# Project Closeout Report: Smart Contract Vulnerabilities Game – Capture the Flag (CTF)

## Project details

**Project name:** Smart Contract Vulnerabilities Game – Capture the Flag (CTF) (IdeaScale link)
**Project number:** 1000162
**Project manager:** Michal Porubský
**Project start:** October 8th, 2023
**Project completion:** May 8th, 2024
**Closeout video:** https://youtu.be/n_98dRM6vB4

## Project summary

We have created a series of 11 interactive tasks focused on Cardano smart contract security called Cardano Capture the Flag (CTF). Each task consists of some purposely vulnerable smart contract(s). It is the users' goal to find the vulnerabilities and create transactions that exploit them. These exploits are then checked by our tests and the users get a confirmation in case of a success.

Accompanying the tasks, there is a series of blog posts that we wrote. Each detail some aspect of Cardano smart contract security (e.g. double satisfaction, time handling, token security, etc). It helps users learn about the vulnerabilities in general and then they can try to find them in the CTF.

## Challenge KPIs

The Open Source Dev Ecosystem sets a number of KPIs. Here, we list those relevant to our project:

**Increase the number and quality of open-source projects**
We have created new open-source educational material about Cardano smart contract security. We believe it is a very important reference material. It stays available and open for anyone to explore.

**Increase the visibility of open-source projects**
We have promoted our CTF through various means s.a. Twitter, Reddit, Discord, in-person at Cardano conferences, and created a series of educational blogs that link to the CTF. The interactivity and game-like fashion of CTF could attract users allowing them to dive deeper into the Cardano ecosystem.

**Improve adoption of Cardano technology**
As an interactive learning material, the Cardano CTF teaches people how smart contracts are written and how they can be interacted with through the off-chain code. It does this with practical tasks, thus it decreases the burden newcomers face when coming to Cardano. Further, it highlights a number of smart

contract vulnerabilities so that smart contract developers know about them and do not repeat them in their code. That means that the new code would hopefully be safer, helping future adoption.

## Project KPIs

In our project proposal, a few quantitative metrics were proposed, measuring the interaction of the users with our CTF project.

- **Git repository.** There have been 41 unique visitors with a total of 425 views of the repository as of May 8th, 2024. There have been 4 unique direct clones along with 6 forks of the repository. 20 GitHub users starred the repository and one person from the community contributed and helped us fix one test.
- **Discord channel users.** 18 people joined our Discord and there's been some positive feedback in the channels as well as in DMs so far.
- **Number of blog readers.** Overall, our Cardano CTF and other smart contract vulnerability blogs received 1465 views and 739 reads as of May 8th, 2024. We also received a few claps.

We didn't set any specific numbers we would like to hit. This was on purpose. Our main goal was to create a unique educational material of the highest possible quality that would be open to the community. The material is timeless, serving any existing and future Cardano developers. The most time was spent on the actual development and we believe that the number of users will rise as Cardano security is an important topic.

Our CTF and blogs are now listed among the first search results when searching for educational material for Cardano security and for now, it is one of a kind. The main goal of this project was to create such materials and make them available.

## Key Achievements

We've created a unique educational material that allows users to learn about Cardano smart contract security and try to break vulnerable contracts on their own. We believe that first-hand experience is a strong tool in one's learning.

The CTF is public and contains a series of 11 gradually harder tasks. We made sure that the whole setup is as smooth as possible and requires only minimal technical skill. It is supported by both written and video tutorials.

We are seeing the first users that are trying to solve the problems and we already have one user who was able to crack all the tasks. We have communicated with him privately through our Discord channel. He didn't encounter any issues, didn't find any loopholes, and was even motivated to write a blog detailing his experience.

The CTF is accompanied by a series of blog posts that delve deep into Cardano security beyond the scope of CTF and this is a great additional education material.

## Key Learnings

At the start of the project, it was not clear how easy it would be to build such a project. Our main concern was the technical complexity expected of a user.

Fortunately, there are strong tools for both on-chain and off-chain that are easy to set up – we have used the combination of Aiken and Lucid. It was therefore possible to create a code bundle that can be set up in under 10 minutes and allows for smooth and quick development. If a user has solid basics in any modern programming language, he should be able to participate even without any prior Cardano knowledge.

However, with our CTF tasks we have probably set the bar a little too high. For now, we only have a handful of successful submits, mostly for the first few tasks. Even though the setup is straightforward, Cardano smart contract security is a complex topic and requires broad knowledge. Even the simplest vulnerable smart contracts require a few hundred lines of code which represents a barrier for users. We hope that the blogs that were released over the last milestone will help to lower this barrier and we will see new successful submissions in the near future. However, we think it would be beneficial if we created a bit more of the easier levels. Maybe we can provide those in the future.

## Next Steps

We will monitor and maintain the Cardano CTF repository. If there are any issues, we will try to fix them in a timely manner.

Our Discord channel is still open and we welcome any users to join and talk to us, send us feedback, report a bug, or ask for help.

Lastly, we are planning to continue with our blog series, tackling more security topics.

## Resources

Cardano CTF GitHub repository – https://github.com/vacuumlabs/cardano-ctf
Cardano smart contract security blogs – https://medium.com/@vacuumlabs_auditing