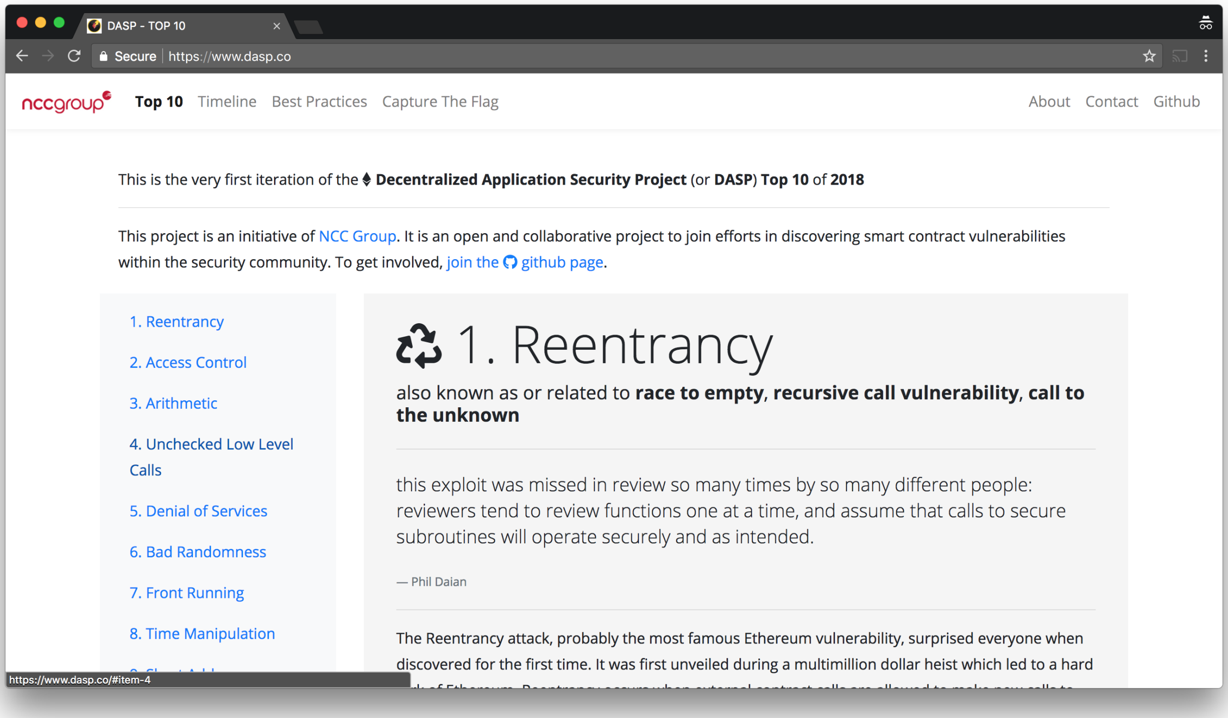
Cryptography Services

Archives About

Ethereum Top 10 Security Vulnerabilities For Smart Contracts

May 1, 2018 • David Wong

I am pleased to announce the launch of the Decentralized Application Security Project (DASP), an open and collaborative project to categorize and rank all known smart contract vulnerabilities. The field of smart contracts, while relatively new, has seen an incredible amount of surprising and devastating attacks. Notably, there was the DAO contract which lost 615,391 ethers (~ $50 million at the time) before forcing a fork of the Ethereum protocol, and then there was the Parity multi-signature wallet bugs which allowed attackers to steal more than 150,000 ethers (~ $30 million dollars at the time) and then block another 513,774 ethers. I believe it is of the utmost importance for the security community to assess the different smart contract issues and educate developers about these risks. This was done by the OWASP for web application vulnerabilities, and was successful in raising awareness of vulnerabilities in web applications.



This is the very first iteration of the ⧫ **Decentralized Application Security Project** (or **DASP**) **Top 10** of **2018**

This project is an initiative of NCC Group. It is an open and collaborative project to join efforts in discovering smart contract vulnerabilities within the security community. To get involved, join the github page.

1. Reentrancy
2. Access Control
3. Arithmetic
4. Unchecked Low Level Calls
5. Denial of Services
6. Bad Randomness
7. Front Running
8. Time Manipulation

1. Reentrancy

also known as or related to **race to empty**, **recursive call vulnerability**, **call to the unknown**

> this exploit was missed in review so many times by so many different people: reviewers tend to review functions one at a time, and assume that calls to secure subroutines will operate securely and as intended.
>
> — Phil Daian

The Reentrancy attack, probably the most famous Ethereum vulnerability, surprised everyone when discovered for the first time. It was first unveiled during a multimillion dollar heist which led to a hard

While Ethereum has created a new and fast-growing field in block chain technology, the security issues surrounding smart contracts have challenged its development, destroying many promising projects and lowering the public trust in smart contracts. Unlike web applications, Ethereum is directly linked with money and exploits typically result in immediate financial loss. These enormous economic losses have created an appreciation for security that most fields have had a hard time achieving (or have still yet to achieve). As the security community is trying to organize itself around cryptocurrencies and smart contracts, we hope to quickly spread knowledge of these issues into the developer community.

To achieve this, a Top 10 of all smart contract security issues was produced, as well as a list of smart contract vulnerabilities found in the wild. As Ethereum is still rapidly evolving, new vulnerabilities are expected to be discovered and the DASP Top 10 should reflect new developments. We hope that the DASP will play an important role in improving the security stance of Ethereum smart contracts.

All of us in the security community are familiar with the well-known mantra “security is a process.” However, the immutability of smart contracts challenges this mindset. Testing contracts has become an important part of gaining confidence in a smart contract’s soundness. It is important that clear guidelines and methods are created and shared to audit smart contracts. While the DASP page currently hosts its first iteration of the Top 10 and a running list of smart contract vulnerabilities, it is really meant to grow into a larger platform that will host more projects in the future. NCC Group supports this initiative and has made the page open-source to further collaboration with the security community. Please do not hesitate to create discussions in the Github issues or submit pull requests to the repository. You can start submitting your findings today.

Cryptography Services

Cryptography Services is a dedicated team of consultants from NCC Group focused on cryptographic security assessments, protocol and design reviews, and tracking impactful developments in the space of academia and industry.