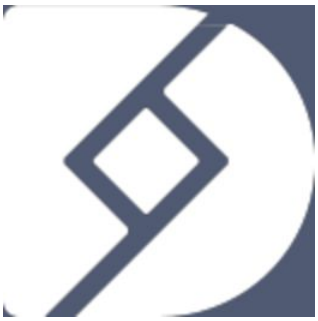
HackerOne Challenge Summary Report



Classification
Confidential

Release date
June 22nd, 2018

Author
Alex Chapman (Technical Program Manager, HackerOne)

Reviewers
Bill Lummis (Technical Program Manager, HackerOne)

HackerOne Challenge **1**

Summary Report **1**

1 - Executive Summary 2

Findings per asset 2

Key Recommendation 1 3

Key Recommendation 2 3

2 - Introduction 4

2.1 - Scope 4

2.2 - Methodology 4

2.3 - Classification 5

2.4 - Framework 5

2.5 - Test Plan 5

2.6 - Team 5

2.6.1 - HackerOne Staff 5

2.6.2 - HackerOne Researchers 5

3 - Findings 5

3.1 - Asset: dex.top 6

3.1.1 - Asset Summary 6

3.1.2 - Vulnerability Summary 6

Appendix - HackerOne Researchers 7

1 - Executive Summary

Dex.top engaged HackerOne to perform a HackerOne Challenge, also known as a crowd-sourced penetration test, from June 1st, 2018 to June 16th, 2018. During this timeframe, five vulnerabilities were identified by three unique researchers.

During the assessment, one vulnerability was found that had a CVSS score of 7.0 or higher, rating either high or critical. This vulnerability represented the greatest immediate risk to Dex.top and was remediated within two days of being reported. Table 1 shows the in scope assets, and breakdown of findings by severity per asset. Section 2.4 contains more information on how severity is calculated.

Findings per asset

	Critical	High	Medium	Low	None	Σ
dex.top	0	**1**	**1**	**3**	0	**5**
https://etherscan.io/address/0x7600977Eb9eFFA627D6BD0DA2E5be35E11566341#code	0	0	0	0	0	0
	0	1	1	3	0	5

Table 1: findings per asset

The security assessment was conducted using a crowd-sourced penetration testing methodology. From its community of over 100,000 hackers, HackerOne curated a set of top-tier researchers to focus on identifying vulnerabilities in Dex.top's scope during the agreed upon testing window, while abiding by the policies set forth by Dex.top. Section 2.2 contains more information about the methodology.

A significant Denial of Service issue was identified which could deny access to the Dex.top application to all legitimate users. This issue was fixed within two days after reporting by the Dex.top team. One medium impact issue was identified, a DOM based Cross Site Scripting issue in a 3rd party library used by the Dex.top application, and three low impact security best practice issues were identified.

During the time limited challenge no security issues were identified in the smart contract code.

Based on the results of this assessment, HackerOne has the following high level key recommendation:

Key Recommendation

Key Issue	A high impact Denial of Service issue was identified in the Dex.top web application which would have allowed an attacker to deny access to the Dex.top application to all legitimate users.
Recommendation	Consider performing further review of compute intensive functions in the web application code for Denial of Service issues. Review computationally intensive functions to make sure that they have upper bounds set and are properly rate limited to avoid consuming excessive system resources.

2 - Introduction

Dex.top engaged HackerOne to perform a HackerOne Challenge, also known as a crowd-sourced penetration test, from June 1st, 2018 to June 16th, 2018. During this timeframe, five vulnerabilities were identified by three unique researchers.

2.1 - Scope

The in-scope assets are outlined in Table 2.

Asset
dex.top
https://etherscan.io/address/0x7600977Eb9eFFA627D6BD0DA2E5be35E11566341#code

Table 2: in-scope assets

2.2 - Methodology

HackerOne worked with Dex.top to identify a scope and testing window for this assessment, as well to determine what types of vulnerabilities are most important to Dex.top. This information was placed into a "Security Page," also known as the rules of engagement, for the Challenge. From its community of over 100,000 hackers, HackerOne curated a set of top-tier researchers to focus on identifying vulnerabilities in Dex.top's scope during the agreed upon testing window, while abiding by the policies set forth in the Security Page.

We encourage the use of individual tools and methods by each researcher. This ensures diversity in the testing. It also ensures that new tools and techniques can be used in the testing. While individuality in testing methodology is encouraged, researchers ascribe to OWASP's (Open Web Application Security Project) standard testing techniques to uncover issues (e.g. OWASP Top 10) within your web applications. Additionally, HackerOne's security analysts triage and categorize all identified vulnerabilities against the CWE (Common Weakness Enumeration) standard, as well as assign a severity ranking based on the CVSS v3.0 (Common Vulnerability Scoring System) standard, providing consistent, easy to understand guidelines on the criticality of each vulnerability.

2.3 - Classification

HackerOne uses a vulnerability taxonomy based on the industry-standard Common Weakness Enumeration (CWE). CWE is a community-developed list of common software security weaknesses. It serves as a common language, a measuring stick for software

security tools, and as a baseline for weakness identification, mitigation, and prevention efforts. More information can be found on MITRE's website: https://cwe.mitre.org/.

2.4 - Framework

HackerOne uses the industry-standard CVSS to calculate severity for each identified security vulnerability. CVSS provides a way to capture the principal characteristics of a vulnerability, and produce a numerical score reflecting its severity, as well as a textual representation of that score. The numerical score can then be translated into a qualitative representation (such as low, medium, high, and critical) to help organizations properly assess and prioritize their vulnerability management processes. More information can be found on the Forum for Incident Response and Security Teams' (FIRST) website: https://www.first.org/cvss.

2.5 - Test Plan

HackerOne researchers were able to self register for the Dex.top web application, and were provided with the source code of the Dex.top smart contract for review.

2.6 - Team

2.6.1 - HackerOne Staff

The following individuals at HackerOne managed this Challenge and generated this report:

- Alex Chapman, Technical Program Manager
  - achapman@hackerone.com
- Bill Lummis, Technical Program Manager
  - bill@hackerone.com

Please feel free to contact these individuals with any questions or concerns you have around the engagement or this report.

2.6.2 - HackerOne Researchers

A full list of researchers that participated in this challenge are available in the appendix.

3 - Findings

This chapter contains the results of the security assessment. Findings are sorted by their severity and grouped by the asset and CWE classification. Each asset section will contain a summary. Table 1 in the executive summary contains the total number of identified security vulnerabilities per asset per risk indication. All findings were entered in the HackerOne platform, which is the authoritative source for the information on the vulnerabilities, and can be referred to for details about each finding using the stated

reference number in the asset vulnerability summary. A point in time summary of the found vulnerabilities is included in Appendix A.

3.1 - Asset: dex.top

During the security assessment, five security vulnerabilities were identified in dex.top

Finding Title	CVSS Score	Full Report on HackerOne
[dex.top] DOM Based XSS charting_library	5.4	hackerone.com/reports/363165
https://dex.top/v1/kline/history endpoint can accept wide range using small `from` parameter or big `to` parameter - causing DoS possibility	7.5	hackerone.com/reports/362217
UI redressing/Clickjacking on the dex.top (deleting the trade adress)	3.1	hackerone.com/reports/360935
[Session hijacking] All Active user sessions should be deleted when user change his password	2.2	hackerone.com/reports/360726
Password reset token and email leakage to 3rd party app via referer header can use to ATO	3.7	hackerone.com/reports/360725

Table 3: findings in dex.top

Appendix - HackerOne Researchers

The following individuals were curated to participate in this Challenge from HackerOne's community of over 100,000 hackers:

Hackers' Usernames
hackerone.com/samidrif
hackerone.com/al88nsk
hackerone.com/akaki
hackerone.com/alku
hackerone.com/4cad
hackerone.com/daniyal_nasir
hackerone.com/missoum1307
hackerone.com/niemand
hackerone.com/rhynorater
hackerone.com/barracuda_
hackerone.com/jensec
hackerone.com/teknogeek
hackerone.com/nullelite
hackerone.com/lincoln9932
hackerone.com/ranjit_p
hackerone.com/skavans
hackerone.com/bobrov
hackerone.com/umfc
hackerone.com/yaworsk
hackerone.com/vijay_kumar1110
hackerone.com/samengmg

hackerone.com/leet-boy
hackerone.com/johnny
hackerone.com/sergeym
hackerone.com/aerodudrizzt
hackerone.com/whitesector
hackerone.com/sp1d3rs
hackerone.com/bagipro
hackerone.com/huxin
hackerone.com/johndoe1492
hackerone.com/vag_mour
hackerone.com/hackedbrain
hackerone.com/japz
hackerone.com/foobar7
hackerone.com/almaco
hackerone.com/kapytein
hackerone.com/grampae
hackerone.com/bountypls
hackerone.com/damian89
hackerone.com/europa