ISSN (Online): 2456-0448
International Journal of Innovative Research in Management, Engineering and Technology
Vol. 6, Issue 4, April 2021

Opinion Minning For Comment Sentiment Analysis Using Machine Learning

[1] D. Rajapriya,[2] K.Rohini

[1] Head Of The Department

[1][2] Department Of Computer Science And Engineering, Rvs Technical Campus, Coimbatore-641402, Anna University, Chennai, India

Abstract *Opinion mining for comment sentiment analysis is the field of study that analyzes people's opinions, sentiments, evaluations, attitudes and emotions from written languages. The system uses sentiment analysis methodology in order to achieve desired functionality. This project is a web application where the registered user will view the product and product features and will comment about the product. System will analyze the comments of various users and will rank product. We use a database of sentiment based keywords along with positivity or negativity weight in database and then based on these sentiment keywords mined in user comment is ranked. Comment will be analyzed by comparing the comment with the keywords stored in database. The system takes the comments of various users, based on the comment, system will specify whether the product is good, bad or worst. Once user login to the system he can view the product and product features. After viewing the product user can comment about the product. User can also view the comment of other user's. The role of the admin is to add product to the system and to add keywords to the database. By this application user can easily identify his needs.*

1. INTRODUCTION

In the field of security, the popularization and application of Internet, communications and computer network technology has been rapid development, especially the emergence of the Internet, makes the computer used in government, business, business, education, health care and other areas of society at an unprecedented rate, which are profound impact on people's economic, work and live. Attackers target the network, database; make the database information security under serious threat.

Structured Query Language (SQL) is a language that is used to query, operate, and administer database systems such as Microsoft SQL Server, Oracle, or MySQL. The general use of SQL is consistent across all database systems that support it. Web Intrusion refers to any attempt to threaten the confidentiality or availability of data in web application. SQL injection is a code injection technique used to attack data-driven applications, in which malicious SQL statements are inserted into an entry field for execution (e.g. to dump the database contents to the attacker). It consists of insertion or injection of a SQL

query via the input data from the client to the application. A successful SQL injection statement can read sensitive data from the database, modify database data (such as Insert/Update/Delete), execute administration operations on the database (such as shutdown the DBMS), recover the content of a given file present on the DBMS file system.

SQL injection can be used to perform the following types of attacks:

- Authentication Bypass: This attack allows an attacker to log on to an application, potentially with administrative privileges, without supplying a valid username and password.
- Information Disclosure: This attack allows an attacker to obtain, either directly or indirectly, sensitive information in a database.
- Compromised Availability of Data: This attack allows an attacker to delete information with the intent to cause harm or delete log or audit information in a database.

I. LITERATURE SURVEY

[1] Analysis of Field Data on Web Security Vulnerabilities

Most web applications have critical bugs (faults) affecting their security, which makes them vulnerable to attacks by hackers and organized crime. To prevent these security problems from occurring it is of utmost importance to understand the typical software faults. This paper contributes to this body of knowledge by presenting a field study on two of the most widely spread and critical web application vulnerabilities: SQL Injection and XSS. It analyse the source code of security patches of widely used web applications

written in weak and strong typed languages. To understand how these vulnerabilities are really exploited by hackers, this paper also presents an analysis of the source code of the scripts used to attack them. The outcomes of this study can be used to train software developers and code inspectors in the detection of such faults.

[2] A Black-Box Testing Tool for Detecting SQL Injection Vulnerabilities

Web applications vulnerabilities allow attackers to perform malicious actions that range from gaining unauthorized account access to obtaining sensitive data. The number of web application vulnerabilities in last decade is growing constantly. Improper input validation and sanitization are reasons for most of them. The most important of these vulnerabilities based on improper input validation and sanitization is SQL injection (SQLI) vulnerability. The primary focus of our research was to develop a reliable black-box vulnerability scanner for detecting SQLI vulnerability - SQLIVDT (SQL Injection Vulnerability Detection Tool). The black-box approach is based on simulation of SQLI attacks against web applications. Thus, the scope of analysis is limited to HTTP responses and HTML pages received from the application server.

[3] Attack Model Based Penetration Test for SQL Injection Vulnerability

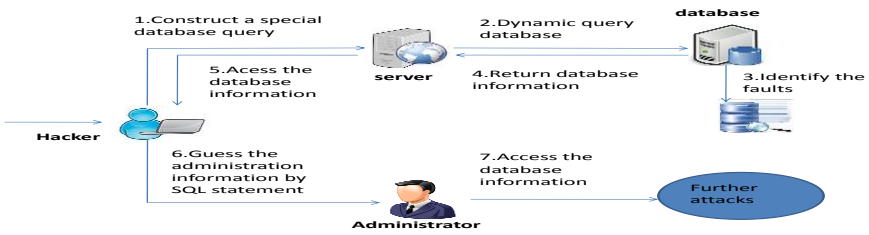
The penetration test is a crucial way to enhance the security of web applications. Improving accuracy is the core issue of the penetration test research. The test case is an important factor affecting the penetration test accuracy. In this paper, we discuss how to generate more effective penetration test case inputs to detect the SQL injection vulnerability hidden behind the inadequate blacklist filter defence mechanism in web applications. We propose a model based penetration test method for the SQL injection vulnerability, in which the penetration test case generation is divided into two steps: i) Building model for the penetration test case, and ii) Instantiating the model of penetration test case. Our method can generate test case covering more types and patterns of SQL injection attack input to thoroughly test the blacklist filter mechanism of web applications. Experiments show the penetration test case generated by our method can effectively find the SQL injection vulnerabilities hidden behind the inadequate blacklist filter defence mechanism thus reduce the false negative and improve test accuracy.

EXISTING SYSTEM AND ITS DRAWBACKS

Existing system emphasizes on several security aspects, including access privacy. As network security practitioners put more resources and effort in to defending against SQL INJECTION ATTACKS, hackers will develop and deploy the next generation of SQLIA (SQL Injection Attacks) bonnets with different control architecture.
A SQL injection attack is an attack that is aimed at subverting the original intent of the application by submitting attacker-supplied SQL statements directly to the backend database. Through this a hacker can easily enter into a user account and access their own information. Thus, he can easily execute oracle function from the select statement. If a DBA knows the user password, he can easily access user account without user permission. Traditionally, as soon as confidentiality becomes a concern, data is encrypted before outsourcing to a service provider.
In the existing system, the faults in the web page are identified using join algorithm but it is not prevented. The authentication process is not secured since there is only single level encryption. User can add SQL injection attacks to the database. It allows execution of oracle function or custom function using the select statement.

EXISTING SYSTEM ARCHITECTURE

The existing system architecture is shown in the below Fig 3.1



ISSN (Online): 2456-0448
International Journal of Innovative Research in Management, Engineering, and Technology
Vol. 6, Issue 4, April 2021

Fig 3.1 Architecture of Existing system

ADVANTAGES OF EXISTING SYSTEM

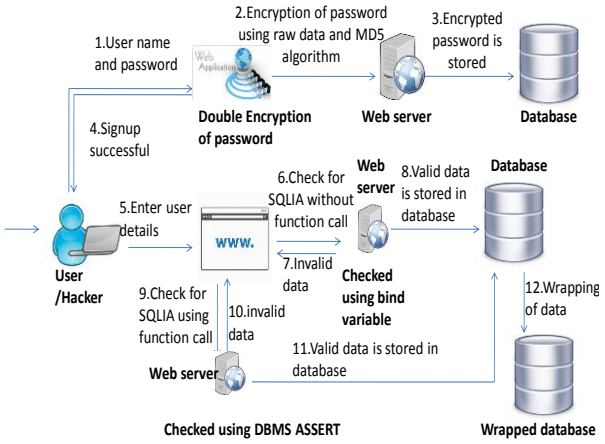
- SQL Injection Attack identification is done.
- Single level security is provided.

DISADVANTAGES OF EXISTING SYSTEM

- Bypasses the login authentication.
- Selects secured information from database tables .
- Security mechanisms are not that efficient in existing system.
- Using function call all the field data can be viewed by the hackers.
- Only single level security for web databases have been made possible.

PROPOSED SYSTEM AND ITS ADVANTAGES

The proposed system is developed with the things that eradicate the drawbacks of the existing system. In the proposed system, privacy enabled secure database is built. The security level is much enhanced from its actual level. The DBA cannot view the user details in its original form. The hacker cannot enter the user login by using tricky queries, cannot run the in-built function in it etc. The faults in the web page are identified and validated using bind variable and DBMS assert. The authentication process can be secured by using double level security. User cannot add SQL injection attacks to the database. User cannot call oracle function or custom function.



A. Fig:4.2.1 System architecture

ADVANTAGES OF PROPOSED SYSTEM

- Avoid unauthorized access to the application.
- User cannot get secure information from database.
- User cannot add SQL injection attacks to the database.
- User cannot call oracle function or custom function.

CONCLUSION

The proposed method shows a deep learning system that classifies objects and facilities in high resolution multi-spectral satellite imagery. The system consists of an ensemble of CNNs with deep learning libraries that combine the predictions from the RF

algorithm with satellite metadata. Combined with a detection component, the system could search large amounts of satellite imagery for objects or facilities of interest. In this way it could solve the problems in various fields. By monitoring a store of satellite imagery, it could help law enforcement officers detect unlicensed mining operations or illegal fishing vessels, assist natural disaster response teams with the mapping of mud slides or hurricane damage, and enable investors to monitor crop growth or oil well development more effectively

FUTURE ENHANCEMENT

This proposed work uses images that have been already taken by any satellite. So the images may be taken before a long time can challenge the security. For that to enable accuracy and security live streaming from satellite can be enabled by using high quality cameras. The proposed work is based on images, but it can also extend for videos taken by satellite by using efficient streaming equipment.

REFERENCES

[1] 1. M. Pritt and G. Chern, "Satellite Image Classification with Deep Learning," 2017 IEEE Applied Imagery Pattern Recognition Workshop (AIPR), Washington, DC, 2017, pp. 1-7.
[2] L. Zhang, Z. Chen, J. Wang and Z. Huang, "Rocket Image Classification Based on Deep Convolutional Neural Network," 2018 10th International Conference on Communications, Circuits and Systems (ICCCAS), Chengdu, China, 2018, pp. 383-386.
[3] C. Shen, C. Zhao, M. Yu and Y. Peng, "Cloud Cover Assessment in Satellite Images Via Deep Ordinal Classification," IGARSS 2018 - 2018 IEEE International Geoscience and Remote Sensing Symposium, Valencia, 2018, pp. 3509-3512.
[4] T. Postadjian, A. L. Bris, C. Mallet and H. Sahbi, "Superpixel Partitioning of Very High Resolution Satellite Images for Large-Scale Classification Perspectives with Deep Convolutional Neural Networks," IGARSS 2018 - 2018 IEEE International Geoscience and Remote Sensing Symposium, Valencia, 2018, pp. 1328-1331.
[5] Q. Liu, R. Hang, H. Song and Z. Li, "Learning Multiscale Deep Features for High-Resolution Satellite Image Scene Classification," in IEEE Transactions on Geoscience and Remote Sensing, vol. 56, no. 1, pp. 117-126, Jan. 2018.
[6] T. Postadjian, A. L. Bris, H. Sahbi and C. Malle, "Domain Adaptation for Large Scale Classification of Very High Resolution Satellite Images with Deep Convolutional Neural Networks," IGARSS 2018 - 2018 IEEE International Geoscience and Remote Sensing Symposium, Valencia, 2018, pp. 3623-3626.
[7] P. Helber, B. Bischke, A. Dengel and D. Borth, "Introducing Eurosat: A Novel Dataset and Deep Learning Benchmark for Land Use and Land Cover Classification," IGARSS 2018 - 2018 IEEE International Geoscience and Remote Sensing Symposium, Valencia, 2018, pp. 204-207. [8] K. Cai and H. Wang, "Cloud classification of satellite image based on convolutional neural networks," 2017 8th IEEE International Conference on Software Engineering and Service Science (ICSESS), Beijing, 2017, pp. 874-877.
[8] A. O. B. Özdemir, B. E. Gedik and C. Y. Y. Çetin, "Hyperspectral classification using stacked autoencoders with deep learning," 2014 6th Workshop on Hyperspectral Image and Signal Processing: Evolution in Remote Sensing (WHISPERS), Lausanne, 2014, pp. 1-4.
[9] M. Lavreniuk, N. Kussul and A. Novikov, "Deep Learning Crop Classification Approach Based on Sparse Coding of Time Series of Satellite Data," IGARSS 2018 - 2018 IEEE International Geoscience and Remote Sensing Symposium, Valencia, 2018, pp. 4812-4815.
[10] L. Bragilevsky and I. V. Bajić, "Deep learning for Amazon satellite image analysis," 2017 IEEE Pacific Rim..