PRISMA METHODOLOGY CHECKLIST

|  |  |  |  |
| --- | --- | --- | --- |
| Section/topic | Item number | ITEM CHECKLIST | Section/page |
| TITLE | 1 | QUICK RESPONSE CODE SECURITY ATTACKS AND COUNTERMEASURES: A SYSTEMATIC LITERATURE REVIEW | Page1 |
| Abstract | 2 | Included a summary (background, objectives, methods, results, and conclusion) | Page 1 |
| Introduction | | | |
| Rationale/objectives | 3 | This study aims to investigate Quick response codes security vulnerabilities and countermeasures | Section 1, page 1 |
| Research questions | 4 | To achieve the objective, the study addresses the following research questions;  RQ1: What are the different types of QR code attacks?  RQ2: What techniques exist for detecting QR code attacks? | Page 1 |
| Methods | | | |
| Eligibility criteria | 5 | Inclusion criteria: articles (1) published within the last 13 years, (2) written in English, and (3) focused on QR code security, vulnerabilities, and detection measures. Conversely, articles were excluded if they (1) were review papers, (2) did not directly address QR code security challenges, (3) were published before 2010, or (4) lacked relevance to QR code attacks. After applying these criteria, a total of 50 articles were deemed eligible and included in the final study | Section 4, page 10-12 |
| Data sources | 6 | Databases searched: IEEE Xplore, ACM, Elsevier, Springer, ScienceDirect, Wiley, Google Search. | Page 10-12 |
| Search strategy | 7 | The selected articles were assessed using six criteria: source, method/technique, attack strategy, detection strategy, and others. Keywords included terms such as "QR code," "QR code security," "QR attacks," "QR code attack detection techniques," and "QR code attack prevention." | Section 4.1, page 10 |
| Risk of bias | 8 | Used PRISMA methodology, use of multiple databases, clear inclusion and exclusion criteria | Section 4 |
| Results | | | |
| Included studies | 9 | 50 articles that met the exclusion criteria were included in the study | Page 10-12 |
| Synthesis of results | 10 | 50 relevant studies published between the year 2010 and 2024 were identified. | Page 10-12 |
| Discussion and interpretation | | | |
| RQ1: What are the different types of QR code attacks? | 11 | phishing, pharming, malware propagation, cross-site scripting, and Structured Query Language/command injection and reader applications attacks | Section 2 (page 2-4), 4.3.1, page 12-13 |
| RQ2: What techniques exist for detecting QR code attacks? | 12 | Techniques such as cryptographic scheme, machine learning, artificial intelligence, two factor authentication, One Time password, and mutual authentication schemes have been used | Section 3 (page 5-10), 4.3.2 page 13-16 |
|  |  |  | Section |
| Other | | | |
| Funding | 13 | The author(s) received no specific funding for this study. | Page 18 |
| Conflict of interest | 14 | The authors declare they have no conflicts of interest to report regarding the present study | Page 18 |
|  |  |  |  |