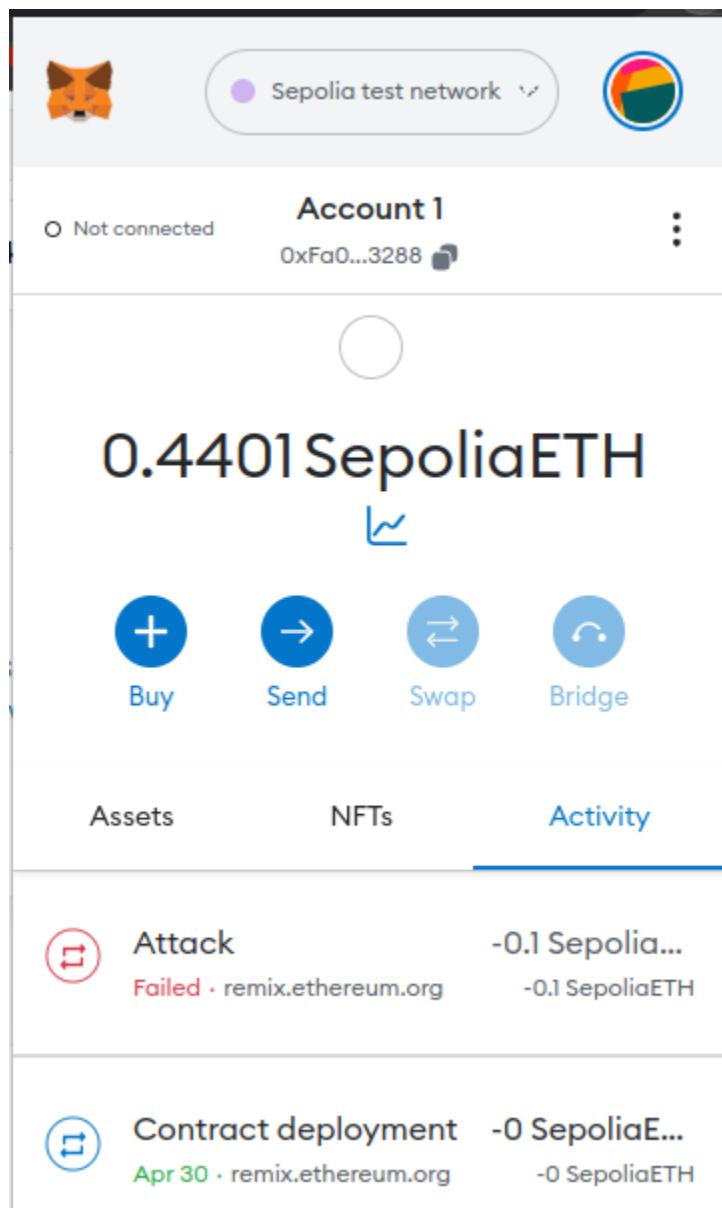


BFSC Ethernaut CTF Assignment

Manmeet Singh Brar
20UCS112

Wallet Address - 0xFa00D29d378EDC57AA1006946F0fc6230a5E3288(Metamask)

<https://sepolia.etherscan.io/address/0xfa00d29d378edc57aa1006946f0fc6230a5e3288>



First Three CTFs (Hello Ethernaut, Fallback, Fallout) were done in class itself.

The screenshot shows the OpenZeppelin challenge interface for the Coin Flip CTF level. The challenge title is "Coin Flip". On the left, there is a sidebar with a "We're hiring!" button and a list of completed challenges: Hello Ethernaut, Fallback, and Fallout. The main area shows the challenge code and a UI for interacting with it. The UI includes a "Send" button and a "Balance" section showing 0.4401 SepoliaETH. The challenge description indicates that the level is not translated or translation is incomplete, with a link to improve the translation.

Coin Flip

Activities Google Chrome

(3) Sikander Kahlon - N x Ethernaut x Sepolia Blocks #336920+ x "Block value calculation" x Units and Globally Available x solidity - Retrieving block x Remix - Ethereum IDE x +

Problems - Lee... Damn Vulnera... HackenProof |... New Chat (34) Introduction CALYXPOD | C... (34) Ultimate... 30 Smart Cont... (5) DeFi MOO...

We're hiring!

Z OpenZeppelin

Coin Flip

This is a coin flipping game where you need to build up your winning streak by guessing the outcome of a coin flip. To complete this level you'll need to use your psychic abilities to guess the correct outcome 10 times in a row.

Things that might help

- See the [?" page above in the top right corner menu, section "Beyond the console"](#)

developed with ❤ and 🚀 by the [OpenZeppelin](#) team

Account 1
0xF00...3288

0.4914 SepoliaETH

Buy Send Swap Bridge

Assets NFTs Activity

Submit Level Instance -0 SepoliaETH Apr 27 - eternaut.openzeppelin.com -0 SepoliaETH

Flip -0 SepoliaETH Apr 27 - remix.ethereum.org -0 SepoliaETH

Error in RPC response:
header not found

(--) Well done, You have completed this level!!!

Uncaught (in promise)
(code: -32000, message: 'header not found')

(--) Well done, You have completed this level!!!

Queue (1)

Submit Level Instance -0 SepoliaETH Pending - eternaut.openzeppelin.com -0 SepoliaETH

Speed up Cancel

Uncaught (in promise)
(code: -32000, message: 'header not found')

Well done, You have completed this level!!!

Telephone

Activities Google Chrome

(3) No Reason (Official) x Ethernaut x Sepolia Blocks #336920+ x "Block value calculation" x Units and Globally Available x solidity - Retrieving block x Remix - Ethereum IDE x +

Problems - Lee... Damn Vulnera... HackenProof |... New Chat (34) Introduction CALYXPOD | C... (34) Ultimate... 30 Smart Cont... (5) DeFi MOO...

We're hiring!

Z OpenZeppelin

Telephone

Claim ownership of the contract below to complete this level.

Things that might help

- See the [?" page above in the top right corner menu, section "Beyond the console"](#)

developed with ❤ and 🚀 by the [OpenZeppelin](#) team

Account 1
0xF00...3288

0.4884 SepoliaETH

Buy Send Swap Bridge

Assets NFTs Activity

Submit Level Instance -0 SepoliaETH Pending - eternaut.openzeppelin.com -0 SepoliaETH

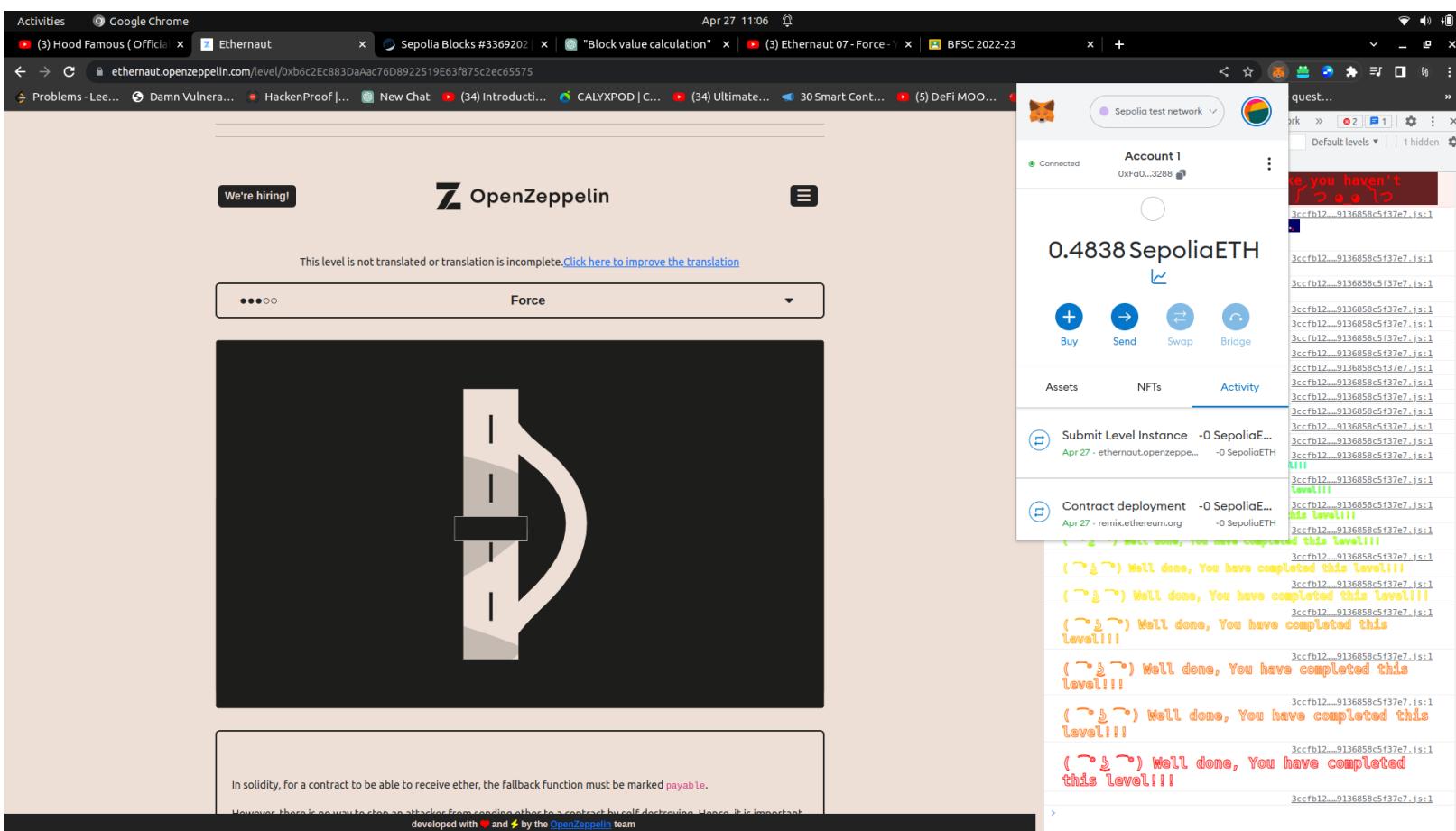
Speed up Cancel

Uncaught (in promise)
(code: -32000, message: 'header not found')

Well done, You have completed this level!!!

Token

Force



Vault

Activities Google Chrome

Ethernaut x Remix - Ethereum IDE x +

April 27 11:15

etherernaut.openzeppelin.com/level/0xB7257D8Ba61BD1b3Fb7249DCd9330a023a5F3670

Problems - Lee... Damn Vulnera... HackenProof | ... New Chat (34) Introducti... CALYXPOD | C... (34) Ultim... 30 Smart Cont... (5) DeFi MOO...

We're hiring!

OpenZeppelin

Vault

Unlock the vault to pass the level!

```
// SPDX-License-Identifier: MIT
pragma solidity ^0.8.0;
```

King

Activities Google Chrome

Ethernaut x Remix - Ethereum IDE x +

April 27 14:44

etherernaut.openzeppelin.com/level/0x3049C00639E6dfC269ED1451764a046f7aE500c6

Problems - Lee... Damn Vulnera... HackenProof | ... New Chat (34) Introducti... CALYXPOD | C... (34) Ultim... 30 Smart Cont... (5) DeFi MOO...

```
// SPDX-License-Identifier: MIT
pragma solidity ^0.8.0;

contract King {
    address king;
    uint public prize;
    address public owner;

    constructor() payable {
        owner = msg.sender;
        king = msg.sender;
        prize = msg.value;
    }

    receive() external payable {
        require(msg.value >= prize || msg.sender == owner);
        payable(king).transfer(msg.value);
        king = msg.sender;
        prize = msg.value;
    }

    function _king() public view returns (address) {
        return king;
    }
}
```

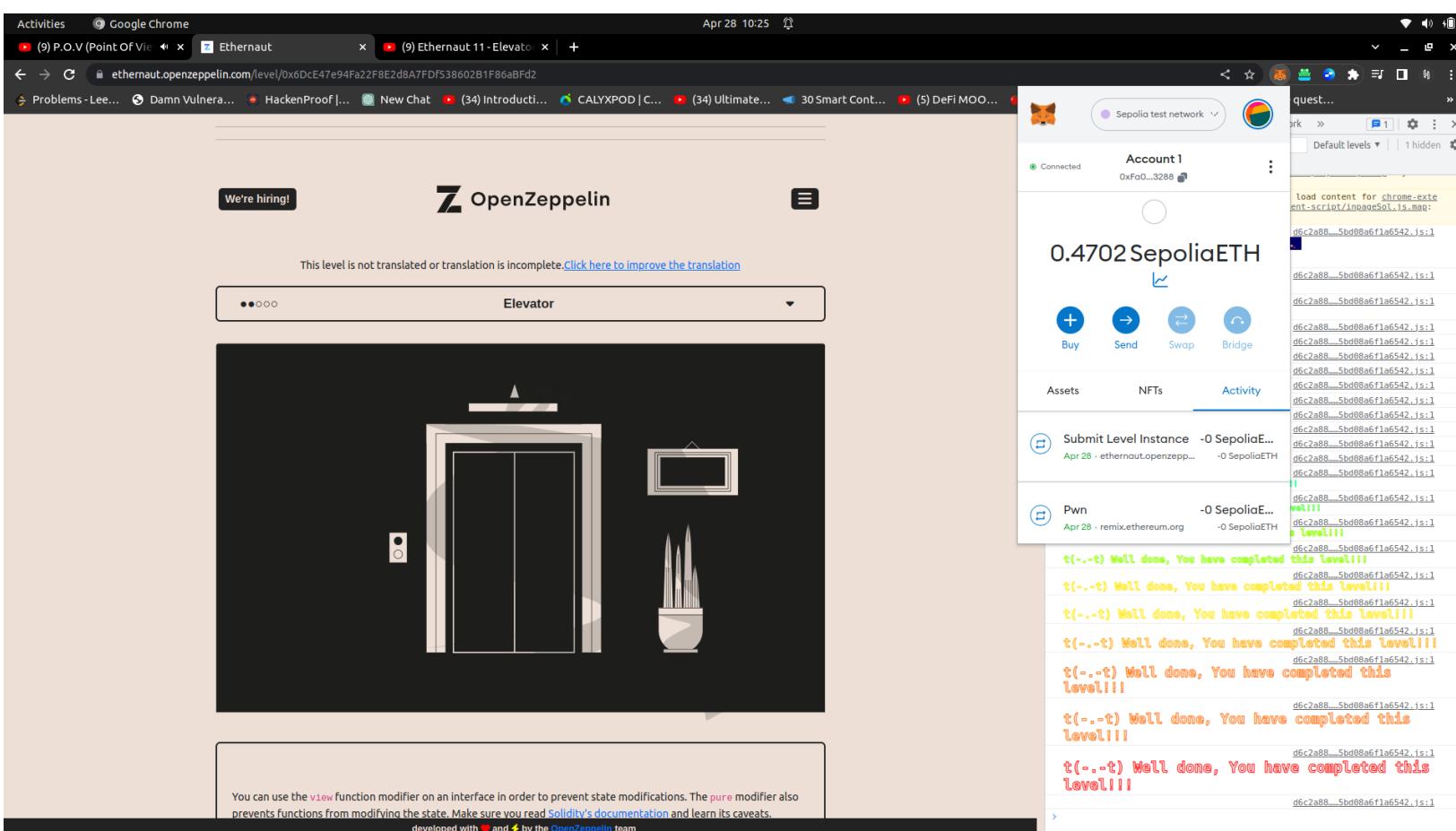
Go to the next level Get new instance

Level author(s): Alejandro Santander

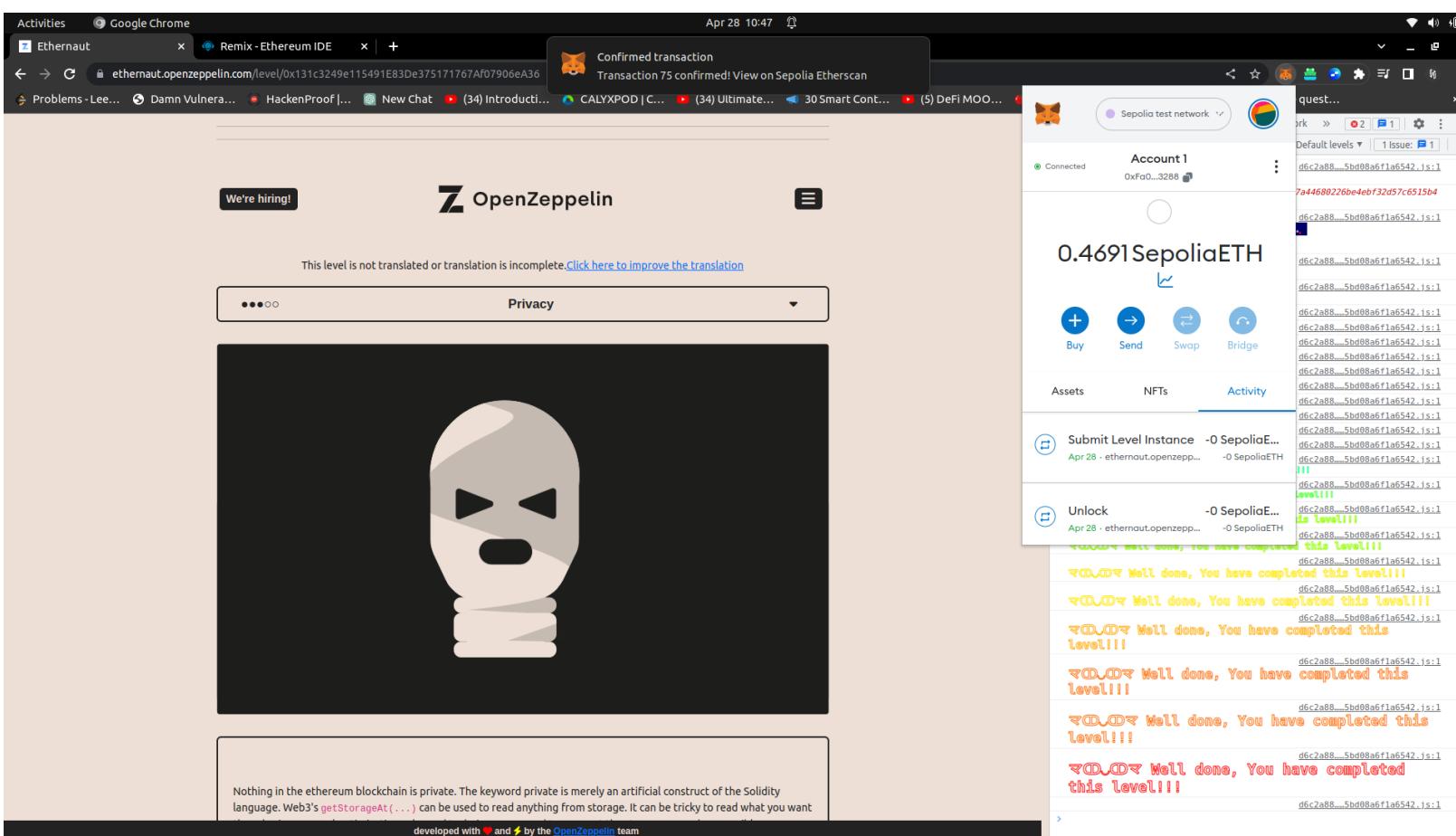
Did this level teach you anything useful? Donate to the level author (on mainnet): 0x31a3801499618d3c4b0225b9e06e228d4795b55d

```
developed with ❤️ and 💎 by the OpenZeppelin team
```

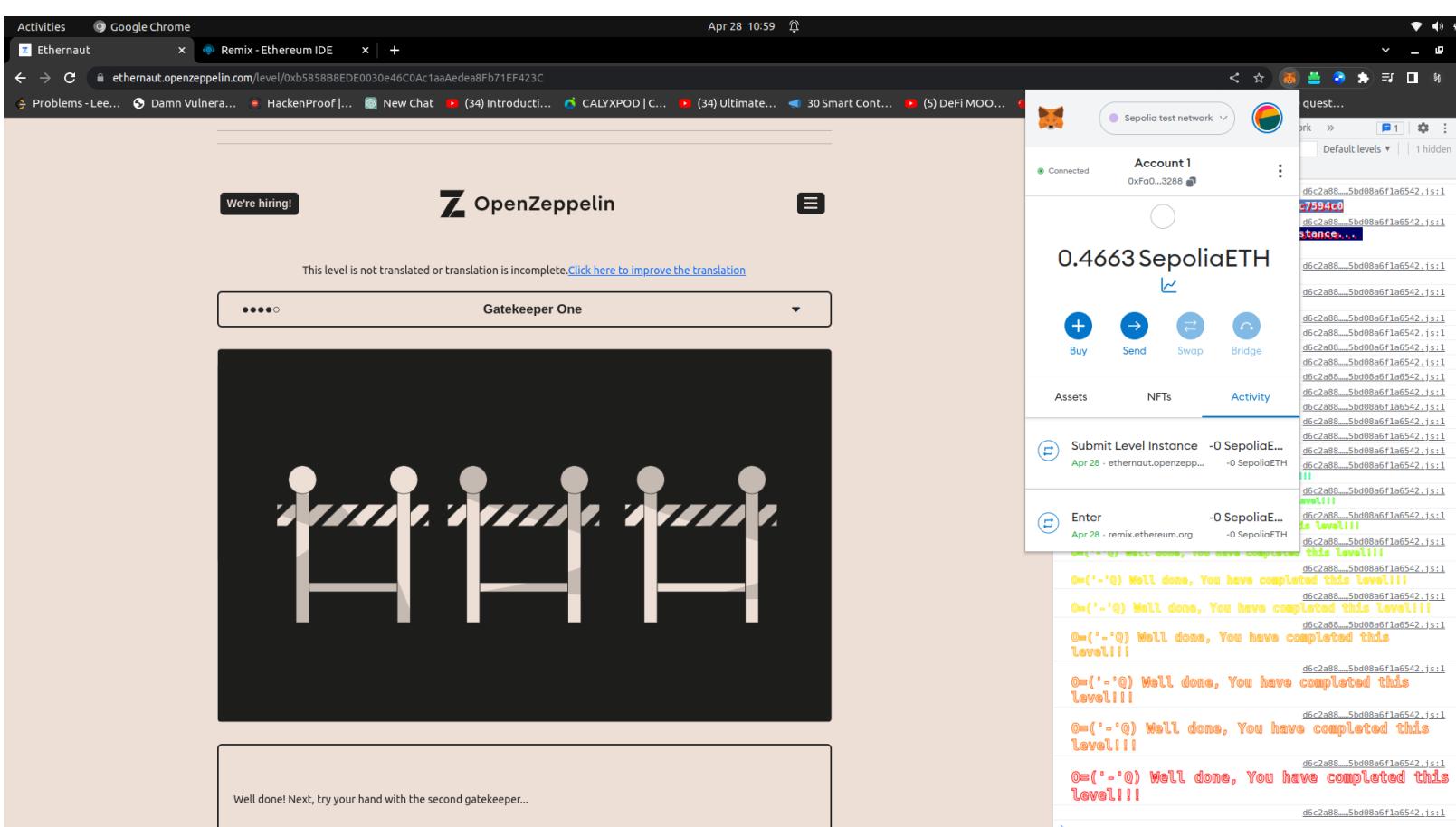
Elevator



Privacy



Gatekeeper One



Gatekeeper Two

Activities Google Chrome

Ethernaut x Remix - Ethereum IDE x + Confirmed transaction Transaction 82 confirmed! View on Sepolia Etherscan

We're hiring!

OpenZeppelin

This level is not translated or translation is incomplete. [Click here to improve the translation](#)

Gatekeeper Two

0.4648 SepoliaETH

Buy Send Swap Bridge

Assets NFTs Activity

Submit Level Instance -0 SepoliaETH Apr 28 - ethernaut.openzeppelin.org -0 SepolioETH

Contract deployment -0 SepoliaETH Apr 28 - remix.ethereum.org -0 SepolioETH

L111
Well done, You have completed this level!!!
Well done, You have completed this level!!!

developed with ❤️ and ✨ by the OpenZeppelin team

Naught Coin

Activities Google Chrome

Ethernaut x Remix - Ethereum IDE x + Confirmed transaction Transaction 82 confirmed! View on Sepolia Etherscan

We're hiring!

OpenZeppelin

This level is not translated or translation is incomplete. [Click here to improve the translation](#)

Naught Coin

0.4612 SepoliaETH

Buy Send Swap Bridge

Assets NFTs Activity

Submit Level Instance -0 SepoliaETH Apr 28 - ethernaut.openzeppelin.org -0 SepolioETH

Pwn -0 SepoliaETH Apr 28 - remix.ethereum.org -0 SepolioETH

L111
Well done, You have completed this level!!!
Well done, You have completed this level!!!

developed with ❤️ and ✨ by the OpenZeppelin team

Preservation

Activities Google Chrome

(12) Ethernaut 16-Present Ethernaut +

for building libraries, as it prevents the libraries from storing and accessing state variables.

```
// SPDX-License-Identifier: MIT
pragma solidity ^0.8.0;

contract Preservation {
    // public library contracts
    address public timeZone1Library;
    address public timeZone2Library;
    address public owner;
    uint storedTime;

    // Sets the function signature for delegatecall
    bytes4 constant setTimeSignature = bytes4(keccak256("setTime(uint256)"));

    constructor(address _timeZone1LibraryAddress, address _timeZone2LibraryAddress) {
        timeZone1Library = _timeZone1LibraryAddress;
        timeZone2Library = _timeZone2LibraryAddress;
        owner = msg.sender;
    }

    // set the time for timezone 1
    function setTime(uint _timeStamp) public {
        timeZone1Library.delegatecallabi.encodePacked(setTimeSignature, _timeStamp);
    }

    // set the time for timezone 2
    function setSecondTime(uint _timeStamp) public {
        timeZone2Library.delegatecallabi.encodePacked(setTimeSignature, _timeStamp);
    }

    // Simple library contract to set the time
    contract LibraryContract {
        // stores a timestamp
        uint storedTime;

        function setTime(uint _time) public {
            storedTime = _time;
        }
    }
}
```

[Go to the next level](#) | [Get new instance](#)

developed with ❤️ and ✨ by the [OpenZeppelin](#) team

The screenshot shows the Ethernaut challenge interface with the Preservation contract code. To the right, a Remix browser window is open on the Sepolia test network. The SepoliaETH interface shows a balance of 0.4587 SepoliaETH. Below the balance, there are four buttons: Buy, Send, Swap, and Bridge. The Activity tab is selected, showing a list of recent interactions:

- Submit Level Instance -0 SepoliaETH
- Contract interaction -0 SepoliaETH
- (*) Well done, You have completed this level!!!
- (*) Well done, You have completed this level!!!
- (*) Well done, You have completed this level!!!
- (*) Well done, You have completed this level!!!
- (*) Well done, You have completed this level!!!
- (*) Well done, You have completed this level!!!
- (*) Well done, You have completed this level!!!
- (*) Well done, You have completed this level!!!

Recovery

Activities Google Chrome

(12) Ethernaut 16-Present Ethernaut +

for building libraries, as it prevents the libraries from storing and accessing state variables.

```
// SPDX-License-Identifier: MIT
pragma solidity ^0.8.0;

contract Preservation {
    // public library contracts
    address public timeZone1Library;
    address public timeZone2Library;
    address public owner;
    uint storedTime;

    // Sets the function signature for delegatecall
    bytes4 constant setTimeSignature = bytes4(keccak256("setTime(uint256)"));

    constructor(address _timeZone1LibraryAddress, address _timeZone2LibraryAddress) {
        timeZone1Library = _timeZone1LibraryAddress;
        timeZone2Library = _timeZone2LibraryAddress;
        owner = msg.sender;
    }

    // set the time for timezone 1
    function setTime(uint _timeStamp) public {
        timeZone1Library.delegatecallabi.encodePacked(setTimeSignature, _timeStamp);
    }

    // set the time for timezone 2
    function setSecondTime(uint _timeStamp) public {
        timeZone2Library.delegatecallabi.encodePacked(setTimeSignature, _timeStamp);
    }

    // Simple library contract to set the time
    contract LibraryContract {
        // stores a timestamp
        uint storedTime;

        function setTime(uint _time) public {
            storedTime = _time;
        }
    }
}
```

[Go to the next level](#) | [Get new instance](#)

developed with ❤️ and ✨ by the [OpenZeppelin](#) team

The screenshot shows the Ethernaut challenge interface with the same Solidity code as the previous screenshot. To the right, a Remix browser window is open on the Sepolia test network. The SepoliaETH interface shows a balance of 0.4587 SepoliaETH. Below the balance, there are four buttons: Buy, Send, Swap, and Bridge. The Activity tab is selected, showing a list of recent interactions:

- Submit Level Instance -0 SepoliaETH
- Contract interaction -0 SepoliaETH
- (*) Well done, You have completed this level!!!
- (*) Well done, You have completed this level!!!
- (*) Well done, You have completed this level!!!
- (*) Well done, You have completed this level!!!
- (*) Well done, You have completed this level!!!
- (*) Well done, You have completed this level!!!
- (*) Well done, You have completed this level!!!
- (*) Well done, You have completed this level!!!

Magic Number

Alien Codex (Level doesn't Exist anymore)

Denial

This level demonstrates that external calls to unknown contracts can still create denial of service attack vectors if a fixed amount of gas is not specified.

If you are using a low level `call` to continue executing in the event an external call reverts, ensure that you specify a fixed gas stipend. For example `call.gas(100000).value()`.

Typically one should follow the [checks-effects-interactions](#) pattern to avoid reentrancy attacks, there can be other circumstances (such as multiple external calls at the end of a function) where issues such as this can arise.

Note: An external `CALL` can use at most $63/64$ of the gas currently available at the time of the `CALL`. Thus, depending on how much gas is required to complete a transaction, a transaction of sufficiently high gas (i.e. one such that $1/64$ of the gas is capable of completing the remaining opcodes in the parent call) can be used to mitigate this particular attack.

```
// SPDX-License-Identifier: MIT
pragma solidity ^0.8.0;
contract Denial {
    address public partner; // withdrawal partner - pay the gas, split the withdraw
    address public constant owner = address(0xA9E);
    uint timeLastWithdrawn;
    mapping(address => uint) withdrawPartnerBalances; // keep track of partners balances

    function setWithdrawPartner(address _partner) public {
        partner = _partner;
    }

    // withdraw 1% to recipient and 1% to owner
    function withdraw() public {
        uint amountToSend = address(this).balance / 100;
        // perform a call without checking return
        // The recipient will revert, the owner will still get their share
        payable(partner).call{value:amountToSend}("");
        payable(owner).transfer(amountToSend);
        // keep track of last withdrawal time
        timeLastWithdrawn = block.timestamp;
        withdrawPartnerBalances[partner] += amountToSend;
    }

    // allow deposit of funds
    receive() external payable {}
}
```

developed with ❤️ and 🚀 by the OpenZeppelin team

Activity pane showing multiple txns from the challenge contract, each with a green "Well done, You have completed this level!!!".

Shop

We're hiring!

Z OpenZeppelin

This level is not translated or translation is incomplete. [Click here to improve the translation](#)

Shop

```
Contracts can manipulate data seen by other contracts in any way they want.
It's unsafe to change the state based on external and untrusted contracts logic.
```

Confirmed transaction Transaction 108 confirmed! View on Sepolia Etherscan

Activity pane showing multiple txns from the challenge contract, each with a green "Well done, You have completed this level!!!".

All Levels

The screenshot shows the Ethernaut challenge interface on the left and the MetaMask wallet interface on the right. The challenge page displays a completed vault named 'Denial' with a 'Privacy' requirement. The MetaMask wallet shows an account connected to the Sepolia test network, holding 0.4389 SepoliaETH. It includes buttons for Buy, Send, Swap, and Bridge, and a tab for Activity showing two failed transactions: 'Create Level Instance' and 'Attack'.

Vault is Completed but for some reason it is not showing in navbar.

I was unable to do reentrancy my transactions kept on failing

The screenshot shows the Remix IDE's Transaction Details page for a failed transaction. The transaction hash is 0x835930fd0eb1b10f4cc2d863907bc793b6190af45bbeef928ad33f0f4665aae7. It failed in block 3390018 with 2 confirmations. The transaction was from 0xFa00D29d378EDC57AA1006946F0fc6230a5E3288 to 0x162BFb1A19950E4a0DEa119DE94071Fc909F7015. A warning message indicates an error during contract execution [execution reverted]. The transaction value was 0.001 ETH (\$0.00) - [CANCELLED]. Gas usage was 3,000,000 with 30,905 (1.03%) used.



We're hiring!

Denial

- ✓ Telephone
- ✓ Token
- ✓ Delegation
- ✓ Force
- Vault
- ✓ King
- Re-entrancy
- ✓ Elevator
- ✓ Privacy
- ✓ Gatekeeper One

Sepolia test network

Connected Account 1 0xFa0...3288

0.4389 SepoliaETH

Buy Send Swap Bridge

Assets NFTs Activity

Create Level Instance -0 SepoliaETH Failed - eternaut.openzeppelin.org -0 SepoliaETH

Attack -0.1 SepoliaETH Failed - remix.ethereum.org -0.1 SepoliaETH

14150a2....1e98d76a9902a6.js:1
14150a2....1e98d76a9902a6.js:1
5168E0f
14150a2....1e98d76a9902a6.js:1
aF802e6