that results in malicious interactions with an already-connected wallet such as modifying transaction arguments or parameters, substituting contract addresses, submitting malicious transactions	Critical
Taking state-modifying authenticated actions (with or without blockchain state interaction) on behalf of other users without any interaction by that user, such as voting in governance.	Critical
A temporary or self-correcting loss of website availability (e.g. a mitigatable vulnerability to DDoS)	High
Lack of valid SSL/TLS	High
Subdomain takeover other than app.bean.money or basin.exchange	High
Persistent content spoofing / text injection	High

issues	

Out of Scope & Rules

The following impacts are out of scope for this bug bounty program:

All Categories:

- Impacts related to attacks that the reporter has already exploited themselves, leading to damage;
- Impacts caused by attacks requiring access to leaked keys/credentials;
- Impacts caused by attacks requiring access to privileged addresses (owner address);
- Impacts relying on attacks involving the depegging of an external stablecoin where the attacker does not directly cause the depegging due to a bug in the code;
- Impacts that involve frontrunning transactions, i.e., impacts that require users to send transactions through the public mempool;
- Mentions of secrets, access tokens, API keys, private keys, etc. in GitHub will be considered out of scope;
- Best practice recommendations;
- Feature requests; and
- Impacts on test and configuration files unless stated otherwise in the bug bounty program.

Smart Contract Specific:

- Incorrect data supplied by third party oracles;
    - Not to exclude oracle manipulation/flash loan attacks;
- Impacts requiring basic economic and governance attacks (e.g. 51% attack);
- Lack of liquidity impacts;
- Impacts from Sybil attacks; and
- Impacts involving centralization risks.

Websites and Apps

- Theoretical impacts without any proof or demonstration;
- Impacts involving attacks requiring physical access to the victim device;
- Impacts involving attacks requiring access to the local network of the victim;
- Any impacts involving self-XSS;
- Captcha bypass using OCR without impact demonstration;
- CSRF with no state modifying security impact (e.g. logout CSRF);

- Impacts related to missing HTTP Security Headers (such as X-FRAME-OPTIONS) or cookie security flags (such as “httponly”);
- Server-side non-confidential information disclosure, such as IPs, server names, and most stack traces;
- Impacts caused by vulnerabilities requiring unprompted, in-app user actions that are not part of the normal app workflows;
- Impacts primarily caused by browser/plugin defects;
- Leakage of non sensitive API keys (e.g. Etherscan, Infura, Alchemy, etc.);
- Any vulnerability exploit requiring browser bugs for exploitation (e.g. CSP bypass); and
- Any vulnerabilities inherent in hosting centralized infrastructure.

Prohibited Activities:

The following activities are prohibited by this bug bounty program and could result in disqualification of reception of a bounty, in the sole and absolute discretion of the BIC:

- Any testing on mainnet or public testnet deployed code; all testing should be done on local forks or private testnets;
- Any testing with pricing oracles or third-party smart contracts;
- Attempting phishing or other social engineering attacks against contributors and/or users;
- Any testing with third-party systems and applications (e.g. browser extensions) as well as websites (e.g. SSO providers, advertising networks);
- Any denial of service attacks;
- Automated testing of services that generates significant amounts of traffic; and
- Public disclosure of an unpatched vulnerability in an embargoed bounty.