International Journal of Research Publication and Reviews

Encrypted Message Traversal using QR codes

Neelanjan Manna

Metapyxl

ABSTRACT

The Japanese automaker Denso Wave created the QR code, also known as a matrix barcode or two-dimensional barcode, in 1994. QR stands for "rapid response code." A barcode is an optical label that can be read by a computer and contains data about the object to which it is attached. In reality, QR codes frequently contain information for a tracker, location, or identifier that directs users to a website or application. To store information efficiently, QR codes use four specified encoding modes: numeric, alphanumeric, byte/binary, and kanji; extensions may optionally be used. Because it can store more data than a conventional UPC barcode and is faster to scan than a typical UPC barcode, the Quick Response system gained popularity outside of the automobile industry. Applications include document management, general marketing, product tracking, item identification, and time monitoring.

Introduction

A frequent sight on billboards and restaurant menus alike, QR codes can actually pose a severe danger to the security of workplace mobile devices. In recent years, scanning a rapid response code (QR code) has gained popularity as a tool to do contactless purchases, access paperless menus, and more. But because they are so practical and common, hackers who are looking for new ways to spread malware and steal data frequently target QR codes. Organizations should educate themselves on the various risks that could masquerade as a useful QR code, as well as how to prevent them.

Method of operation

The security of QR codes

Although QR codes have many beneficial uses, malevolent individuals can also make advantage of them. The FBI issued a warning in January 2022 that fraudsters might tamper with QR codes to lead victims to nefarious websites. For fresh cybercrime strategies, scammers frequently resort to the most recent trends.

Cybercriminals primarily employ one of two different kinds of QR code exploits. The first is a phishing attempt using a QR code, often known as quishing. In this attack, a victim is tricked into visiting a phishing website using a QR code in order to obtain their login credentials, personal information, or other sensitive data.

Another common form of QR code assault is known as QRLjacking.

What is QRL jacking

Quick Response (QR) codes are really cool. They can be used to encode pretty much anything digital and alphabetic. They also have a futuristic appearance. Bar codes (X-axis, left to right) have been technologically improved with QR codes. QR codes are two-dimensional (X and Y axes—left to right and top to bottom), in contrast to bar codes, which are thought of as one-dimensional. Up to 4296 characters or 7089 digits can be stored in a QR code. Punctuation and other special characters are included in this. Therefore, words, phrases, internet URLs, and login passwords can all be encoded using QR codes.

attacks on QRLjacking in real life

A GitHub repository providing software tools to carry out QRLjacking attacks was established by OWASP.org, The Open Web Application Security Project, in April 2019. The repository includes instructions and a Wiki. Sometimes "nasty" content is posted by security researchers.

The online services that, as of April 2019, were known to be susceptible to QRLjacking attacks are listed by OWASP on the GitHub page. The list is repeated below. You might be surprised by some of the internet services on OWASP's list.

These services are primarily offered in Chinese or Russian, where QR codes are much more prevalent.

Applications for Chat

- WhatsApp

- WeChat

- Line

- Weibo

- Instant Messaging on QQ

- Postal Services

- A QQ Mail (Personal and Business Corporate),

- Yahoo Mail

- eCommerce

- Alibaba

- Aliexpress

- Taobao

- Tmall

- 1688.com

- Alimama

- Taobao Vacations

- Banking online

- AliPay

- Yandex Finance

Services for TenPay Passports

Yandex Passport, which offers services including Yandex Mail, Yandex Money, Yandex Maps, and Yandex Videos
Software for mobile management
Other Services for Airdroid
Zapper & Zapper for MyDigiPass Trustly App's QR Code Plugin for WordPress Login
Yelophone
Abdul Yunos
reducing QRLjacking assaults
Beyond not using QRLs at all, there isn't much consumers can do to defend themselves against QRLjacking assaults. In fact, it's OWASP's top suggestion for reducing the risk of QRLjacking.

t to verify their users'

ser doesn't receive the

ly knows the user's IP
king an authentication
ion.

ight be challenging to
ne passwords (OTP)?
pp instead of opening
extra swipes make a
col then QR code can

References

1. Thangavelu, S., Sonai, V., Malaisamy, P. and Nallakannu, S.M., 2020. A Novel Permutation Based Encryption Using Tree Traversal Approach. *Recent Advances in Computer Science and Communications (Formerly: Recent Patents on Computer Science)*, *13*(6), pp.1278-1283.
2. Sivakumar, T., Veeramani, S., Pandi, M. and Gopal, G., 2020. A novel encryption of text messages using two fold approach. *Recent Advances in Computer Science and Communications (Formerly: Recent Patents on Computer Science)*, *13*(6), pp.1106-1112.