SLIIT
Discover Your Future

BSc (Hons) in IT Specialized in CS
Year 2, 2022

Tutorial 08

SNP **Smart Contract Vulnerabilities**

---

1. What are some of the attacks on smart contracts?

- Front-Running AKA Transaction-Ordering Dependence.
- DoS with Block Gas Limit.
- DoS with (Unexpected) revert.
- Forcibly Sending Ether to a Smart Contract.
- Insufficient Gas Griefing.
- Reentrancy.
- Honeypot.

2. What is a Reentrancy attack?

- A reentrancy attack occurs when a function makes an external call to another untrusted contract. Then the untrusted contract makes a recursive call back to the original function in an attempt to drain funds.

3. Find a famous Reentrancy attack in the world and the attack explain the attack that was carried out based on the asset loss and do a small Root Cause Analysis.

4. How to Protect Smart Contract Against a Reentrancy Attack?

- Ensure all state changes happen before calling external contracts, i.e., update balances or code internally before calling external code
- Use function modifiers that prevent reentrancy