hackerone

HackerOne Challenge
Security Assessment

JANUARY 3RD, 2024 • CONFIDENTIAL

Author
HackerOne Staff (Senior Technical Engagement Manager, HackerOne)
examplestaff@hackerone.com

Reviewers
HackerOne Staff (Senior Manager, Technical Engagements, HackerOne)
examplestaff@hackerone.com

Prepared for: Example Company (ExCom)

<Example Company (ExCom) Logo>

Table of Contents

1. Executive Summary

Example Company (ExCom) engaged HackerOne to perform a HackerOne Challenge from November 18th, 2023 to December 18th, 2023. During this timeframe, eleven (11) vulnerabilities were identified by two (2) unique researchers.

The goal of this engagement was to identify as many vulnerabilities across the provided attack surface as possible, with particular emphasis on finding information disclosure vulnerabilities.

During the assessment, one (1) vulnerability was found that had a CVSS score of 7.0 or higher, rating either high or critical. This vulnerability represents the greatest immediate risk to ExCom and should be prioritized for remediation. Table 1 shows the in-scope assets and a breakdown of findings by severity, per asset. Section 2.4 contains more information on how severity is calculated.

	Critical	High	Medium	Low	None	**Total**
Asset 1	-	**1**	-	-	-	**1**
Asset 2	-	-	-	-	-	-
Asset 3	-	-	**5**	**5**	-	**10**
	-	**1**	**5**	**5**	**-**	**11**

Table 1: Findings per asset

The most common vulnerability type was File and Directory Information Exposure, with four (4) unique vulnerabilities. The most severe vulnerability found was an authentication bypass resulting in a user account takeover (#XXXXXX). This vulnerability could allow an attacker to take over any targeted accounts using the verification email sent.

1.1 Key Recommendations

Based on the results of this assessment, HackerOne has the following high-level key recommendations.

1.1.1 Key Issue - Most Severe Finding

One of the researchers identified a High severity vulnerability related to an account takeover.

KEY RECOMMENDATION 1	
Key Issue	An account takeover is possible via the verification email sent from username@excom.com. This vulnerability allows an attacker to bypass authentication and log in as their victim.
Recommendation	It is recommended to: ● Perform adequate input validation. ● Where possible, implement multi-factor authentication to prevent automated, credential stuffing, brute force, and stolen credential reuse attacks. ● Ensure registration, credential recovery, and API pathways are hardened against account enumeration attacks by using the same messages for all outcomes. ● Use a server-side, secure, built-in session manager that generates a new random session ID with high entropy after login. Session IDs should not be in the URL, be securely stored and invalidated after logout, idle, and absolute timeouts.

1.1.2 Key Issue - Most Common Finding

File and Directory Information Exposure vulnerabilities were the most prevalent during this engagement.

KEY RECOMMENDATION 2	
Key Issue	Example Company (ExCom) is vulnerable to multiple File and Directory Information Exposure vulnerabilities, and whilst these are primarily disclosing elements such as full paths and logs rather than PII, these still present an opportunity to attackers by increasing the attack surface they can work with.
Recommendation	The following are some general best practices that can be followed to minimize the risk of information disclosures: ● Make sure that everyone involved in producing the website is fully aware of what information is considered sensitive. Sometimes seemingly harmless information can be much more useful to an attacker than people realize. Highlighting these dangers can help make sure that sensitive information is handled more securely in general by your organization. ● Audit any code for potential information disclosure as part of your QA or build processes. It should be relatively easy to automate some of the associated tasks, such as stripping developer comments. ● Use generic error messages as much as possible. Don't provide attackers with clues about application behavior unnecessarily. ● Double-check that any debugging or diagnostic features are disabled in the production environment. ● Make sure you fully understand the configuration settings, and security implications, of any third-party technology that you implement. Take the time to investigate and disable any features and settings that you don't actually need.

2. Methodology

ExCom engaged HackerOne to perform a HackerOne Challenge. The following sections cover how the engagement was put together and performed.

2.1 Preparation phase

HackerOne worked with ExCom to identify the types of vulnerabilities most important to them and understand the goal of this assessment. This collaborative process was used to:

- develop a scope for the engagement;
- determine what user permissions levels exist and which ones are in scope;
- determine a sufficient testing window;
- identify the areas of ExCom's scope that researchers should pay special attention to;
- and what types of vulnerabilities ExCom is most interested in testing for.

All of this information was then placed into a "Policy Page", also known as the rules of engagement. From its community of over 1,000,000 researchers, HackerOne curated a set of top-tier researchers to focus on identifying vulnerabilities in ExCom's scope during the agreed-upon testing window, while following the guidelines and instructions from the Policy Page. The hand-chosen researchers were tailored based on the size of the scope and the types of assets that were in scope to ensure broad coverage of skill and experience.

During the preparation phase, a testing window from November 18, 2023 to December 18, 2023 was agreed upon.

The contents of the Policy Page were approved by ExCom before moving to the testing phase.

2.1.1 Scope

During the preparation phase the following scope for the engagement was determined:

IN-SCOPE ASSETS
Asset 1
Asset 2
Asset 3

Table 2: In-scope assets

2.1.2 Test plan

The selected researchers were able to create and use their own accounts in order to test for vulnerabilities within the agreed-upon scope. There was no testing environment setup for the researchers, all testing was performed in a public production environment.

2.2 Testing phase

2.2.1 Information gathering & reconnaissance

The information gathering and reconnaissance step is the critical starting point for every researcher. This step is used to explore the boundaries of the targets in scope and develop a plan of attack. Each member of the security research team is incentivized to be creative in uncovering what may have been missed with conventional reconnaissance steps and tools, using unique methodologies and techniques. This includes but is not limited to:

- Conventional port and banner scanning using tools such as nmap and masscan
- DNS discovery and subdomain enumeration
- Reviewing certificate transparency records
- Exploration of Shodan and Censys public data
- Enumeration of possible hidden web directories
- Content spidering and crawling using tools such as Burp Suite

HackerOne further facilitates this testing by providing the testing team with useful documentation and guides to allow researchers to consume the service in the same manner used by a typical customer.

2.2.2 Testing & exploitation

Upon starting the testing phase, all eligible researchers selected in the preparation phase were invited to participate in the engagement. A list of researchers that accepted invites is available in Appendix A. The testing period ran from November 18, 2023 until December 18, 2023.

HackerOne's methodology encourages the use of individual tools and methods by each researcher. This ensures diversity in the testing and realistically simulates real-world attacks while also putting emphasis on vulnerabilities that are exploitable and have great impact. 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 ExCom's scope. Through aligned incentives, HackerOne also actively encourages creative thinking by its researchers to combine potentially low-severity vulnerabilities into greater bugs that can have more impact, also known as "chaining".

Additionally, HackerOne's team of security analysts validated each vulnerability as they were reported throughout the testing phase. They also categorized all identified vulnerabilities against the CWE (Common Weakness Enumeration) standard, as well as assigned a severity rating based on the CVSS v3.0 (Common Vulnerability Scoring System) standard, providing consistent, easy to understand guidelines on the severity of each finding. Each finding was made available immediately to ExCom through HackerOne's vulnerability management platform.

Throughout the testing phase, HackerOne continuously managed the engagement and aligned incentives based on results to maximize output and ensure the focus areas of the engagement are thoroughly covered.

2.3 Reporting phase

At the conclusion of the engagement, HackerOne worked with ExCom to analyze the results of the testing phase and identify any potential trends in vulnerabilities found across ExCom's assets and key recommendations. The results of the engagement and post-engagement analysis were then summarized in this report. The final report was discussed with and approved by ExCom during an engagement wrap-up meeting.

Any identified vulnerabilities were made available immediately through HackerOne's vulnerability management platform to ensure quick action can be taken by ExCom.

2.4 Vulnerability classification and severity

To categorize vulnerabilities according to a commonly understood vulnerability taxonomy, HackerOne uses the industry standard Common Weakness Enumeration (CWE). CWE is a community-developed taxonomy 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.

To rate the severity of vulnerabilities, HackerOne uses the industry standard Common Vulnerability Scoring System (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.

To help prioritize vulnerabilities and assist vulnerability management processes, HackerOne translates the numerical CVSS rating to a qualitative representation (such as low, medium, high, and critical):

- **Critical:** CVSS rating 9.0 - 10
- **High:** CVSS rating 7.0 - 8.9
- **Medium:** CVSS rating 4.0 - 6.9
- **Low:** CVSS rating 0.1 - 3.9
- **None:** CVSS rating 0.0

More information about CWE can be found on MITRE's website: https://cwe.mitre.org/.

More information about CVSS can be found on the Forum for Incident Response and Security Teams' (FIRST) website: https://www.first.org/cvss.

2.5 HackerOne staff

The following individual at HackerOne managed this engagement and produced this report:

- HackerOne Staff (Senior Technical Engagement Manager, HackerOne)
- examplestaff@hackerone.com

Please feel free to contact this individual with any questions or concerns you have about the engagement or this document.

2.6 HackerOne researchers

During the engagement, fifteen (15) hand-picked researchers participated in this assessment. Two (2) of the participating researchers submitted valid vulnerability reports. The first vulnerability was identified on November 21, 2023. Hackers from fourteen (14) different countries were invited to participate.

A full list of researchers that accepted invitations ƒpar can be found in **Appendix A**.

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 information on the vulnerabilities and can be referred to for details about each finding using the stated reference number in the asset vulnerability summary.

3.1 Findings Overview

During the engagement, eleven (11) unique vulnerabilities were found across six (6) different vulnerability categories (CWE). The most common vulnerability type was File and Directory Information Exposure with four (4) unique reports. Vulnerabilities of the following kinds were identified:

- File and Directory Information Exposure
- Authentication Bypass
- Exposure of Sensitive Information Through Data Queries
- Server-Side Request Forgery (SSRF)
- Cleartext Storage of Sensitive Information
- Improper Access Control - Generic

Table 3 shows the distribution of severity across each vulnerability type.

	Critical	High	Medium	Low	None
File and Directory Information Exposure	-	-	**3**	**1**	-
Authentication Bypass	-	**1**	-	-	-
Exposure of Sensitive Information Through Data Queries	-	-	-	**2**	-
Server-Side Request Forgery (SSRF)	-	-	**1**	-	-
Cleartext Storage of Sensitive Information	-	-	-	**1**	-
Improper Access Control - Generic	-	-	**1**	**1**	-

Table 3: Severity distribution across vulnerability types

Vulnerabilities were found in the following assets:

- Asset 2
- Asset 3

There were no vulnerabilities found in the following assets:

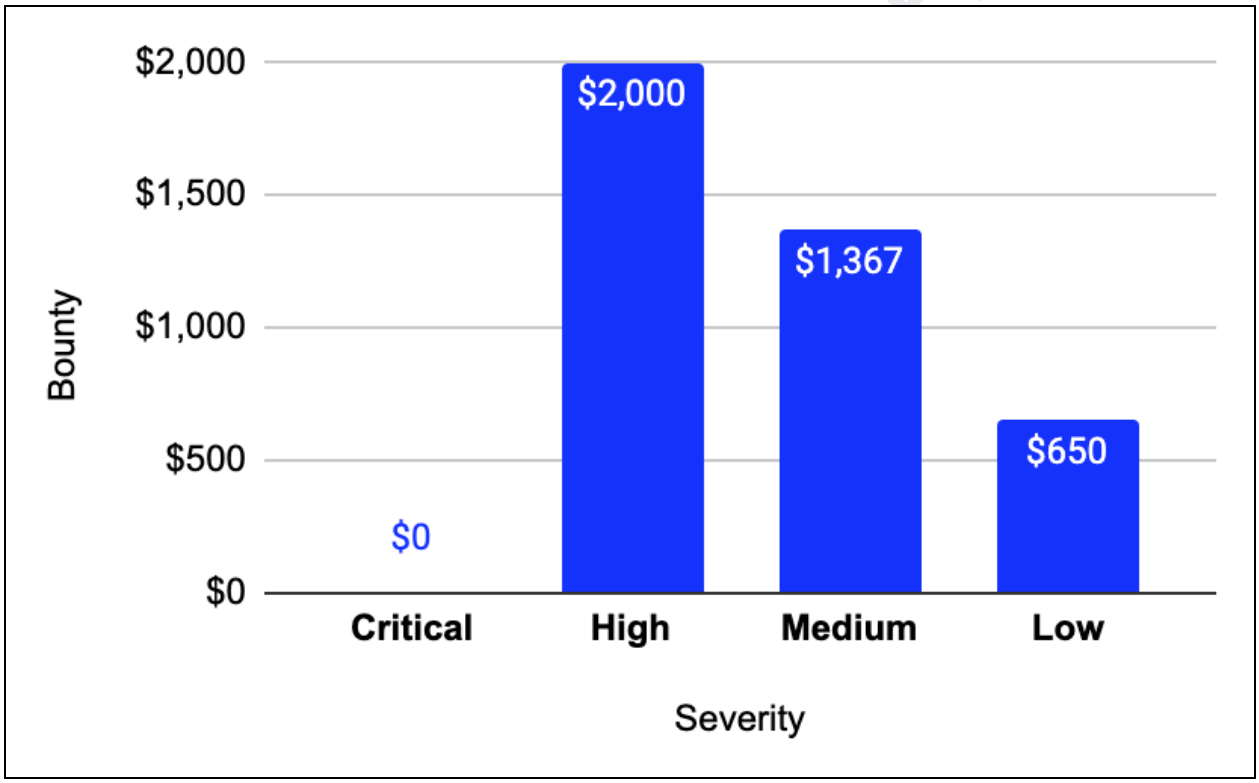
- Asset 1

3.1.1 Bounties paid to researchers

A bounty pool of $25,000 was allocated to award bounties to researchers for valid reports during the course of the engagement. The size of each bounty was determined by the severity of the vulnerability, as explained in section 2.4. The final bounty structure can be found in Appendix B.

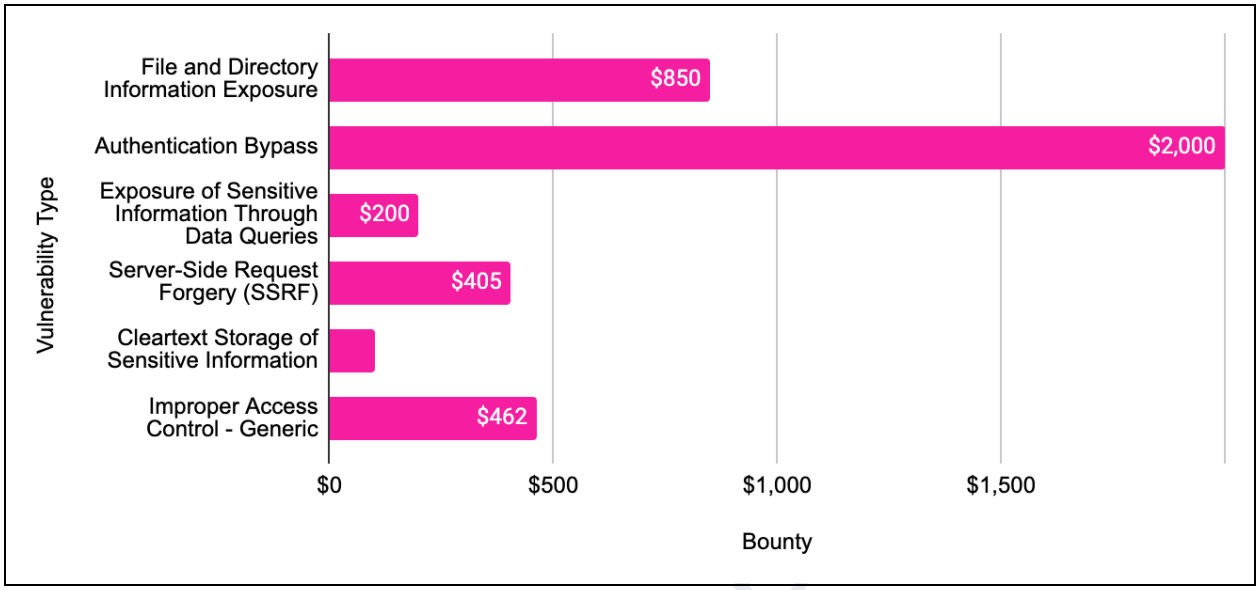
Of all reports that were submitted, eleven (11) were awarded a bounty. A total of $4,017 was awarded to researchers in bounties.

Graph 1 breaks down the bounties awarded by severity.



Graph 1: Bounties by severity

Graph 2 breaks down bounties paid by vulnerability type (CWE).



Graph 2: Bounties by vulnerability type

3.2 Asset: Asset 2

3.2.1 Asset Summary

This IP range makes up part of ExCom's external network.

3.2.2 Vulnerability Summary

During the security assessment, one (1) security vulnerability was identified for this asset.

VULNERABILITY TITLE	SEVERITY	CWE
#XXXXXXX Account Take Over via Hijacking Verifying Email Token	High	Authentication Bypass

Table 4: Findings relevant to Asset 2

3.3 Asset 3

3.3.1 Asset Summary

This IP range makes up part of ExCom's external network.

3.3.2 Vulnerability Summary

During the security assessment, ten (10) security vulnerabilities were identified for this asset.

VULNERABILITY TITLE	SEVERITY	CWE
#XXXXXXX CVE-2021-40438 - Unauthenticated SSRF	Medium	Server-Side Request Forgery (SSRF)
#XXXXXXX php_errors.log exposure on first endpoint on Asset 3	Medium	File and Directory Information Exposure
#XXXXXXX php_errors.log file exposure on second endpoint on Asset 3	Medium	File and Directory Information Exposure
#XXXXXXX php_errors.log file exposure on third endpoint on Asset 3	Medium	File and Directory Information Exposure
#XXXXXXX Improper Access Control - Ability to list internal usernames via drupal-jsonapi-user-listing	Medium	Improper Access Control - Generic
#XXXXXXX debug.log file exposure on Asset 3	Low	File and Directory Information Exposure
#XXXXXXX PHPinfo() File Disclosure on Asset 3	Low	Exposure of Sensitive Information Through Data Queries
#XXXXXXX phpinfo() file disclosure	Low	Exposure of Sensitive Information Through Data Queries
#XXXXXXX PHPinfo() file disclosure on third endpoint on Asset 3	Low	Cleartext Storage of Sensitive Information
#XXXXXXX SpringBoot Actuator Endpoints Exposed Leads To Leak Internal Services	Low	Improper Access Control - Generic

Table 5: Findings relevant to Asset 3

Appendix A

HackerOne researchers

The following individuals were curated to participate in this Challenge from HackerOne's community of over 1,000,000 researchers:

Username	Member Since	Reputation	# Of Lifetime Findings	# Of Programs Participated
rhynorater	May 2016	18,998	634	120
fattselimi	August 2019	2,629	337	15
reactors08	February 2014	6,567	300	62
whhackersbr	October 2014	2,355	222	51
jon_bottarini	November 2014	4,930	184	41
curiositysec	March 2017	4,367	163	62
shaikhyaser	April 2015	3,269	138	38
sam_exploit	August 2018	3,190	130	89
ltidi	February 2020	2,309	125	47
n0nce	May 2020	2,513	96	14
byq	November 2017	2,533	89	7
ultimatex	January 2020	2,191	83	8
maara	July 2018	2,302	83	75
0xbeefed	March 2019	2,249	82	15
aroly	November 2015	2,632	66	12

Table 6: Participating researchers

Appendix B

Bounty structure

CRITICAL (CVSS 9.0-10)	HIGH (CVSS 7.0-8.9)	MEDIUM (CVSS 4.0-6.9)	LOW (CVSS 0.0-3.9)
$2,000-$5,000	$1,000-$2,000	$500-$1,000	$250-$500

Table 7: Bounty structure

End of Summary Report