e-ISSN: 2582-5208

International Research Journal of Modernization in Engineering Technology and Science

(Peer-Reviewed, Open Access, Fully Refereed International Journal)

Volume:06/Issue:04/April-2024 Impact Factor- 7.868 www.irjmets.com

SECURING WEB TRANSACTIONS: A NOVEL APPROACH USING EXTENDED VISUAL CRYPTOGRAPHY, QR CODE INTEGRATION, AND OTP SPLITTING

Piyush Singh*1, Tushar Prakash*2, Dr. Saritha Chakrasali*3

*1,2Information Science And Engineering, B.N.M. Institute Of Technology, Bengaluru, India.

*3Professor & Head (T&P), Information Science And Engineering, B.N.M. Institute Of Technology, Bengaluru, India.

DOI : https://www.doi.org/10.56726/IRJMETS54480

ABSTRACT

In the current digital age, ensuring the security of web applications is of utmost importance, particularly due to the threats posed by Server-Side Request Forgery (SSRF) and Cross-Site Request Forgery (CSRF) vulnerabilities. Conventional methods of mitigation often prove inadequate in delivering comprehensive defense against these complex attack vectors. This study presents an innovative approach to tackling SSRF and CSRF vulnerabilities by leveraging Extended Visual Cryptography (EVC) and integrating QR codes. Extended Visual Cryptography expands upon the concepts of Visual Cryptography, providing improved flexibility and effectiveness in sharing images. By incorporating QR codes into security protocols, our methodology aims to securely transmit cryptographic shares, thus reducing the risks associated with SSRF and CSRF attacks. Through an extensive review of existing literature, theoretical examination, and practical assessment, we illustrate the viability and efficacy of our proposed strategy. Our results underscore the potential of EVC and QR code integration in enhancing the security of web applications and offer valuable insights for future exploration in this field.

Keywords: Extended Visual Cryptography (EVC), OTP Splitting, SSRF Prevention, CSRF Mitigation, QR Code Integration.

I. INTRODUCTION

Server-Side Request Forgery (SSRF) and Cross-Site Request Forgery (CSRF) vulnerabilities represent significant menaces to the security of web applications within the contemporary digital environment. SSRF attacks transpire when a malevolent actor can prompt the server to execute unintended requests on their behalf, potentially resulting in unauthorised entry to internal systems or sensitive information. Conversely, CSRF attacks encompass duping a user's browser into dispatching unauthorised requests to a web application for which the user is authenticated, leading to activities such as account hijacking or unauthorised transactions [3].

The pervasiveness of these vulnerabilities accentuates the crucial necessity for robust mitigation methodologies. Conventional strategies for mitigating SSRF and CSRF vulnerabilities commonly hinge on input validation, token-based authentication, and other server-side mechanisms. Even though these approaches are somewhat effective, they may not furnish comprehensive safeguarding against intricate attack vectors.

Visual Cryptography (VC) has surfaced as a promising cryptographic methodology for safeguarding the transmission of sensitive data. VC entails encoding a clandestine image into multiple shares, each of which does not divulge any information about the original image independently but collectively reconstruct the secret. This attribute renders VC especially appropriate for secure data distribution and authentication.

Expanding on the principles of Visual Cryptography, Extended Visual Cryptography (EVC) broadens the functionalities of conventional VC schemes by permitting more adaptable and effective image distribution. Through the utilisation of EVC, it could be plausible to elevate the security of web applications and alleviate vulnerabilities like SSRF and CSRF.

Additionally, the assimilation of Quick Response (QR) codes into security protocols introduces a captivating pathway for enhancing security measures. QR codes, with their capacity to encode diverse forms of information, including cryptographic shares, present a convenient and accessible approach to securely transmitting sensitive data.

In this manuscript, we advocate an innovative strategy for thwarting SSRF and CSRF attacks by employing Extended Visual Cryptography and integrating QR codes. We will scrutinise the theoretical underpinnings of Visual Cryptography, delve into the potential advantages of EVC within the realm of web application security, and explore the feasibility of leveraging QR codes to amplify the efficacy of SSRF and CSRF mitigation methodologies.

II. LITERATURE REVIEW

1. Server-Side Request Forgery (SSRF) and Cross-Site Request Forgery (CSRF) vulnerabilities persist as ongoing challenges to the security of web applications, necessitating the implementation of robust mitigation strategies to counter potential exploits [2]. This section offers a thorough examination of the current literature on techniques for preventing SSRF and CSRF, along with insights into the integration of Visual Cryptography (VC) and Quick Response (QR) codes in security protocols.

2. SSRF vulnerabilities empower malicious actors to manipulate requests on the server side, potentially resulting in unauthorised access to internal systems or sensitive data. Traditional mitigation methods encompass input validation, token-based authentication, and server-side access controls. Nonetheless, recent research has shed light on the shortcomings of these strategies in addressing intricate SSRF attack scenarios, especially those involving dynamic request routing and integration with third-party services.

Similarly, CSRF vulnerabilities introduce substantial risks to web applications by enabling attackers to deceive users' browsers into executing unauthorised actions. Existing CSRF prevention strategies centre around mechanisms like Same-Site Cookies, Double Submit Cookies, and Anti-CSRF tokens. While effective in numerous instances, these approaches may be vulnerable to exploitation in specific conditions, such as cross-origin interactions and multi-step workflows.

3. Visual Cryptography (VC) has emerged as a promising cryptographic method for ensuring secure data transmission and authentication. VC schemes encode a confidential image into multiple shares in a manner where no individual share discloses any information about the original image. The secret image only becomes visible when the shares are combined, offering a reliable approach for secure data sharing.

Several VC schemes have been put forth in the literature, including (2,2) and (2,n) threshold VC, each presenting distinct trade-offs between security, share size, and reconstruction complexity[1]. Extended Visual Cryptography (EVC) enhances the capabilities of traditional VC schemes by enabling more flexible and efficient image sharing, making it well-suited for applications requiring dynamic access control and privacy preservation [4].

QR codes have become widely adopted as a versatile method for encoding information, providing benefits such as simplicity, accessibility, and compatibility with mobile devices. Within security protocols, QR codes present an intriguing opportunity for improving authentication mechanisms, secure data transfer, and user engagement [4]. Prior studies have delved into the utilisation of QR codes in various security scenarios, including two-factor authentication, secure document exchange, and cryptographic key transfer. Through encoding cryptographic shares or authentication tokens within QR codes, sensitive data can be securely transmitted between parties, mitigating risks related to interception or tampering.

III. PROPOSED SCHEME: ENHANCING WEB APPLICATION SECURITY AGAINST SSRF AND CSRF

In light of the enduring dangers presented by Server-Side Request Forgery (SSRF) and Cross-Site Request Forgery (CSRF) vulnerabilities found in web applications, a new framework is suggested that exploits Extended Visual Cryptography (EVC), incorporation of QR codes, and utilisation of One-Time Passwords (OTPs) to bolster security protocols. The primary objective of our framework is to hinder unauthorised requests and transactions through the introduction of a multi-factor authentication system that mandates active user involvement and validation.

1. OTP Generation and Splitting:

- Initiation commences with the generation of a cryptographically sound One-Time Password (OTP) through a reliable algorithm or service. This OTP functions as a unique identifier for the respective transaction or request.

- Following this, the OTP undergoes a division process resulting in two random OTPs facilitated by a secure splitting algorithm. These divisions are executed in a manner that ensures neither individual OTP discloses any details regarding the original OTP.

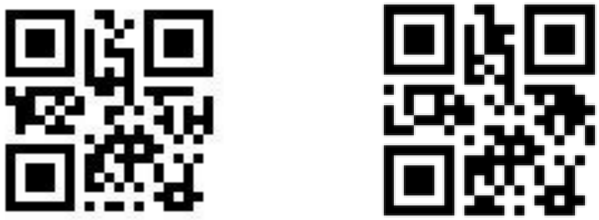
- Subsequently, the initial OTP undergoes hashing utilising a secure hashing algorithm (e.g., MD5) and is securely stored within the server's database. This hashed OTP acts as a point of reference for authentication during the transaction validation phase.

2. QR Code Encoding and User Interaction:

- One of the OTP divisions is transformed into a QR code image via a trustworthy QR code generation library. This QR code is then dispatched to the user through a secure communication channel, such as email or SMS.

- Concurrently, the other OTP division is exhibited on the payment page or transaction interface, accompanied by guidelines for the user to proceed.

- The QR code functions as a visual representation of a segment of the OTP, while the displayed division operates as the corresponding part.



Split 1 Split 2

Fig. 1: Sample QR Code Splits Generated by the Algorithm for Enhanced Security

3. Transaction Approval Process:

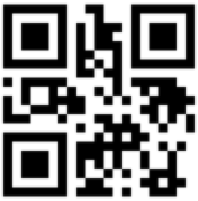
- In order to authorise a transaction or request, the user is required to actively engage in the authentication procedure by scanning the received QR code and inputting the displayed OTP division on the payment page.

- Upon scanning the QR code, the user acquires one portion of the OTP, while the remaining part is visible on the payment page.

- The user is then mandated to manually input the displayed OTP division to finalise the OTP verification process.

- Solely when both OTP divisions are amalgamated and align with the original hashed OTP preserved on the server, is the transaction sanctioned and executed. Otherwise, the transaction is rejected, thereby reducing the likelihood of unauthorised requests or transactions.

Table 1: OTP Split Methodology for Enhanced Security

Original OTP	6647
Hashed OTP	8ce8b102d40392a688f8c04b3cd6cae0
Split 1: Shown to User on payment gateway	

Original OTP	6647
Split 2: Sent Securely	

4. Security Implications and Considerations:

- Through the division of the OTP and utilisation of QR code integration, our framework introduces a multi-factor authentication mechanism necessitating active involvement from the user.

- The incorporation of QR codes enriches user experience by furnishing a convenient and secure avenue for transmitting confidential data.

- Furthermore, the hashing of the initial OTP guarantees that even if one OTP division is compromised, the transaction's security remains intact, as validation necessitates both divisions.

IV. CONCLUSION

In conclusion, our proposed scheme offers a robust solution for mitigating SSRF and CSRF vulnerabilities in web applications by combining Extended Visual Cryptography, QR code integration, and One-Time Passwords.

- By requiring active user participation and verification, our scheme enhances security measures while maintaining usability and convenience.
- Future research may focus on further enhancing the scalability and efficiency of the proposed scheme, as well as evaluating its effectiveness in real-world deployment scenarios.

This proposed scheme integrates various security techniques to address the specific challenges posed by SSRF and CSRF vulnerabilities, offering a holistic approach to enhancing web application security. Further refinement and validation through rigorous testing and evaluation will be crucial in ensuring its effectiveness and practicality in real-world applications.

V. REFERENCES

[1] Vineetha, K. R., & Sinu, Habeeba. "Design And Implementation of Secure Qr Payment Based on Visual Cryptography." International Journal for Multidisciplinary Research (IJFMR) 5(2), 1-10 (2023).

[2] Cao, X., Feng, L., Cao, P., & Hu, J. "Secure QR Code Scheme Based on Visual Cryptography." Conference Paper. January 2016. DOI: 10.2991/aiie-16.2016.99.

[3] Mirzaei, O., Jabiyev, B., Kharraz, A., & Kirda, E. "Preventing Server-Side Request Forgery Attacks." Conference Paper. December 2020. DOI: 10.1145/3412841.3442036.

[4] Fu, Z., Cheng, Y., & Yu, B. "Visual Cryptography Scheme With Meaningful Shares Based on QR Codes." IEEE Access. October 8, 2018. DOI: 10.1109/ACCESS.2018.2874527.

[5] Jianfeng Lu, Zaorang Yang, Lina Li, Wenqiang Yuan, Li Li, Chin-Chen Chang, "Multiple Schemes for Mobile Payment Authentication Using QR Code and Visual Cryptography", Mobile Information Systems, vol. 2017, Article ID 4356038, 12 pages, 2017. https://doi.org/10.1155/2017/4356038