Uber Report

Security Assessment Findings Report

Business Confidential

Table of Contents

[Table of Contents 1](#_Toc904619428)

[Executive Summary 1](#_Toc1585564824)

[Confidentiality Statement 1](#_Toc585899570)

[Disclaimer 1](#_Toc537018383)

[Contact Information 1](#_Toc991707090)

[Assessment Overview 2](#_Toc679695377)

[External Penetration Test 2](#_Toc1788876125)

[Finding Severity Ratings 2](#_Toc1553613322)

[Scope 3](#_Toc1734879433)

[Scope Exclusions 4](#_Toc570141638)

[Client Allowances 4](#_Toc1747103083)

[Attack Summary 4](#_Toc1987130943)

[Security Strengths 5](#_Toc2114622480)

[Siem alerts of vulnerability scans 5](#_Toc1010423609)

[Security Weaknesses 5](#_Toc11083783)

[Missing Multi-Factor Authentication 5](#_Toc1232563618)

[Weak Password Policy 5](#_Toc1332405927)

[Unrestricted Logon Attempts 5](#_Toc2009194079)

[Vulnerabilities by Impact 5](#_Toc1413982208)

[External Penetration Test Findings 5](#_Toc1022443848)

[Insufficient Lockout Policy – Outlook Web App (Critical) 5](#_Toc753330171)

[Additional Reports and Scans (informational) 6](#_Toc1286366624)

# **Executive Summary**

We evaluated Uber’s external security posture through an external network penetration test on September 12th, 2023. By leveraging a series of attacks and search queries, we evaluated Uber’s online presence for possible vulnerabilities. It is highly recommended that Uber address these vulnerabilities as soon as possible as the vulnerabilities are easily found through basic reconnaissance and exploitable without much effort.

# **Confidentiality Statement**

**This document is the exclusive property of Noumeir Morales and Uber. This document contains proprietary information. Duplication, redistribution, or use, in whole or in part, in any form, requires consent of both Noumeir and Uber.**

**Uber may share this document with auditors under non-disclosure agreements to demonstrate penetration test requirement compliance.**

# **Disclaimer**

**A penetration test is considered a snapshot in time. The findings and recommendations reflect the information gathered during the assessment and not any changes or modifications made outside of that period.**

**Time-limited engagements do not allow for a full evaluation of all security controls. We prioritized the assessment to identify the weakest security controls an attacker would exploit. We recommend conducting similar assessments on an annual basis by internal or third-party assessors to ensure the continued success of the controls.**

# 

# **Contact Information**

|  |  |  |  |
| --- | --- | --- | --- |
| ****NAME TITLE CONTACT INFORMATION****  Uber | | | |
| Chirag ramani | **VP, Information Security (CISO)** | **Office: (555)555-5555**  **Email: chirag.ramani@uber.com** |  |
| **Tomasz krawczyk** | **IT Manager Office: (555)555-5555**  **Email: krawczykt@uber.com** | | |
| **India Uber** | **Network Engineer Office: (555)555-5555**  **Email: uber.india.com** | | |
| **Denis oflynn** | **Operations & Logistics Office: (555)555-5555**  **Email: denis@uber.com** | | |
| **Ramona prieto** | **Account Manager Office: (555)555-5555**  **Email: ramona.prieto@uber.com** | | |
| **andreas hinterberger** | **Account Manager Office: (555)555-5555**  **Email: ahinterberger@uber.com** | | |
| **Laura miller** | **Assistant Manager Office: (555)555-5555**  **Email:** [laura.miller@uber.com](mailto:laura.miller@uber.com) | | |
| **Becky davis** | **SOC Team Lead Office: (555)555-5555**  **Email: beckydavis@uber.com** | | |

# **Assessment Overview**

On September 12th, 2023, Uber engaged Hackerone to contract third parties to evaluate the security posture of its infrastructure compared to current industry best practices that included an external penetration test. All testing performed is based on the NIST SP 800-115 Technical Guide to Information Security Testing and Assessment, OWASP Testing Guide(v4), and customized testing frameworks.

Phases of penetration testing activities include the following:

* Planning - customer goals are gathered and rules of engagement obtained.
* Discovery – perform scanning and enumeration to identify potential vulnerabilities, weak areas and exploits.
* Attack – confirm potential vulnerabilities through exploitation and perform additional discovery upon new access.
* Reporting – document all found vulnerabilities and exploits, failed attempts, and company strengths and weaknesses.
* Improving – provide recommendations to harden systems and boost security posture in the future.

Planning

Discovery

Attack

Reporting

Additional Discovery

Improving

**Assessment Components**

## **External Penetration Test**

An external penetration test emulates the role of an attacker attempting to gain access to an internal network without internal resources or inside knowledge. Our engineer attempts to gather sensitive information through open-source intelligence (OSINT), including employee information, historical breached passwords, and more that can be leveraged against external systems to gain internal network access. The engineer also performs scanning and enumeration to identify potential vulnerabilities in hopes of exploitation.

# 

# **Finding Severity Ratings**

The following table defines levels of severity and corresponding CVSS score range that are used throughout the document to assess vulnerability and riskl impact.

|  |  |  |
| --- | --- | --- |
| severity | CVSS V3  Score range | Definition |
| **Critical** | 9.0-10.0 | Exploration is straightforward and usually results in system-level compromise. It is advised to form a plan of action and patch immediately. |
| **High** | 7.0-8.9 | Exploration is more difficult but could cause elevated privileges and potentially a loss of data or downtime. It is advised to form a plan of action and patch as soon as possible. |
| **Moderate** | 4.0-6.9 | Vulnerabilities exist but are not exploitable or require extra steps such as social engineering. It is advised to form a plan of action and patch after high-priority issues have been resolved. |
| **Low** | 0.1-3.9 | Vulnerabilities are non-exploitable but would reduce an organization’s attack surface. It is advised to form a plan of action and patch during the next maintenance window. |
| **Informational** | N/A | No vulnerability exists. Additional information is provided regarding items noticed during testing, strong controls, and additional documentation. |

# 

# **Scope**

|  |  |
| --- | --- |
| Assessment | Details |
| External Penetration Test | 34.98.127.226 |

* **Full scope information provided in “Uber-867-19 Full Findings\_xslx”**

## **Scope Exclusions**

Per client request, Uber & Hackerone

* Vulnerabilities dependent on Phishing in a DNS domain that is not in one of our primary service domains
* Most vulnerabilities that rely on a runtime context within a sandbox, lab, staging, testing or non-production environment
* Vulnerabilities involving stolen or compromised credentials
* Open redirect resulting in a low security impact. In the event you are able to chain with other vulnerabilities (e.g., steal tokens, SSRF, etc.), please let us know
* Credential stuffing or physical access to a device
* Any vulnerabilities requiring significant and unlikely interaction by the victim, such as disabling browser controls
* Man-in-the-Middle attacks except in mobile applications
* Account enumeration with a pre-defined and known list of UUIDs
* Invite/Promo code enumeration
* Ability to send push notifications/SMS messages/emails without the ability to change content
* Information disclosures related to existence of accounts: Account oracles, the ability to submit a phone number, email, UUID and receive back a message indicating an account exists
* Reports against Uber services that state that a particular software component is of a specific version, and is vulnerable without an accompanying proof-of-concept
* Vulnerabilities only affecting users using outdated, unpatched, or unsupported browsers, mobile application, mobile operating system, and end-point client software, including the versions of our applications currently in the app stores
* Stack traces, path disclosure, and directory listings
* CSV injection vulnerabilities
* Best practices concerns without a demonstrable information assurance issue and proof-of-concept
* Ability to take over social media pages (Twitter, Facebook, Linkedin, etc.)
* Negligible security severity
* Speculative reports about theoretical damage -- please always provide a proof-of-concept
* Vulnerabilities that cannot be used to exploit other users or Uber (e.g., self-xss or having a user paste JavaScript into the browser console)
* Vulnerabilities as reported by automated scanning and/or enumeration tools without additional analysis, validation, or reasoning as to how such Submissions have a demonstrable information assurance impact and vulnerability
* Distributed or denial of service attacks (DDoS/DoS) and/or reports on rate limiting issues
* Content injection or content spoofing issues
* Cross-site Request Forgery (CSRF) with minimal security implications or lack of information assurance issues (e.g., Logout CSRF, etc.)
* Missing cookie flags on non-authentication cookies
* Submissions that require physical access to a victim’s computer/device for successful exploitation
* SSL/TLS protocol scan reports reporting purported vulnerable protocol versions or handshakes
* Banner grabbing issues (figuring out what web server we use, etc.).
* Open ports or services without an accompanying proof-of-concept demonstrating a vulnerability or bonafide information assurance issues
* Physical or social engineering attempts (this includes phishing attacks against Uber employees)
* Exposed login panels without an accompanying proof-of-concept demonstrating a vulnerability or path of exploitation
* Dangling IPs
* Gift card enumeration
* Subdomain takeovers - please demonstrate that you are able to take over the page by leaving a non-offensive message, such as your username
* Reports on third-party products, services, or applications not owned by Uber
* Out-of-scope domains – Please refer to the scoping section

**Client Allowances**

* Provided “sheriff” service for SSRF testing '[http://dca11-pra.prod.uber.internal:31084](http://dca11-pra.prod.uber.internal:31084/)’

## 

# **Security Strengths**

## During the assessment, our team attempted multiple queries and attacks against Uber but failed to gain access except for readily available information through passive reconnaissance. Examples are denied access into user accounts due to requirements for strong and unique passwords as well as multi-factor authentication.

# **Security Weaknesses**

Dozens of Uber employee email addresses are public which does make Uber completely susceptible to phishing attacks.

Multiple subdomains for Uber.com were found with a simple web search leaving Uber open for a possible subdomain takeover.

.**Vulnerabilities by Impact**

The following chart illustrates the vulnerabilities found by impact:

Critical

High

Moderate

Moderate

Low

5

4

3

2

1

0

Vulnerabilities by Impact

## **External Penetration Test Findings**

|  |  |
| --- | --- |
| **Description:** | Recon-ng search revealed a list of Uber’s subdomains |
| **Impact:** | **medium** |
| **System:** | 34.98.127.226 |
| **References:** | NIST SP800-57 part 1d |

|  |  |
| --- | --- |
| **Description:** | Recon-ng and google search resulted in multiple company email addresses found |
| **Impact:** | **low** |
| **System:** | 34.98.127.226 |
| **References:** | NIST SP800-53r4 AC-17 – Remote Access |