**B**

TALHA SECURITY, Inc.

Security Assessment Report

Date: Feb 1, 2023

Project: No: #001

Version 1.0

Table of Contents

[Confidential Statement 3](#_Toc126417522)

[Disclaimer 3](#_Toc126417523)

[Contact Information 3](#_Toc126417524)

[Assessment Overview 4](#_Toc126417525)

[Assessment Components 4](#_Toc126417526)

[Internal Penetration Test 4](#_Toc126417527)

[Finding Severity Ratings 5](#_Toc126417528)

[Risk Factors 5](#_Toc126417529)

[Likelihood 5](#_Toc126417530)

[Impact 5](#_Toc126417531)

[Scope 6](#_Toc126417532)

[Scope exclusion 6](#_Toc126417533)

[Client Allowances 6](#_Toc126417534)

[Executive Summary 7](#_Toc126417535)

[Attack Summary 7](#_Toc126417536)

[Security strengths 8](#_Toc126417537)

[Security Weaknesses 8](#_Toc126417538)

[Vulnerability Summary & Report Card 9](#_Toc126417539)

[Internal Penetration Test Findings 9](#_Toc126417540)

[Technical Findings 10](#_Toc126417541)

# Confidential Statement

This document exclusively belongs to Talha Security, Inc. It contains proprietary and confidential information, as such, any redistribution or duplication, as a whole or in part or in any form requires the consent of Talha Security, Inc.

However, in accordance with nondisclosure agreement and in line with the need to demonstrate compliance with penetration test requirement, Talha Security, Inc. may share the contents of this document with auditors.

# 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. Talha Security INC. prioritized the assessment to identify the weakest security controls an attacker would exploit. Talha Security INC. recommends conducting similar assessments on an annual basis by internal or third-party assessors to ensure the continued success of the controls

# Contact Information

UBER TECHNOLOGIES INC

|  |  |  |
| --- | --- | --- |
| NAME | TITLE | COTACT INFORMATION |
| Latha Maripuri | Chief Information Security Officer | Linkedin.com/in/lathamaripuri |
| Jeremy Goh | Engineering Manager | Linkedin.com/in/jeremygoh1 |
| Anusha Kannan | Sr Network Engineer | Linkedin.com/in/anusha-kannan |

Talha Security INC.

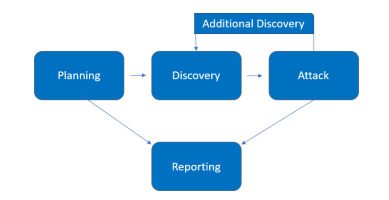
|  |  |  |
| --- | --- | --- |
| NAME | TITLE | CONTACT INFORMATION |
| Talha Yilmaz | Lead Penetration Tester | Talhabugra9999@gmail.com |
|  |  |  |
|  |  |  |

# Assessment Overview

On , Uber Technologies INC engaged Talha Security INC. to evaluate the security posture of its infrastructure compared to current industry best practices that included an internal network 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



# Assessment Components

## Internal Penetration Test

An internal penetration test emulates the role of an attacker from inside the network. An engineer will scan the network to identify potential host vulnerabilities and perform common and advanced internal network attacks, such as: LLMNR/NBT-NS poisoning and other man- in-the-middle attacks, token impersonation, kerberoasting, pass-the-hash, golden ticket, and more. The engineer will seek to gain access to hosts through lateral movement, compromise domain user and admin accounts, and exfiltrate sensitive data.

# 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 risk impact.

|  |  |  |
| --- | --- | --- |
| SEVERITY | CVSS V3 SCORE RANGE | DEFINITION |
| CRITICAL | 9.0-10.0 | Exploitation 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 | Exploitation 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. |

# Risk Factors

Risk is measured by two factors: Likelihood and Impact:

## Likelihood

Likelihood measures the potential of a vulnerability being exploited. Ratings are given based on the difficulty of the attack, the available tools, attacker skill level, and client environment.

## Impact

Impact measures the potential vulnerability’s effect on operations, including confidentiality, integrity, and availability of client systems and/or data, reputational harm, and financial loss.

# Scope

|  |  |
| --- | --- |
| ASSESSMENT | DETAILS |
| External Penetration Test | 34.98.127.226  13.110.24.10  13.110.24.11  13.110.24.16  35.184.61.224  108.139.38.6  108.139.38.130  52.2.56.64  52.21.33.16  52.184.251.130  35.168.187.155  Uber.com |

## Scope exclusion

Per client request, Talha security INC. did not perform any of the following attacks during testing:

## Client Allowances

Uber Technologies INC did not provide Talha Security INC. any allowances.

# Vulnerability Summary & Report Card

The following tables illustrate the vulnerabilities found by impact and recommended remediations:

## Internal Penetration Test Findings

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 0 | 1 | 7 | 1 | 0 |
| CRITICAL | HIGH | MODERATE | LOW | INFORMATIONAL |

|  |  |  |  |
| --- | --- | --- | --- |
| FINDING | HOSTS | SEVERITY | RECOMMENDATION |
| SSH weak key exchange algorithms enabled | 35.184.61.224 | 3.7 | Contact the vendor or consult product documentation to disable the weak algorithms. |
| TLS version 1.0 protocol detection | 108.139.38.6, 108.139.38.130 | 6.5 | Enable support for TLS 1.2 and 1.3 and disable support for TLS 1.0. |
| TLS version 1.1 protocol deprecated | 108.139.38.6, 108.139.38.130 | 6.5 | Enable support for TLS 1.2 and/or 1.3 and disable support for 1.1 |
| HSTS missing form HTTPS server (RFC 6797) | Uber.com | 6.5 | Configure the remote web server to use HSTS |
| SSL Certificate with wrong hostname | 52.21.33.16, 52.256.64 | 5.3 | Purchase or generate a proper SSL certificate for this service |
| SSL certificate expiry | 35.168.187.155, 52.2.56.64, 52.21.33.16 | 5.3 | Purchase or generate a new SSL certificate to replace the existing one |
| SSL self-signed certificate | 35.168.155, 52.2.56.64, 52.21.33.16 | 6.5 | Purchase or generate a proper SSL certificate for this service |
| SSL certificate cannot be trusted | 35.168.187.155, 52.2.56.64,  52.21.33.16 | 6.5 | Purchase or generate a proper SSL certificate for this service. |
| SSL medium strength cipher suits supported (SWEET32) | 108.139.38.6, 108.139.38.130 | 7.5 | Reconfigure the affected application, if possible, to avoid use of medium strength ciphers |

# Technical Findings

Uber’s subdomains: 13.110.24.10, 13.110.24.11, 13.110.24.16 ,35.184.61.224, 108.139.38.6, 108.139.38.130, 52.2.56.64, 52.21.33.16, 52.184.251.130, 35.168.187.155

Ip address of uber.com: 34.98.127.226

Type of webserver: Nginx

Languages used: JAVA, PHP

Database being used: MySQL

DNS host: Google

Server hosts: Google

Open ports: 80/TCP, 443/TCP

APIs discovered: 3

BASIC Authentication: NO, MFA enabled