Decurity EVM/Solidity test

Questions

Describe the pitfalls you see in this code

```
mapping(bytes => bool) used;
address signer;

function claimToken(uint256 tokenId, bytes memory sig) public {
    require(
        verifysig(keccak256(abi.encodePacked("Token_", tokenId)), sig) == signer,
        "Invalid signature!"
    );
    require(!used[sig], "Signature already used!");
    used[sig] = true;
    super._safeMint(msg.sender, tokenId);
}

function verifysig(bytes32 hash, bytes memory sig) internal pure returns (address) {
    bytes32 r;
    bytes32 s;
    uint8 v;

    if (sig.length != 65) {
        return address(0x0);
    }

    assembly {
        r := mload(add(sig, 32))
        s := mload(add(sig, 64))
        v := and(mload(add(sig, 65)), 255)
    }

    if (v < 27) {
        v += 27;
    }

    return ecrecover(hash, v, r, s);
}
```

Your answer

What would be the calldata length when calling such a function with the arguments a=[1,2], b=[] ?

```
function dosmth(uint256[] memory a, uint256[] memory b) public {
    . . .
}
```

Your answer

Imagine you've been debugging a contract on the testnet and accidentally called the same address on the mainnet and sent ETH to it. There's no contract on this address on the mainnet. Can the funds be retrieved and how?

Your answer

Under which circumstances is it possible to recover private key from a transaction (Bitcoin/Ethereum)?

Your answer

Is it possible to send ether to this contract?

```
contract Bank {
    function () payable {
        revert();
    }

    function somethingBad() {
        require(this.balance > 0);
        // Do something bad
    }
}
```

Your answer

Describe what happens if you call the function `proxycall` and specify an EOA address as a target?

```
function proxycall(address target, bytes memory data) public returns (bool) {
    (bool success, bytes memory returnData) = address(target).call(data);
    return success;
}
```

Your answer

Can you perform a code injection attack in Solidity?

Your answer

Can you perform a memory corruption attack in Solidity?

Your answer

Under what circumstances may the wrapped asset contract become insolvent?

Your answer

Can you use a flash loan to exploit the oracle manipulation via the CEX trades?

Your answer

Back Submit Clear form