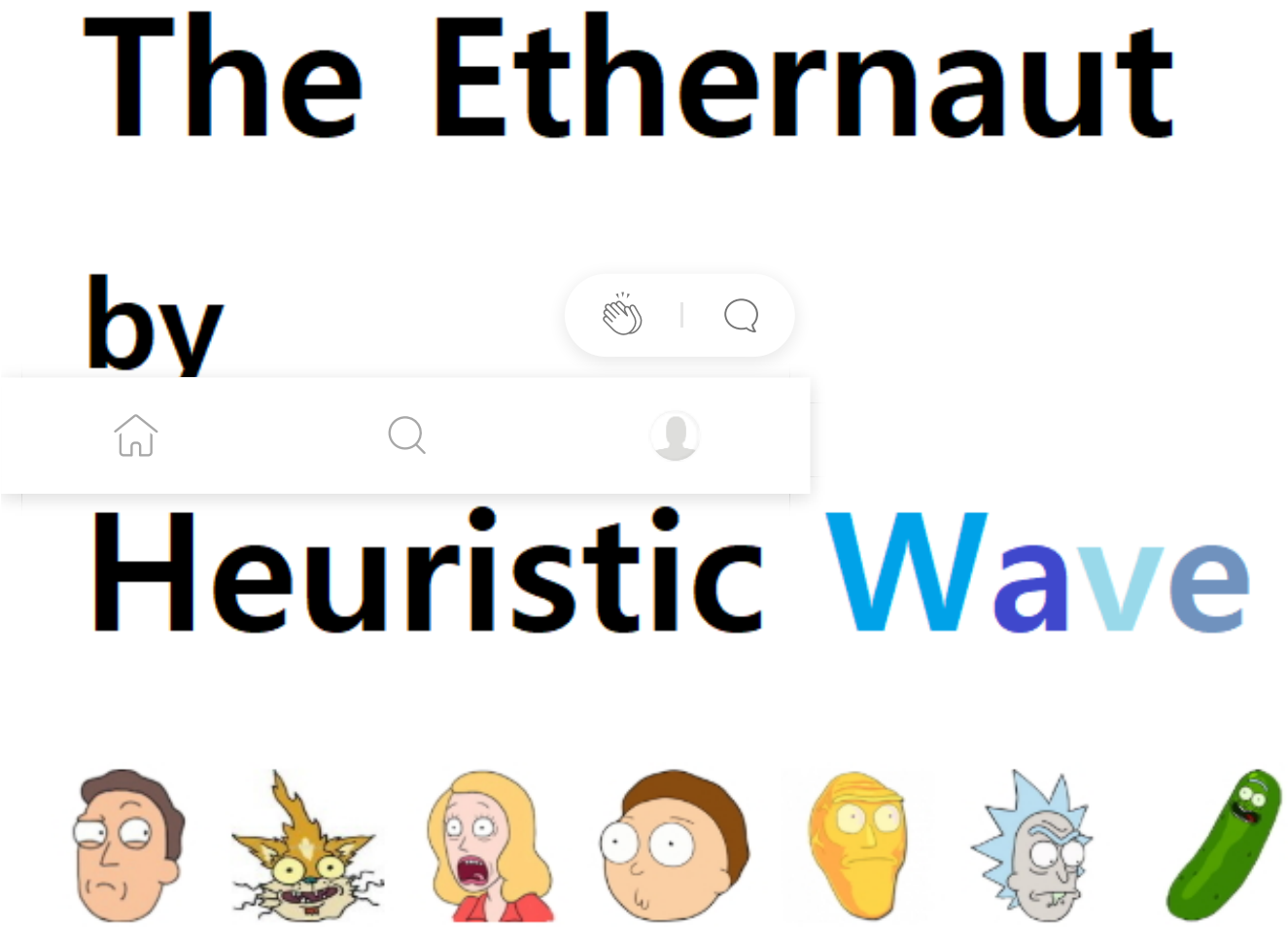
Heuristic Wave Follow
Dec 20, 2018 · 4 min read

Ethernaut Vault Problem — 이더넛 8단계 문제 해설

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



. . .

Vault Problem

이번 문제의 목표는 valut 컨트랙트의 비밀번호를 알아내는 문제다. 그동안 이더리움을 공부하였다면 이더리움에서의 거래는 암호화되지 않는 다는 사실을 알것이다. 거래뿐만이 아니라 계정의 storage영역의 내용도 파악이 가능하다. 상태를 private 혹은 internal로 선언하여도 decode작업을 통해서 무슨 정보가 담겨 있는지 알아 낼 수 있다.

당신이 만약, 싱크가 되어 있는 게스가 있다면 geth내에서 아래와 같은 명령어로 decode 작업을 할 수 있다.

```
> eth.getTransaction('0x해당컨트랙트의 트랜잭션 해쉬').input
```

이후 필요한 부분을 구해서 16진수를 ASCII 문자열로 변환해주는 함수를 사용해 접근이 불가능한 문자열도 알아 낼 수 있다.

```
> web3.toAscii("0x~~~~~~~~~");
```

그러나 우리는 싱크를 받은 게스도 없을 뿐더러, 싱크를 받는다고 하더라고 롭슨의 경우 싱크가 되기까지 하루 이상이 걸리기 때문에 이더스캔에서 제공하는 API를 활용하여 decode 작업을 진행하겠다. 사실 이번문제는 API를 활용하는 방법말고도 더 간편한 방법들이 있지만, API활용방법을 알았으면 하는 차원에서 소개한다.

web3.eth.getStorageAt API

우리는 위에서 소개한 decode작업을 위한 API를 eth.getStorageAt API를 활용하여 해결 할 수 있다.

1. 위 API를 사용하기 위해서 우선적으로 https://ropsten.etherscan.io/ 에 들어간다.

2. MISC -> APIs -> Introduction 가운데 링크로 있는 MyApiKey링크를 클릭한다.
3. 로그인을 하라고 하는데 만약 등록이 되어있지 않다면 가입을 하고 로그인을 하여 My Account에 들어가자
4. 왼쪽 하단 Developers -> API-KEYs를 클릭하여 API키를 만든후 복사하여 어딘가에 저장해두자.
5. 이후, 다시 Ethereum Developer APIs에 들어가서 GETH/Parity Proxy안에서 우리의 API를 찾자. 아래 주소가 우리가 사용해야 할 API이다. https://api-ropsten.etherscan.io/api?module=proxy&action=eth_getStorageAt&address=0x6e03d9cce9d60f3e9f2597e13cd4c54c55330cfd&position=0x0&tag=latest&apikey=YourApiKeyToken
6. 4번에서 복사한 API키를 위 주소 마지막에 위치한 YourApiKeyToken자리에 붙여넣는다.
7. 위 주소에서 position위치를 찾아 뒤에 위치한 0x0을 0x1로 바꾼다

- Vault 컨트랙트에서 상태변수 locked가 인덱스 0, password가 인덱스 1이기 때문이다.

8. 0x6e03d9cce9d60f3e9f2597e13cd4c54c55330cfd에 위치하는 것은 instance의 주소이다. 즉, 문제를 받고 받은 CA주소를 해당 위치에 대체하여 완성된 주소에 접속한다.

이때! API를 받으러 이더스캔 페이지를 이동하는 사이에 나도 모르게 메인넷의 API를 받아 올 수도 있기 때문에 항상 롭슨인지 아닌지 확인하자!

```
{"jsonrpc":"2.0","result":"0x4120766572792073747
5637265742070617373776f7264203a29","id":1}
```

이후, 위와 같이 제이슨 형식의 result값을 복사하여 vault의 매개변수로 넣어 트랜잭션

을 발생시키면 성공한다.

이번 문제통해 우리는 컨트랙트 내부에 외부에 노출되어서는 안되는 중요한 정보를 기입하면 안된다는 것을 확인했다.

다음번에는 9단계 King에서 만나요!