Uber Security Assessment Findings Report

MLR Security

Business Confidential

Date: 11/2/2023
Project: 897-19
Version 1.0

Table of Contents

EXECUTIVE SUMMARY

Offensive Security was contracted by Uber to conduct a penetration test in order to determine its exposure to a targeted attack. All activities were conducted in a manner that simulated a malicious actor engaged in a targeted attack against Uber with the goals of:

- Identifying if a remote attacker could penetrate Uber's defenses
- Determining the impact of a security breach on:
    - Confidentiality of the company's private data
    - Internal infrastructure and availability of Uber's information systems

Efforts were placed on the identification and exploitation of security weaknesses that could allow a remote attacker to gain unauthorized access to organizational data. The attacks were conducted with the level of access that a general Internet user would have. The assessment was conducted in accordance with the recommendations with all tests and actions being conducted under controlled conditions.

CONFIDENTIALITY STATEMENT

This document is the exclusive property of Uber and MLR Security (MLRS). This document contains proprietary and confidential information. Duplication, redistribution, or use, in whole or in part, in any form, requires consent of both Uber and MLRS. MLRS 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. MLRS prioritized the assessment to identify the weakest security controls an attacker would exploit. MLRS recommends 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
Matthew Robinson	Lead Penetration Tester	Office: (555) 555-5555 Email: matthew.robinson@mlr-sec.com
Jim Smith	Penetration Tester	Office: (555) 555-5555 Email: jim.smith@mlr-sec.com
Joe Smith	Account Manager	Office: (555) 555-5555 Email: joe.smith@mlr-sec.com

ASSESSMENT OVERVIEW

From October 15th, 2023 to October 31st, 2023, Uber engaged MLRS 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, WASP 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

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. A MLRS 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 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.

SCOPE

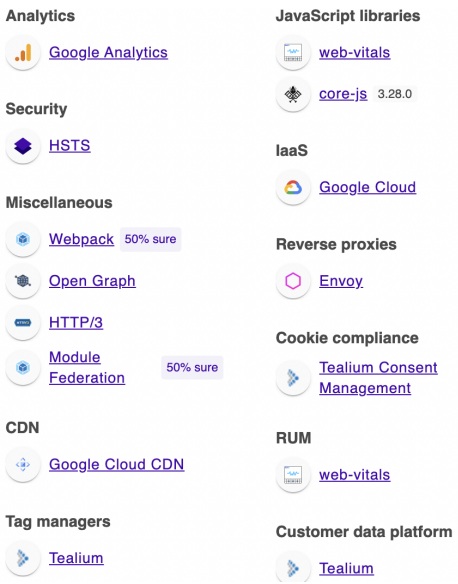
The following information was gathered through various methods of reconnaissance. Reconnaissance is defined as a preliminary survey to gain information. After reconnaissance has taken place the penetration team will use gathered information to attempt to exploit the target, Uber.

Wappalyzer

Wappalyzer is a lookup solution that allows sales and marketing teams to find the right contact data. Wappalyzer includes lookup capabilities for market research, competitive analysis, data enrichment, email verification, website monitoring, and lead generation.

For the purpose of this penetration test, Wappalyzer was used to discover Uber's website technology:

- **Type of web server(s):** Bedrock (built on Express)
- **Language(s)/stack:** Python, Node, Go, and Java
- **Database(s) being used:** MySQL, Apache Cassandra



SCOPE

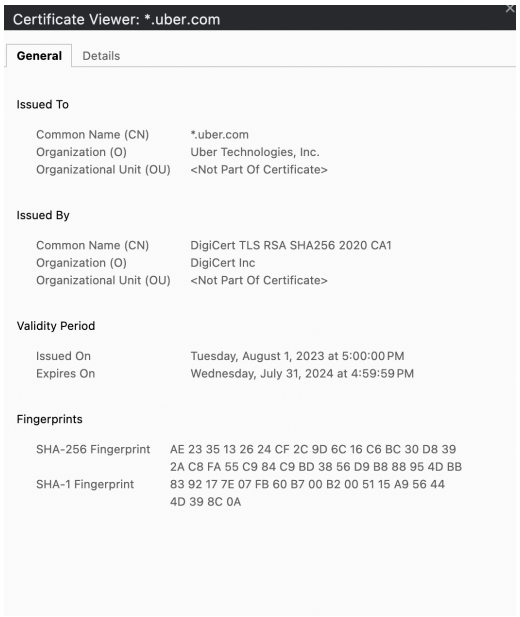
Web Reconnaissance

Web application reconnaissance refers to the explorative data gathering phase that generally occurs prior to hacking a web application.

Through a basic Linkedin search, MLRS was able to find a list of Uber employees, their role, and as well as other potentially relevant information about them. Here is a list of ten of them as well as their associated LinkedIn link:

1. **Dara KhosrowshahiCEO**
2. **Nelson ChaiCFO Uber**
3. **Tony West Chief Legal Officer**
4. **Nikki Krishnamurthy Chief People officer**
5. **Bo Young Lee Board Director**
6. **Sundeep Jain Chief Product Officer**
7. **Andrew Macdonald Senior Vice President**
8. **Jill Hazelbaker Senior Vice President**
9. **Albert Greenberg Vice President**
10. **Pierre-Dimitri Gore-Coty Senior Vice President**

More information about a corporation can be gathered from their **public certificate**. Below is a screenshot of Uber's public certificate.



SCOPE

Web Reconnaissance

WHOIS Search is a way to find information on any domain name or website. Large database of **whois** information, DNS, domain names, name servers, IPs, and tools for searching. Below is information on who hosts Uber's servers and DNS:

DNS	Whois.markmonitor.com Mark Monito Inc.
Servers	dns1.p04.nsone.net 198.51.44.4 dns2.p04.nsone.net 198.51.45.4 dns3.p04.nsone.net 198.51.44.68 dns4.p04.nsone.net 198.51.45.68 edns126.ultradns.biz 204.74.67.126 edns126.ultradns.com 204.74.66.126 edns126.ultradns.net 204.74.110.126 edns126.ultradns.org

APIs

It was found that Uber uses **Rest API**. An API, or application programming interface, is a set of rules that define how applications or devices can connect to and communicate with each other. A REST API is an API that conforms to the design principles of the REST, or representational state transfer architectural style.

SCOPE

Recon-ng

Recon-ng is a full-featured reconnaissance framework designed with the goal of providing a powerful environment to conduct open source web-based reconnaissance quickly and thoroughly. The information gathered from recon-ng is listed in the following table.

Assessment	Details
Uber's subdomains (first 10)	1. frontends-cloud.uber.com 2. a.uber.com 3. cn-ecg.cfe.uber.com 4. a.uber.com 5. frontends-all.uber.com 6. accounts.uber.com 7. geo-frontends-all-phx2.uber.com 8. cn-phx.uber.com 9. ad.uber.com 10. admin.uber.com
Uber's IP addresses (first 5 addresses)	34.98.127.226 104.36.192.148 207.231.168.151 104.36.197.136 13.110.30.13
whois points of contact?	bt@uber.com Brian Tam corpnet-eng@uber.com gni-notifications@uber.com neteng+arin@uber.com neteng@uber.com Gabriel Ramos Ramos@Uber.com
Naming convention of employee email addresses?	firstname.lastname@domain.tld

Screenshots of the commands directed to retrieve this information using recon-ng are provided at R1 and R2 and R3

SCOPE

Nessus

Nessus is an open-source network vulnerability scanner that works by testing each port on a computer, determining what service it is running, and then testing this service to make sure there are no vulnerabilities in it that could be used by a hacker to carry out a malicious attack.

Using the data from the recon-ng reconnaissance MLRS performed a scan on the first 5 IP addresses, as a sample, found from the website, https://www.uber.com. It has been found that the highest risk vulnerability within the sample is 34.98.127.226 (7 vulnerabilities).

A documentation of this completed scan can be seen in detail in the link attached to the following form.

Linux

A DNS 'mail exchange' (MX) record directs email to a mail server. The MX record indicates how email messages should be routed in accordance with the Simple Mail Transfer Protocol (SMTP, the standard protocol for all email). Like CNAME records, an MX record must always point to another domain.The MX records for uber are:

- alt4.aspmx.l.google.com
- alt3.aspmx.l.google.com
- alt2.aspmx.l.google.com
- alt1.aspmx.l.google.com
- aspmx.l.google.com

SCOPE

Nmap

Nmap is a short form of Network Mapper and it's an open-source tool that is used for mapping networks, auditing and security scanning of the networks. The reason behind its development is to quickly find large networks at a specific location. For the discovery of networks, the raw IP packets are used by Nmap. Banner grabbing is the act of getting software banner information (name and version). Below is the information gathered for Uber using nmap

Through nmap it was found that the server being used is **ufe** via **1.1 google**. As seen in the above screenshot are a list of a few open ports and their service type giving the attacker potentially relevant information to carry out an attack.

SUMMARY

The reconnaissance phase of the penetration test for Uber relied on various tools:

- **Wappalyzer**
- **Web Reconnaissance**
- **Recon-ng**
- **Linux**
- **Nmap**

The use of these tools can be used to gain information about the target and provide an insight into the possible vulnerabilities it may have.

Conclusion

Understanding past exploitations will help diminish the severity of any imminent threats. Through web reconnaissance it was found Uber had suffered an attack in recent history. In this attack the hacker gained access to the company's VPN and discovered Microsoft Powershell scripts containing the login credentials of an admin user in Thycotic - the company's Privileged Access Management (PAM) solution.

Threat actors leaked employee email addresses, corporate reports, and IT asset information on a hacker forum after an attack on an Uber technology partner. Uber has suffered yet another high-profile data leak that exposed sensitive employee and company data.

As a result, Uber’s biggest cybersecurity risk must be the **risk of personal information** of 57 million customers and drivers **getting leaked**.

The next step of the penetration test will be to test these vulnerabilities and record the process. This will act as an in depth report of the target’s security weaknesses. The final step of this process is to find best practices to mitigate these risks.