International Journal of Research in Engineering, Science and Management
Volume 6, Issue 2, February 2023
https://www.ijresm.com | ISSN (Online): 2581-5792

Security Issues in Web Application

K. P. Shana Sherin[1*], T. Ambikadevi Amma[2], K. Sivakumar[3], K. Arun[4]
[1]PG Student, Department of Computer Science and Engineering, Nehru College of Engineering and Research Centre, Thrissur, India
[2,3]Professor, Department of Computer Science and Engineering, Nehru College of Engineering and Research Centre, Thrissur, India
[4]Assistant Professor, Department of Computer Science and Engineering, Nehru College of Engineering and Research Centre, Thrissur, India

***Abstract*: Given that it serves as the fundamental underpinning for the global digital society, web security presents a significant challenge to businesses. This essay examines the several flaws in web security, including passwords, encryption, authentication, and integrity. It also examines a variety of defence strategies for dealing with these group of dangers and evaluates why they have not been more effective. Additionally, the level of web page security in educational systems is assessed, and the variations in web application security between academic institutions are explored. Finally, a suggestion for safeguarding websites is discussed.**

***Keywords*: Security, Attacks, Web application.**

1. Introduction

Web security is a crucial component of web applications, as it is susceptible to attacks like worms, browser attack, cookie-session theft, and cross-site scripting. The security evaluation conducted by application defence centre found that more than 85% of web apps were open to assaults.75% of Internet dangers are tied to Web apps, and 75% of attacks have been directed at application-level targets. The education industry is one of the major sectors that heavily uses web apps and websites for information dissemination, lectures, assignments, collaborations, discussions, conferences, grading, training, remote learning, research activities, and many more objectives. Unfortunately, scholars have not paid much attention to the importance of protecting these data.

2. Methodology

Two prevalent security flaws are SQL injection and XSS, according to research of various vulnerabilities in the literature. An unintentional command known as SQL injection is sent to an interpreter and user input into form fields for database queries is made possible. A well-crafted attack URL called an XSS can be changed to allowing access which enable an assault to be launched. The client and the server are the two components that make up a web application. Cross-site scripting assaults, clickjacking, the use of scripts, and plug-in technologies are some of the security risks that the browser faces.

Server-side web applications are similarly impacted by the persistence of malicious code, coming under attack from the Webpage Trojan horse. The two main types of attacks we frequently experience are aggressive attacks and passive attacks.

Our objective was to categorise 12 higher education, academic, and research institutions in Kuwait into governmental and commercial sectors. Examples of government-funded institutions include Kuwait University (KU), the Public Authority for Applied Education and Training (PAAET), and the Kuwait Institute for Scientific Research (KISR). The profit-driven private institutions have a partial focus on governmental rules. Both categories of applications are aimed for websites that offer services in the form of web applications, such as student information systems (SIS). Website security flaws or vulnerabilities are found using tools like Web scanners and scanner. Acunetix is an online vulnerability scanner tool with various cutting-edge capabilities like an automatic JavaScript analyser, the most thorough and comprehensive SQL injection and Cross-site scripting testing available in the industry, and a multi-threaded, blazing-fast scanner. An intelligent crawler can determine the languages used by web servers and apps by scanning hundreds of thousands of pages, crawl, analyse websites, including those with flash content, and cross-reference the OWASP top ten vulnerability list. The approach used to assess the security of web application servers includes crawling each targeted website and listing any vulnerabilities discovered, categorising them into four categories: High, Medium, Low, and Informational. If any of the vulnerabilities were met, a 10% number was added.

3. Results

Web applications are less safe due to malicious attacks. Users should utilize parameterized statements or well filtered sanitized input to protect themselves from SQL injection attacks. Whenever possible, developers should employ filter metacharacters rather than relying on user input to prevent cross-site scripting attacks. The most important aspects of this study are the client programme code security, client and server security technology, security risk provided by Web client script, AJAX protection method, and client programme code security. The client's security technology involves the operating system's real-time patches and the browser version, and it is important to promptly fix any vulnerabilities in both. The four components of the server's security protection method are the user end's application system, an external program's mechanism, data

*Corresponding author: shanasherinkp999@gmail.com

calls, and data processing protection mechanisms. the ability to respond to data requests by interacting with the data, the capacity to transmit data, and the ability to place information calls, etc. are all contained by the AJAX protection methods. Input validation entails confirming the accuracy of all the information provided by clients and servers, including HTTP header, cookie, parameter, and data validation as well as length and user data specification checks. HTTPS, which is used to run HTTP based on SSL, is the structure that results from the merger of HTTP and SSL. The voice stream and the video stream are the two contents that the SRTP protocol principally examines and develops in terms of security performance. Additionally, SRTP offers cognitive techniques and AES-compatible encryption options.

After SSL encryption, the RTMPS security protocol was established, and its main goal is to provide a security protocol with data integrity and authentication. Web application security measures can be implemented at several implementation levels, from coding to monitoring, from administrative to technical, and from prevention to protection. To make web technology in education more secure, it is advised that higher education institutions establish a central body to supervise the security of digital information. System administrators should regularly update their system software, run routine configuration management tests, close potential exploits, test for user enumeration, look for authentication bypass, and look for the usage of inappropriate algorithms. Security challenges can be tackled from the bottom up if adequate security mechanisms are integrated into online applications.

4. Conclusion

This study identifies a group of web application vulnerabilities that are frequently present in educational systems. Risk levels for These risks range in severity from informational threats to high vulnerabilities. Additionally, it demonstrates how well security methods defend online applications from a variety of recognized dangers. The most crucial lesson here is that educational institutions retain very sensitive digital data and information that hackers find appealing., and they should update their web-based programmers to address potential dangers and vulnerabilities.

References

[1] S. Kumar, R. Mahajan, N. Kumar and S. K. Khatri, "A study on web application security and detecting security vulnerabilities," 2017 6th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions) (ICRITO), Noida, India, 2017, pp. 451-455.

[2] K. Fanxing. “Research on Security Technology based on WEB Application,” 2016.

[3] Mohamed Al-Ibrahim and Yousef Shams Al-Deen, “The Reality of Applying Security in Web Applications in Academia” International Journal of Advanced Computer Science and Applications (IJACSA), 5(10), 2014.

[4] Atefeh Tajpour, Mohammad Zaman Heydari, Maslin Masrom and Suhaimi Ibrahim, "SQL injection detection and prevention tools assessment," 2010 3rd International Conference on Computer Science and Information Technology, Chengdu, China, 2010, pp. 518-522.

[5] Xiaojie X, Yang X, Shuo J., Research and Design of Web Application Firewall Based on Feature Matching. Netinfo security, (11)53-59, 2015.

[6] Acunetix. Auditing your web site security with Acunetix web vulnerability scanner. Retrieved March 15, 2013, from website: http://www.acunetix.com/