Homework 9

Read the Smart Contract Best Practices page thoroughly.

The following code has a critical security vulnerability that can be exploited to hijack the contract and steal its ether. Find the vulnerability and then thoroughly explain 1) how an attacker can exploit it and 2) how the contract can be fixed to patch the vulnerability. Submit as a Word document, text file, or PDF through Blackboard.

```
pragma solidity ^0.4.25;

contract Benchmark {
    uint[] private records;
    address private owner;

    constructor() public {
        records = new uint[](0);
        owner = msg.sender;
    }

    function () public payable {
    }

    function add(uint c) public {
        records.push(c);
    }

    function removeLast() public {
        require(0 <= records.length);
        records.length--;
    }

    function replace(uint i, uint c) public {
        require(i < records.length);
        records[i] = c;
    }

    function destroy() public {
        require(msg.sender == owner);
        selfdestruct(msg.sender);
    }
}
```