Indian Computer Emergency Response Team
Ministry of Electronics and Information Technology
Government of India
सत्यमेव जयते

CERT-In Advisory CIAD-2017-0055

Quick Response (QR) code Security Best Practices

Original Issue Date: December 07, 2017

Description

QR code (or Quick Response code) is a matrix bar code which can be read by an imaging device (camera) and then processed to read its data. The QR code is simply an array of bits to be identified by a scanner. Bits are reserved for the scanner to be able to identify and orient the image, as well as for version and format information. QR codes are really useful and help us to complete tasks faster in smartphones. You can quickly open a website just by scanning a QR code and you do not need to manually type the URL in your smartphone.

QR code has been successfully implemented in the global payments industry, as well. Because it is easy to generate a QR code, the system offers convenience to businesses and consumers, alike. It can be printed on business cards, points of sale, and product labels which customers can simply scan to pay for a product or service.

With the increase in usage of QR codes in the general public, it is necessary to ensure that the data conveyed through the QR code is not harmful to the user. There are currently two major attack vectors for potential vulnerabilities: attacks on human interactions and automated attacks.

Attacks on human interactions

Attacks on human interactions rely on the fact that humans by themselves are unable to interpret what information is encoded in QR codes, and thus rely on QR code readers to decode the information. Since the information in the QR code is completely obfuscated, it is possible to trick and attack users via phishing, pharming, and other social engineering attacks by putting up fake QR codes. It is also possible to attack users by manipulating and exploiting existing QR code readers that users use via command injection or buffer overflows.

Phishing

Phishing is the main security issue involved with QR codes. It is also described as QRishing. QR codes are generally scanned by a smartphone camera to visit a website. Now, many website advertisements put QR code along with a URL so users can quickly scan QR code to visit the website. Hackers or scammers try to change the QR code added in the poster. They can also print the similar kind of fake posters and put in public places. Innocent customers will scan these fake QR codes to visit the websites but they will be redirected to phishing websites. In mobile devices, it is hard to check the full address in the browsers. Due to limited space, browsers do not show the full address in the URL field. And most people never try to check the full address, which makes users more vulnerable. When they use this phishing page to login, their passwords are compromised.

In the same way, attackers can use QR codes to point to malicious websites to distribute malware via drive by download attack. Drive by download attacks are attacks in which a website forcefully downloads software in your device when you visit the website.

Automated attacks

Automated attacks often result from the assumption that the encoded information in QR codes is sanitized. However, it is known that QR codes themselves can easily be manipulated in order to change encoded information, potentially producing attacks on backend software. Without QR code input sanitation, it is possible to produce attacks such as SQL injection, command injection, and fraud.

Best practices for users

QRishing & Drive by download attacks can be prevented by following the below mentioned best practices.

Observe before use:

If you find a QR code in any banner advertisement in a public place, look at it closely. Most of the times, hackers stick their fake QR code above the legitimate QR code in a legitimate poster. So try to see if it is real or not. One can check by touching the poster. If it does not look like it's actually printed on the poster, do not use it. If you are not sure, never scan that QR code.

Be suspicious and never giver personal or login info:

Always be suspicious of the page you land on via QR code. Never share your personal information on these pages. Only do this if the QR code is from a very trusted source and you trust the website. For login, always enter the URL manually on the browser's address bar.

Look at URL before proceeding:

Looking at the QR code does not confirm whether it is malicious or not. Some QR Code readers let you see the URL and ask to confirm whether you want to visit the URL before it links you to the destination. You can use these QR code scanners to know what URL the QR code will send you. Just remember that many QR Codes use shortened URLs so this strategy won't always work.

Best practices for merchants

- Include signage telling the user what the code does. Otherwise the user has no way of knowing if the code should point to a URL, phone number, or SMS.
- Print the URL near to the code. This way if the code is hijacked and pointed to http://evilwebsite.com/ the user can see they're not visiting the correct site.
- Include https in the URL. Get users used to checking for https before they interact with you.
- Every time you put out a QR code in a public area, you should know where it is. If a code is on a billboard, on a storefront, or anywhere else it can be accessed by the public, it could be at risk. You will know your code is working correctly when you see "normal" traffic through it. If the traffic suddenly stops, ensure that the code is still there and hasn't been tampered with.
- Distinctive, branded QR codes with special colours or other design features are far more likely to get attention, and it will help people to know that they are dealing with a legitimate link to your brand and not a counterfeit code. It will be much more difficult for a hacker to simulate a highly designed and colourful code than a plain one.

References

http://resources.infosecinstitute.com/security-attacks-via-malicious-qr-codes/#qref
https://courses.csail.mit.edu/6.857/2014/files/12-peng-sanabria-wu-zhu-qr-codes.pdf

Disclaimer

The information provided herein is on "as is" basis, without warranty of any kind.

Contact Information

Email: info@cert-in.org.in
Phone: +91-11-24368572

Postal address

Indian Computer Emergency Response Team (CERT-In)
Ministry of Electronics and Information Technology
Government of India
Electronics Niketan
6, CGO Complex, Lodhi Road,
New Delhi - 110 003
India