e-ISSN 2320 –7876 www.ijfans.org
Vol.11, S Iss.1, 2022
Research Paper **UGC CARE Listed (Group -I) Journal**

Security Issues in Modern Web Applications followed by OWASP-2021

Authors

Mohammed Abdul Raheem, Department of Computer Science and Engineering, Shadan College of Engineering and Technology, Hyderabad, Telangana, India – 500086.

Subramanian K.M, Department of Computer Science and Engineering, Shadan College of Engineering and Technology, Hyderabad, Telangana, India – 500086.

Jothikumar R., Department of Information Technology, Shadan College of Engineering and Technology, Hyderabad, Telangana, India – 500086.

e-ISSN 2320 –7876 www.ijfans.org
Vol.11, S Iss.1, 2022
  UGC CARE Listed (Group -I) Journal

Abstract:

Over the last decade, there has been a considerable growth in the use of web-based applications that process sensitive data, such as personal, financial, and medical data. As the use of such applications has grown, the security of such applications has become increasingly important in ensuring the data's safety, integrity, and validity. Web applications can be run from an internet browser without the need to download or establish, however these require modules. Modern web applications allow users to access data from any location at any time. As a result, Hackers will be able to access the information. In this paper, we try to demonstrate the security issues in the web application followed by the OWASP Security Standards.

Keywords: Security, Internet, Web, Business

Introduction:

The Open Web Application Security Project 10 (OWASP-Top10) is a testing framework for web applications that focuses on web application security to find vulnerabilities in websites. The goal of the Open Web Application Security Project 10 is to ensure that the website in form checklists is safe.

- Injection attacks
- Attacks of broken authentication
- sensitive data disclosure
- External entities – XML (XXE)
- access control issues
- security misconfigurations
- (XSS)cross-site scripting
- insecure deserialization vulnerabilities
- Components/Libraries with known vulnerabilities
- insufficient logging & monitoring

are ten of the most hazardous website vulnerability categories that the OWASP 10 - (Open Web Application Security Project 10) has identified. This project examines and evaluates the web's security, as well as the security of an application, with the goal of determining and assessing a website's security level, whether extra protection is required, and website recommendations.

Research Method:

In order to avoid data theft and dissemination by negligent parties and to ensure the long-term viability of the website and website-based information systems, the application of OWASP 10 has criteria for analyzing website security needs and website-based information systems. To demonstrate the security vulnerabilities in the modern web applications followed by OWASP 10 the intentionally vulnerable web application has been developed. To develop the intentionally vulnerable web app the below steps are followed:

- Step1

- Step2

- Step3

- Step4

- Step5

- Step6

Research Flow

The next step comprises reading up on all subjects related to the notion of creating a vulnerable app, security testing, and website security. By researching and reading books, theses, final projects, scientific research, and a variety of internet information sources, you can perform a literature study.

The following stage entails selecting a test method based on literature searches that have been done to identify an appropriate method. The finished target will next be set through the testing process. The test data will be analyzed to determine the outcomes and the best course of action.

Research Tool

Hardware and software are used as instruments. The device is a MacBook laptop, with Burp Suite and macOS serving as the operating system and applications, respectively.

The minimal requirements and the laptop's specifications are listed in the following table.

Software Tools

S No	Phase	Tools
1.	Development	Visual Studio Code
2.	Scanning/Vulnerability Assessment	Nmap Nessus OWASP ZAP
3.	Exploitation/Penetration Testing	Burpsuite

Hardware Tools

Processor	Minimum Pentium 4 orAMD64
RAM	Minimum 1GB RAM & above
Hard Disk	50GB & above

Proposed System with Features

The most recent Open Web Application Security Project (OWASP) 10 2021 has not been used to create intentionally vulnerable web applications. The purpose of this study is to develop the intentionally vulnerable web app and perform penetration testing from the viewpoint of the general public using the most recent OWASP 10 2021 standard.

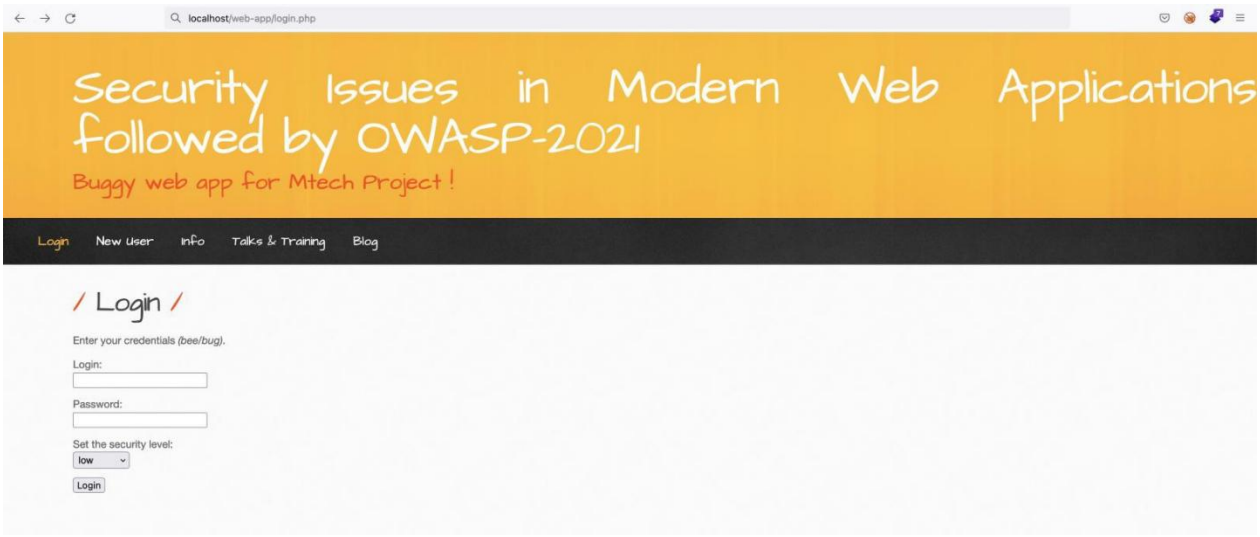
Utilizing this most recent Open Online Application Security Project (OWASP) 10 2021 framework allows for penetration testing of websites using the most recent and cutting-edge web assaults, protecting user data from being stolen by hackers and sold on the dark web or compromised.

Implementation Results

The overall results of the application development, implementation and penetration testing execution of some of the OWASP top-10 vulnerabilities can be shown in the screenshots below

For the application hosting and implementation the setup has been done using some tools such as XAMPP, mySQL etc.

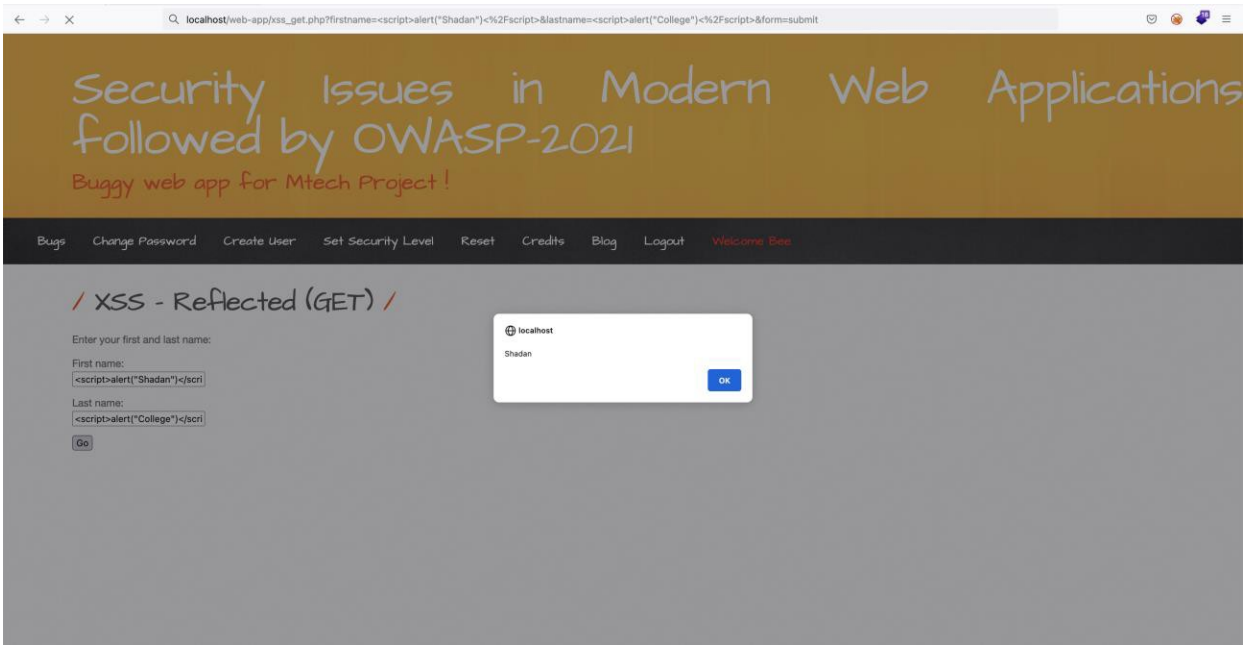
Login page



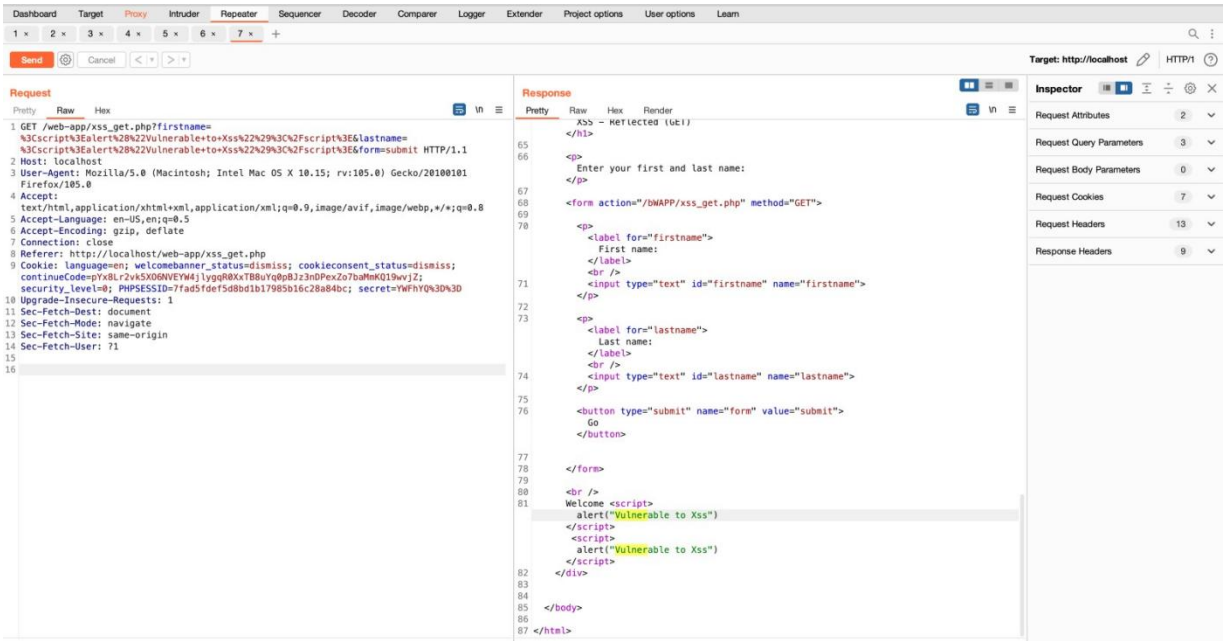
Reflected Cross Site Scripting

e-ISSN 2320 –7876 www.ijfans.org
Vol.11, S Iss.1, 2022
Research Paper **UGC CARE Listed (Group -I) Journal**

Reflected XSS Execution



Burp Suite Results



Conclusion

The use of web-based applications that process sensitive data, such as personal, financial, and medical data, has increased significantly. As the use of such apps has expanded, so has the security of such applications in assuring the data's safety, integrity, and validity. Web apps can be run directly from a browser without the requirement for download or installation, but they do require modules. Users can access data from any location and at any time using modern web applications. As a result, hackers will have access to the data. In this project, we attempt to demonstrate security vulnerabilities in the modern web application using the OWASP Security Standards 2021. The application has been developed to exploit and understand these vulnerabilities in a way that an attacker can exploit. Based on earlier research, there are numerous websites with security values of 60%, indicating a risk of interference; this requires the installation of security measures such port closures or the addition of SSH Security, as well as logging in open ports.

Future Improvement:

It is a good idea to integrate logging & monitoring so that you can keep track of the history of user activity on websites, network traffic, and network traffic generation to stop these vulnerabilities and attacks.

References

[1] D. E. Simos et al., "Combinatorial Methods in Security Testing.," Creat. Inf. Technol. J., vol. 49, no. 4, pp. 78–84, Jun. 2016.

[2] M. Madou et al., "Application security testing," 2016 IEEE/ACM

11th Int. Work. Autom. Softw. Test, vol. 49, no. 10, pp. 80–83, Jun.

2016.

[3] M. Mohammadi, B. Chu, H. R. Lipford, and E. Murphy-Hill,

"Automatic web security unit testing: XSS vulnerability detection," in 2016 IEEE/ACM 11th International Workshop in Automation of Software Test (AST), 2016, pp. 78–84.

[4] F. Zaidi, H. Abu-Zaydeh, M. S. Allen, R. Bosi, B. E. Doyle, and M. E. Feeny, "Identifying and maintaining secure communications." Google Patents, Nov. 2018.

[5] M. I. Tariq and V. Santarcangelo, "Analysis of ISO 27001: 2013 Controls Effectiveness for Cloud Computing," in International Conference on Information Systems Security and Privacy, 2016, vol. 2, pp. 201–208.

[6] A. Iskandar et al., "Web based testing application security system using semantic comparison method," in IOP Conference Series: Materials Science and Engineering, 2018, vol. 420, no. 1, p. 12122.

[7] M. D. Dzulfiqar, D. Khairani, and L. K. Wardhani, "The Development of University Website using User Centered Design Method with ISO 9126 Standard," 2019, doi: 10.1109/CITSM.2018.8674325.

[8] M. A. Tate, Web wisdom: How to evaluate and create information quality on the Web. CRC Press, 2018.

[9] M. A. Helmiawan, Y. H. Akbar, and Y. Y. Sofian, "Evaluasi dan Uji Kualitas Website dengan Metode Webqual (Studi Kasus: STMIK Sumedang)," Jt. (Journal Inf. Technol., vol. 1, no. 1, pp. 1– 4, 2019.

[10] D. Wichers, "Owasp top-10 2013," OWASP Found. Febr., 2013.

[11] S. Clunie and D. A. Parrish, "How assessment websites of academic libraries convey information and show value," Perform. Meas. 191. Metrics, 2018.

[12] D. E. Simos, R. Kuhn, A. G. Voyiatzis, and R. Kacker, "Combinatorial Methods in Security Testing.," IEEE Comput., vol. 49, no. 10, pp. 80–83, 2016.

[13] E. Burato, P. Ferrara, and F. Spoto, "Security analysis of the OWASP benchmark with Julia," Proc. ITASEC, vol. 17, 2017.

[14] S. Kumar, R. Mahajan, N. Kumar, and S. K. Khatri, "A study on web application security and detecting security vulnerabilities," in 2017 6th International Conference on Reliability,

Infocom Technologies and Optimization (Trends and Future Directions) (ICRITO), 2017, pp. 451–455.

[15] B. Mburano and W. Si, "Evaluation of Web Vulnerability Scanners Based on OWASP Benchmark," in 2018 26th International Conference on Systems Engineering (ICSEng), 2018, pp. 1–6.

[16] G. Chu and A. Lisitsa, "Poster: Agent-based (BDI) modeling for automation of penetration testing," in 2018 16th Annual Conference on Privacy, Security and Trust (PST), 2018, pp. 1–2.

[17] M. Maass, P. Wichmann, H. Pridöhl, and D. Herrmann, "Privacyscore: Improving privacy and security via crowd-sourced benchmarks of websites," in Annual Privacy Forum, 2017, pp. 178–

[18] R. Brewer, "Advanced persistent threats: minimising the damage," Netw. Secur., vol. 2014, no. 4, pp. 5–9, 2014.

[19] A. C. Perera, K. Kesavan, S. V. Bannakkotuwa, C. Liyanapathirana, and L. Rupasinghe, "E-commerce (WEB) Application security: Defense against Reconnaissance," in 2016 IEEE International Conference on Computer and Information Technology (CIT), 2016, pp. 732–742.

[20] M. Crouse, B. Prosser, and E. W. Fulp, "Probabilistic performance analysis of moving target and deception reconnaissance defenses," in Proceedings of the Second ACM Workshop on Moving Target Defense, 2015, pp. 21–29.

[21] Y. CHEN and Z. SUN, "Performance Test and Optimization of Web System Based on LoadRunner," Softw. Guid., no. 9, p. 8, 2017.

[22] L. Nan and G. Sheng, "Application of Convolution Optimization Algorithm Based on Neural Network in Web Attack Test," in Journal of Physics: Conference Series, 2019, vol. 1325, no. 1, p. 12001.