Analyzing Security Risks in Browser Extension Search Tools: A Literature Review

Malik Sadaf Allauddin[1], Prashant Lokhande[2]

[1] Computer Department, Pillai College of Engineering, New Panvel, Mumbai,Maharashtra - 410206, India

[2] Professor, Computer Department, Pillai College of Engineering, New Panvel,Mumbai, Maharashtra - 410206, India

ABSTRACT

The literature review titled "Analyzing Security Risks in Browser Extension Search Tools" explores the growing interconnection between the digital and physical domains and the vulnerabilities and threats that accompany it. The study highlights how the Darkweb can be used for communication and anonymity, but because it is encrypted, it presents difficulties for law enforcement. Although browser extensions are essential for improving user experiences when browsing, they also offer security vulnerabilities like cross-site scripting and privilege escalation that can be used maliciously. The study emphasizes the necessity of better detection techniques for malicious extensions using Static and dynamic analysis combined, as well as the significance of advanced threat analysis and AI integration to foresee and mitigate cyber attacks.In order to improve the practical applicability of security measures, the study also urges a deeper comprehension of user behaviors and socioeconomic dynamics inside the Darkweb ecosystem. In order to successfully handle evolving cyber risks, future research topics include developing automated security testing procedures, upgrading authorship attribution algorithms for user privacy, and developing tools such as the WAP static analysis tool.

Keywords: Browser add-ons, security hazards, Darkweb, online threats, sophisticated threat analysis, artificial intelligence integration, methods of detection, user conduct, and acknowledgment of authors WAP tool, cybersecurity, and automated security testing.

1. Introduction

The physical and digital realms are becoming increasingly merged every day, and the modern world is more connected than it has ever been[1]. In addition to benefits, living in a digitally connected society raises the possibility of fraud, theft, and other online abuses. People are more susceptible to cyberattacks as they become more dependent on contemporary technologies[1]. Furthermore, a cyberattack is not restricted to a specific region or nation; rather, the digitally connected globe is global[1]. It can occur remotely from any location in the globe. Internet users may seek anonymity and identity protection for a variety of reasons.

Users of the network use the Darkweb, an anonymous, encrypted, and extremely private communication channel[1]. Since the dark web's main feature is its anonymity, law enforcement agencies (LEAs) find it challenging to track down the Users of the dark web and the IP addresses of hosted services who use them to access hidden services, which is why criminals choose to operate there[1].

By installing browser extensions, users of modern web browsers can enhance and personalize their browsing experience[2]. These extensions' functionalities might include everything from altering a website's looks to adding accessibility features, obstructing adverts, and enhancing security and privacy[2].

However, only a small percentage of extensions could cause security or privacy problems are malicious[4]. Indeed, by utilizing an extension's features, an attacker can escalate their privileges by abusing it[4]. To do this, a hacker can use an extension's communication channels to transmit payloads that are specifically designed to take advantage of its weaknesses to the extension. These flaws may result in sensitive user data exposure or universal cross-site scripting (XSS), which allows code to run on any website—even [4]without a flaw in the website itself. These susceptible extensions are harder to find than malicious ones because of their essentially good intentions, such as the fact that they are not acting suspiciously[4]. Additionally, even though they do need strong privileges.

In contrast to browser plugins, extensions are made up of HTML, CSS, and JavaScript[6]. However, they can change webpages at will and get beyond the browser's SameOrigin Policy thanks to privileged APIs. Malicious browser[6] extensions have previously exploited this capability to take control of session cookies, alter website content at will, steal user information, and show users intrusive advertisements[6].

PHP is the most used language for online applications, and WAP [7] is a new free and open-source static analysis program that finds weaknesses in eight different categories of PHP code[7]. With over 6700 downloads listed on SourceForge, it appears to be well-liked[7].
The program installs minor PHP code modifications to address vulnerabilities and employs data mining to predict false positives, or false security alerts[7]. However, it can be seen from examining its source code that WAP is difficult to expand for additional vulnerability classes[7].

As the digital and physical worlds continue to blend together, society becomes more interconnected, which has advantages but also poses serious hazards, especially in the case of anonymous, worldwide cyberattacks. Because of its strong anonymity qualities, the Darkweb is a sanctuary for cybercriminals, which makes law enforcement activities difficult. Furthermore, the extensive use of browser extensions—which are meant to improve user experience—may unintentionally result in the introduction of security flaws. Even though these extensions typically serve good reasons, they can be used maliciously to carry out tasks like cross-site scripting and privilege escalation. In this particular case, strong security measures are necessary because the PHP language is widely used in web application development. The identification and mitigation of vulnerabilities in PHP code are made possible in large part by tools such as the WAP static analysis tool. WAP has limitations when it comes to extending its capability to cover new vulnerability classes, despite its widespread use and efficacy. In order to ensure complete security for web applications, future research must concentrate on improving these technologies To be up to date with the always changing online threat scenario.

2. Literature Review

Ch A S Murty, Harmesh Rana et al.(2023) authors said that the methodology put forth in the study takes a thorough approach to finding weaknesses in web apps that are available on the dark web. To find dark web sites, URL mining and data collection are the first steps. Automated and manual testing are then used to check for security vulnerabilities and confirm findings. The vulnerabilities are then categorized and prioritized using different vulnerability assessment approaches[1]. In order to comprehend the security posture of dark web sites, an additional comparison with analogous websites on the surface web is made. By enhancing the identification and evaluation of security threats on the hidden network, this multi-step procedure seeks to improve web application security on the dark web by offering insightful information.

Benjamin Eriksson, Pablo Picazo-Sanchez et al. (2022) authors state that the methodology employed in this paper involves a methodical analysis of the browser extension ecosystem's attack entry points, utilizing Static and dynamic analysis combined techniques to identify vulnerabilities and potential attacks. By examining the behavior

of extensions in various scenarios, including password stealing and inter- extension history poisoning, the research aims to uncover novel security risks and assess the prevalence of these threats in real-world settings. Additionally, a thorough analysis of well-known "New Tab" extensions is conducted to provide insights into specific vulnerabilities and potential attack vectors[2]. Countermeasures to address the identified issues are proposed to enhance the security of browser extensions and mitigate the risks associated with malicious activities.

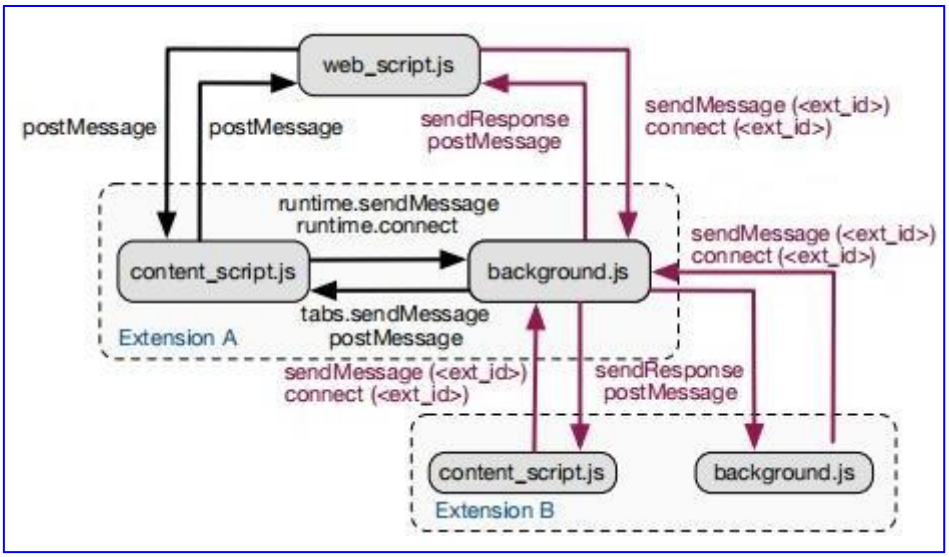

Figure 1: Browser extensions and message forwarding[2]

Shahriar Sobhan, Timothy Williams et al. (2022) author state that in order to examine numerous publications pertaining to the topic, the study technique on the dark web comprised a methodical assessment of relevant research papers were found by doing searches utilizing particular keywords, such as "Dark Web" and "Cybersecurity," [3]in reliable scientific databases. Based on publication subjects and time constraints, the paper classification process—which was inspired by earlier works—aided in eliminating unrelated studies[3]. The C4.5 technique for decision tree generation, Random Forest (RF) technique for classification tasks, and Bayesian Networks (BNs) for modeling dependent connections are some of the equations listed in the document. These approaches and formulas are crucial for comprehending the dark web's tendencies and difficulties.

Aurore Fass, Dolière Francis Somé et al. (2021) writer said that double uses an abstraction of the extension code into an Extension Dependence Graph (EDG) that contains information on control flows, data flows and pointer analysis to identify susceptible data flows in browser extensions statically. Through the observation of interactions within and outside of an extension, this EDG enables the identification of dubious data flows between security-critical APIs and external parties. Data flow analysis is performed by adding data flow edges to the Control Flow Graph (CFG) to create a Program Dependency Graph (PDG), which is used to track variable dependencies and calculate variable values[4]. By implementing CFG, control flow analysis can be improved by reasoning about possible execution paths depending on conditions. To examine the messages that are transferred between extension components and outside entities, message flow analysis is done[4].
The following equations are employed in this methodology: Pointer Analysis =

{Variable Value Computation Principles}, CFG = {Statement Nodes + Control Flows}, and EDG = {AST + Control Flows + Data Flows + Pointer Analysis}[4].

Ehsan Arabnezhad, Massimo La Morgia et al. (2020) authors said that by connecting aliases across various forums and de-anonymizing Dark Web users, the methodology outlined in the PDF file aims to shatter pseudo-anonymity on the Dark Web[5]. Using text pre-processing techniques like tokenization and lemmatization, the strategy takes advantage of writing style and behavioral patterns to extract features like word and character n-grams. In order to efficiently manage big datasets, the methodology entails computing cosine similarity between known and unknown profiles, sorting the results, and using iterative batch processing[5]. Performance is evaluated using accuracy and recall measurements, and precision-recall curves are produced. The extracts given do not explicitly include any equations related to the technique[5].

Nikolaos Pantelaios, Nick Nikiforakis, et al. (2020) authors told that a multifaceted technique integrating user feedback analysis, keyword extraction, anomaly identification in extension ratings, and cluster analysis of extension code deltas is the methodology used in the paper to detect malicious browser extensions[6]. The system can effectively identify potentially malicious behavior in extensions by clustering extension versions based on API sequences with the DBSCAN[6] algorithm, identifying anomalies in extension ratings using Anomalize statistical techniques, and calculating trustworthiness scores for keywords based on average ratings of reviews containing them. The paper employs statistical techniques for detecting anomalies in extension ratings and computes trustworthiness scores by averaging reviews thatcontain particular keywords.

Ib´eria Medeiros, Nuno Neves et al. (2016) authors said that the modified WAP tool, an open-source static analysis tool designed specifically for identifying vulnerabilities in PHP web applications, is the main tool used in this paper's methodology. With its modular and extensible design, this improved version of WAP makes it easier to identify and address new sorts of vulnerabilities without requiring extra coding[7]. The program finds both known and zero-day vulnerabilities by thoroughly analyzing large amounts of code from various packages in order to assess its effectiveness. To assess classifier performance, a number of measures are produced, such as True Positive Rate, False Positive Rate, Predictive value that is positive, Specificity, Precision, Precision, Informedness, and Jaccard Similarity[7]. These metrics demonstrate how WAP's modular and extendable nature improves vulnerability detection, reduces false positives, and provides insights for strengthening security in PHP online applications. They are computed using formulas specific to each.

Formulas[7]:

1. The True Positive Rate (tpp/recall) is expressed as Tp / (tp + fn)[7].
2. The False Positive Rate (pfp/fallout) is expressed as fp / (tn + fp)[7].
3. Tp / (tp + fp) is the Positive Predictive Value (prfp/precision)[7].
4. Specificity (pd) = (tn + fp) / tn[7]
5. tn / (tn + fn) is the inverse positive predictive value (ppd).
6. Accuracy: N / (tp + tn)[7]
7. Accuracy: (ppd + prfp) / 2
8. Knowledge: tpp - pfp = tpp + pd - 1

9. Similarity to Jaccard: tp / (tp + fn + fp)[7]

3. Observation

1) Limited Attention to Exploitation Techniques: While discovering vulnerabilities in web apps on the dark web is the main focus of the article, there isn't much discussion of the exploitation strategies that cybercriminals employ to take advantage of these flaws. Gaining insight into how vulnerabilities are exploited can be very helpful in improving security protocols.

i) Advanced Threat Analysis: To improve defensive planning, future study should concentrate on comprehending the tactics employed by advanced threat actors on the dark web.

ii) AI for Security: Improving security preparedness can be achieved by investigating machine learning and AI for dark web threat prediction.

iii) Law Enforcement Cooperation: Sharing insights about the dark web with law enforcement can help battle cybercrime more successfully.

iv) Constant Monitoring: By keeping ahead of emerging threats, continuous monitoring and threat intelligence collecting helps strengthen security.

2) The research discussed in "Hardening the Browser Extension Security Analysis" fills in a number of holes in the body of knowledge regarding browser extension security. The paper's methodical examination Numerous points of entry for attacks within the ecosystem of web browser extensions is one of its main contributions; it aids in the identification of potential threats and vulnerabilities that may have gone unnoticed in earlier studies. The report highlights new security threats that extensions provide to users by concentrating on unique attacks like password stealing, traffic stealing, and inter-extension assaults.

i) Improved Detection Techniques: To find and address security flaws in browser extensions, detection techniques are being developed further. This involves combining static and dynamic analysis.

ii) Behavioral Analysis: To comprehend how extensions interact with web pages and any potential security ramifications, conduct a thorough behavioral analysis of the extensions.

iii) Automated Security Testing: To make the process of finding vulnerabilities more efficient, researching the viability of automated security testing solutions for browser extensions.

iv) User Education and Awareness: Investigating methods to raise user knowledge of the dangers of installing extensions and provide advice on how to use them securely.

v) Extension Permission Models: Investigating methods to improve extension permission models to restrict access to private user information and lessen attack surface.

3) With less attention on the socioeconomic factors and user behaviors inside the dark web ecosystem, the article primarily focuses on methods for minimizing difficulties related to the dark web. It also doesn't provide a comparison evaluation of the merits of other technologies, such as crawling methods and machine learning. Moreover, the technologies and approaches covered are mainly theoretical and lack empirical support from case studies or real-world applications.

Future research should examine the socioeconomic dynamics of the dark web, taking into account market trends, user motives, and how laws affect illegal activity. The best techniques for gathering information and analyzing threats can be found by conducting comparative research on the different technologies utilized in dark web analysis. Furthermore, the practical applicability of the discussed approaches will be improved by putting them to use in real-world circumstances and assessing their effectiveness through empirical investigations. Targeted security measures and a better understanding of the dark web ecosystem can be achieved by analyzing user behaviors, trust dynamics, and interaction patterns.

4) Although DoubleX is primarily concerned with identifying security and privacy risks in browser extensions, more research into how these flaws affect end users may be warranted. Gaining insight into how these vulnerabilities could be used in practicalsituations and the possible repercussions for users could be beneficial.
Subsequent investigations may improve DoubleX's capacity to identify sophisticated vulnerabilities like as injection attacks and privilege escalation. To better identify and mitigate security issues in browser extensions, it would be beneficial to combine static and dynamic analysis. Furthermore, designing more safe and user-friendly extensions may result from analyzing the usability and user experience of security mechanisms. Creating automated solutions to fix discovered vulnerabilities could make it easier for engineers to improve security.

5) The study that is included in the PDF file tackles the important problem of using authorship attribution strategies to connect actual Internet identities with Dark Web aliases. The work highlights a significant research gap pertaining to the advancement of software tools that can anonymize writing patterns, with the aim of augmenting user privacy and security during online interactions. The study also emphasizes how difficult it is to evaluate approaches when There is not enough of readily available actuality data, indicating the necessity for more reliable validation methods in tasks involving huge amounts of authorship attribution.
Subsequent investigations ought to concentrate on creating sophisticated instruments that conceal writing styles and safeguard users' privacy when interacting online. The precision of authorship attribution algorithms can be raised by investigating automated and crowdsourced validation techniques. Furthermore, improving these methods' efficiency and scalability is essential for managing massive data volumes. Designing safe and easy-to-use privacy tools can benefit from research on user behavior and understanding of online anonymity.

6) A number of significant holes in the realm of browser security are filled by the research on update deltas that is provided in the paper on the detection of malicious browser extensions. This study closes a significant research gap by developing scalable methods for identifying and detecting harmful extensions in the enormous and ever-changing market for extensions. The suggested system provides a promising first step in filling this gap by concentrating on the deltas of browser extensions and using previously identified dangerous extensions to identify new ones.
In the future, there exist multiple avenues for prospective investigation and improvement. Future work may focus on enhancing the clustering algorithms that are used to examine extension code deltas, possibly by using machine learning methods to increase the precision and efficacy of detecting harmful clusters. Furthermore, investigating how behavior-based analysis and anomaly detection techniques might be integrated could improve the system's capacity to identify zero-day assaults and new dangers in browser extensions. Additionally, examining how user behavior and interaction with extensions affect security concerns may yield important information for creating security protocols that are stronger. In summary, this paper's research establishes a strong basis for subsequent investigations to further enhance the identification and alleviation of malicious browser extensions within a dynamic threatenvironment.

7) A significant gap in the field of software security is addressed by the research article on providing the "weapons"-equipped WAP tool for finding new vulnerability classes in web applications. The challenge of expanding current open source static analysis tools to efficiently detect new vulnerability classes is the main research gap noted in the report. The authors' proposal for An interchangeable and expandable WAP tool version represents a considerable advancement in addressing this constraint.

Future research can enhance the detection capabilities of static analysis tools like WAP to identify a wider range of vulnerabilities using new techniques or algorithms for improved accuracy and coverage. Additionally, automating the correction process further could be valuable, with tools not only identifying vulnerabilities but also suggesting and implementing fixes. Integrating these tools into the software development lifecycle, through plugins for popular IDEs, could facilitate seamless security checks during development. As web applications grow in

complexity, optimizing the performance and scalability of tools like WAP is crucial for handling large codebases efficiently. Furthermore, adapting these tools to address vulnerabilities in emerging technologies such as cloud computing, IoT, and AI will ensure they remain effective in the evolving tech landscape.

4. Conclusion And Knowledge Gaps

The various security threats connected to browser extensions and the dark web have been thoroughly examined in this study, highlighting the significance of improved detection and mitigation techniques. The merging of the digital and physical realms has resulted in a rise in cyberthreats, especially via anonymous platforms such as the dark web and seemingly innocuous browser extensions that can be misused for malevolent intent.

The main conclusions of this study point out a number of shortcomings and possible enhancements in the present approaches for vulnerability identification and management:

i) Dark Web Vulnerabilities: To anticipate and reduce cyber threats, advanced threat analysis and AI integration are required. Continuous monitoring and cooperation with law enforcement are crucial.

ii) Security of Browser Extensions: Better detection methods combining static and dynamic analysis are required. The development of automated security testing techniques and an understanding of user behavior are essential for dealing withharmful extensions.

iii) Socioeconomic Dynamics of the Dark Web: To make theoretical approaches more applicable, actual research on the socioeconomic aspects and user behaviors within the dark web is necessary.

iv) DoubleX Tool and Privacy: More investigation is needed to determine how vulnerabilities affect users in the actual world. Static and dynamic analysis should be combined, and vulnerability solutions should be automated.

v) Authorship Attribution: By increasing the precision of authorship attribution algorithms and creating scalable solutions for big datasets, improved tools are required to safeguard user privacy.

vi) Finding Malevolent Extensions: Techniques for behavior-based and scalable analysis are crucial. Future research ought to incorporate anomaly detection and enhance clustering techniques.

vii) WAP Tool Enhancement: It's critical to expand the WAP tool's capacity to identify fresh vulnerabilities in PHP web applications. Automation, including security checks into development, and adjusting to new technologies like cloudcomputing, IoT, and AI should be the main areas of concentration.

REFERENCES

1. Murty, C. A., Rana, H., Verma, R., Pathak, R., & Rughani, P. H. (2021, October). A review of web application security risks: Auditing and assessment of the dark web. In 2021 International Conference on Electrical, Computer, Communications and Mechatronics Engineering (ICECCME) (pp. 1-7). IEEE.

2. Eriksson, B., Picazo-Sanchez, P., & Sabelfeld, A. (2022, April). Hardening the security analysis of browser extensions. In Proceedings of the 37th ACM/SIGAPP Symposium on Applied Computing (pp. 1694-1703).

3. Sobhan, S., Williams, T., Faruk, M. J. H., Rodriguez, J., Tasnim, M., Mathew, E., ... & Shahriar, H. (2022, June). A review of dark web: Trends and future directions. In 2022 IEEE 46th Annual Computers, Software, and Applications Conference (COMPSAC) (pp. 1780-1785). IEEE.

4. Fass, A., Somé, D. F., Backes, M., & Stock, B. (2021, November). Doublex: Statically detecting vulnerable data flows in browser extensions at scale. In Proceedings of the 2021 ACM SIGSAC Conference on Computer and Communications Security (pp. 1789-1804).

5. Arabnezhad, E., La Morgia, M., Mei, A., Nemmi, E. N., & Stefa, J. (2020, November). A light in the dark web: Linking dark web aliases to real internet identities. In 2020 ieee 40th international conference on distributed computing systems (icdcs) (pp. 311-321). IEEE.

6. Pantelaios, N., Nikiforakis, N., & Kapravelos, A. (2020, October). You've changed: Detecting malicious browser extensions through their update deltas. In Proceedings of the 2020 ACM SIGSAC conference on computer and communications security (pp. 477-491).

7. Medeiros, I., Neves, N., & Correia, M. (2016, June). Equipping wap with weapons to detect vulnerabilities: Practical experience report. In 2016 46th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN) (pp. 630-637).IEEE.

8. Nayak, A., Khandelwal, R., Fernandes, E., & Fawaz, K. (2024). Experimental Security Analysis of Sensitive Data Access by Browser Extensions.

9. Marimuthu, M., Mohanraj, G., Karthikeyan, D., & Vidyabharathi, D. (2023). Safeguard confidential web information from malicious browser extension using Encryption and Isolation techniques. Journal of Intelligent & Fuzzy Systems, 45(4), 6145-6160.

10. Fowdur, T. P., & Hosenally, S. (2024). A real-time machine learning application for browser extension security monitoring. Information Security Journal: A Global Perspective, 33(1), 16-41.

11. Zonta, T., & Sathiyanarayanan, M. (2024, February). A Holistic Review on Detection of Malicious Browser Extensions and Links using Deep Learning. In 2024 IEEE 3rd International Conference on AI in Cybersecurity (ICAIC) (pp. 1-6). IEEE.

12. Xie, Q., Murali, M. V. K., Pearce, P., & Li, F. Arcanum: Detecting and Evaluating the Privacy Risks of Browser Extensions on Web Pages and Web Content.

13. Rao, P. S. (2023). Analyzing Communications and Software Systems Security.

14. Ursell, S., & Hayajneh, T. (2020). Desktop browser extension security and privacy issues. In Advances in Information and Communication: Proceedings of the 2019 Future of Information and Communication Conference (FICC), Volume 2 (pp. 868-880). Springer International Publishing.

15. Johnson, C. A., Paramiswaran, S., & Mailewa, A. B. Discovering Vulnerabilities in Web Browser Extensions Contained by Google Chrome.

16. Kuchhal, D. (2023). BUILDING TRUST IN THE ONLINE ECOSYSTEM THROUGH EMPIRICAL EVALUATIONS OF WEB SECURITY AND PRIVACY CONCERNS (Doctoral dissertation, Georgia Institute of Technology).

17. Qamar, S., Anwar, Z., & Afzal, M. (2023). A systematic threat analysis and defense strategies for the metaverse and extended reality systems. Computers &Security, 128, 103127.

18. Pour, M. S., Nader, C., Friday, K., & Bou-Harb, E. (2023). A comprehensive survey of recent internet measurement techniques for cyber security. Computers & Security, 128, 103123.

19. Shaikh, M. I., & Lokhande, P. S. (2024). Tackling Threats: A Study of Vulnerability Testing and Mitigation in Web Applications. Available at SSRN 4823623.

20. Bui, D., Tang, B., & Shin, K. G. (2023, May). Detection of inconsistencies in privacy practices of browser extensions. In 2023 IEEE Symposium on Security and Privacy (SP) (pp. 2780-2798). IEEE.

21. Yang, Y., Wang, C., Zhang, Y., & Lin, Z. (2023). Sok: Decoding the super app enigma: The security mechanisms, threats, and trade-offs in os-alike apps. arXiv preprint arXiv:2306.07495.

22. Sathvik, D., Dhanalakshmi, D., Prahasith, A., Hariharan, S., Pendam, K., & Kukreja, V. (2023, November). Web Extension For Phishing Website Identification: A Browser-Based Security Solution. In 2023 International Conference on Research Methodologies in Knowledge Management, Artificial Intelligence and Telecommunication Engineering (RMKMATE) (pp. 1-5). IEEE.

23. Chia, K., Lee, J., Wan, W., Chua, R., & Guo, H. (2023, August). MalAware: A Tool for Safe Internet Browsing. In IRC Conference on Science, Engineering and Technology (pp. 303-315). Singapore: Springer Nature Singapore.

24. Guru, S. D., Pattnaik, A., Kolte, R., Sharma, N., & Varshapriya, J. N. (2023, July). A Survey Paper on Browser Extensions to Detect Web Attacks. In 2023 14th International Conference on Computing Communication and Networking Technologies (ICCCNT) (pp. 1-7). IEEE.

25. Iqbal, U., Kohno, T., & Roesner, F. (2023). LLM Platform Security: Applying a Systematic Evaluation Framework to OpenAI's ChatGPT Plugins. arXiv preprint arXiv:2309.10254.

26. Shaikh, M. I., & Lokhande, P. S. (2024). Tackling Threats: A Study of Vulnerability Testing and Mitigation in Web Applications. Available at SSRN 4823623.

27. Vlachos, V., Stamatiou, Y. C., & Nikoletseas, S. (2023). The privacy flag observatory: A crowdsourcing tool for real time privacy threats evaluation. Journal of Cybersecurity and Privacy, 3(1), 26-43.

28. Andersson, L. (2023). Detecting reputation manipulation among browserextensions.

29. Sharma, A., & Mishra, S. (2023, December). A Security Analysis of Password Managers on Android. In International Conference on Information Systems Security (pp. 3-22). Cham: Springer Nature Switzerland.

30. Kaur, J., Garg, U., & Bathla, G. (2023). Detection of cross-site scripting (XSS) attacks using machine learning techniques: a review. Artificial Intelligence Review, 56(11), 12725-12769.

31. Sharma, S., & Jevitha, K. P. (2023, December). Security Analysis of OAuth 2.0 Implementation. In 2023 Innovations in Power and Advanced Computing Technologies (i-PACT) (pp. 1-8). IEEE.

32. Tyagi, S., Sawarkar, S. D., & Lokhande, P. Performance and Security Measure of Highly Performed Enterprise Content Management System. International Journal of Computer Applications, 975, 8887.

33. Aslam, F. A., Mohammed, H. N., & Lokhande, P. S. (2015). Efficient Way Of Web Development Using Python And Flask. International Journal of Advanced Research in Computer Science, 6(2).

34. Lokhande, P. S. (2009). Learning from the Past Intrusion Attacks: Digital Evidence Collection to Make e-Commerce Systems More Secure. Conference ICL2009.

35. Tyagi, S., Sawarkar, S. D., & Lokhande, P. (2012). A Critical Analysis Study into the Use of Enterprise Content Management System. In International Conference and Workshop on Emerging Trends in Technology, Mumbai.

36. Lokhande, P. S. (2016). SQL Injection Prevention Using Random4 Algorithm.

37. Shaikh, M. I., & Lokhande, P. S. (2024). Tackling Threats: A Study of Vulnerability Testing and Mitigation in Web Applications. Available at SSRN 4823623.

38. Zimmeck, S., Wang, O., Alicki, K., Wang, J., & Eng, S. (2023). Usability and enforceability of global privacy control. Proceedings on Privacy Enhancing Technologies.

39. Fowdur, T. P., & Hosenally, S. (2024). A real-time machine learning application for browser extension security monitoring. Information Security Journal: A Global Perspective, 33(1), 16-41.

40. Agarwal, S. (2022, November). Helping or Hindering? How Browser Extensions Undermine Security. In Proceedings of the 2022 ACM SIGSAC Conference on Computer and Communications Security (pp. 23-37).

41. Xie, Q., Murali, M. V. K., Pearce, P., & Li, F. Arcanum: Detecting and Evaluating the Privacy Risks of Browser Extensions on Web Pages and Web Content.