IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 2, July 2023

Research on Security Challenges in Web Application

Keerthika Krishnan Adapan
Student, Master of Computer Application
Late Bhausaheb Hiray S.S Trust's Hiray Institute of Computer Application, Mumbai, India
krithikakrishna522@gmail.com

Abstract: *There are millions of websites in the world now but it has been observed since very long time that Web Security has been one of most important areas of research whether be it either analysis or detection and later developing to mitigation plans. Web security threats are very much present now days and they have undergone much sophistication comparing to their initial phase. Now they are becoming more & more evolved each day. The evolution of threat on websites might be in terms of new ways of attack or bringing in resistance to using simulated Operating Systems or VM ware environments. Also, there has been considerable shift in the target of attacks in recent years. Earlier, clients were ignored while choosing targets. But, in recent years client user has become the main target for attacks as the adversary believe that the end user is the weakest link in the security chain. This paper is presented here to study the issues related to web security in cyber world.*

Keywords: web application, security, development, checklist

I. INTRODUCTION

Web applications have become an integral part of our daily lives, facilitating various online activities and services. However, this widespread adoption has also attracted malicious actors seeking to exploit vulnerabilities for their gain. This paper aims to identify and analyze the significant security challenges faced by web application developers, offering insights into mitigating strategies and best practices.

After successful inception of the websites, online stores are very common now days and Web applications are one of the most prevalent platforms for information and services delivery over Internet in present time as they are increasingly used for many critical services. Web applications have become quite popular in present times. Due to growing popularity of websites and web application, these are now soft targets to cyber criminals. Although a large body of techniques has been developed to fortify web applications and mitigate the attacks toward web applications, there is little effort devoted to drawing connections among these techniques and building a big picture of web application security research. Web Services are not only associated with advantages. There are many more issues that need to be addressed by standard bodies and technology vendors in order for Web Services to become a viable solution for building global service oriented architectures. Security is one such very important issue in this regard. Many of today's web service implementations are not publicly exposed because of the lack of security that the SOAP version 1.1 specifications left.

II. REVIEW OF LITERATURE

Websites are integral part of our lives now days and they are very much vulnerable to cyber attack by hackers. We all know there are lots of work has been done on this subject. SoI went through following literature to carry the study on this topic: -

- Technical report of Threats, Challenges and Emerging Standards in Web Services Security
- Book Hacking Made Easy 2nd Edition by Rajendra Maurya
- Periodic journal : Website Security Statistics Report

Journal : A Survey on Web Application Security

- Article on Security Issues for the Semantic Web
- Journal on Guidelines on securing public websites

III. STATEMENT OF THE PROBLEM

Web application security faces various challenges that threaten user privacy, data confidentiality, and application functionality. This section introduces the research paper's

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 2, July 2023

focus on the security challenges encountered during web application development.

3.1 SQL Injection(SQLi)Vulnerabilities:

SQL Injection attacks manipulate database queries through malicious inputs, potentially granting unauthorized access to sensitive information.The problem lies in inadequate input validation and improper handling of user-generated content.

3.2 Cross-Site Scripting(XSS) Threats:

XSS attacks inject malicious scripts into web pages, compromising users' browsers and enabling unauthorized data theft or unauthorized actions. The problem arises from improper output encoding and validation practices

3.3 Authentication and Authorization Weaknesses:

Weak authentication mechanisms and improper authorization policies can lead to unauthorized access and privilege escalation. This problem demands robust authentication and authorization implementations to prevent unauthorized access.

IV. RESEARCH METHODOLOGY

Our research methodology was very simple but accurate for this paper. We contacted several cyber security professionals and experts in various organizations who are looking after web development along with cyber security through LinkedIn. We contacted them also but they were hesitant respond our request, only few has cooperated with our query. Then we also gone through journals and articles based which were on the breach on web security. After lots of efforts, we could finally collect data for our research work. In the subsequent Para we will see the results of our study.

IV. RESULT AND DISCUSSION

As simple as these questions sound, the answers have proven elusive. Most responses by the so 5 called experts are based purely on personal anecdote and devoid of any statistically compelling evidence, such as the data presented in this report. Many of these experts will cite various “best practices,” such as software security training for developers, security testing during QA, static code analysis, centralized controls, Web Application Firewalls, penetration-testing, and more; However, the term “best-practices” implies the activity is valuable in every organization at all times. Following are the result for our research and survey;-

4.1 Securing Coding Practices:

Implementing secure coding practices during development is essential to minimize vulnerabilities. This section emphasizes the importance of input validation, output encoding and secure configurations to prevent security breached.

4.2 Web Application Firewalls(WAFs) and Intrusion Detection System(IDS):

Deploying WAFS and IDS provides an additional layer of protection against web application attacks.

4.3 Regular Security Audits and Penetration Testing:

Conducting regular security audits and penetration testing helps identify and address potential vulnerabilities proactively. This section highlights the significance of continuous monitoring and timely remediation of security issues.• 55% of companies said they provide some amount of computer-based software security training to their web developers. These organizations experienced 42% lesser vulnerabilities and resolved them 60 % faster.

V. CONCLUSION

Web application development faces a multitude of security challenges that necessitate vigilant efforts to protect user data and uphold the integrity of online services. By understanding and addressing common vulnerabilities like SQL injection, cross-site scripting, and authentication weaknesses, developers and organizations can build more resilient web applications. Implementing effective mitigation strategies and staying informed about emerging threats will ensure a safer digital environment for all users.

REFERENCES

[1]. http://hackingmadeeasy.com/
[2]. http://link.springer.com/chapter/10.1007%2F978-3-642-25541-0_51
[3]. http://www.di.unipi.it/~ghelli/didattica/bdldoc/A97329_03/core.902/a90146/fundamen.htm
[4]. https://www.whitehatsec.com/assets/WPstatsReport_052013.pdf
[5]. http://www.symantec.com/connect/articles/five-common-web-applicationvulnerabilities
[6]. http://www.beyondsecurity.com/websecurity-and-web-scanning.html
[7]. https://www.whitehatsec.com/assets/WPstatsReport_052013.pdf

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 2, July 2023

[8]. http://www.quotium.com/content/uploads /2014/01/SeekerApplication_Security_in_the_SDLC.pdf
[9]. http://www.beyondsecurity.com/websecurity-and-web-scanning.html
[10]. Halfond, W. G. J., &Orso, A. (2006). A classification of SQL-injection attacks and countermeasures. Proceedings of the 2006 International Symposium on Software Testing and Analysis, 1-10.