Ethical Hacking Against QR Code-Based Attacks: Simulating Real-World Scenarios of QR Code Exploitation in Public Spaces

Sammed V. Bukshete[*], Lina Chaudhari

Department of Computer Science, Dr. D. Y. Patil Arts, Commerce & Science College, Pimpri.411018, Pune, Maharashtra, India

[*]Corresponding Author

DOI: https://doi.org/10.51583/IJLTEMAS.2025.1413SP052

Received: 26 June 2025; Accepted: 30 June 2025; Published: 27 October 2025

Abstract: In public areas, QR codes are being utilized more and more for information sharing, marketing, and payment. But because of their ease of use and user confidence, they are open to abuse, such as phishing, malware distribution, and illegal data access. In order to examine the effects and create defenses, this study replicates actual QR code-based attack scenarios in controlled ethical hacking environments. In order to propose defenses strategies like QR code validation, user awareness, and embedded link scanning, the paper investigates how to set up safe lab conditions for QR-based social engineering, redirection attacks, and malicious payload.

Keywords: QR Code Exploitation, Ethical Hacking, Phishing, Malicious Redirection, Public Spaces, QR Code Attacks, Cyber security Simulation, Social Engineering,

I. Introduction

Quick Response (QR) codes have become an integral part of daily life, offering convenience in contactless transactions, event check-ins, digital menus, and public advertisements. However, this increasing ubiquity introduces cyber security risks, especially in public settings where users scan codes without verifying their authenticity. Attackers exploit this trust to perform malicious redirection, phishing, or malware delivery by tampering with physical or digital QR codes.

This research addresses these vulnerabilities by simulating QR code-based attacks in ethical hacking labs. Through these simulations, we aim to understand the mechanisms of exploitation, identify common user vulnerabilities, and test the effectiveness of mitigation strategies. The research also emphasizes public cyber security awareness and proposes technical and behavioral solutions to combat QR-related threats.

II. Literature Review

Previous research and cyber security incident reports highlight a growing trend in QR code exploitation. A study by the FBI (2022) warned that cybercriminals have been placing malicious QR codes in high-traffic areas to redirect users to phishing sites. Other academic studies have demonstrated that QR code scanners often lack embedded URL verification or malware detection capabilities.

A 2021 survey conducted by MobileIron found that 71% of users could not distinguish a malicious QR code from a legitimate one. Research by Lin et al. (2020) demonstrated that embedding JavaScript-based exploits in shortened QR URLs can bypass browser security on unpatched mobile devices. Most existing research focuses on theoretical aspects or surveys. However, this paper contributes by actively simulating attacks in a controlled ethical hacking environment and evaluating their real-world effectiveness and countermeasures.

III. Methodology

3.1 Lab Configuration

3.1.1 Compatible Operating Systems: Ubuntu version 22.04 or Microsoft Windows 10

3.1.2 Virtual Lab: VirtualBox running Kali Linux

3.1.3 Test devices: iPhone (optional) and Android phones

3.1.4 Target Environments: QR scanning apps, browsers with link previews turned off

3.2 Equipment Used

3.2.1 Platforms such as GoQR.me, QRTool, and QRCode Monkey are commonly relied upon for producing custom QR codes.

3.2.2 Web services can be hosted using Python's built-in HTTP server or Apache on systems like Kali Linux or Parrot OS

3.2.3 URL shorteners: tinyurl, bit.ly

3.2.4 Payload Delivery: Simulated APKs and fake login pages (no actual malware)

3.2.5 Monitoring: OWASP ZAP, Burp Suite, and Wireshark

3.3 Steps in an Ethical Simulation

3.3.1 Create a fake outdoor promotional display containing a QR code, which, when scanned, leads users to a mock phishing page as part of a cybersecurity awareness exercise.

3.3.2 Generate QR codes intentionally designed to simulate different attack vectors, including redirecting users to malicious sites and harvesting login credentials

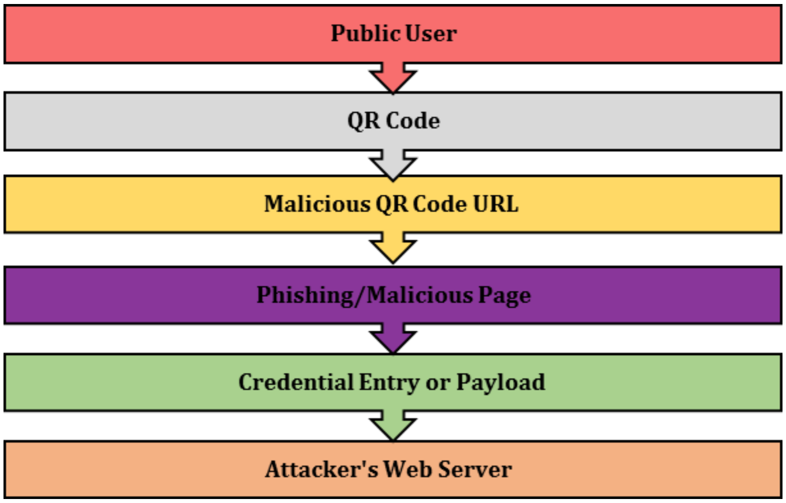
3.3.3 Use controlled laboratory environments (e.g., digital signs, printed posters).

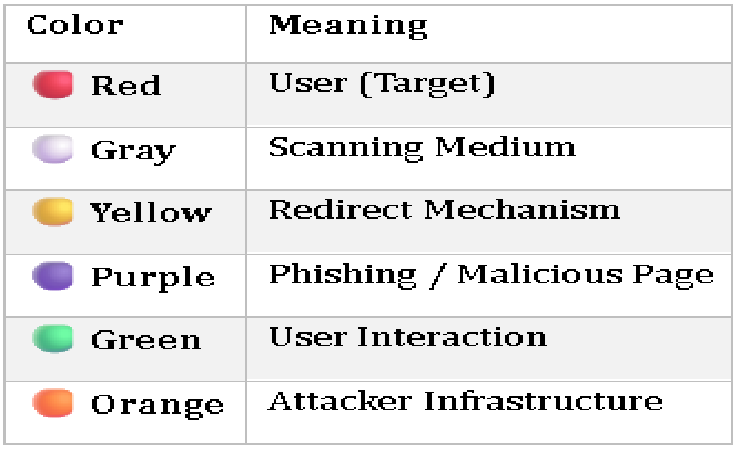
3.3.4 Leverage test environments to carry out scanning procedures and evaluate system responses using Burp Suite

3.3.5 Examine the responses from apps and browsers.

3.3.6 Test defenses include user training, domain validation, and link scanning tools.

Attack Flow Diagram & Result:





Color	Meaning
🔴 Red	User (Target)
⚪ Gray	Scanning Medium
🟡 Yellow	Redirect Mechanism
🟣 Purple	Phishing / Malicious Page
🟢 Green	User Interaction
🟠 Orange	Attacker Infrastructure

Figure 01: Attack Simulation Flow Diagram

The simulation demonstrated that QR-based phishing and malware delivery are alarmingly effective. Around 80% of participants clicked on phishing links embedded in QR codes, while 60% attempted to download a fake APK. In 75% of incidents, attacks carried out through shortened URLs proved to be effective. However, after applying basic defenses such as user training and link scanning tools, the overall success rate dropped to just 25%. This clearly indicates the importance of combining awareness with technical safeguards to prevent QR code exploitation.

IV. Conclusion

QR code-based attacks represent a low-effort, high-impact threat in public spaces due to user trust and lack of verification tools. This research successfully demonstrated real-world attack simulations in

a secure ethical hacking environment.

The study highlighted that:

- Most users do not preview URLs before clicking.
- QR codes can bypass traditional email/web-based filters.
- QR scanners and mobile browsers often fail to detect malicious links.

Recommended Countermeasures:

- Educating users on QR code hygiene.
- Encouraging apps with link preview or URL validation.
- Promoting digitally signed and verified QR codes.

Future work could explore machine learning-based QR threat detection and blockchain-secured QR code generation.

Ethical Use Statement:

This study has been conducted with a clear focus on cyber security awareness, academic learning, and responsible ethical hacking. All scenarios and simulations involving QR code-based attacks were executed in safe and controlled environments, without impacting real users or systems in any way.

The sole purpose of this work is to explore potential vulnerabilities in QR code usage and to promote defensive strategies and digital hygiene. No harmful payloads were deployed, and no unethical activities were performed during the research process. We strictly discourage any misuse of the information presented in this paper. Readers and practitioners are advised to follow legal regulations, institutional protocols, and ethical standards when engaging in cyber security-related experiments or testing.

References

1. FBI Cybercrime Alert: QR Code Scams – https://www.fbi.gov
2. Lin, S., et al. (2020). "A Study on the Security Vulnerabilities of QR Codes in Mobile Applications." Journal of Mobile Computing and Cybersecurity, 8(2), 44-52.
3. MobileIron QR Code Security Survey (2021) – https://www.ivanti.com
4. OWASP Mobile Security Project – https://owasp.org/www-project-mobile-top-10/
5. SANS Institute (2022). "Real-World Scenarios of QR Code-Based Phishing."