StarShell Security Audit Funding Request

StarShell wallet, which has been under development for almost a year now, and in beta testing for the last 4 months, is finally at the stage where we are ready to hire an independent party to conduct a security review of our open-source codebase. We see this as the last step to launching v1.0 into production.

- Site: https://starshell.net/
- Repo: GitHub - SolarRepublic/starshell-beta
- Beta: https://install.starshell.net/
- Features overview: Secret Feature: StarShell | Secret Network Blog

Choosing a Security Audit Firm

I interviewed and got quotes from 7 different security audit firms but was honestly quite disappointed with the quality behind most of them. However, two of those firms have shown us true attention to detail and demonstrated a solid understanding of the actual threats facing crypto wallet web extensions. Those firms are Least Authority and CertiK.

Our top choice was initially Least Authority given their history, the quality of the quote they gave us, and the strong alignment of our ethos, but the full audit they proposed (which includes a thorough assessment of the security and privacy of the wallet) is far too expensive for what I'm sure this community would be willing to spend (>$100k).

We have since followed up with CertiK and after a few rounds of discussion, arrived at $20k for a security audit that will focus primarily on finding any vulnerabilities that could lead to loss of funds. I met with the lead engineer who would be conducting the audit and went over the exact details of the scope. We also talked about some of the things working in our favor that significantly reduce the attack surface: (1) the extension deploys to all platforms using chrome's Manifest V3, which is only a very recent development for Firefox and Safari, (2) we are leveraging content security policies in said MV3, (3) we are not using any javascript libraries to perform signing/verification nor encryption/decryption, and (4) we are using ses to lockdown intrinsics and deep freeze to further harden globals, preventing typical supply-chain attacks in runtime dependencies. None of this is to say we are taking implied security for granted, just that these intentional design decisions are now also proving to simplify the audit process, which is how we were able to obtain a more affordable quote. Win-win

Funding History Background

As many of you know, the journey to this point has been fraught with market upsets. When I initially requested grant funds, SCRT was worth $6 and I had budgeted about $180k equivalent of fiat to finance this project, paid out in milestones. By the time we released beta, SCRT had fallen to $1. However, none of the funds I received had been converted to fiat (nor have they since – I also strongly believe that SCRT is undervalued). Instead, I've hired developers and a designer using personal funds, and have already spent way more than I'm willing to share publicly. Let's just say that even if I had converted the milestone payments to USD immediately at the time they were received, I would still be in considerable deficit today. When the overspend started to become apparent, I had to reduce the team to just me (the lead developer), a designer, and a friend who pitches in pro bono. I know several projects have faced similar challenges and we are not alone in that, but we are still here!

At the end of the day, at that really matters is that I am committed to this project because I love the work - it is my passion. I also strongly believe in the future of Secret Network. I have committed a substantial amount of time and money to this project for those reasons. If I didn't have the extra capital laying around or wasn't developing without pay, we would have easily washed out like other projects months ago. I only share this because I believe it's important to take into consideration with this funding request.

Request:

I am asking for $35k worth of SCRT from the community pool to be immediately converted into USD for the following spends:

- $20k for the CertiK security audit
- $10k white hat bounty after release for any properly disclosed vulnerability that could lead to loss of funds (to be stored in a multi-sig wallet)
- $5k for overhead & incidentals to help get us across the finish line including legal fees and marketing