Audit Findings 201

Secureum Bootcamp

#102

ConsenSys Audit
Umbra Finding 5.2

Access Control & Input Validation

External Contract Call w/ Untrusted Parameters

Document/Validate Potential Edge Cases

#103

ConsenSys Audit
Umbra Finding 5.3

Specification/
Documentation

Deflationary/
Inflationary/Rebasing

Document Token Behavior
Restrictions

#104

ConsenSys Audit
DeFi Saver Finding 5.5

Testing

Incomplete/Failing Tests

Add Full Coverage
Test Suite

#105

ConsenSys Audit
DeFi Saver Finding 5.6

Naming/Documentation/
Refactoring

Misleading Function
Names & Assumptions

Refactor Code
Document Assumptions

#106

ConsenSys Audit
DeFi Saver Finding 5.10

Error Checking

Unchecked Return Value
Transferred Tokens

Check Return Value

#107

ConsenSys Audit
Umbra Finding 5.11

Access Control & Logging

Missing Access Control for Logging Function

Add Access Control

#108

ConsenSys Audit
DAOfi Finding 3.1

Documentation

Stale Comments about Storage Slots

Remove Stale Comments

#109

ConsenSys Audit
MStable-1.1 Finding 6.14

Documentation

Mismatch b/w Code & Comment

Make Comment & Code Consistent

#110

ConsenSys Audit
DAOfi Finding 3.2

Unnecessary Code/Logic

Getter Function for
Immutable Address

Replace Function Call w/
Variable Read

#111

ConsenSys Audit
DAOfi Finding 3.4

Testing

Insufficient Validation for Complex Math

Add Fuzzing & Unit/ Property Tests

#112

ConsenSys Audit
Fei Protocol Finding 3.10

Application Logic

Proposal Cancellation
& States Allowed

Restrict Cancellation to
Certain States

#113

ConsenSys Audit
eRLC Finding 4.3

Access Control & Timing

Immediate Privilege
Escalation

Add TimeLock to
Granting Privileges

#114

ConsenSys Audit
1inch Finding 4.1

Documentation & Testing

Minimal Comments
Limited Test Coverage

Add Comments
Increase Test Coverage

#115

ConsenSys Audit
1inch Finding 4.6

Configuration

Floating/Unlocked
Solidity Compiler Pragma

Fixed Pragma
Recommended Version

#116

ConsenSys Audit
1inch Finding 4.7

Denial-of-Service

Hardcoded Gas
Assumptions

Document & Validate

#117

ConsenSys Audit
1inch Finding 5.1

Access Control & Input/
Data Validation

User-controlled Contract
& Tokens

Specify & Document &
Validate

#118

ConsenSys Audit 1inch Finding 5.7

Privileged Roles & Timing

Critical Changes & Front-running

Two-step Change w/ Time Window for Users

#119

ConsenSys Audit
Growth DeFi Finding 4.2

Specification/
Documentation

Single README w/ Code
Comments

Improve Specification &
Documentation

#120

ConsenSys Audit
Growth DeFi Finding 4.3

Access Control
Least Privilege Mechanism

Loosely Defined Roles/
Permissions

Document & Monitor
Roles & Permissions

#121

ConsenSys Audit Growth DeFi Finding 5.2

Specification/Access Control

Callbacks/Deflationary/Inflationary/Rebasing

Evaluate Token Behavior before Inclusion

#122

ConsenSys Audit
Growth DeFi Finding 5.6

Naming Convention &
Readability

Multiple Contracts
Code Reuse & Naming

Use Descriptive Names

#123

ConsenSys Audit
Growth DeFi Finding 5.8

Initialization & Timing

User Interaction before
Contract Initialization

Initialize before
Interaction

#124

ConsenSys Audit
Growth DeFi Finding 6.2

Denial-of-Service

Unbounded Loop
Gas Exhaustion

Reconsider Logic or
Bound Loop

#125

ConsenSys Audit
Paxos Finding 3.1

Access Control
Stale Privileges

Old Owners Never Removed

Remove Old Owners
Add New Owners

#126

ConsenSys Audit
Aave V2 Finding 5.6

Flash Loans

Flash Loans -> Interest Rate Fluctuations

Monitor -> Rebalanced Interest Rate

#127

ConsenSys Audit
Aave Gov Finding 2.3

Validation

Malicious Tokens

Audit Whitelisted Tokens

#128

ConsenSys Audit
Aave CPM Finding 6.2

Specification
Input Validation

Token Decimals > 18
-> Underflow

Validate or Document
Design Assumption

#129

ConsenSys Audit
Aave CPM Finding 5.1

Testing

Price Volatility
Chainlink Performance

Validate Performance
Assess Risk

#130

ConsenSys Audit
Lien Protocol Finding 2.1

Configuration

Multiple Complex Parts
High Attack Surface

Min. Viable System
Iterative/Guarded Launch

#131

ConsenSys Audit
Balancer Finding 3.6

Code Refactoring

Repeated Checks
Error-prone

Repeated Checks ->
Modifiers

#132

ConsenSys Audit
Balancer Finding 5.4

Ordering

Modifier Ordering
Reentrancy Guard

Modifier Order: L -> R

#133

ConsenSys Audit
MCDEX V2 Finding 2.3

Fragile Code

System Side-effects
Interdependence

Function Purpose
Reduce Dependence

#134

ToB Audit
Liquidity Finding 6

Undefined Behavior
Logging

Reentrancy -> Event
Ordering

Apply CEI Pattern

#135

ToB Audit
Origin Dollar Finding 16

Undefined Behavior

Inheritance
Variable Shadowing

Remove Shadowed
Variables

#136

ToB Audit
Origin Dollar Finding 17

Error Handling

Missing Return
Caller Check

Add Return Statements

#137

ToB Audit
Origin Dollar Finding 18

Undefined Behavior

Interface Impl -> Missing Inheritance

Inherit from Interfaces

#138

ToB Audit
Yield Finding 7

Optimizations

Solidity Compiler
Optimization Risks

Evaluate Trade-off
Gas Benefits vs Risk

#139

ToB Audit
Yield Finding 2

Access Control

Coarse Permissions

Rearchitect Permissions
Least Privilege

#140

ToB Audit
Yield Finding 4

Data Validation

Timestamp Value
Past/Future Maturity

Sanity/Threshold Check
Constructor Parameters

#141

ToB Audit
Yield Finding 5

Auditing & Logging

Delegate Add/Remove ->
Emit Event

Check Delegate
Enabled/Disabled

#142

ToB Audit
0x Protocol Finding 8

Auditing & Logging

Critical Operations
No Events

Add Events
Off-chain Monitoring

#143

ToB Audit
0x Protocol Finding 20

Error Handling

No Function Return
Only False/Revert

Add/Remove Return
Document Otherwise

#144

ToB Audit
DFX Finance Finding 2

Specification

max & min: Open Range
Unorthodox Definitions

Use Conventional Norms
Document Otherwise

#145

ToB Audit
DFX Finance Finding 3

Undefined Behavior

Curve: New/Existing
No Indication

Existing Curve -> Revert
Check New/Existing

#146

ToB Audit
DFX Finance Finding 4

Data Validation

Missing Checks
Zero-address

Add Checks
Best-practice

#147

ToB Audit
DFX Finance Finding 8

Error Handling

Own safeApprove()
No Return Check

Use OZ Libraries
Add Checks

#148

ToB Audit
DFX Finance Finding 9

Configuration

ERC20 Token
No Name/Symbol/Decimals

Confirm to Specification

#149

ToB Audit
DFX Finance Finding 11

Data Validation

Missing SafeMath
Inconsistent Use

Consistently Use SafeMath

#150

ToB Audit
DFX Finance Finding 16

Timing & DoS

Temp. Contract Freeze
Malicious Owner

Low Freeze Time or
Permanent Freeze

#151

ToB Audit
Hermez Network Finding 4

DoS

Account Creation
No Fee -> Max Accounts

Add Fee
Monitor Account Creation

#152

ToB Audit
Hermez Network Finding 11

Undefined Behavior

Empty Functions ->
Interfaces -> Error-prone

Use Interfaces

#153

ToB Audit
Hermez Network Finding 19

Data Validation

Cancel Non-existing Transaction -> Event

Validate Transaction Existence

#154

ToB Audit
Hermez Network Finding 20

Patching

Dependencies Copied
Tracking Bug Fixes

Document/Import
Dependencies -> Tracking

#155

ToB Audit
Hermez Network Finding 21

Access Control

Adding New Tokens
Anyone or Governance

Sync Specification ->
Implementation

#156

ToB Audit
Hermez Network Finding 22

Undefined Behavior

Contract Names
Duplicates

Avoid Duplicate Names

#157

ToB Audit
Advanced Blockchain Finding 27

Patching

Hardcoded Contract Addresses

Contract Deployer Set Addresses

#158

ToB Audit
Advanced Blockchain Finding 22

Configuration

Borrow Rate
Blocks/Year

Analyze Deviation
Document Risks

#159

ToB Audit
Advanced Blockchain Finding 25

Data Validation

Flash Loan Rate
No Bounds

Set Low/High Bounds

#160

ToB Audit
Advanced Blockchain Finding 4

Patching

Duplicated Code
Error-prone

Code Reuse
Inheritance

#161

ToB Audit
Advanced Blockchain Finding 5

Testing

Insufficient Testing

Unit Tests
Good Coverage

#162

ToB Audit
Advanced Blockchain Finding 11

Patching

Vulnerabilities in (Off-chain) Dependencies

Track/Verify/Patch/Audit Dependencies

#163

ToB Audit
Advanced Blockchain Finding 16

Documentation

Low Documentation ->
Low Auditability

Documentation
Specification

#164

ToB Audit
Advanced Blockchain Finding 18

Patching

ABIEncoderV2
Issues & Bugs

Avoid ABIEncoderV2
Refactor Code

#165

ToB Audit
dForce Lending Finding 10

Access Controls

Contract Owner
Over-privileged

Least Privilege
Document Risks

#166

ToB Audit
dForce Lending Finding 14

Error Handling

Test Suite
Poor Error-handling

Check Errors
Follow Best-practices

#167

Sigma Prime Audit
Synthetix Finding SEC-04

Patching

Redundant & Unused Code

Use or Remove

#168

Sigma Prime Audit
Synthetix Finding SEC-05

Data Validation

Single Account
Entire ETH -> Loan

Enforce Cap
Document Behavior

#169

Sigma Prime Audit
Synthetix Finding SEC-06

Input Validation

Constructor Parameters
Zero Addresses

Check Addresses

#170

Sigma Prime Audit
Synthetix Finding SEC-08

Auditing & Logging

Events Declared
No Emits

Emit Events or
Remove Events

#171

Sigma Prime Audit
InfiniGold Finding INF-03

Data Validation

transferFrom()
Burn Address

Add require()
to != Burn Address

#172

Sigma Prime Audit
InfiniGold Finding INF-06

DoS

reset() -> Unbound List
Block Gas Limit

Restrict List Length
Check Gas

#173

Sigma Prime Audit
InfiniGold Finding INF-08

Timing

ERC20 approve()
Front-running

increaseAllowance()
decreaseAllowance()

#174

Sigma Prime Audit
InfiniGold Finding INF-09

Error Checking

Unnecessary require()
Zero-address Check

ERC20 _transfer()
Remove Check -> Gas

#175

Sigma Prime Audit
InfiniGold Finding UNI-05

Data Validation

Rounding to Zero
Division

Document
Claim -> Rounding Dust

#176

Sigma Prime Audit
InfiniGold Finding UNI-06

Auditing & Logging

No Check
Event Emitted -> Spam

Check Amount
Amount > 0? -> Emit Event

#177

OpenZeppelin Audit
HoldeFi Finding M04

Specification

Account Liquidation
Insufficient Incentives

Change Design
Align Incentives

#178

OpenZeppelin Audit
HoldeFi Finding M06

Specification

Insolvent Market
Collateral -> Borrow

Minimize Risk
Document/Communicate

#179

OpenZeppelin Audit
HoldeFi Finding M09

Patching

Copy/Reimplement
Maintain & Bug Fixes

Import OZ Libraries
Reuse & Extend

#180

OpenZeppelin Audit
HoldeFi Finding L09

Auditing & Logging

Event Parameters
Not Indexed

Indexed Parameters
Topic vs Data

#181

OpenZeppelin Audit
HoldeFi Finding N06

Readability

Named Returns
Inconsistent Use

Remove Named Returns
Explicit Returns

#182

OpenZeppelin Audit
HoldeFi Finding N07

Timing

block.timestamp
Unreliable -> Miners

Test & Document
Warn Users

#183

OpenZeppelin Audit
BarnBridge Finding N01

Error Checking

Assignment in require()

require() -> Checks
No Side-effects

#184

OpenZeppelin Audit
BarnBridge Finding N02

Patching

Commented Code
Readability & Auditability

Uncomment or Remove

#185

OpenZeppelin Audit
Compound Finding N02

Error Handling

Revert Messages
Uninformative & Misleading

Use Informative &
Meaningful Messages

#186

OpenZeppelin Audit
Fei Protocol Finding L04

Configuration

Solidity Versions
Outdated & Multiple

Recent & Single & Fixed

#187

OpenZeppelin Audit
Fei Protocol Finding N22

Testing

Code Constants
Test & Production

Test & Production
Different Environments

#188

OpenZeppelin Audit
Fei Protocol Finding N23

Specification

Integer Constants
Size < 256 Bits

Gas Costs
Execution vs Storage

#189

OpenZeppelin Audit
Fei Protocol Finding N28

Specification

Integers
uint vs uint256

Favor Explicitness
Use uint256

#190

OpenZeppelin Audit
UMA Protocol Finding M02

Specification

Function Names
Unexpected Side-effects

Sync Names -> Actions
Specific Setters/Getters

#191

OpenZeppelin Audit
GEB Protocol Finding M06

Data Validation

Unsafe Casting
uint -> int

Verify Range
Use SafeCast

#192

OpenZeppelin Audit
GEB Protocol Finding L06

Error Checking

Missing Error Messages
require()

Specific & Informative
Error Messages

#193

OpenZeppelin Audit
GEB Protocol Finding L11

Testing

Assembly Code

Avoid/Test/Document

#194

OpenZeppelin Audit
GEB Protocol Finding N03

Error Checking

Catch Clause
Not Handled

Emit Event
Handle Error

#195

OpenZeppelin Audit
GEB Protocol Finding N11

Auditing & Logging

Unnecessary Event Emits
No Significance

Remove Emits
Save Gas

#196

OpenZeppelin Audit
Opyn Gamma Finding M01

Data Validation

Non-whitelisted Assets

Whitelist
Validate Whitelisting

#197

OpenZeppelin Audit
Opyn Gamma Finding L07

Specification

Function Mismatches
Interfaces & Contracts

Sync Mismatches
Interfaces & Contracts

#198

OpenZeppelin Audit
Opyn Gamma Finding L08

Timing

Non-Atomic Functions
Inconsistent State

Combine Functions
Same Tx -> Atomic Effects

#199

OpenZeppelin Audit
Opyn Gamma Finding L11

Patching

Deprecated APIs
Chainlink V2 vs V3

Deprecated -> Stop Work
Use Latest APIs

#200

OpenZeppelin Audit
PoolTogether V3 Finding C01

Data Validation

sweepTimelockBalances()
Duplicate Users -> Funds Lost

Check Duplicate Users

#201

OpenZeppelin Audit
Set Protocol Finding N09

Patching

Clear Variables
Zero Address vs delete

Use delete
Intention & Idiomatic