HackerOne Pentest

SECURITY ASSESSMENT

November 6, 2019 • CONFIDENTIAL

Description

This document details the process and results of a PCI penetration test performed by HackerOne on behalf of ExCom between October 23 2019 and November 6, 2019.

Prepared for ExCom

Author

Shlomie Liberow, CISSP, OSCP (Technical Program Manager, HackerOne)

shlomie@hackerone.com

About HackerOne

HackerOne is trusted by over 1,350 organizations worldwide to find and fix security vulnerabilities using the largest team of security researchers on the planet.

Our community of over 500,000 researchers has found over 120,000 valid vulnerabilities for organizations including Starbucks, Google, Lufthansa, Toyota, Hyatt, and Goldman Sachs, as well as for high-profile programs for the U.S. Department of Defense such as Hack the Pentagon, Hack the Army, Hack the Air Force, and Hack the Marines.

HackerOne customers worldwide depend on our penetration testing products and services to secure their applications, data, and people, and to make the internet a safer place for everyone.

Table of contents

1. Executive summary

ExCom (Example Company, Inc.) engaged HackerOne to perform a HackerOne penetration test, from October 23, 2019 to November 6, 2019. During this timeframe, 9 vulnerabilities were identified by 8 distinct researchers.

The goal of this engagement was to conduct targeted testing and to ensure broad coverage of the most common types of vulnerabilities as defined by the OWASP (Open Web Application Security Project) Top 10. In particular, issues that expose users' personally identifiable information (PII) were of interest. Benchmarking against other organizations within the industry, ExCom performed in the 80th percentile with six total valid reports being found.

During the assessment, 3 vulnerabilities were found that had a CVSS rating of 7.0 or higher, rating either high or critical. These vulnerabilities represent the greatest immediate risk to ExCom and should be prioritized for remediation. Table 1 shows the in scope assets and breakdown of findings by severity per asset. Section 2.5 contains more information on how severity is calculated.

	Critical	High	Medium	Low	None	Σ
excom.com	0	**1**	**3**	**2**	0	**6**
api.excom.com	**1**	**1**	**1**	0	0	**3**
payments.excom.com	0	0	0	0	0	**0**
	1	**2**	**4**	**2**	**0**	**9**

Table 1: findings per asset

From its community of pentesters, HackerOne curated a team of three pentesters whose skills and interests align best with the nature of ExCom's business and the types of assets in scope for this penetration test. The team of three - led by a lead pentester - focused on identifying vulnerabilities in ExCom's scope during the agreed-upon testing window. Chapter 2 contains more information about the penetration testing methodology that was used in this engagement.

The most common vulnerability type was Cross-Site Scripting (XSS). The most severe vulnerability found was a privilege escalation in excom.com. This vulnerability could have been used to exfiltrate all of ExCom's customer data, including saved credit card numbers, full names, dates of birth, social security numbers, phone numbers, and home addresses.

State of security

Maintaining a healthy security posture requires constant review and refinement of existing security processes. Running a HackerOne Pentest allows ExCom's internal security team to not only uncover specific vulnerabilities but gain a better understanding of the current security threat landscape.

The overall findings indicated both a lack of general data sanitization across multiple endpoints along with weaknesses in access control.

The reported sanitization issues were remediated and retested by the hackers responsible for the finding, to ensure it has been patched.

From our conversations with ExCom's lead architect, we understand that the highlighted access control issues led to a formal decision to overhaul the access control framework. The overhaul will help prevent the future introduction of new access control weaknesses.

Reviewing the remaining resolved reports for a root cause analysis can further educate ExCom's internal development and security teams and allow manual or automated procedures to be put in place to weed out entire classes of vulnerabilities in the future. This proactive approach helps contribute to future proofing the security posture of ExCom's assets.

Recommendations

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

KEY RECOMMENDATION 1	
Key Issue	Excom has multiple injection vulnerabilities present across its properties. These vulnerabilities could allow an attacker to exfiltrate all confidential data, leading to reputational damage, as well as potential regulatory fines.
Recommendation	Implement a consistent approach to input validation across the platform and create QA and coding standards guidelines to ensure that it is adhered to. In practice, this should include mandatory training with the development team. This training should focus on the multiple types of injection vulnerabilities and common mitigations available. Furthermore, there are various additional controls such as Content Security Policy (CSP), that can naturalize client-side injection vulnerabilities if they are accidentally introduced.
Resources	More information can be found in this Google-developed guide, which outlines implementation options and common pitfalls of CSP: https://developers.google.com/web/fundamentals/security/csp/. Google's CSP Evaluator can be used to review content security policies to ensure its effectiveness: https://csp-evaluator.withgoogle.com/.

KEY RECOMMENDATION 2	
Key Issue	Excom's API does not have an access control model that is consistent with its web interface. This means that users could execute unauthorized actions in the API, causing damage to data and role integrity. This could cost Excom both monetary damage in staff resources required to remediate these infractions, as well as reputational damage if the issues were to become public.

Recommendation	Use a consistent permissions model for all areas of the application, and ensure that there is a single area that contains the authoritative permissions model that can be referred to by the component applications.
Resources	The OWASP Cheatsheet on Access Control provides actionable guidance to developers maintaining access control mechanisms: https://github.com/OWASP/CheatSheetSeries/blob/master/cheatsheets/Access_Control_Cheat_Sheet.md.

2. Methodology

ExCom (Example Company, Inc.) engaged HackerOne to perform a HackerOne Pentest. 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:

- gain an overview of the Application and network components supporting the Cardholder Data Environment (CDE);
- develop a scope for the engagement;
- determine what user permissions levels exist and which ones are in scope;
- determine a sufficient testing window;
- determine the risk levels associated with each asset;
- gather shareable documentation covering ExCom's APIs and services;
- 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.

This information was then placed into a "Security Page", also known as the rules of engagement. From its community of pentesters, HackerOne curated a team of three pentesters to focus on identifying vulnerabilities in ExCom's scope during the agreed-upon testing window while following the guidelines and instructions from the Security Page. The hand-picked team - led by a lead pentester - was 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 October 23, 2019 to November 6, 2019 was agreed upon. The contents of the Security 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 agreed upon:

ASSETS IN SCOPE
excom.com
api.excom.com
payments.excom.com

Table 2: assets in scope

The following assets were specifically declared as out of scope for the engagement:

ASSETS OUT OF SCOPE
support.excom.com

Table 3: assets out of scope

2.1.2 Test plan

The researchers in the security testing team 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 hackers, all testing was performed on a 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 pentest team useful documentation and guides to allow hackers to consume the service in the same manner used by a typical customer.

2.2.2 Penetration testing & exploitation

The penetration testing period ran from October 23, 2019 until November 6, 2019 and was timeboxed at 100 hours.

HackerOne's penetration testing methodology targets specific categories of vulnerabilities, such as the OWASP (Open Web Application Security Project) Top 10. Our testing methodology ensures diversity in testing, realistically simulates real-world attacks, emphasizes the discovery of exploitable, impactful, vulnerabilities, and promotes the use of the most modern testing tools and techniques.

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 assign 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.

2.3 Retesting phase

While ExCom worked to resolve any identified vulnerabilities, HackerOne kicked off a retest of those findings to ensure they are no longer reproducible. Each finding was validated by the original finder to ensure the vulnerability was mitigated properly. The results of the retesting phase are outlined in chapter 4.

2.4 Report 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.

2.5 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.

2.6 HackerOne testing engagement leaders

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

- **Shlomie Liberow**, CISSP, OSCP, Technical Program Manager
  shlomie@hackerone.com

Document and engagement review was performed by:

- **Zachary Dando**, Security Analyst Manager
  zdando@hackerone.com
- **Jon Bottarini**, Technical Program Manager

jon@hackerone.com

- **Joaquin Silva Jr.**, Technical Program Manager
  joaquin@hackerone.com

Please feel free to contact these individuals with any questions about the engagement or this document.

2.7 HackerOne Pentest team

3 HackerOne Pentesters	**52** Total HackerOne Customer Engagements Worked On	**2,056** Total Vulnerabilities Found for HackerOne Customers

Testing was performed by a hand-selected team of 3 security researchers with a combined 12 years of testing experience across 52 HackerOne customer engagements.

Together, this team has found a total of 2,056 vulnerabilities, including 4069 of high or critical severity, for organizations including Starbucks, General Motors, Goldman Sachs, Hyatt, and U.S. Department of Defense.

Pete Yaworski (@yaworsk)

3 years and 3 months of security testing experience with HackerOne

252 vulnerabilities found for 49 HackerOne customers including Airbnb, Salesforce and Verizon Media

Eric Head (@todayisnew)

4 years of security testing experience with HackerOne

2,527 vulnerabilities found for 255 HackerOne customers including Adobe, Riot Games, Verizon Media

@try_to_hack

3 years and 10 months of security testing experience with HackerOne

1,682 vulnerabilities found for 15 HackerOne customers including Twitter, Salesforce and Verizon Media

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.

3.1 Findings overview

During the engagement, 9 unique vulnerabilities were found across 6 different vulnerability categories (CWE). The most common vulnerability type was Cross-Site Scripting (XSS) with 3 unique vulnerabilities. Vulnerabilities of the following kind were identified:

- Cross-Site Scripting (XSS)
- Server-Side Request Forgery (SSRF)
- Cross-Site Request Forgery (CSRF)
- Information Disclosure
- Security Misconfiguration
- Privilege Escalation

Table 4 shows a visualization of how ExCom’s assets performed against the most common types of vulnerabilities as defined by the OWASP Top 10.

OWASP TOP 10 CATEGORY	TEST RESULT	FINDINGS
A1 – Injection	✔	
A2 – Broken Authentication	✔	
A3 – Sensitive Data Exposure	✘	1 finding
A4 – XML External Entities (XXE)	✔	
A5 – Broken Access Control	✘	1 finding
A6 – Security Misconfiguration	✘	1 finding
A7 – Cross-Site Scripting (XSS)	✘	4 findings
A8 – Insecure Deserialization	✔	
A9 – Using Components with Known Vulnerabilities	✔	
A10 – Insufficient Logging & Monitoring	✔	

Table 4: vulnerabilities by OWASP Top 10 category

Exploring the findings further by their actual vulnerability type as defined by CWE, Table 5 shows the number of individual findings and its distribution of severity.

	Critical	High	Medium	Low	Σ
Cross-Site Scripting (XSS)	0	**1**	**3**	0	**4**
Server-Side Request Forgery (SSRF)	0	**1**	0	0	**1**
Cross-Site Request Forgery (CSRF)	0	0	0	**1**	**1**
Information Disclosure	0	0	**1**	0	**1**
Security Misconfiguration	0	0	0	**1**	**1**
Privilege Escalation	**1**	0	0	0	**1**
	1	**2**	**4**	**2**	**9**

Table 5: severity distribution across vulnerability types

Vulnerabilities were found in the following assets:

- Excom.com
- api.excom.com

There were no vulnerabilities found in the following assets:

- payments.excom.com

3.2 Asset: excom.com

3.2.1 Asset summary

excom.com is the primary customer facing website for Example Company. It is part informational but also contains the portal customers use to login and manage their account with ExCom.

3.2.2 Vulnerability summary

During the engagement, 6 security vulnerabilities were identified in this asset.

VULNERABILITY TITLE	SEVERITY	CWE
#171870 Stored wormable XSS in share widget	High (8.0)	Cross-Site Scripting (XSS)
#171872 Reflected XSS on profile page	Medium (4.3)	Cross-Site Scripting (XSS)
#171873 Reflected XSS in search bar	Medium (4.3)	Cross-Site Scripting (XSS)
#171875 Reflected XSS in login form (POST)	Medium (4.3)	Cross-Site Scripting (XSS)
#198328 CSRF in logout	Low (2.1)	Cross-Site Request Forgery (CSRF)
#168325 Admin UI elements viewable	Low (2.1)	Security Misconfiguration

Table 6: findings in excom.com

3.3 Asset: api.excom.com

3.3.1 Asset summary

api.excom.com is the programmatic API exposed for use by clients of Excom. Users are provided API keys that they can then use to invoke similar functionality to that in the web interface of excom.com. The API is used to automate certain workflows users of Excom commonly perform.

3.3.2 Vulnerability summary

During the engagement, 3 security vulnerabilities were identified in this asset.

VULNERABILITY TITLE	SEVERITY	CWE
#197248 Privilege escalation Guest > Admin	Critical (9.9)	Privilege Escalation
#189172 SSRF in Excel import feature	High (7.5)	Server-Side Request Forgery (SSRF)
#178822 API key leakage on GitHub	Medium (4.3)	Information Disclosure

Table 7: findings in api.excom.com

3.4 Asset: payments.excom.com

3.4.1 Asset summary

payments.excom.com is ExCom's payment processing endpoint and primarily used when its customers sign up for or renew their subscription.

3.4.2 Vulnerability summary

During the engagement, no vulnerabilities were found in this asset.

4. Remediation status

ExCom engaged HackerOne to retest the findings made during the assessment to ensure vulnerabilities were patched properly. Each finding was validated by the original finder to ensure the vulnerability was mitigated properly. Table 8 shows the remediation status of each finding.

VULNERABILITY TITLE	SEVERITY	STATUS
#197248 Privilege escalation Guest > Admin	Critical (9.9)	Fixed (Mar 11, 2019)
#171870 Stored wormable XSS in share widget	High (7.5)	Fixed (Mar 11, 2019)
#189172 SSRF in Excel import feature	High (7.5)	Fixed (Mar 11, 2019)
#171872 Reflected XSS on profile page	Medium (4.3)	Fixed (Mar 14, 2019)
#171873 Reflected XSS in search bar	Medium (4.3)	Fixed (Mar 13, 2019)
#171875 Reflected XSS in login form (POST)	Medium (4.3)	Fixed (Mar 11, 2019)
#178822 API key leakage on GitHub	Medium (4.3)	Fixed (Mar 12, 2019)
#198328 CSRF in logout	Low (2.1)	Fixed (Mar 14, 2019)
#168325 Admin UI elements viewable	Low (2.1)	Not retested

Table 8: summary of findings and status of remediation

End of Security Assessment Report