



Open in app

Get started



Heuristic Wave

Follow

Dec 20, 2018 · 5 min read



Save



Ethernaut Force Problem — 이더넷 7단계 문제 해설

문제 해설에 들어가기 전, 이번 포스팅은 이더넷 내에서 콘솔창과 상호작용을 할 줄 알고 기본적인 리믹스 및 메타마스크 사용법이 숙지되어 있다는 가정 하에 해설을 진행합니다.

The Ethernaut

by



Heuristic Wave



Force Problem

이번 문제의 목표는 어떤 컨트랙트에 입금을 시키는 문제다. (원문 : make the balance of the contract greater than zero)

이번에도 문제를 푸는데 실마리가 되는 부분을 잘 확인해보자!

- Fallback 함수
- 다른 컨트랙트를 사용하여 공격하기
- 콘솔 창을 활용하여 해결하기

이번 문제는 텅 빈 컨트랙트가 주어졌다.

```
pragma solidity ^0.4.18;

contract Force { /*
    /\_/\
   /  o o \
  /~_____\~\  =Ø= /
 (_____)__m__m)
 */ }
```

그냥 단순히 메타마스크에서 주어진 CA주소에 송금을 하면 어떻게 될까?

안타깝게도 위와 같은 방법은 통하지 않는다. 그럼 어떤 방법을 써야 할까?

솔리디티 문서에서는 아래와 같은 `selfdestruct`에 대한 설명이 있다.

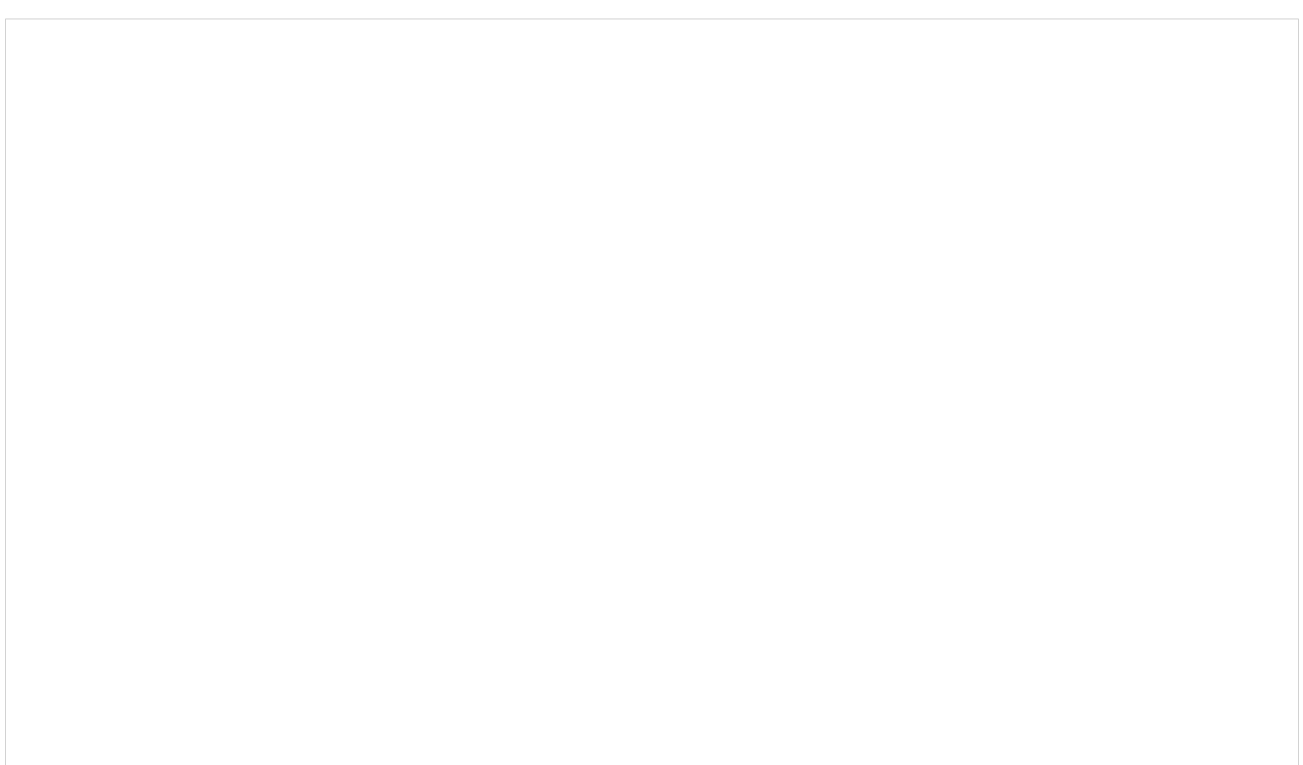
A contract without a payable fallback function can receive Ether as a recipient of a coinbase transaction (aka miner block reward) or as a destination of a `selfdestruct`.

`payable` 함수가 없는 컨트랙트가 이더를 받으려면, `selfdestruct`의 목적지가 되어야 한다고 한다. 여기서 힌트를 얻어 바로 컨트랙트를 작성해보자!

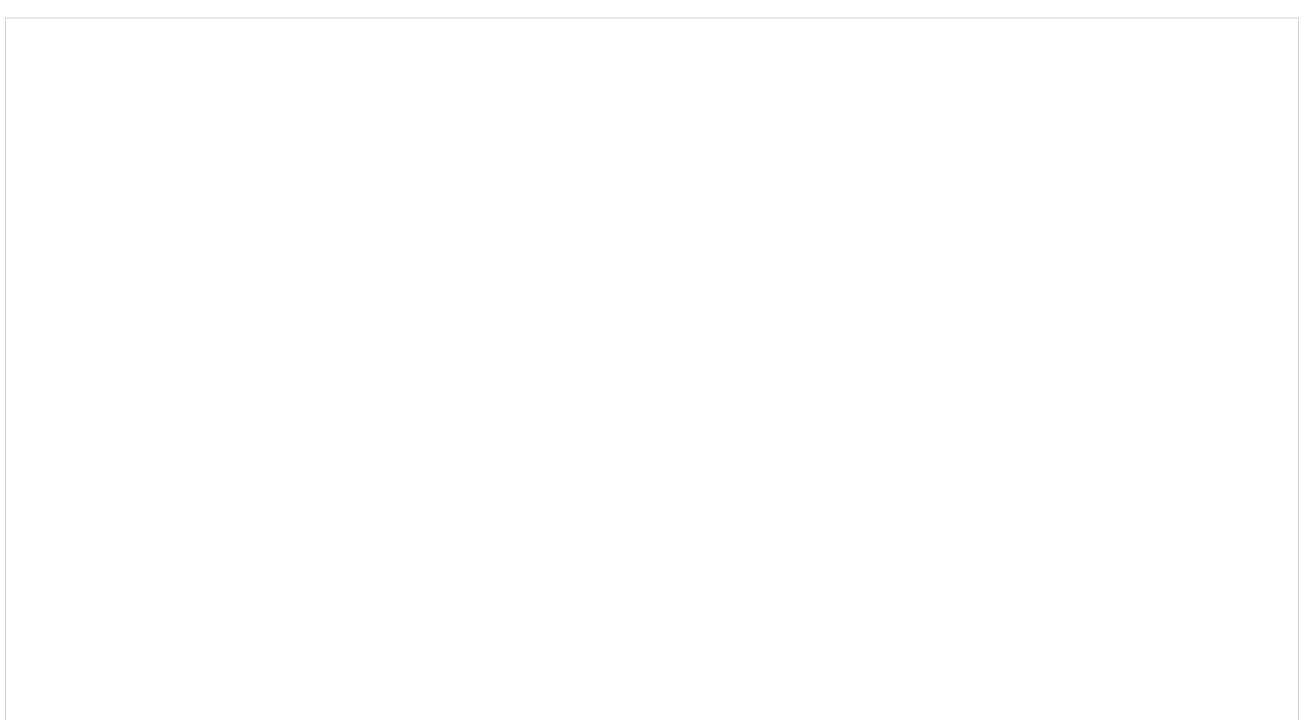
```
contract ForceHack {
    function() payable {}

    function destination(address target) {
        selfdestruct(target);
    }
}
```

ForceHack 컨트랙트는 이더를 받을 수 있도록 `payable` 함수와 이더를 옮길 수 있게 `selfdestruct`를 구현해야 한다.



위 소스코드를 담은 ForceHack을 배포한 이후에, 리믹스 왼쪽 상단 value에 0.1이더를 적고 (fallback)을 실행시킨다.



이더스캔에서 확인해보면 나의 EOA주소에서 배포한 CA주소로 0.1이더가 잘 들어 간것을 확인 할 수 있다.

마지막으로 리믹스에서 ForceHack에 담긴 이더를 Force컨트랙트로 이동시키기 위해서 리믹스 destination함수에 Instance address 를 넣고 호출하면 앞으로 ForceHack컨트랙트는 사용할 수 없고 담겨있던 돈은 Force컨트랙트로 이동된다.

우리는 여기까지 힌트로 주어진 폴백함수와 다른컨트랙트로 공격하기를 사용하였다.

마지막으로 확인은 콘솔창을 활용하여 이더가 잘 전송되었는지 확인하자!

```
await getBalance("Instance address")
```

이어서 결과물을 제출하면 성공!!

Force 문제를 통해서 selfdestruct의 기능과 payable 함수 유무에 따른 이더전송 가능 유무를 알 수 있었다. <https://medium.com/loom-network/how-to-secure-your-smart-contracts-6-solidity-vulnerabilities-and-how-to-avoid-them-part-2-730db0aa4834> 이 글을 읽고보고 언제 selfdestruct를 사용해야하는지 고민해보고 여러분의 컨트랙트에 적용해보자.

이번 문제는 난이도가 5단계 였지만, 평상시 selfdestruct를 만나본 경험이 있고 어떤 기능이 있는지 정확히 알고있다면 수월하게 해결할 수 있었을 것이다. 필자도 이전 글에 포

스팅한 IoT관련 컨트랙트에서 selfdestruct를 만나본 경험이 있어서 헤매이지 않고 풀 수 있었다.

다음번에는 8단계 vault에서 만나요!

Ethernaut Vault Problem — 이더넷 8단계 문제 해설

문제 해설에 들어가기 전, 이번 포스팅은 이더넷 내에서 콘솔창과 상호 작용을 할 줄 알고 기본적인 리믹스 및 메타마스크 사용법이 숙지되어

medium.com

ne Ethernaut

euristic Wav



[About](#) [Help](#) [Terms](#) [Privacy](#)

Get the Medium app

