As of this post, the bug bounty program has officially begun. The bounty program will continue until the end of the token sale

Bug Bounty Program

High: Up to 10 ETH,
Critical: Up to 15 ETHThe last, but not the least part of the Cappasity bounty campaign is the bug bounty program. Bounties for finding a bug will be accredited separately from the rest of the campaign.

Please send your bug reports to support@cappasity.com. As soon as your bug report is received, our bounty judges will evaluate the severity of the bug and will contact you.

Most of the rules on the Ethereum Foundation bug bounty program apply:

- First come, first served.
- Issues that have already been submitted by another user or are already known to Cappasity are not eligible for bounty rewards.
- Public disclosure of a vulnerability makes it ineligible for a bounty.
- Paid auditors of the code are not eligible for rewards.
- Determinations of eligibility, score and all terms related to the award are at the sole and final discretion of Cappasity.

Scope

- Find bugs in all contracts related to the ARToken crowdsale. You may find them in our GitHub repository.
- Test and search for bugs there. It is important to do testing on computers that comply with the minimum configuration.
- Test the platform — https://3d.cappasity.com. Provide us with the information on ways to disable or disrupt the security system and its database.
- Find an attack on the artoken.io website or via a user account. Please describe the way attackers deceive contributors.
- If none of the above describes your request, you still have a chance to receive a reward by sending the found vulnerabilities to us.

Please note that we will *not* be rewarding the identification of spam or social engineering usage to deceive contributors.

Timeline.

Compensation

The bounty judges will determine the size of the reward (up to 15 ETH for severe vulnerabilities), based on their evaluation of both the likelihood and impact of the bug.

Note: Up to 0.3 ETH,
Low: Up to 3 ETH,
Medium: Up to 7 ETH,

Severity

		Likelihood		
		Low	Medium	High
Impact	High	Medium	High	**Critical**
	Medium	Low	Medium	High
	Low	Note	Low	Medium

Example

An identified attack that could steal raised funds would be considered a critical threat.
If there was a way for someone to spend more tokens than owned or to mint more ARTokens, the bug would be considered a high threat.

Please note that the submission's quality will factor into the level of compensation. A high quality submission includes an explanation of how the bug can be reproduced, a failing test case and a fix that makes the test case pass. High quality submissions may be awarded amounts higher than those specified above.

Note that bounties will be paid in ETH and that our team members and auditors are not eligible for bounty compensation. If in doubt about other aspects of the bounty, most of the Ethereum Foundation bug bounty program rules will apply.

Contact

Anonymous submissions are more than welcome. Public disclosure of the bug or indication of an intention to exploit it on the mainnet will make the report ineligible for a bounty.

Please report bug bounty submissions to support@cappasity.com.