International Journal of Innovative Research in Science, Engineering and Technology (IJIRSET)

|| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.512| || Volume 9, Special Issue 2, October 2020 ||

3rd International Conference on Emerging Trends in Science, Technology and Mathematics [ICETSTM 2020]

18th September 2020

Organized by

Department of Computer Science, Parvathy's Arts and Science College, Dindigul, Tamilnadu, India

An Investigation and Study of Vulnerabilities of Web Applications: Injection Attack in Cross-Site and Structured Query Language and Protection Techniques

R. Janaki

Lecturer, Department of Computer Science, Vagdevi Vilas College, Bangalore, India

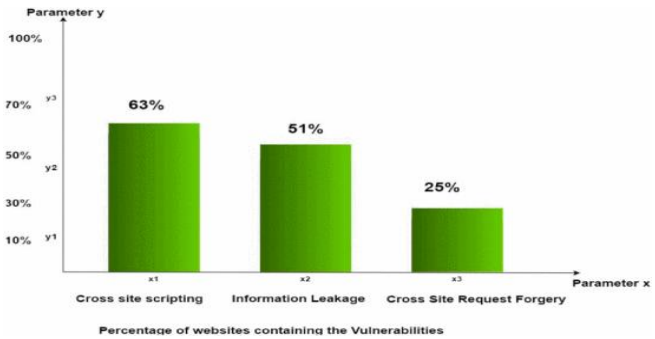
ABSTRACT: A web Application or web service is a software application that is accessible using web Browser or HTTP agent. Web Application Security is a branch of information security of web site. The World Wide Web consists of web sites. The flow of information was one way from server to the browser. Web Application security is a central component of any web based business. It deals specifically with the security surrounding websites, web services such as APIS. This paper summarizes the different aspect of web security and its weakness. The main element of web security techniques such as cross – site Injection and Structured Query Language injection attack are discussed here. This paper proposes a better way for minimizing these types of web vulnerabilities. It also provides the better security mechanisms for the attacks.

KEYWORDS: Web Service, Web Application Security, Vulnerabilities, Cross-site Injection, Structured Query Language Injection, XSS Attack

I. INTRODUCTION

A Web Application or Web service is software applications that are accessible using web browser (or) HTTP user agent. Web Security is an important aspect for web applications. Today Web Security is a real concern related to the internet. Web Applications provide a better interface for a client through a web page. Web Applications are main base of attacks such as cross-site scripting, Structured Query Language in email and websites. These types of attacks are called 'injection attacks' which attacks by the use of malicious code. Injection attacks have commanded the highest point of web application vulnerability for the significant part of previous decade.

The literature survey describes the study of different vulnerabilities defines the two common security vulnerabilities are SQL and XSS.Many technology and mechanisms are proposed by different researchers to prevent SQL and XSS attacks.



|| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.512| || Volume 9, Special Issue 2, October 2020 ||

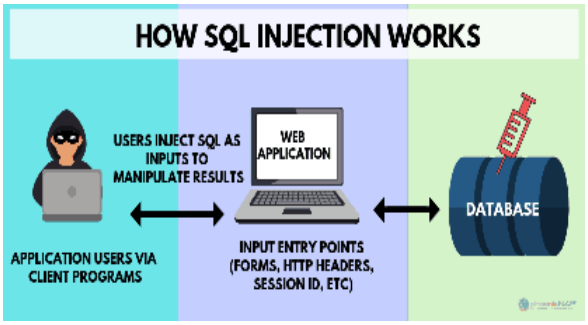
3rd International Conference on Emerging Trends in Science, Technology and Mathematics [ICETSTM 2020]

18th September 2020

Organized by

Department of Computer Science, Parvathy's Arts and Science College, Dindigul, Tamilnadu, India

From the research it has been identified that SQL Injection attack and XSS attack are still possible even after implementing and preventing mechanism presently available in the market and so a preventive mechanism have been proposed in the below given figure



II. SERVER

A server is a computer program or a machine that accepts a process request generated by another program or machine and respond to them. There are so many types of computer server, like FTP server, Application server, Web server and Online Game Server. Some other types of servers are List Sever, Mail server, IRC server, chat server etc

III. WEB SERVER

Web server is an IT component that processes user requests via HTTP. A web server stores, process and deliver web page to client. Web server works as Receive requests from client, generate response and send response to client
Attacker tracks the session id of the user by sending http request to the server using several malicious code. After this request the server responds to the user's session id. Finally attacker will attaches malicious script into the database and get responses for the query accordingly

IV. PROTECTION AGAINST CROSS-SITE INJECTION ATTACK

Cross – site scripting attack occurs because the developers add some vulnerability to the code .The developer should understand what kind of attack are possible on web application .User input is always not trustable because the user can insert any type of characters and always use filter meta characters as it reduce the XSS attack .XSS holes can damage your application because the attacker willdisclose these types of holes to the public

V. THREE TYPES OF CROSS-SITE SCRIPTING

- Reflected
- Stored
- DOM Injection

VI. PREVENTION (XSS ATTACK)

- By validating of all incoming data or input data
- Appropriate encoding of all output data can prevent this attack

VII. PROTECTION AGAINST SQL INJECTION ATTACKS

Attacker used to understand the concept of Surface area; they use the error messages to learn about the structure of underlying SQL statements and databases; they exploit the SQL formatting characters (single quotes , semi colon etc)

|| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.512| || Volume 9, Special Issue 2, October 2020 ||

3rd International Conference on Emerging Trends in Science, Technology and Mathematics [ICETSTM 2020]

18th September 2020

Organized by

Department of Computer Science, Parvathy's Arts and Science College, Dindigul, Tamilnadu, India

VIII. DEFENCE AGAINST SQL INJECTION

1. Comprehensive data sanitization

Email addresses should be filtered to allow only the characters allowed in an email address

2. Use Web Application Firewall

Mod security provides a sophisticated and ever evolving set of rules to filter potentially dangerous web requests

3. Limit database privileges by context

Create multiple database user account with minimum levels of privileges; the code behind the login page should query the database using an account limited only to the relevant credential tables

4. Avoid constructing SQL queries with user Input

Use SQL variable binding with prepared statements or stored procedures is much faster than constructing full queries

IX. CONCLUSION

This paper provides a complete survey of current research results under web application security. In this paper all properties of web application development, understood the important security functions and properties that secure web applications should use and existing works into two major classes.

The logics and code resides at client side that is our browser that exposes programmer concepts. So for attackers it becomes easy to intercept the logics and cause total damage to the server-side of the application.

REFERENCES

[1] Gowthamaraj Rajendran, R S Ragul Nivash, Purushotham Parthiban Parthy, S Balamurugan, "Modern security threats in the Internet of Things (IoT): Attacks and Countermeasures", Security Technology (ICCST) 2019 International Carnahan Conference on, pp. 1-6, 2019.

[2] S. K. Mahmoud, M. Alfonse, M. I. Roushdy and A. M. Salem, "A comparative analysis of Cross Site Scripting (XSS) detecting and defensive techniques," 2017 Eighth International Conference on Intelligent Computing and Information Systems (ICICIS), Cairo, 2017, pp. 36-42, doi: 10.1109/INTELCIS.2017.826002

[3] S. Mukherjee, P. Sen, S. Bora and C. Pradhan, "SQL Injection: A sample review," 2015 6th International Conference on Computing, Communication and Networking Technologies (ICCCNT), Denton, TX, 2015, pp. 1-7, doi: 10.1109/ICCCNT.2015.7395166.