ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 4, Issue 1, pp: (214-216), Month: January - March 2016, Available at: www.researchpublish.com

SQL Injection Tester

[1]Kshitij Tambde, [2]Mukesh Bhikane, [3]Dinkar Telap

Atharva college of Engineering, City-Mumbai, Country-India

Abstract: **SQL injection is the most common attack for web applications and widely used exploit by hackers all over the world. A malicious hacker can do a lot of harm if he wishes to. SQL injection is a security vulnerability that occurs in the database layers of an application. SQL injection is a technique to pass SQL code into interactive web applications that employ in database services. The employment of SQL Injection Attacks, can lead to the leak of confidential information such as credit card numbers, commercial information & table structure. The attackers can get the entire schema of the original database and also corrupt it. In this paper, we have proposed the Detection Model of SQL Injection Vulnerabilities and SQL Injection Mitigation Framework. These approaches are based on SQL Injection grammar to identify the SQL Injection vulnerabilities during software development and SQL Injection Attack on web applications. SQL injection tester will secure web applications from all the above SQL injection attacks. It will test any web application for sql injection attack & will generate the report which will inform the web developer that for which sql injection attacks his web application is vulnerable. In today's world where security is becoming very critical issue this application is going to be very useful.**

Keywords: **SQL injection, Vulnerabilities, software development, Framework.**

1. INTRODUCTION

SQL injection is a technique where malicious users can inject SQL commands into an SQL statement, via web page input Injected SQL commands can alter SQL statement and compromise the security of a web application.

An SQL injection attack consists of insertion or "injection" of either a partial or complete SQL query via the data input or transmitted from the client (browser) to the web application. A successful SQL injection attack can read sensitive data from the database, modify database data (insert/update/delete), execute administration operations on the database (such as shutdown the DBMS), recover the content of a given file existing on the DBMS file system or write files into the file system, and, in some cases, issue commands to the operating system. SQL injection attacks are a type of injection attack, in which SQL commands are injected into data-plane input in order to affect the execution of predefined SQL commands.

2. BASIC CONCEPT

An SQL injection attack consists of insertion or "injection" of either a partial or complete SQL query via the data input or transmitted from the client (browser) to the web application. A successful SQL injection attack can read sensitive data from the database, modify database data (insert/update/delete), execute administration operations on the database (such as shutdown the DBMS), recover the content of a given file existing on the DBMS file system or write files into the file system, and, in some cases, issue commands to the operating system. SQL injection attacks are a type of injection attack, in which SQL commands are injected into data-plane input in order to affect the execution of predefined SQL commands. An application under test might have a user interface that accepts user input that is used to perform the following tasks:

1. Show the relevant stored data to the user e.g. the application checks the credentials of the user using the log in information entered by the user and exposes only the relevant functionality and data to the user

2. Save the data entered by the user to the database e.g. once the user fills up a form and submits it, the application proceeds to save the data to the database; this data is then made available to the user in the same session as well as in subsequent sessions.

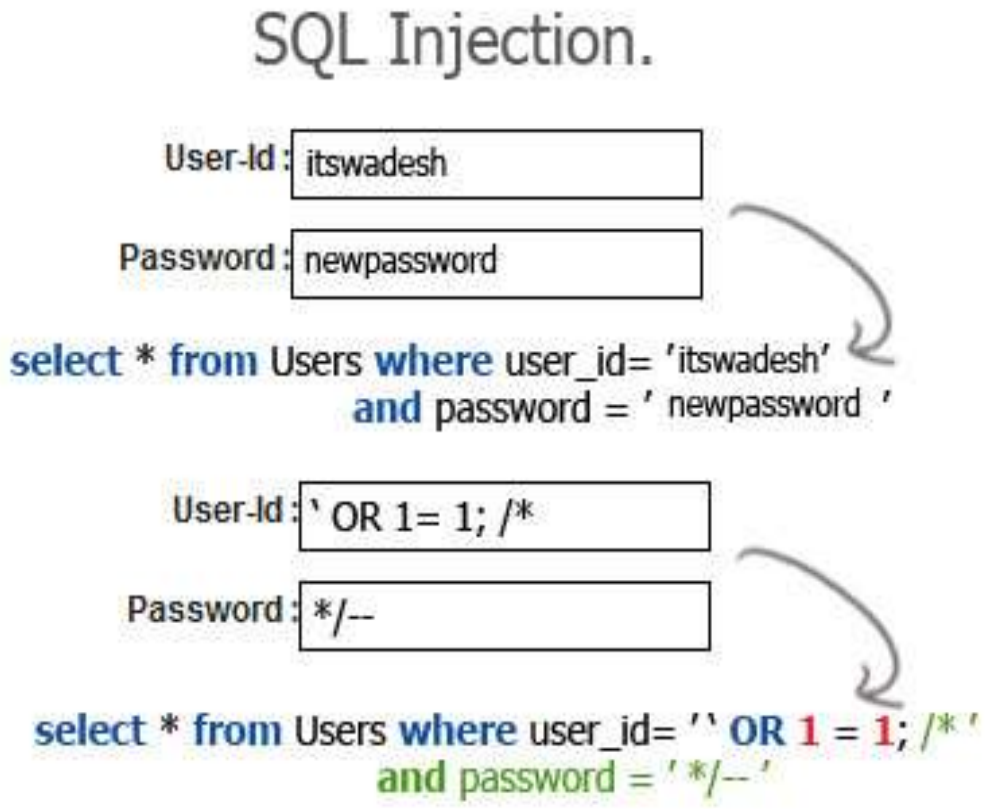
ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 4, Issue 1, pp: (214-216), Month: January - March 2016, Available at: www.researchpublish.com

'SQL INJECTION TESTER' sql is a web application which will test any web application and network system for sql injection vulnerability as well as generate a report which will tell client about how secured his web application is as well as make him aware towards network security.

The project is going to be useful for all the network security users, all those companies whose daily transactions are based on network.

In many fields daily transfer of important and confidential data is done in such fields protecting data is the most important task for such field sql injection attack may bring huge loss.

For such needs we have created an easy to use web application which is making significant awareness about network security.



3. CONCLUSION

The sql injection tester can be used to secure a website from sql injection attack.

Advantages:

1. It secures website forms
2. It secures Database.
3. It secures php forms.
4. It secures from http attack.

Disadvantages:

1. Does not secure from XSS.
2. Does not secure from DOS attack.

ACKNOWLEDGMENT

We would like to thank our project guide Prof. Archita lad for her enormous co-operation and guidance. We have no words to express our gratitude for a person who wholeheartedly supported the project and gave freely of her valuable time while making this project. All the inputs given by her have found a place in the project. The technical guidance provided by her was more than useful and made the project successful. She has always been a source of inspiration for us. It was a memorable experience learning under such a highly innovative, enthusiastic and hard working teacher.

We are also thankful to our Principal Dr. S.P. Kallurkar, our Project co-ordinator Prof. Deepali Maste and all the staff members of the Computers department who have provided us various facilities and guided us to develop a very good project idea.

Finally, we would also like to thank teachers of our college and friends who guided and helped us while working on the project.

REFERENCES

[1] Halfond W. G., Viegas, J., and Orso, A., A Classification of SQL-Injection Attacks and Countermeasures. In Proc. of the Intl. Symposium onSecure Software Engineering, Mar. 2006.

[2] Kemalis, K. and T. Tzouramanis. SQL-IDS: A Specification-based Approach for SQL injection Detection. SAC'08. Fortaleza, Ceará, Brazil, ACM 2008, pp. 2153-2158.

[3] Fu, X., Lu, X., Peltsverger, B., Chen, S., Qian, K, and Tao, L., A Static Analysis Framework for Detecting SQL Injection Vulnerabilities. Proc. 31st Annual International Computer Software and Applications Conference 2007 (COMPSAC 2007), 24-27 July (2007), pp. 87-96.

[4] Thomas, S., Williams, L., and Xie, T., On automated prepared statement generation to remove SQL injection Vulnerabilities. Information and Software Technology, Volume 51 Issue 3, March 2009, pp. 589–598.

[5] Ruse, M., Sarkar, T., and Basu. S., Analysis & Detection of SQL Injection Vulnerabilities via Automatic Test Case Generation of Programs. Proc. 10th Annual International Symposium on Applications and the Internet, 2010, pp. 31-37.

[6] Junjin, M., An Approach for SQL Injection Vulnerability Detection. Proc. of the 6th International Conference on Information Technology: New Generations, Las Vegas, Nevada, April 2009, pp. 1411-1414.

[7] Haixia, Y. and Zhihong, N., A database security testing scheme of web application. Proc. of 4th International Conference on Computer Science & Education 2009 (ICCSE '09), 25-28 July 2009, pp. 953-955.

[8] Roichman, A., Gudes, E., Fine-grained Access Control to Web Databases. Proceedings of 12th SACMAT Symposium, France 2007.