SOLIDIFIED

Responses on Lighting Security Pen Test. June 2018.

## Summary

Solidified Ltd. engaged Lightning Security for an external penetration test of `web.solidified.io` (Solidified bug bounty platform) and `solidified.io` (Solidified landing page) which was delivered June 12th, 2018. The following are our responses to each issue they reported.

## Issues Found

### Critical

### 1. Race condition in pulling contract allows stealing ETH from escrow

Added missing check for pulled status of the contract.

### 2. Negative bounty amount allows for infinite account balance

Added validation of bounty amounts requiring them to be positive.

### High

### 3. Two-factor authentication bypass

We're working on a fix for this. Until the fix is implemented users should not rely on TFA, and as always use a strong password.

### 4. Enumeration of private profile fields via API

Added validation of field to enumerate, only allowing safe ones.

SOLIDIFIED

Responses on Lighting Security Pen Test. June 2018.

# Medium

## 5. Hashed password of current user exposed in API response

Filtered out sensitive data in account response.

## 6. 401 Response Injection via markdown images

Prohibited using images in Markdown texts.

# Low

## 7. Notifications of all users exposed in API response

Filtered notifications to only display public ones.

## 8. Contract can be created with lower bounty than permitted

Added validation of bounty pool value on backend.

## 9. Arbitrary file extension allowed in contract

Added validation of saved files to only allow `.sol` on backend.

## 10. Profile images stored in database as strings

Profile photos are stored on S3, they are just made part of the profile for frontend convenience.

SOLIDIFIED

Responses on Lighting Security Pen Test. June 2018.

## Closing Summary

All issues reported by Lightning Security have been addressed, except issue #3 (2FA bypass). A patch for this issue is actively being worked on, and is planned for production by the end of June 2018. Until that time, users should NOT rely on the two-factor authentication feature.