

SRI SIDDHARTHA ACADEMY OF HIGHER EDUCATION

(Declared as Deemed to be University Under Section 3 of the UGC Act, 1956)

Approved by AICTE, Accredited by NBA, NAAC 'A' Grade)

AGALKOTE, TUMAKURU – 572107

KARNATAKA



KSCST Student Project selected for

46th Series of SSP

A Synopsis

On,

“QR CODE – JACKING: AN AUTOMATED PHISHING TOOL”

PROJECT PROPOSAL REF. NO.: 46S_BE_4645



KSCST

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

SRI SIDDHARTHA INSTITUTE OF TECHNOLOGY

(A Constituent College of Sri Siddhartha Academy of Higher Education,

Approved by AICTE, Accredited by NBA, NAAC 'A' Grade)

MARALUR, TUMAKURU-572105

2022-2023

- 1) **PROJECT REFERENCE NUMBER** – 46S_BE_4645
- 2) **TITLE OF THE PROJECT:** QR Code – Jacking: An Automated Phishing Tool
- 3) **NAME OF THE COLLEGE & DEPARTMENT:**
 - 2.1. **Name of the college:** SRI SIDDHARTHA INSTITUTE OF TECHNOLOGY
 - 2.2. **Name of the department:** DEPARTMENT OF COMPUTER SCIENCE ENGINEERING
- 4) **NAME OF THE STUDENT & GUIDE:**
 - 3.1. **Name of the student:**

AISHWARYA A	(19CS004)
ANIL P ROKHADE	(19CS010)
BASAVARAJ GURUNATH BADIGER	(19CS017)
BHAVANA RAGATE	(19CS020)
 - 3.2. **Name of the Guide:**

Dr. GURUPRAKASH C D
M.Tech., Ph.D., MISTE
Professor, Dept. of CSE
SSIT, Tumakuru – 572105
- 5) **KEYWORDS:** QR-code, phishing, information gathering, phishing URL

6) INTRODUCTION OF THE PROJECT:

QR code hacking refers to the process of exploiting vulnerabilities in QR code systems to gain unauthorized access or steal sensitive information. QR codes, short for Quick Response codes, are two-dimensional barcodes that can be scanned using a smartphone or a QR code reader. These codes are widely used for a variety of purposes such as making payments, sharing contact details, and accessing website URLs.

QR-Code phishing works by creating a QR code that, when scanned, redirects the user to a malicious website or application. The QR code can be printed on a physical object or displayed on a digital screen, such as a website or social media platform. When the user scans the code using their smartphone or other mobile device, the device's camera reads the code and automatically opens the URL encoded in the QR code.

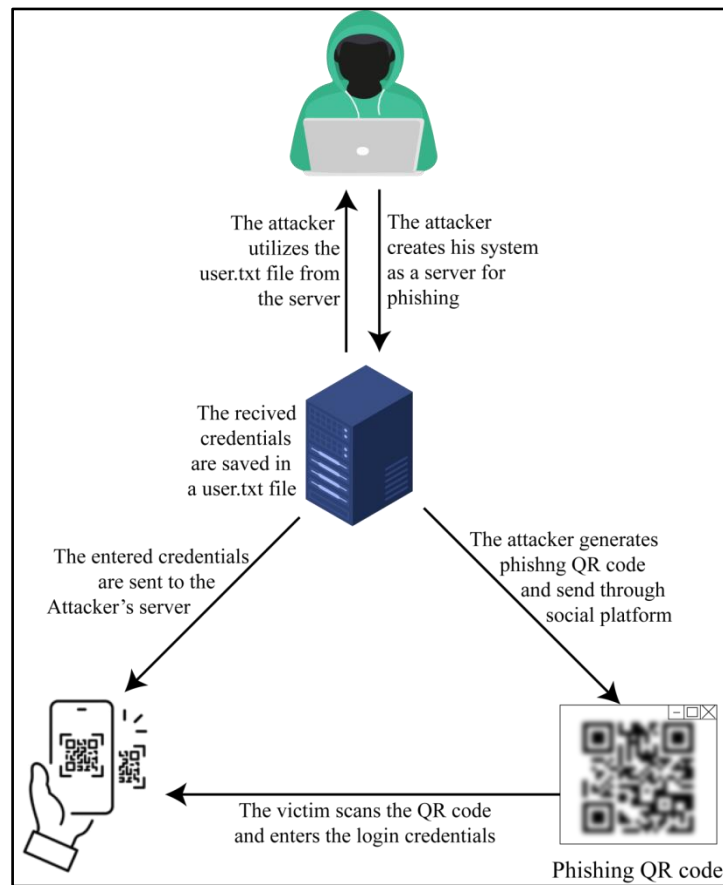
This URL can direct the user to a fake website or application that looks like a legitimate one but is designed to steal sensitive information, such as login credentials or credit card details. The user may be prompted to enter their login credentials, which are then captured by the attacker. In some cases, the malicious website or application may also install malware on the user's device, giving the attacker access to the user's personal data.

7) OBJECTIVES

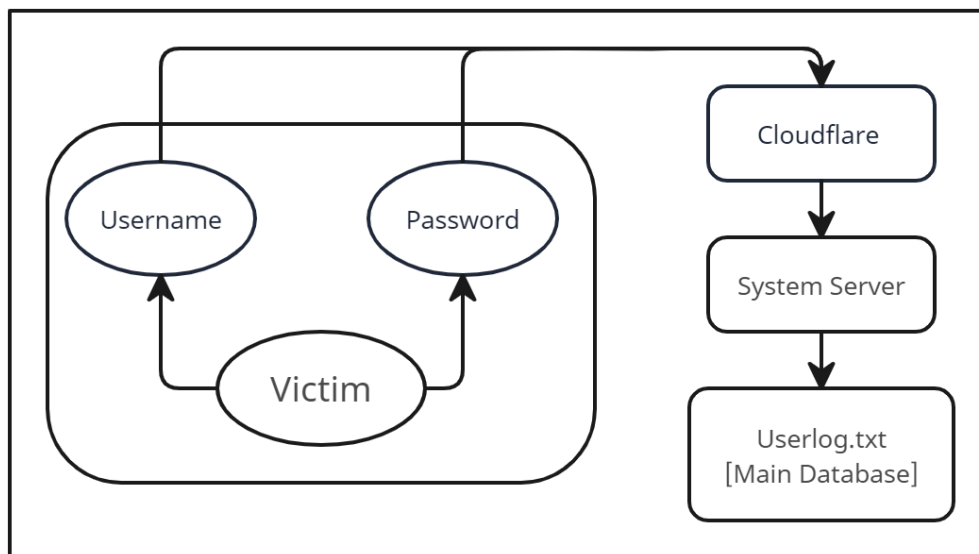
- Identifying vulnerabilities
- Exploiting vulnerabilities
- Recommending improvements
- Raising awareness

Overall, the objective of a QR code hacking project is to improve the security of QR code systems and prevent potential attacks.

8) METHODOLOGY

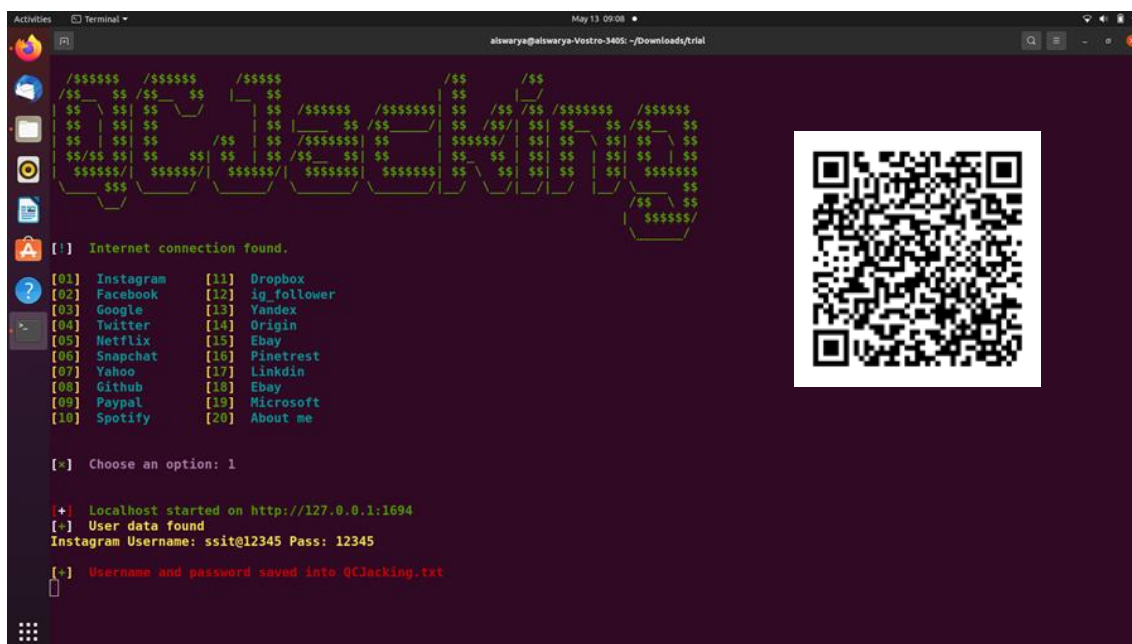


- 1) The attacker initials a client side QR session and clone the Login QR Code into a phishing website.
- 2) The attacker sends the phishing page to the victim.
- 3) The victim scans the QR Code with a specific targeted mobile app. Step 4: The
- 4) Attacker gains control over the victim's account.
- 5) The service is exchanging all the victim's sessions.

DATABASE DESIGN

1. When the victim enters their login information, Cloudflare receives it.
2. Cloudflare is a sizable server network that can boost the security, functionality, and dependability of everything connected to the Internet.
3. Cloudflare gets all of the victim's usernames and passwords.
4. Later the system server (LocalHost) will receive the credential.
5. The userlog.txt file, which is the primary database, will get the login information.

8) RESULTS AND CONCLUSION



```

/##### /##### /##### /## /##
## ## /## ## |## ## /##### /##### ## /## /## /##### /#####
## ## ## /## ## |## ## /##### ## /## /## ## ## ## ## ##
## ## ## /## ## /##### |## ## /##### /## ## /## ## ## ##
#####/##### /#####/#####/##### /## /## /## /## /##
#####/##### /#####/##### /#####/##### /## /## /## /##

[!] Internet connection found.

[01] Instagram [11] Dropbox
[02] Facebook [12] ig_follower
[03] Google [13] Yandex
[04] Twitter [14] Origin
[05] Netflix [15] Ebay
[06] Snapchat [16] Pinetrest
[07] Yahoo [17] Linkdin
[08] Github [18] Ebay
[09] Paypal [19] Microsoft
[10] Spotify [20] About me

[~] Choose an option: 1

[+] Localhost started on http://127.0.0.1:1694
[+] User data found
Instagram Username: ssit@12345 Pass: 12345

[+] Username and password saved into 0CJacking.txt
  
```

RESULT

Select the website from which the phishing link will be generated, [01] The Instagram option was selected. Using the previously constructed phishing link (local host), create the public link. Cloudflare was used to create a public link (dynamic link) in different terminal for port forwarding. The selected website will be updated with the generated public URL. To generate the QR code, run the QR module. Enter the created public link to create a QR Code. The generated public link will be transformed into a QR in png and svg format in current directory. The QR Code will be saved in the current directory.

CONCLUSION

QR code phishing is a growing security threat that exploits the convenience and prevalence of QR codes to trick users into revealing sensitive information. To prevent QR code phishing attacks, users should be educated about the risks and advised to only scan QR codes from trusted sources. Website owners should also take steps to secure their websites and detect any unauthorized changes to their content.

In conclusion, QR code phishing is a serious security threat that requires vigilance and proactive measures to prevent. By following best practices and implementing strong security measures, individuals and organizations can reduce their risk of falling victim to these types of attacks.

9) SCOPE FOR FUTURE WORK

As technology continues to advance, it is likely that QR code phishing attacks will evolve and become more sophisticated. Here are some potential future developments for QR code phishing:

1. Integration with augmented reality
2. Use of social engineering techniques
3. Advanced malware payloads
4. Targeted attacks
5. Cross-platform attacks

To stay ahead of these potential developments, it is important for individuals and organizations to stay informed about the latest security threats and to implement strong security measures, such as regularly updating software and using multi-factor authentication. Regular security testing and penetration testing can also help identify potential vulnerabilities and address them before they can be exploited by attackers.