

**Penetration Test Report**

Uber

June 30th, 2024

**Caywood Security, LLC**

1564 Natural Bridge Blvd.

Suite C #303

Dallas, TX 75398

United States of America

|  |  |
| --- | --- |
| Phone: | 1-402-608-1337 |
| Email: | [info@csec.com](mailto:info@csec.com) |

**Table of Contents**

[**Executive Summary** **3**](#_Toc170844403)

[Summary of Results 3](#_Toc170844404)

[Domain Information 4](#_Toc170844405)

[**DNS Analysis 5**](#_Toc170844406)

[Name Server 5](#_Toc170844407)

[Additional Name Server’s 5](#_Toc170844408)

[Name Server Enumeration 6](#_Toc170844409)

[Enumeration Results 7](#_Toc170844410)

[DNS Server & MX Record 8](#_Toc170844411)

[Additional Records 9](#_Toc170844412)

[**Technology Stack 10**](#_Toc170844413)

[Additional Technologies 11](#_Toc170844414)

[**Subdomains 12**](#_Toc170844415)

[**Conclusion 13**](#_Toc170844416)

[Recommendations 13](#_Toc170844417)

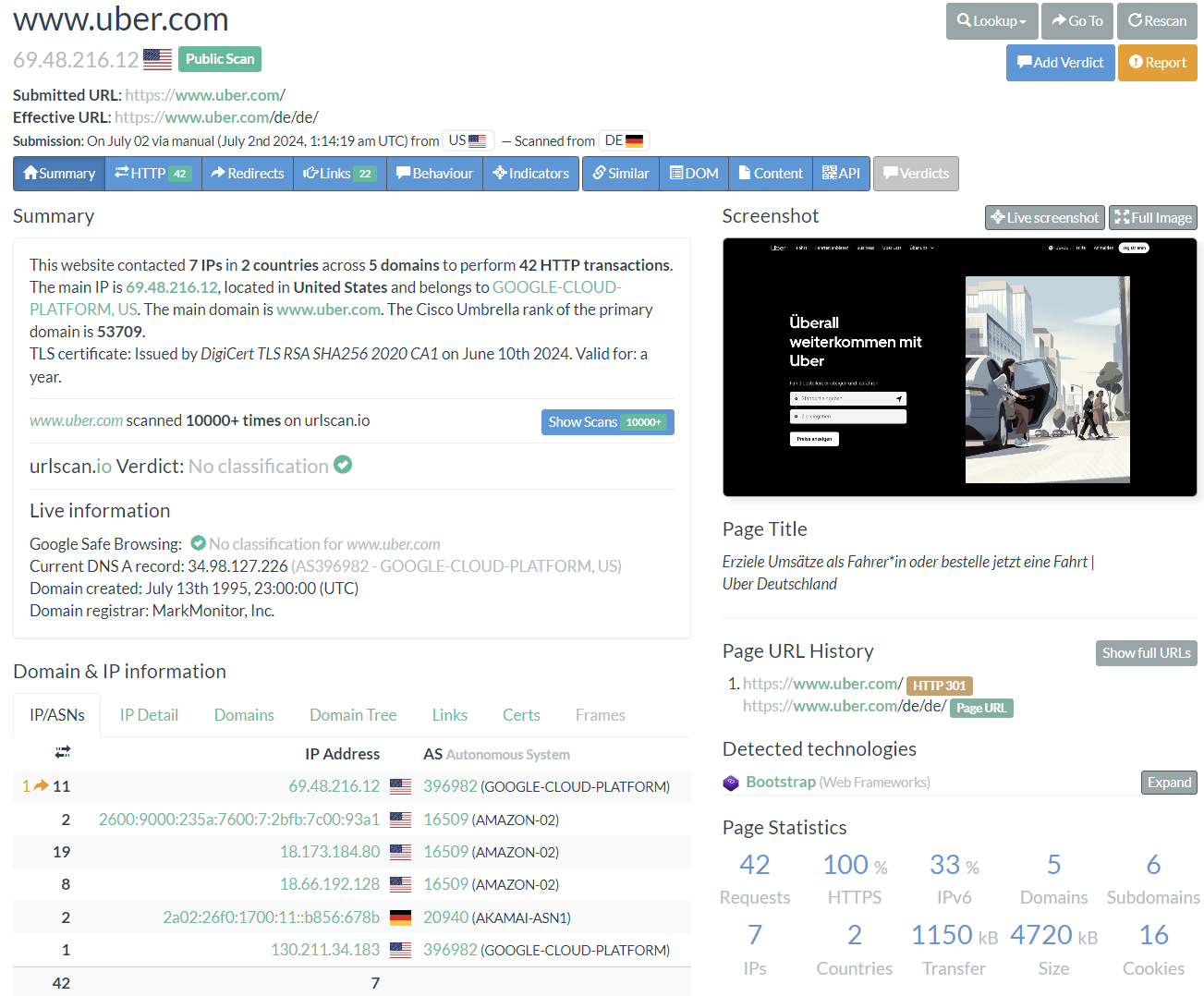
# Executive Summary

This penetration test report outlines the findings of a comprehensive security assessment conducted on Uber's digital assets as part of their HackerOne bug bounty program. The assessment aimed to identify potential vulnerabilities and weaknesses in Uber's online presence, providing a comprehensive overview of their digital footprint. The assessment revealed a range of potential vulnerabilities and weaknesses in Uber's online presence, including DNS misconfigurations, exposed APIs, and running services that could be exploited by attackers. Additionally, the assessment identified potential avenues for social engineering attacks, including employee information and email configuration. The report highlights the importance of implementing robust security measures to protect Uber's digital assets and recommends additional security controls to prevent potential attacks.

## Summary of Results

The assessment yielded a significant amount of information about Uber's digital assets, including the discovery of 9935 subdomains and associated IP addresses. DNS analysis revealed potential vulnerabilities in Uber's name servers, including open ports and service versions. The assessment also identified Uber's DNS hosting provider and server hosting provider information, as well as MX records and WHOIS points of contact. Furthermore, the assessment uncovered 15 APIs, including those for user authentication and data retrieval, and obtained banner information, including server software and operating system details. The technology stack analysis provided valuable insights into Uber's infrastructure and potential vulnerabilities, including the use of RESTful APIs and Swift programming language. The report highlights the importance of securing DNS services, implementing robust access controls, and addressing potential vulnerabilities in Uber's digital assets.

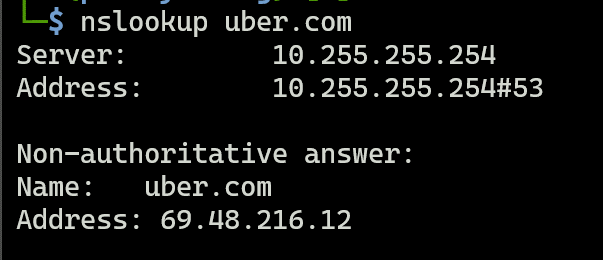
## Domain Information

For the purposes of this assessment, Uber has provided minimal information outside of the organizational domain name: uber.com. The intent was to closely simulate an adversary without any internal information. To gain a basic understanding of the domain a URL scan via urlscan.io was executed. The purpose of the URL scan is to analyze the website and its associated resources from an external perspective. This scan provides insights into the following areas: domain and subdomain discovery, resource analysis, IP address and geolocation, certificate information, security headers and their technology stack.

# DNS Analysis

## Name Server

**A screenshot of a computer

Description automatically generated**In an attempt to further identify the potential attack surface, we examined the name servers of the uber.com domain name. In the case of Uber, the nslookup tool was used to identify the non-authoritative name servers and check for potential vulnerabilities. Two different techniques were used to identify as much as possible.

## Additional Name Server’s

A screenshot of a computer

Description automatically generatedAdditional name servers were also found using DomainIQ, a freely available domain intelligence tool.

## Name Server Enumeration

After identifying the name servers, an Nmap scan was performed to gather detailed information about each server. This scan aimed to identify open ports, determine the versions of running services, and detect the operating systems of the name servers. The aggressive timing template and verbose output were used to speed up the scan and provide detailed information. The scan results revealed open ports, service versions, and operating systems, which are crucial for identifying potential vulnerabilities and assessing the security posture of Uber's name servers.

A screen shot of a computer

Description automatically generated

The results of the Nmap scan provide valuable insights into the security posture of Uber's name servers. The Nmap scan of Uber's name servers revealed that each server has TCP port 53 open, indicating the presence of DNS services protected by TCP wrappers. The scan identified the servers as running various versions of the Linux kernel, suggesting they are up-to-date and maintained. These findings highlight the importance of securing DNS services and ensuring robust access controls, providing a foundational understanding of the security posture and potential vulnerabilities that need to be addressed.

## A black screen with white text Description automatically generatedEnumeration Results

A screenshot of a computer program

Description automatically generated

## DNS Server & MX Record

A screenshot of a computer program

Description automatically generatedTo gain additional information regarding DNS, DNSDumpster was utilized to gather comprehensive DNS information for Uber's domain, including DNS hosts, MX records, TXT records, and host records. This tool provides a visual representation of the domain's DNS structure and helps identify various associated records. By identifying the DNS hosting providers for Uber, we reveal critical details about the name servers managing the domain. We can also see from this that they are using UltraDNS, a cloud-based DNS solution.

From the MX records we can see they are using ProofPoint as their email security solution. Knowing that Uber uses ProofPoint for email security helps attackers by highlighting the specific defenses in place, such as anti-phishing and malware protection. This information directs attackers to consider more sophisticated methods or alternative attack vectors to bypass these defenses effectively.

## Additional Records

Uber's TXT records, obtained through DNSDumpster as well, reveal critical information such as SPF, DKIM, and DMARC configurations, helping guide potential attackers in crafting more targeted email spoofing or phishing campaigns. Along with the information provided in the MX record, this makes the information invaluable to potential attackers. It reveals the level of email security in place and potential weaknesses or misconfigurations that could be exploited to bypass these protections.



Uber's A records provide insights into their server infrastructure by revealing the IP addresses associated with their domain and subdomains. Exposing their server IP addresses, aides’ attackers in identifying potential entry points for network attacks or unauthorized access attempts. These were also acquired with DNSDumpster, but were exported due to the amount found, as seen on the right of this page

# Technology Stack

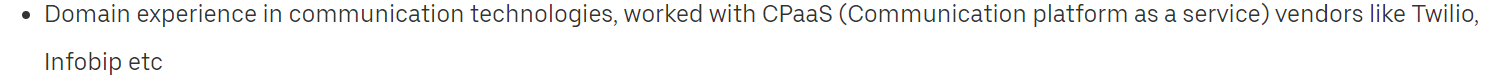
The technology stack analysis provides valuable insights into Uber's infrastructure and potential vulnerabilities. This information can be used to identify potential attack vectors and tailor our testing approach to maximize the effectiveness of the penetration test. By understanding the technologies and services used by Uber, we can focus our efforts on areas that are most likely to yield vulnerabilities and prioritize our testing accordingly. This information is crucial to the penetration test, as it allows us to identify potential weaknesses and provide actionable recommendations for remediation.



|  |  |
| --- | --- |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |

## Additional Technologies

Additional technology stack information gathered from job listings provides further insight into Uber's infrastructure and potential vulnerabilities. The use of RESTful APIs to connect iOS applications to back-end services suggests that API security may be a critical area to focus on during the penetration test. Additionally, the proficiency in Swift, the primary programming language used for iOS development, may indicate that iOS-specific vulnerabilities should be considered. Below are some more languages mentioned that give us additional insight into the makeup of their products. The culmination of information gathered below can be used to better inform our testing approach and identify potential areas of weakness in Uber's infrastructure. By understanding the technologies and tools used by Uber, we can tailor our testing to maximize the effectiveness of the penetration test.



* Familiarity with RESTful APIs to connect iOS applications to back-end services.
* A white background with black text

  Description automatically generatedA black text on a white background

  Description automatically generatedProficiency in Swift

# Subdomains

To identify the subdomains associated with Uber's domain, we utilized Subfinder, a powerful subdomain enumeration tool. Subfinder is designed to quickly and efficiently identify subdomains by querying various DNS servers and databases.

The following command was used to run Subfinder against Uber's domain:

The list of subdomains identified by Subfinder is too extensive to include in this report. However, a sample of the subdomains found is provided below:

A screenshot of a computer

Description automatically generated

A screenshot of a computer screen

Description automatically generated

# Conclusion

This penetration test report provides a comprehensive overview of the security assessment conducted on Uber's digital assets as part of their HackerOne bug bounty program. The assessment aimed to identify potential vulnerabilities and weaknesses in Uber's online presence, providing a detailed understanding of their digital footprint.

The assessment revealed a range of potential vulnerabilities and weaknesses in Uber's online presence, including DNS misconfigurations, exposed APIs, and running services that could be exploited by attackers. Additionally, the assessment identified potential avenues for social engineering attacks, including employee information and email configuration.

The report highlights the importance of implementing robust security measures to protect Uber's digital assets and recommends additional security controls to prevent potential attacks. The findings of this assessment can be used to improve Uber's overall security posture and identify potential vulnerabilities.

## Recommendations

Based on the findings of this assessment, we recommend that Uber:

* Implement robust access controls and secure DNS services to prevent potential attacks
* Conduct regular security audits and penetration tests to identify and address potential vulnerabilities
* Implement robust email security measures, including anti-phishing and malware protection
* Secure APIs and ensure proper authentication and authorization mechanisms are in place