International Journal for Modern Trends in Science and Technology
Volume 10, Issue 02, pages 1170-121.
ISSN: 2455-3778 online
Available online at: http://www.ijmtst.com/vol10issue02.html
DOI: https://doi.org/10.46501/IJMTST1002016

Develop a Purposely Insecure Web Application for Practicing Security Testing

B.Venkateswara Reddy, Kajjam Pavithra, Vakkalagadda Prudhviraj, Malisetty Narasimha Naidu, Kadiyala Sai Krishna

Department of Computer Science and Engineering – Cyber Security, Chalapthi Institute of Technology,Guntur, Andhra Pradesh, India.

To Cite this Article
B.Venkateswara Reddy, Kajjam Pavithra, Vakkalagadda Prudhviraj, Malisetty Narasimha Naidu, Kadiyala Sai Krishna, Develop a Purposely Insecure Web Application for Practicing Security Testing, International Journal for Modern Trends in Science and Technology, 2024, 10(02), pages. 117-121. https://doi.org/10.46501/IJMTST1002016

Article Info
Received: 24 January 2024; Accepted: 19 February 2024; Published: 20 February 2024.

ABSTRACT

This project aims to design and implement a purposely insecure web application tailored for security testing and educational purposes. The application will simulate common vulnerabilities found in real-world web applications, providing a safe environment for individuals to practice security testing techniques and hone their skills in identifying and mitigating security flaws.The development process will involve intentionally incorporating vulnerabilities such as SQL injection, cross-site scripting (XSS), insecure authentication mechanisms, and others, ensuring a diverse range of security challenges for testers to address. By offering a hands-on learning experience, this project seeks to empower security enthusiasts and professionals to enhance their understanding of web application security principles and improve their ability to safeguard against cyber threats.

Keywords: SQL injection, cross-site scripting (XSS), Security Testing Techniques andcross-site request forgery (CSRF).

1. INTRODUCTION

In the ever-evolving landscape of cyber security, the development and testing of secure web applications are paramount. One instrumental approach to bolstering expertise in this domain involves the intentional creation of an insecure web application. This project is designed to provide a hands-on, immersive learning experience for individuals keen on honing their skills in security testing [1]. By deliberately infusing vulnerabilities into a web application, participants can explore, analyze, and address security issues in a controlled environment, thereby enhancing their capabilities in safeguarding digital assets.

In the ever-evolving landscape of cyber security, the development and testing of secure web applications are paramount [2]. One instrumental approach to bolstering expertise in this domain involves the intentional creation of an insecure web application. This project is designed to provide a hands-on, immersive learning experience for individuals keen on honing their skills in security testing. By deliberately infusing vulnerabilities into a web application, participants can explore, analyze, and

address security issues in a controlled environment, thereby enhancing their capabilities in safeguarding digital assets.

Goals of Creating an Insecure Web Application:

1. Skill Development: The central goal is to elevate the participants' skills in security testing. Through hands-on exercises, individuals can actively identify and exploit vulnerabilities, gaining invaluable experience that transcends theoretical knowledge.

2. Realistic Exposure: By intentionally introducing vulnerabilities, the project aims to provide a realistic exposure to common security pitfalls encountered in web applications. This exposure allows participants to comprehend the diverse attack vectors that malicious actors might exploit [3].

3. Bridge Theory and Practice: The project aims to bridge the theoretical knowledge of security concepts with practical application. Participants are encouraged to apply security principles live environment, fostering a seamless integration of security measures into the development lifecycle [4].

Security testing is a critical facet of ensuring the resilience of web applications against cyber threats. This project underscores the importance of systematic evaluation, identification, and remediation of vulnerabilities through active security testing. In an era where the stakes of cyber security are higher than ever, this intentional exercise serves as a proactive means to cultivate a robust security mindset [5].

2. LITERATURE REVIEW

Web Application Hacker's Handbook: Finding and Exploiting Security Flawsthis book serves as a comprehensive guide to understanding web application security vulnerabilities. It covers various hacking techniques such as injection attacks, cross-site scripting (XSS), and more, with practical examples and case studies for hands-on learning [1].

Hacking: The Art of Exploitation Andy Gill provides insights into building a career in information security, offering strategies for gaining relevant skills, certifications, and practical experience. It's valuable for individuals interested in developing expertise in web application security testing [2].

The Tangled Web: A Guide to Securing Modern Web Applications Jon Erickson explores the fundamentals of hacking and exploitation techniques, covering topics such as buffer overflows, shellcode development, and network hacking. It provides foundational knowledge essential for understanding vulnerabilities in web applications [3].

Web Security Testing Cookbook: Systematic Techniques to Find Problems Fast Paco Hope and Ben Walther present a cookbook-style approach to web security testing, offering practical recipes and techniques for identifying and mitigating security vulnerabilities. It includes step-by-step instructions and real-world scenarios for effective testing [4].

Security Testing with Kali Linux This book focuses on security testing using Kali Linux, a popular penetration testing distribution. It covers various tools and techniques available in Kali Linux for assessing web application security, providing hands-on exercises and tutorials for effective testing [5].

3. SYSTEM ANALYSIS

3.1 Existing System: Purposefully Insecure Web Application:The existing system consists of a web application intentionally developed with known vulnerabilities and security flaws. The primary objective of this system is to serve as a training ground for individuals interested in practicing security testing techniques. The application is designed to mimic real-world scenarios where security vulnerabilities commonly exist, allowing users to identify, exploit, and remediate them in a controlled environment.

The application incorporates a variety of common security vulnerabilities found in web applications, such as SQL injection, cross-site scripting (XSS), cross-site request forgery (CSRF), in secure direct object references (IDOR), insecure authentication mechanisms, etc. Each vulnerability is deliberately implemented within the application to provide users with opportunities to practice identifying and exploiting them [12].

Disadvantages:Dependency on Vulnerabilities: Over time, users may become overly reliant on the known vulnerabilities present in the insecure application, potentially overlooking emerging threats or less common attack vectors. This could limit their ability to adapt to new security challenges effectively [14].

3.2 Proposed system: The system will involve the design and development of a web application intentionally engineered with various security vulnerabilities. Developers will create the application using standard web development technologies, frameworks, and languages, ensuring it closely resemble real-world web applications.

The development team will carefully select and incorporate a range of common security vulnerabilities into the application, such as SQL injection, cross-site scripting (XSS), cross-site request forgery (CSRF), insecure authentication mechanisms, etc.Each vulnerability will be deliberately implemented, documented, and categorized to facilitate learning and testing.

4. SYSTEM DEVELOPMENT

Developing a purposely insecure web application for practicing security testing in Python with a focus on cyber security involves several steps. Below is a high-level overview of the system development process:

Requirement Analysis: Define the objectives of the insecure web application and gather requirements related to cyber security [16]. Identify the types of security vulnerabilities to be included in the application, such as SQL injection, cross-site scripting (XSS), and insecure authentication mechanisms.

Design Phase: Design the architecture of the web application, including the user interface, server-side components, and database structure. Create wireframes or mock-ups to visualize the application's layout and functionality. Define the modules and components of the application, each focusing on specific security vulnerabilities.

Development Phase: Implement the design plan using Python web frameworks such as Django or Flask.Set up the database using SQLite, MySQL, or another suitable database management system. Introduce deliberate security vulnerabilities into the application code, ensuring they are realistic and representative of common flaws found in web applications.

Testing and Quality Assurance: Conduct thorough testing of the insecure web application to identify and validate security vulnerabilities. Utilize Python-based security testing tools such as Bandit for static analysis, OWASP ZAP for dynamic scanning, and SQLMap for SQL injection testing [8]. Perform manual penetration testing and code review to identify potential security weaknesses.

Documentation and Training: Develop comprehensive documentation for the insecure web application, including installation instructions, user guides, and security testing methodologies [11]. Provide training materials and tutorials to help users understand security concepts and practice security testing techniques effectively using Python.

Deployment and Implementation: Deploy the insecure web application on a suitable web server environment such as Apache. Configure the necessary security mechanisms, including SSL/TLS encryption, access controls, and logging. Ensure proper security configurations to protect against common web application attacks.

User Feedback and Iterative Improvement: Gather feedback from users and stakeholders to identify areas for improvement and refinement [16]. Iterate on the development process to address user feedback, enhance usability, and improve the effectiveness of security testing. Continuously update and maintain the insecure web application to address emerging security threats and vulnerabilities.

Security Monitoring and Incident Response: Implement monitoring and logging mechanisms to track security-related events and activities within the application. Establish incident response procedures to handle security incidents and breaches effectively [16]. Regularly review security logs and conduct security audits to ensure the ongoing integrity and security of the application.

5. SYSTEM DESIGN

Web Application Framework: Utilize a chosen framework such as Flask, based on language preference and project requirements.

Database Management System (DBMS): Choose a DBMS like MySQL, or SQLite to store and manage application data in a secure manner.XAMPP (Data Base).

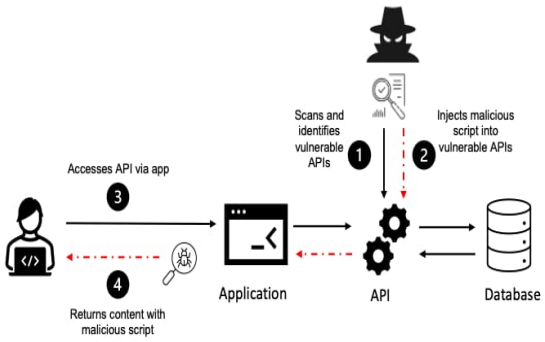

Fig:1 System Architecture

Programming Language: Select a programming language supported by the chosen framework, ensuring compatibility and efficient development

Web Server: Implement a web server to host and serve the insecure web application securely.

6. CONCLUSION

In conclusion, the purposely insecure web application designed for security testing serves as an invaluable tool for enhancing the skills of security professionals. By intentionally incorporating a diverse set of vulnerabilities and providing comprehensive documentation, tutorials, and a user-friendly interface, the application creates a realistic and controlled environment for hands-on practice. Regular updates and the option for cloud deployment contribute to the relevance and accessibility of the platform.

7. FUTURE SCOPE

The development and use of purposely insecure web applications for practicing security testing hold significant potential for enhancing cyber security knowledge and skills among developers, security professionals, and students.

Conflict of interest statement

Authors declare that they do not have any conflict of interest.

REFERENCES

[1] DafyddStuttard and Marcus Pinto "Web Application Hacker's Handbook: Finding and Exploiting Security Flaws" 2011-books.google.com

[2] Jon Erickson "Hacking: The Art of Exploitation"2008 - books.google.com

[3] Michal Zalewski "The Tangled Web: A Guide to Securing Modern Web Applications" 2011-books.google.com

[4] Kalyan Kumar Dasari& Dr, K.Venkatesh Sharma, "Mobile Agent Applications in Intrusion Detection System (IDS)"-JASC, Volume 4, Issue 5, October/2017, ISSN NO:1076-5131, Pages: 97-103.

[5] Kalyan Kumar Dasari& Dr, K.Venkatesh Sharma, "Analyzing the Role of Mobile Agent in Intrusion Detection System"-JASRAE, Vol. XV, Issue No. 1, April-2018, ISSN 2230-7540, Pages: 566-573.

[6] Kalyan Kumar Dasari& Dr, K.Venkatesh Sharma, "A Study on Network Security through a Mobile Agent Based Intrusion Detection Framework"-JASRAE, Vol. XI, Issue No. 22, July-2016, ISSN 2230-7540, Pages: 209-214

[7] K. K. Kumar, S. G. B. Kumar, S. G. R. Rao and S. S. J. Sydulu, "Safe and high secured ranked keyword searchover an outsourced cloud data," 2017 International Conference on Inventive Computing and Informatics (ICICI), Coimbatore, India, 2017, pp. 20-25, doi: 10.1109/ICICI.2017.8365348.

[8] K. K. .Kommineni and A. . Prasad, "A Review on Privacy and Security Improvement Mechanisms in MANETs", Int J IntellSystApplEng, vol. 12, no. 2, pp. 90–99, Dec. 2023.

[9] Kalyan Kumar Dasari& M.Prabhakar "Professionally Resolve the Password Security knowledge in the Contexts of Technology"-IJCCIT, Vol. 3, Issue. 1, April' 2015;ISSN: 2345 – 9808 (2015).

[10] V.Mounika& D. Kalyan Kumar "Background Subtraction by Using DE Color Algorithm" -IJATCSE, ISSN 2278-3091 Vol: 3, No: 1, Pages: 273-277(2014).

[11] Vellela, S.S., Balamanigandan, R. Optimized clustering routing framework to maintain the optimal energy status in the wsn mobile cloud environment. Multimed Tools Appl (2023). https://doi.org/10.1007/s11042-023- 15926-5

[12] Vellela, S. S., Reddy, B. V., Chaitanya, K. K., &Rao, M. V. (2023, January). An Integrated Approach to Improve E-Healthcare System using Dynamic Cloud Computing Platform. In 2023 5th International Conference on Smart Systems and Inventive Technology (ICSSIT) (pp. 776-782). IEEE.

[13] K. N. Rao, B. R. Gandhi, M. V. Rao, S. Javvadi, S. S. Vellela and S. KhaderBasha, "Prediction and Classification of Alzheimer's Disease using Machine Learning Techniques in 3D MR Images," 2023 International Conference on Sustainable Computing and Smart Systems (ICSCSS), Coimbatore, India, 2023, pp. 85-90, doi: 10.1109/ICSCSS57650.2023.10169550.

[14] VenkateswaraRao, M., Vellela, S., Reddy, V., Vullam, N., Sk, K. B., &Roja, D. (2023, March). Credit Investigation and Comprehensive Risk Management System based Big Data Analytics in Commercial Banking. In 2023 9th International Conference on Advanced Computing and Communication Systems (ICACCS) (Vol. 1, pp. 2387-2391). IEEE [6]

[15] S Phani Praveen, RajeswariNakka, AnuradhaChokka, VenkataNagarajuThatha, SaiSrinivasVellela and UddagiriSirisha, "A Novel Classification Approach for Grape Leaf Disease Detection Based on Different Attention Deep Learning Techniques" International Journal of Advanced Computer Science and Applications(IJACSA), 14(6), 2023. http://dx.doi.org/10.14569/IJACSA.2023.01406128

[16] Vellela, S. S., &Balamanigandan, R. (2022, December). Design of Hybrid Authentication Protocol for High Secure Applications in Cloud Environments. In 2022 International Conference on

Automation, Computing and Renewable Systems (ICACRS) (pp. 408-414). IEEE.

[17] Vullam, N., Vellela, S. S., Reddy, V., Rao, M. V., SK, K. B., &Roja, D. (2023, May). Multi-Agent Personalized Recommendation System in E-Commerce based on User. In 2023 2nd International Conference on Applied Artificial Intelligence and Computing (ICAAIC) (pp. 1194-1199). IEEE.

[18] Vellela, S. S., Balamanigandan, R., & Praveen, S. P. (2022). Strategic Survey on Security and Privacy Methods of Cloud Computing Environment. Journal of Next Generation Technology (ISSN: 2583-021X), 2(1).

[19] Vellela, S. S., & Krishna, A. M. (2020). On Board Artificial Intelligence With Service Aggregation for Edge Computing in Industrial Applications. Journal of Critical Reviews, 7(07), 2020.

[20] Madhuri, A., Jyothi, V. E., Praveen, S. P., Sindhura, S., Srinivas, V. S., & Kumar, D. L. S. (2022). A New Multi-Level Semi-Supervised Learning Approach for Network Intrusion Detection System Based on the 'GOA'. Journal of Interconnection Networks, 2143047.

[21] Madhuri, A., Praveen, S. P., Kumar, D. L. S., Sindhura, S., &Vellela, S. S. (2021). Challenges and issues of data analytics in emerging scenarios for big data, cloud and image mining. Annals of the Romanian Society for Cell Biology, 412-423.

[22] Praveen, S. P., Sarala, P., Kumar, T. K. M., Manuri, S. G., Srinivas, V. S., &Swapna, D. (2022, November). An Adaptive Load Balancing Technique for Multi SDN Controllers.In 2022 International Conference on Augmented Intelligence and Sustainable Systems (ICAISS) (pp. 1403-1409).IEEE.

[23] Vellela, S. S., BashaSk, K., &Yakubreddy, K. (2023). Cloud-hosted concept-hierarchy flex-based infringement checking system. International Advanced Research Journal in Science, Engineering and Technology, 10(3).

[24] Rao, M. V., Vellela, S. S., Sk, K. B., Venkateswara, R. B., &Roja, D. (2023). SYSTEMATIC REVIEW ON SOFTWARE APPLICATION UNDERDISTRIBUTED DENIAL OF SERVICE ATTACKS FOR GROUP WEBSITES. DogoRangsang Research Journal UGC Care Group I Journal, 13(3), 2347-7180.

[25] Venkateswara Reddy, B., Vellela, S. S., Sk, K. B., Roja, D., Yakubreddy, K., &Rao, M. V. Conceptual Hierarchies for Efficient Query Results Navigation. International Journal of All Research Education and Scientific Methods (IJARESM), ISSN, 2455-6211.

[26] Sk, K. B., Roja, D., Priya, S. S., Dalavi, L., Vellela, S. S., & Reddy, V. (2023, March). Coronary Heart Disease Prediction and Classification using Hybrid Machine Learning Algorithms. In 2023 International Conference on Innovative Data Communication Technologies and Application (ICIDCA) (pp. 1-7). IEEE.