Audit Findings 101

Secureum Bootcamp

#1

ConsenSys Audit
Aave V2 Finding 5.4

Error Handling
Medium Severity

transfer/transferFrom
Return Values

Use SafeERC20 Wrappers

#2

ConsenSys Audit
DeFi Saver Finding 5.1

Reentrancy
Critical Severity

Malicious External Calls

Add Reentrancy Guard

#3

ConsenSys Audit
DeFi Saver Finding 5.2

Input Validation
Major Severity

Tokens w/ >18 Decimals

Use SafeMath

#4

ConsenSys Audit
DeFi Saver Finding 5.3

Error Handling
Major Severity

Function Return Values
Unchecked Error Codes

Check Error Code
Revert if Necessary

#5

ConsenSys Audit
DeFi Saver Finding 5.4

Ordering
Medium Severity

Incorrect Parameter Ordering

Fix Ordering

#6

ConsenSys Audit
DAOfi Finding 4.1

Input Validation
Critical Severity

No Address Validation
Token Transfer

From Address ->
msg.sender

#7

ConsenSys Audit
DAOfi Finding 4.4

Error Handling
Major Severity

Incorrect Check
Swap Tokens

Use Correct Check

#8

ConsenSys Audit
DAOfi Finding 4.5

Denial-of-Service
Medium Severity

Zero Liquidity Deposit
Single Deposit

Check Non-Zero Deposit
Amount

#9

ConsenSys Audit
Fei Finding 3.1

Application Logic
Critical Severity

Overwrite Value instead-of
Adding Value

Add to Existing Value

#10

ConsenSys Audit
Fei Finding 3.2

Timing
Critical Severity

Purchase & Commit
After Launch

State-tracking
Function Validation

#11

ConsenSys Audit
Fei Protocol Finding 3.3

Data Validation
Major Severity

Overflow-Prone Casting

Use SafeCast

#12

ConsenSys Audit
Fei Protocol Finding 3.4

Timing
Medium Severity

Allocate before Genesis Launch

Prevent Allocate before Launch

#13

ConsenSys Audit
Fei Protocol Finding 3.5

Error Handling
Medium Severity

Timer Returns
True instead-of False

Return False before
Initialization

#14

ConsenSys Audit
Fei Protocol Finding 3.6

Data Validation
Medium Severity

Math Operations
Overflow/Underflow

Use SafeMath or
Compiler >=0.8

#15

ConsenSys Audit
Fei Protocol Finding 3.7

Error Handling
Medium Severity

Unchecked Return Value
ERC20 transfer

Add require or
Use SafeERC20 Wrapper

#16

ConsenSys Audit
Fei Protocol Finding 3.8

Timing
Medium Severity

EmergencyExit vs Launch

Ensure Mutually Exclusive

#17

ConsenSys Audit
bitbank Finding 5.1

Error Handling
Major Severity

Incorrect Return Value
Check on ERC20 transfer

Use SafeERC20 Wrapper

#18

ConsenSys Audit
MetaSwap Finding 4.1

Reentrancy
Major Severity

Swap Reentrancy

Use Reentrancy Guard

#19

ConsenSys Audit
MetaSwap Finding 4.2

Access Control
Medium Severity

Malicious Adaptor
User Tokens

Redesign Token Approvals

#20

ConsenSys Audit
MetaSwap Finding 4.3

Timing
Medium Severity

Front-Running
Modify Implementation

Disallow Modifications

#21

ConsenSys Audit
mstable-1.1 Finding 6.2

Timing
Major Severity

Abuse of Sliding Window

Remove Window
Anticipate/Prevent Abuse

#22

ConsenSys Audit
Bancor V2 Finding 5.1

Timing
Critical Severity

Oracle Front-running
Sandwich Attack

Enforce per Block/Tx
Constraints

#23

ConsenSys Audit
Shell Protocol Finding 6.2

Input Validation
Major Severity

Parameter Checks
Valid/Threshold/0/+ve

Add Checks
Testing

#24

ConsenSys Audit
Shell Protocol Finding 6.3

Access Control
Major Severity

Admin Abuse/Backdoor
Least Privilege

Make Code Static
Increase Trust

#25

ConsenSys Audit
Lien Protocol Finding 3.1

Denial-of-Service
Critical Severity

Reverting ETH Transfer
Batch Failure

Ignore Failed Transfers
Pull over Push

#26

ConsenSys Audit
The Lao Finding 5.1

Denial-of-Service
Critical Severity

Partial Withdrawal
Lose Remaining Tokens

Pull over Push

#27

ConsenSys Audit
The Lao Finding 5.2

Denial-of-Service
Critical Severity

Proposal Rejected
Lose Tribute Tokens

Pull over Push

#28

ConsenSys Audit
The Lao Finding 5.3

Denial-of-Service
Critical Severity

Emergency Processing
Proposal/LAO Blocked

Pull over Push

#29

ConsenSys Audit
The Lao Finding 5.4

Denial-of-Service
Major Severity

Token Overflows
System Halt

Allow Overflows
Broken/Malicious Tokens

#30

ConsenSys Audit
The Lao Finding 5.5

Denial-of-Service
Major Severity

Whitelist Token List
Gas Limit

Limit/Prune List

#31

ConsenSys Audit
The Lao Finding 5.6

Denial-of-Service
Major Severity

bailout() -> Summoner
Kicked User Funds

Pull over Push

#32

ConsenSys Audit
The Lao Finding 5.7

Timing & DoS
Major Severity

Front-running
Proposal Block

Pull over Push

#33

ConsenSys Audit
The Lao Finding 5.8

Timing & DoS
Major Severity

Front-running
Delegate Address

Approve/Cancel
Commit-Reveal

#34

ToB Audit
Origin Dollar Finding 6

Denial-of-Service
High Severity

Governor -> Timelock
cancelTransaction()

Add Governor Function
Inheritance

#35

ToB Audit
Origin Dollar Finding 8

Access Control
High Severity

Timelock
executeTransaction()

Only Admin
executeTransaction()

#36

ToB Audit
Origin Dollar Finding 9

Access Control
High Severity

Timelock.admin Change
Proposal Transaction

Prevent setPendingAdmin

#37

ToB Audit
Origin Dollar Finding 10

Reentrancy
High Severity

mintMultiple
Untrusted Contracts

Reentrancy Guard
No Untrusted Contracts

#38

ToB Audit
Origin Dollar Finding 19

Error Handling
High Severity

Unchecked Return Values

Check Return Values

#39

ToB Audit
Origin Dollar Finding 20

Denial-of-Service
High Severity

External Calls
Unbounded Loops

Bound Loops

#40

ToB Audit
Origin Dollar Finding 22

Data Validation
High Severity

User Tokens > Balance
Rounding Issue

Check Balance
Arithmetic Invariants

#41

ToB Audit
Origin Dollar Finding 23

Data Validation
High Severity

Total Supply < Balances
Optional Rebasing

Specify Invariants
Prevent Violations

#42

ToB Audit
Yield Protocol Finding 1

Undefined Behavior
Medium Severity

Flash Mint Any Number
Mature Tokens

Disallow Flash Minting

#43

ToB Audit
Yield Protocol Finding 8

Access Control
High Severity

ERC20Permit Signatures
Replay on Forks

Include ChainID Opcode

#44

ToB Audit
Hermez Finding 1

Data Validation
High Severity

No Contract Existence
Check -> Token Theft

Check Contract Existence

#45

ToB Audit
Hermez Finding 2

Timing
Medium Severity

No Incentive -> Vote Early

Weighted Bids

#46

ToB Audit
Hermez Finding 5

Access Control
High Severity

Same Account
Frequent/Rare Updates

Least Common Mechanism

#47

ToB Audit
Hermez Finding 6

Data Validation
High Severity

One-step Change
Critical Operations

Two-step Procedure
Less Error-prone

#48

ToB Audit
Hermez Finding 12

Configuration
High Severity

Front-running
Initialization Functions

Factory-pattern
Atomic Deploy/Init Script

#49

ToB Audit
Uniswap V3 Finding 1

Data Validation
Medium Severity

Incorrect owner
Redeploy Contract

Owner = msg.sender
Two-step Change

#50

ToB Audit
Uniswap V3 Finding 5

Data Validation
High Severity

Incorrect Operator
Token Drain

Change '>=' to '<='
require() Statement

#51

ToB Audit
Uniswap V3 Finding 6

Denial-of-Service
Medium Severity

Unbounded Loop
Attacker/Malicious Miner

Bound Loops
Document Bounds

#52

ToB Audit
Uniswap V3 Finding 7

Timing/Access Control
Medium Severity

Front-run Initialization
Drain LP deposit

Use Constructor
Protect Initialization

#53

ToB Audit
Uniswap V3 Finding 8

Application-logic
Medium Severity

Zero Liquidity
Control Pool Price

Design/Warn Appropriately

#54

ToB Audit
Uniswap V3 Finding 9

Data Validation
High Severity

Contract Existence
Token Loss

Check Existence
Avoid Low-level Calls

#55

ToB Audit
DFX Finding 10

Undefined Behavior
High Severity

Variable Assign & Use
LHS & RHS of Check

Rewrite Expression
Avoid Undefined Usage

#56

ToB Audit
DFX Finding 12

Data Validation
High Severity

Raw vs Numeraire
Missed Conversion

Consistent Values
Unit Tests & Fuzzing

#57

ToB Audit
DFX Finding 13

Data Validation
Medium Severity

Incorrect Assumption
1 USDC == 1 USD

Avoid Hardcoding
Use Price Oracle

#58

ToB Audit
DFX Finding 1

Patching
Undetermined Severity

Deprecated Chainlink API

Use Latest Versions of Dependencies

#59

ToB Audit
0x Protocol Finding 3

Data Validation
High Severity

Cancel Future Orders
Large Value Parameter

Document or Disallow

#60

ToB Audit
0x Protocol Finding 13

Specification
High Severity

Spec: 2-week Timelock
Code: No Timelock

Sync Spec-Code

#61

ToB Audit
0x Protocol Finding 17

Specification
High Severity

Unclear Specification
Orders Fillable or Not

Specify & Warn Users

#62

ToB Audit
0x Protocol Finding 2

Timing
Medium Severity

Market Makers
Subsidized Front-running

Document/Cap Fee
No tx.gasprice -> Fee

#63

ToB Audit
0x Protocol Finding 4

Timing
Medium Severity

Compromised Validator
Sig Validation Race

Document
Monitor for Front-running

#64

ToB Audit
0x Protocol Finding 6

DoS
Medium Severity

Batch tx Processing
One Revert -> Batch Revert

NoThrow Variant
Evaluate Batch Risk

#65

ToB Audit
0x Protocol Finding 7

Data Validation
Medium Severity

Zero Gas -> Zero Fee

Minimum Fee
No tx.gasprice -> Fee

#66

ToB Audit
0x Protocol Finding 21

Data Validation
Medium Severity

No setParams Validation
Undefined Behavior

Add Validation
Document Behavior

#67

Sigma Prime Audit
EtherCollateral Finding 1

Data Validation
High Severity

Supply Cap
openLoan -> Exceeds Cap

Add require()
Enforce Supply Cap

#68

Sigma Prime Audit
EtherCollateral Finding 2

Data Validation & DoS
High Severity

Open Loan
No Account Checks

Check Account/Loan
Limit Loans/Account

#69

Sigma Prime Audit
EtherCollateral Finding 3

Configuration
Medium Severity

Contract Owner
Change Fees & Interest

Prevent Changes

#70

Sigma Prime Audit
Infinigold Finding 1

Configuration
Critical Severity

Broken Proxy Impl
Constructor vs Initialize

Correct Proxy Impl
Initialize(), State Vars

#71

Sigma Prime Audit
Infinigold Finding 2

Access Control
High Severity

Missed Blacklisting
transferFrom() from Addr

Apply notBlacklisted()
from Addr

#72

Sigma Prime Audit
Unipool Finding 1

Ordering
Critical Severity

Wrong Ordering
Operands in Expression

Correct Operand Ordering

#73

Sigma Prime Audit
Unipool Finding 2

Timing/Ordering
High Severity

Stake before Notify
-> More Rewards

Prevent stake() before
notifyRewardAmount()

#74

Sigma Prime Audit
Unipool Finding 3

Error Handling
High Severity

External Call Reverts
-> Mint Blocked

Handle Condition
Without Reverting

#75

Sigma Prime Audit
Unipool Finding 3

Timing/DoS
Medium Severity

Stakers -> getReward()
SNX Deficit -> No Rewards

No Gap Between Periods

#76

Sigma Prime Audit
Chainlink Finding 2

Timing/DoS
High Severity

Arbitrary Callback
Legitimate Requests Fail

Restrict Arbitrary
Callbacks

#77

OpenZeppelin Audit
UMA Finding M01

Auditing & Logging
Medium Severity

Sensitive Actions
No Events

Events -> Offchain
Tracking

#78

OpenZeppelin Audit
UMA Finding M02

Specification
Medium Severity

Function Names
Function Side-effects

Sync Names & Actions

#79

OpenZeppelin Audit
1inch Finding

DoS
Medium Severity

No Unpause
Factory Redeployment

Add Unpause Ability

#80

OpenZeppelin Audit
Futureswap V2 Finding H01

Timing/DoS
High Severity

Front-running
Prevent Instant Withdraw

Access Control
Submit oracleMessages

#81

OpenZeppelin Audit
Futureswap V2 Finding M01

Configuration
Medium Severity

Upgradeable Contract
Unsafe Inheritance

Inherit -> Upgrade Safe
Contracts

#82

OpenZeppelin Audit
Futureswap V2 Finding M03

Error Handling
Medium Severity

ECDSA.recover
Unchecked address(0)

ECDSA.recover address(0)
-> Revert

#83

OpenZeppelin Audit
Notional Finding M02

Configuration
Medium Severity

New Variables
Inherited/Upgradeable

Add Gap
Reserve Storage

#84

OpenZeppelin Audit
GEB Finding M07

Data Validation
Medium Severity

Divide-by-Zero

Add require()
Use SafeMath

#85

OpenZeppelin Audit
1inch Finding M07

Timing
Medium Severity

Incorrect safeApprove()
No Non-zero -> Non-zero

safeIncreaseAllowance
safeDecreaseAllowance

#86

OpenZeppelin Audit
Opyn Gamma Finding H01

DoS
High Severity

Extra ETH
Locked in Contract

Return ETH
Withdraw()

#87

OpenZeppelin Audit
Opyn Gamma Finding M04

DoS
Medium Severity

Solidity transfer()
Payable fallback() & 2300

OpenZeppelin sendValue()
CEI Pattern

#88

OpenZeppelin Audit
Endaoment Finding H02

Timing
High Severity

Token Transfer -> State
Update => Fund Drained

Follow CEI
Use Reentrancy Guard

#89

OpenZeppelin Audit
Audius Finding H03

Auditing/Logging
High Severity

Critical Address Updates
No Events

Add Events
Offchain Monitoring

#90

OpenZeppelin Audit
Audius Finding H07

Identification
High Severity

Sybil Accounts
Quorum Bypass

Unique Accounts ->
Token Percentage

#91

OpenZeppelin Audit
Audius Finding M02

Timing
Medium Severity

Initialization Checks
Inconsistent

Consistent Checks
Deployment Script

#92

OpenZeppelin Audit
Audius Finding M06

Data Validation
Medium Severity

Voting Period/Quorum
Setter Checks

Non-Zero
Add Setter Checks

#93

OpenZeppelin Audit
Audius Finding M10

Configuration
Medium Severity

Initialization
State Variables

Initialize+Checks
Document

#94

OpenZeppelin Audit
Primitive Finding M08

Timing
Medium Severity

Expired/Paused Options
Trading

Prevent
Document

#95

OpenZeppelin Audit
ACO Finding M01

Data Validation
Medium Severity

External ERC20s
Fees & Failures

Vet & Check

#96

OpenZeppelin Audit
Compound Finding M04

Auditing & Logging
Medium Severity

Event Emit
Stale Data

State Update -> Emit Event

#97

OpenZeppelin Audit
MCDEX Mai Finding C01

Access Control
Critical Severity

liquidateFrom
Public Visibility

Change Visibility
Public -> Internal

#98

OpenZeppelin Audit
MCDEX Mai Finding C02

DoS
Critical Severity

cancelOrder
No effects

Cancel Orders
Add Checks

#99

OpenZeppelin Audit
MCDEX Mai Finding M03

Timing
Medium Severity

Reentrancy Possibilities
Interactions -> Effects

CEI Pattern
Reentrancy Guard

#100

OpenZeppelin Audit
MCDEX Mai Finding M06

Timing
Medium Severity

Governance Changes
Enforced Instantly

Timelock
User Notice

#101

OpenZeppelin Audit
UMA Finding H01

Data Validation
High Severity

Commit-Reveal
Duplicate Votes

Tie Vote -> Voter
Timestamp