REVIEW ON DETECTION OF SQLi AND XSS ATTACKS

[1]Varsha Venkatesh, [2]B.U. Kavya, [3]Sri Harsha A, [4]Architha J, [5]Deepthi V S
[1]UG student, [2] UG student, [3]UG student, [4]UG student, [5]Assistant Professor,
[1]Department of Information Science and Engineering,
[1]Global Academy of Technology, Bengaluru, India.

Abstract : Now a days, people are mostly dependent on internet for many things such as online shopping, bank transactions, internet surfing and many more. Also, adoption of web in areas like communications and productivity via the Internet has outpaced user security awareness. Technologies like smart devices and high-speed mobile networks have allowed for an always-connected vector of malware, fraud, virus, spyware and other complications. The rapid digitalization of the world has increased the usage of online services due to which vast amount of information is shared over the internet. The web-based applications that accept critical information from users stock this information in databases. These applications and the databases are susceptible to all kinds of information security threats due to being accessible through the Internet. Regardless of intent or cause, the consequences of a web threat may vandalize both individuals and organizations. The threats include attacks such as Cross Site Scripting (XSS), Denial of Service Attack, SQL Injection attacks, Phishing attacks, Man in the Middle attack, Brute force attacks, water hole attacks and many more. Among these, SQLi and XSS are the two major web application attacks. This paper focuses on the survey of various approaches used to detect SQLi and Cross Site Scripting (XSS)attacks.

IndexTerms **- Malware, virus, spyware, Web application attacks, SQL Injection attacks, Cross Site Scripting (XSS), Denial of Service Attack, Phishing attacks, Man in the Middle attack, Brute force attacks, water hole attacks.**

I. INTRODUCTION

A cyber-attack is any kind of offensive action that targets computer information systems, small businesses, government agencies or sensitive personal information and business information using various strategies to steal, alter or destroy data systems and many more.

Web attacks: It is the attack during which some data will be injected into a web application to control the application and fetch the desired data. There are client-side vulnerabilities and server-side vulnerabilities that cause a web application attack.

Most Common kinds of Web Attacks:

• Cross-site scripting (XSS): It involves an attacker uploading malicious code onto a website which can then be used to steal the data. This strategy can cause significant damage to the information systems.

• SQL Injection (SQLI): This occurs when an attacker submits harmful code into an input form. If a system fails to scour this data, it is often submitted into the database where it can expose, alter or delete the data.

• Path traversal-results from improper protection of data that has been entered, these web server attacks involve injecting patterns into the webserver hierarchy that permit attackers to get user credentials, databases, configuration files and other sensitive data stored on hard drives.

• Local File Inclusion: This comparatively uncommon attack involves forcing the web application to execute a file situated elsewhere on the system.

• Distributed Denial of Service (DDoS) attacks: Such harmful events happen once a hacker bombards the server with requests. In several cases, hackers use a network of compromised computers or bots to mount this offensive. Such actions paralyze the server and forestall legitimate guests from gaining access to the services.

• Server aspect includes (SSI): Server side includes injection vulnerability permits an attacker to exploit a web application by injecting scripts or SSI directives in HTML pages. SSI injection attack is achieved through manipulation of SSI employed within the application through user inputs.

• OS command injection (also called shell injection): may be a web security vulnerability that enable a hacker to execute discretional software (OS) commands on the server that is running an application, and usually compromise the application and its information.

Cyber Security plays a vital role in the field of information technology. Cyber security is a way of defending computers, servers, networks, electronic systems and data from malicious attacks. Securing the data has become one of the greatest challenges nowadays. Today internet is the fastest growing infrastructure in daily life. In today's technical world, several latest technologies are changing the face of the mankind. However, due to the rapid growth of these technologies, it is difficult to safeguard the private data in an effective manner and hence cybercrimes are increasing day by day. Web applications do raise variety of security issues from improper cryptography. Serious vulnerabilities permit criminals to gain direct access to databases so as to steal sensitive data – this is often known as web attack.

Traditionally, machine learning algorithms were used in the security events to profile and baseline every user and network element in the IT environment. Now, deep learning-based models are used to detect many other types of anomalies.

1.1 Scope

Cyber Security is an important component of any company or enterprise across the world, hence the scope of Cyber Security is gigantic. Cyber Security is the process and practice, designed to safe guard devices, programs, and data from attacks and other unauthorized access. Many authorized institutions like the financial institutions, military, government agencies, Banking Sector, etc. have confidential data that's stored on computers and transmitted to networks. With growing cyber-attacks, it has become

necessary to safe guard this sensitive data and private information. Here stopping the identity theft isn't the sole goal, but protecting data integrity equally important. As cybercriminals are getting more advanced, there is a requirement to know their change in target, how are that affecting organizations, and their methods used in targeting.

1.2 Motivation

Cybercrime is an illegal activity that involves a series of issues for committing a crime which remains as a growing challenge in terms of security and privacy practices. Today's interconnected world makes everyone more vulnerable to cyber-attacks. The threat of attacks on web applications to extract data or to distribute malicious scripts persists. Few security issues with web applications are XSS attacks, SQL injection, Local file inclusion, Path traversal and many more. Some of these attacks are designed to prevent competitors from participating in major events, while others target the entire shutdown of online businesses for months. Effects of these attacks include: Authentication bypass, information disclosure, compromised data integrity, user's session hijacking, and access cookies.

II. LITERATURE REVIEW

In [1], the author Sonali Mishra proposed a method that detects SQL injection attacks using a machine learning based heuristic algorithm. The pre-processed spreadsheet file which contained injected and non-injected SQL statements was imported into the proposed feature extractor. The feature extractor analyses the statements and generates a feature array for each. A MATLAB program was developed to investigate each statement and analyze it to produce an array of features. The features that were selected are: presence of comment character, number of semicolons, the number of commands per statement, presence of always true conditions, presence of abnormal commands, and presence of special key words. The dataset consists of 616 SQL statements. The MATLAB classification learners were used to train and test the dataset with 23 different machine learning algorithms. Based on the accuracy of the results the best five classifiers to develop the proposed SQL injection detection system were selected. The proposed system was extensively tested, and the results showed that both Ensemble Boosted and Bagged Trees classifiers provided the highest classification accuracy (93.8%). The system was also scalable to easily implement minor modifications. To enhance the efficiency of the system, more non-injected SQL statements need to be considered in the dataset and more features need to be studied and experimented in future.

In [2], the authors of the paper Musaab Hasan, Zayed Balbahaith, and Mohammed Tarique, proposed the usage of machine learning algorithm called Gradient Boosting Classifier from ensemble machine learning approaches to classify and detect SQL Injection attacks. Naive Bayes classifier was used to classify between malicious and non-malicious SQL queries. To train the model they have used a training dataset that consists of both malicious and non-malicious SQL queries and also every query in the training data was labelled. The dataset was divided into two parts. The first part consists of plain text sentences of 4000 rows and the second part consists of SQL injected statements of 6000 rows that were created from a tool named Libinjection. Regex in python was used for tokenizing each entry in both the SQL Injection and plain-text datasets. After tokenization of the dataset, feature extraction was performed on the data and G-test scores; entropy was calculated for all token values in dataset. The prediction accuracy of Naïve Bayes classifier was 92.8% and gradient boosting classifier was 97.4%. The results from both experiments show that Gradient Boosting approach does perform better in terms of prediction accuracy. The model identified all three types of SQL Injection attacks. Gradient boosting has several trade-offs: gradient boosting is computationally expensive than simple classifiers in terms of memory and computation. They are more susceptible to overfitting and tend to take longer time in learning phases. The machine learning model can also be advanced further with better feature extraction.

In [3] the author Harsh Bhagwani proposed a method that uses logs for intrusion detection of web applications. This aims to address the classification of malicious HTTP requests received by a web application and identification of the smallest attack requests. The dataset consists of a total of 50116 samples, out of which 35006 were valid requests and 15110 were attack requests. Dataset has been created using Torpeda framework. Data processing involves URL Decoding of the requests, Lowercasing the requests (except CRLF where we are uppercasing the requests) and Replacing some characters. These features are labelled as 0/1 showing whether a particular keyword or punctuation is present or not in the HTTP request and these features have been validated with all the classifiers using k-fold cross validation with k=10. The 6 classifiers were used to detect all the attacks. Random Forest model provides accuracy of 99.34% was considered best classifier to detect XSS. For SQLi, Random Forest classifier provides highest accuracy of 97.91%. Gradient boosting and Random Forest classifiers provide best accuracy of 99.28% while detecting Path traversal attack. Lightweight Directory Access Protocol (LDAP) Injection was detected better with SVM classifier with accuracy of 99.89%. XML Path (XPath) Injection was detected by Random Forest with high accuracy of 99.89%. Gradient boosting was able to detect OS command injection with the accuracy of 98.13%. Server Side Includes (SSI) Injection was detected best by Random Forest Algorithm with accuracy of 99.89%. Carriage Return Line Feed (CRLF) was detected by all the classifiers with accuracy of 100%. Any Anomaly Detection was detected by Random forest with accuracy of 96.92%. The models which were used have shown good results in the discovery of attacks. The proposed work gives a good average detection accuracy of 99.02%, and use of subsequent attack models has made the system more robust.

In [4] the authors Xin Xie, Chunhui Ren, Yusheng Fu, Jie Xu, and Jinhong Guo proposed a method to detect SQL injection based on Elastic-Pooling CNN (EPCNN). Elastic-Pooling CNN uses text-CNN and spp-net can output fixed size of one-dimensional vectors one-dimensional vectors when non-fixed size matrices input to them. These methods can realize text classification of different lengths and image recognition of different sizes, but the output is a one-dimensional vector. In Data pre-processing Word2vec method is used to vectorize each original query string and the single character is used as the minimum training unit Elastic-Pooling CNN for SQL injection detection mainly uses regular matching. Regular technology has high recognition accuracy and speed. Elastic-Pooling CNN methods cannot identify new attacks. The accuracy obtained using Elastic-Pooling CNN is 99%.

In [5], the authors Rajashree A. Katole, Dr. Swati S. Sherekar, Dr. Vilas M. Thakare, proposed a method that detected SQL injection attacks by using a combined static and dynamic analysis. The attribute values of a fixed parameter value are the static

query. Dynamic queries are the attribute values with dynamic pretender values. These two queries are compared and if they are the same then it is a normal query, else it is a malicious query. It could detect all types of SQL injection. A total of 120 questions were issued for each page of which 45 were malicious and 75 were normal. All the 75 normal queries were labelled normal and 40 out of 45 malicious queries were detected., hence raising the detection rate to 96%. The work on efficient methods for detecting the SQL injection attack and methods to prevent it. A less time must be consumed to detect the SQL injection for more new and robust methods are to be developed. Impact on business must be understood to reduce the risk of SQLi attack.

In [6], Zhuang Chen, Min Guo, Lin zhou, proposed an approach that detects SQL injection based on SVM. The dataset consists of black and white samples. A 1000 samples of SQL injected in GitHub and exploitdb. The texts in the dataset are broken into word segmentation and one hour encoded. Word to Vec is a way to express text features as N-dimensional vectors. Words such select, Union, null, where are marked and others are marked as none. Support vector machine algorithm is used to classify the SQLi which provides an accuracy of 95%. However, there are some problems faced in practical application. In order to identify malicious behaviour from a large number of labels and combinations of the functions and high-quality dataset. Secondly, word 2vec saves the text vector into memory. The memory required for model training depends on the size of the dataset.

In [7] the authors Fawaz A. Mereani and Jacob M. Howe, proposed machine learning approach to detect stored XSS with high accuracy and precision. The paper collects both malicious and benign scripts in order to balance dataset. For the training set, malicious scripts were obtained from developer sites, a selection from XSSed, the largest online archive of XSS vulnerable websites and additional scripts were collected by crawling sites known to be untrustworthy. Structural Features: They contain complete set of non-alphanumeric characters that can occur in JavaScript. Behavioral Features: These are a selection of the commands and functions that can be used in JavaScript. The feature data is used as input for supervised learning algorithms. In this work, support vector machines (SVM), k-nearest neighbor (k-NN), and Random Forests. Two variations on SVMs are used, with a linear kernel and with a polynomial kernel. The training dataset was divided at random into five folds, with training on four of the five folds. SVM (Linear Kernel) Evaluation provided an average accuracy of 94.74%. SVM (Polynomial Kernel) Evaluation provides average accuracy of 97.06%. 97.12% average accuracy was obtained using k-NN Classifier Evaluation. Random Forest Classifier Evaluation provides average accuracy of 97.22%. These classifiers can be added as a security layer either in a browser or (as intended) on a server. Future work is to investigate these aspects, as well as to use the same features with a Neural Network classifier.

In [8] the authors Melody Moh, Santhosh Pininti, Sindhusha Doddapaneni, and Teng-Sheng Moh, proposed a method to detect web attacks using multi-stage log analysis. Most existing solutions for detecting these attacks use log analysis, and employ either pattern matching or machine learning methods. One commonly used pattern matching methods is ELK (Elasticsearch, Logstash, and Kibana).Pattern matching methods can be effective, dynamic they however cannot detect new kinds of attacks. Supervised machine learning methods can detect new attacks. This work proposes a multi-stage log analysis architecture, which combines both pattern matching and supervised machine learning methods. It uses logs generated by the application during attacks to effectively detect attacks and to help preventing future attacks. the two-stage system has combined the advantages of both systems, and has substantially improved the detection accuracy. The multi-stage log analysis concept would be highly applicable to many intrusion detection applications. Single-Stage Architecture: Using Kibana, the pattern matching method results in 85.3% accuracy in detecting the SQL injections. Using Machine Learning method results in 80.04% accuracy. Multi-stage Architecture: Pattern Matching followed by Machine Learning this combination has achieved 94.7 % accuracy. Machine Learning followed by Pattern Matching this combination has achieved 95.4% accuracy.

In [9], the authors Kunal Gupta, Rajni Ranjan Singh, Manish Dixit, proposed a system that detects Cross-Site Scripting (known as XSS) attack using Intrusion Detection system (IDS). Here attack signature was utilized to detect XSS attack. To test the usefulness and effectiveness of proposed work a proof-of-concept prototype was implemented using SNORT IDS. The process includes capturing of all the packets that are in transition on the network and selection of relevant packets that are filtered. Here selective packet capturing is done. Next, signature-based detection was applied on the selective packets in this case only TCP packets were used. After detection, the alerts were generated, and metadata logs were created. A Cisco tool SNORT IDS was installed on the Network to inspect the network traffic data and then packets were filtered according to rules provided on the tool Snort. The components of snort architecture included: The sniffer, The pre-processor, The detection engine and the output. When the console was run, all attacks were detected effectively then it created alerts and logs successfully. After successful implementation of rule, XSS attack was able to be detected through Alert File containing details of the attack and attack was also logged in the form of dumps as metadata in same directory in snort. Experiments were done in real network environment. Few false-positive were generated, but it caught all the scripting attack successfully. The speed of the detection process can be increased using other keywords with Perl Compatible Regular Expression (PCRE) in future.

In [10], the authors Shailendra Rathore, Pradip Kumar Sharma, Jong Hyuk Park, proposed a system that detects XSS attacks using machine learning classifier on SNS. Social Networking servicing applications such as Twitter, Facebook have certain features on the webpages which make these applications more susceptible to the XSS attack. The proposed approach has four major steps: feature identification, collection of webpages, feature extraction and training dataset construction, and machine learning classification. The paper lists three main features: URL feature, HTML tag feature, SNS features. In the second step collecting webpages, A database is created by collecting malicious and benign webpages from internet resources such as XSSed, Alexa, Elgg. Each webpage is manually labeled as XSS or non-XSS based on extracted features and the training dataset is 1000 webpages in which 400 malicious and 600 benign webpages were constructed. Decorate and ADTrees were the two machine learning classifiers used to classify the instance. ADTree provides an accuracy of 97% and Decorate provides an accuracy of 96%. The two major contributions in the area of SNS. Firstly, it provides an analysis on recent characteristics of SNS. Secondly, the paper purposed a machine learning approach to detect XSS attacks. In the future, the enhancement in the proposed future set is required. Secondly, it can enhance its application to advanced machine learning algorithms such as deep learning and extreme machine learning.

In [11], the author Deepthi V S proposed a Behaviour Analysis and Detection of Blackhole Attacker Node under Reactive Routing Protocol in MANETs. This paper's objective is to analyze the effects of blackhole attack under reactive routing protocol such as Adhoc on Demand Distance Vector routing (AODV). The working of the proposed Blackhole Detection model is as follows: First the sender sends Route Request message to the next nodes for fetching the path to destination node. In return the RREP messages are arrived at the sender node which are sent from multiple paths. The first RREP message which is received is considered to be as response from malicious node and that route is discarded by the sender and removes its entry in the routing table. The source can then send the data through the path where it has got the second RREP message. The performance of this protocol is assessed to find the vulnerability of attack and also compared the impact of attack on both AODV, AODV with blackhole and proposed AODV protocols. The proposed model is simulated in NS-2 against blackhole attack. Comparatively the data loss that occurred due to malicious node has been decreased. The delay is decreased by increase in throughput. There is 99.7% average packet delivery ratio, which is nearing 100%. The average energy consumed by each node is 15.78 joules and total energy consumed is 789 joules for a packet size of 1500. The number of packets dropped is 20 for AODV and zero for proposed AODV approach. Throughput achieved is 51.25 with blackhole and 100% in proposed method. In future, the analysis of malicious behaviour can be done for different routing protocol.

In [12], the author Deepthi V S proposed a multiphase detection and evaluation of AODV for Malicious Behaviour of a node in MANETs. The proposed solution involves the detection of malicious node by checking the destination node sequence number with the next node seq number. The detection of malicious behaviour is done by the three phases. The first phase is to set the location and mobility of the node to transfer the packets from sender to receiver. In the second phase, the malicious node can be introduced to analysis the network behaviour. These malicious nodes are responsible to degrade the overall performance of MANET by creating false reply messages and by creating congestion which leads to packet drop. The phase three is responsible identifying malicious node and avoiding the route by eliminating its entry in the routing table. The simulation of network model is carried out using ns2.35. The tcl scripts are written to analyze the performance of AODV and blackhole attacker node. The solutions given by the proposed system are tested for many numbers of nodes. The average packet delivery ratio achieved for this scenario recorded is 99.6%, 99.37%, 97.14%, 94.90% & 94.76% for 10,20,30,40 and 50 nodes respectively. Throughput achieved is 51.25 with blackhole and 100% in proposed method. The congestion window of aodv protocol is also analyzed. Comparatively the data loss that occurred due to malicious node has been decreased. The delay is decreased by increase in throughput. In future, the analysis of malicious behaviour can be done for different routing protocol.

Table 3.1: Brief Description on Literature Survey

Title of the paper and year	Methodology	Merits	Demerits
SQL Injection Detection Using Machine Learning Year: (2019, San Jose State University)	Naïve Bayes Classifier and Gradient Boosting Classifier from ensemble machine learning approaches to classify and detect SQL Injection attacks	Identifies union based, error based and Boolean SQL injections Good accuracy	Gradient Boosting approach is computationally expensive than simple classifiers in terms of memory and computation. More memory is needed to store multiple trees.
Detection of SQL Injection Attacks: A Machine Learning Approach Year: (2019, ICECTA)	Machine learning based heuristic algorithm to prevent the SQL injection attack.	System is also scalable is a sense that any enhancement can be easily implemented with minor modification.	more non-injected SQL statements need to be considered in the dataset
Log based Dynamic Intrusion Detection of Web Applications Year(2019,Indian Institute of Technology, Kanpur)	A new machine learning based IDS which feeds on the log files of the web applications to detect attacks like SQLi, XSS, CRLF etc. (LR, SVM, gradient boosting , decision trees, KNN, random forest)	proposed work gives a good average detection accuracy of 99.02%.	This can be extended to all the other areas like 'Accept-Encoding,' 'Cookie,' 'Referrer', etc.
SQL Injection Detection for Web Applications Based on Elastic-Pooling CNN Year: (2019,School of Information and Communication Engineering)	This paper proposes elastic pooling CNN technique to detect SQL injections.	Based on the irregular matching characteristics, it can identify new attacks and is harder to bypass.	Regular technology has high recognition accuracy and speed, but it cannot identify new attacks. It is inevitable that new bypassing methods will emerge to avoid rules such as URL multiple encoding.
Detection of SQL Injection Attacks by Removing the Parameter Values of SQL Query Year: (2018, IEEE)	The proposed workflow is to Compare the static and the dynamic query, And based on the result it is detected as SQL attack or not.	Combining existing SQL injection detection mechanisms to develop more strong mechanism to make web application more robust.	It works on efficient methods for detecting the SQL injection attack and methods to prevent it. A less time must be consumed to detect the SQL injections.
Research on SQL injection detection technology based on SVM Year:(2018, MATEC Web of Conferences)	SVM algorithm word2vec method is selected to process the text data of HTTP requests.	The proposed method effectively solves SQL injection mutation and overcomes the defects of the existing rule matching	Large numbers of dataset required Word2vec consumes large memory.

		methods.	
Detecting Cross-Site Scripting Attacks using Machine Learning Year: (2018, City, University of London Institutional Repository)	This paper detects using KNN, RF, SVM algorithms and compares them to provide better accuracy.	Structural and behavioral functions of XSS are checked and therefore accuracy increased.	Future works: Neural network classifier.
Detecting Web Attacks Using Multi-Stage Log Analysis Year:(2017, San Jose State University, USA)	This work proposes a multi-stage log analysis architecture, which combines both pattern matching and supervised machine learning methods.	The trained model had good accuracy with less probability of false alarm.	The techniques used are not compactable with the updated technologies.
CROSS SITE SCRIPTING (XSS) attack detection using intrusion detection system Year: (2017,ICICCS)	Here they are introducing snort rule that can detect XSS Attack efficiently and create an alert entry for it in snort alert file.	After successful implementation of rule, XSS attack was able to be detected through Alert File containing details of the attack and attack was also logged in the form of dumps.	Few false-positive were generated, not able to see the rejected packets on Iptables output.
XSS Classifier: An Efficient XSS Attack Detection Approach Based on Machine Learning Classifier on SNSs Year: (2017,Journal of information processing systems)	The proposed method is usage of ADTrees and decorates algorithms to detect the attack.	The features selected are URL, HTML tags. In addition, The Social Networking services (SNSs) features are added to provide and enhance the accuracy.	Enhancement in feature set and usage of Advance learning algorithm such as deep learning.
Behaviour Analysis and Detection of Blackhole Attacker Node under Reactive Routing Protocol in MANETs Year: (2018, IEEE)	The proposed method analyze the effects of blackhole attack under reactive routing protocol such as Adhoc on Demand Distance Vector routing (AODV), analysis is done by simulated using NS- 2.35 and QoS parameters.	100% packet delivery ratio and zero packets dropped for proposed AODV approach.	The number of packets dropped is 20 for AODV. In future, the analysis of malicious behaviour can be done for different routing protocol
Multiphase Detection and Evaluation of AODV for Malicious Behaviour of a node in MANETs. Year: (2018, ICEECCOT)	Detection of malicious node by checking the destination node sequence number with the next node sequence number. Simulation is carried out in ns-2.35.	The average packet delivery ratio achieved for this scenario recorded is 99.6%, 99.37%, 97.14%, 94.90% & 94.76% for 10,20,30,40 and 50 nodes respectively.	In future, the analysis of malicious behaviour can be done for different routing protocol.

III. CONCLUSION

Cyber-crime is constantly on the rise, and many smaller businesses are extremely vulnerable as a result of ineffective cyber security due to enormous usage of internet. The impact of cyber-crime can range from financial losses to business losses, due to which different industries can also suffer many disastrous consequences as a result of criminal cyberattacks. SQL injection can leave the application at a high-risk of compromise resulting in a threat to the integrity, and confidentiality of data as well as authorization and authentication aspects of the application. A successful attack may end in the unauthorized viewing of user lists, the deletion of tables and, in certain cases, the attacker gaining admin rights to a database, all of which are highly deleterious to a business. The effect of XSS attack ranges from user's Session Hijacking to disclosure of sensitive data, Cross site request forgery (CSRF) attacks and other security vulnerabilities. In times like these it is crucial to protect the sensitive personal and business information through prevention, detection and response to different online attacks. This paper describes different pattern matching and machine learning approaches proposed by various authors to detect SQLi and XSS attacks. In future, Deep learning can be used with web logs for an effective detection of these attacks.

IV. REFERENCES

[1] Mishra, Sonali. 2019. SQL Injection Detection Using Machine Learning. San José State University, Master's Projects. 727.

[2] Musaab Hasan, Zayed Balbahaith, and Mohammed Tarique. 2019. Detection of SQL Injection Attacks: A Machine Learning Approach. International Conference on Electrical and Computing Technologies and Applications (ICECTA), IEEE.

[3] Harsh Bhagwani. 2019. Log based Dynamic Intrusion Detection of Web Applications. Indian Institute of Technology, Kanpur.

[4] Xin Xie, Chunhui Ren, Yusheng Fu , Jie Xu , and Jinhong Guo. 2019. SQL Injection Detection for Web Applications Based on Elastic-Pooling CNN. IEEE Access (Volume: 7).

[5] Rajashree A. Katole, Dr. Swati S. Sherekar, Dr. Vilas M. Thakare. 2018. Detection of SQL Injection Attacks by Removing the Parameter Values of SQL Query. Proceedings of the Second International Conference on Inventive Systems and Control (ICISC 2018) , IEEE Xplore.

[6] Zhuang Chen, Min Guo, Lin zhou. 2018. Research on SQL injection detection technology based on SVM. MATEC Web of Conferences 173, 01004.

[7] Citation: Howe, J. M. and Mereani, F. 2018. Detecting Cross-Site Scripting Attacks Using Machine Learning. Advances in Intelligent Systems and Computing, 723, doi:10.1007/978-3-319-74690-6_20.

[8] Melody Moh*, Santhosh Pininti, Sindhusha Doddapaneni, and Teng-Sheng Moh. 2017. Detecting Web Attacks Using Multi-Stage Log Analysis Year. 6th International Conference on Advanced Computing, IEEE.

[9] Kunal Gupta, Rajni Ranjan Singh, Manish Dixit. 2017. CROSS SITE SCRIPTING (XSS) attack detection using intrusion detection system. International Conference on Intelligent Computing and Control Systems (ICICCS).

[10] Shailendra Rathore, Pradip Kumar Sharma, Jong Hyuk Park. 2017. XSSClassifier: An Efficient XSS Attack Detection Approach Based on Machine Learning Classifier on SNSs. Journal of information processing systems, 1014~1028.

[11] Deepthi V S. 2018. Multiphase Detection and Evaluation of AODV for Malicious Behaviour of a node in MANETs. Third International Conference on Electrical, Electronics, Communication, Computer Technologies and Optimization Techniques (ICEECCOT) 14-15, IEEE.

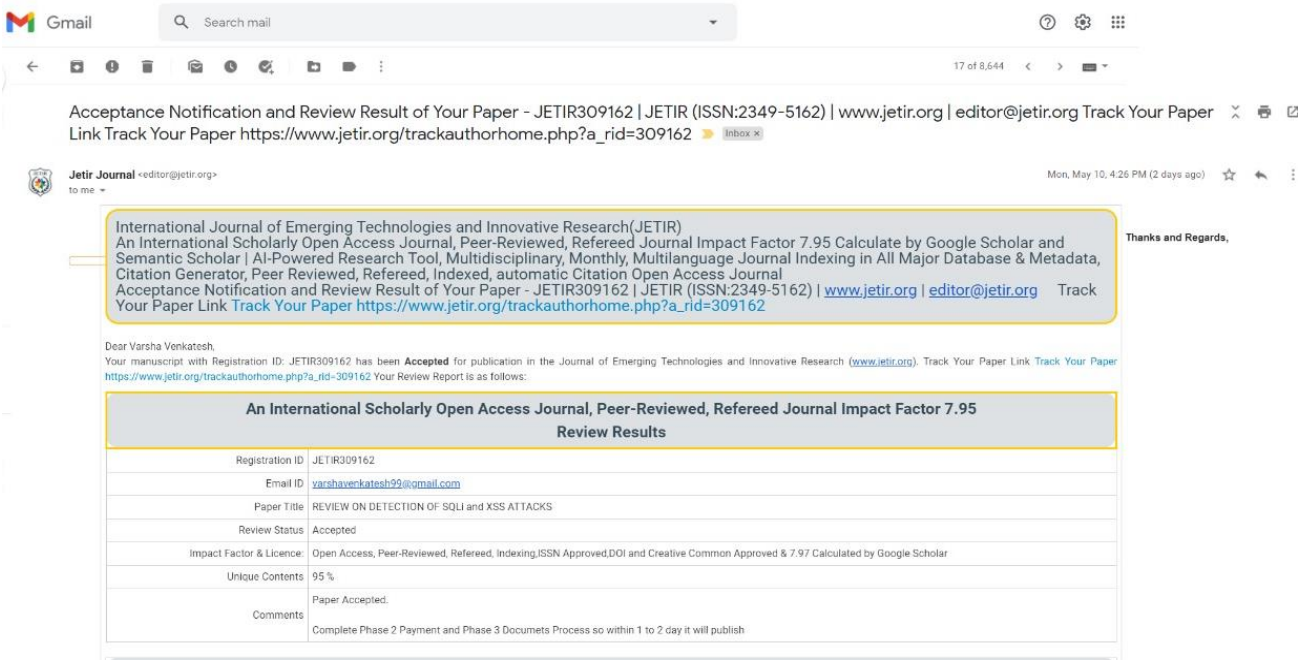
[12] Deepthi V S. 2018. Behaviour Analysis and Detection of Blackhole Attacker Node under Reactive Routing Protocol in MANETs. IEEE.

APPENDIX

A. Taxonomy:

IDS	**Intrusion Detection System**
XSS	**Cross Site Scripting**
CNN	**Convolutional Neural Network**
DOS	**Denial Of Service**

B. Proof of Acceptance:



Gmail Search mail

17 of 8,644

Acceptance Notification and Review Result of Your Paper - JETIR309162 | JETIR (ISSN:2349-5162) | www.jetir.org | editor@jetir.org Track Your Paper Link Track Your Paper https://www.jetir.org/trackauthorhome.php?a_rid=309162 Inbox ×

Jetir Journal <editor@jetir.org> to me

Mon, May 10, 4:26 PM (2 days ago)

International Journal of Emerging Technologies and Innovative Research(JETIR)
An International Scholarly Open Access Journal, Peer-Reviewed, Refereed Journal Impact Factor 7.95 Calculate by Google Scholar and Semantic Scholar | AI-Powered Research Tool, Multidisciplinary, Monthly, Multilanguage Journal Indexing in All Major Database & Metadata, Citation Generator, Peer Reviewed, Refereed, Indexed, automatic Citation Open Access Journal
Acceptance Notification and Review Result of Your Paper - JETIR309162 | JETIR (ISSN:2349-5162) | www.jetir.org | editor@jetir.org Track Your Paper Link Track Your Paper https://www.jetir.org/trackauthorhome.php?a_rid=309162

Thanks and Regards,

Dear Varsha Venkatesh,
Your manuscript with Registration ID: JETIR309162 has been **Accepted** for publication in the Journal of Emerging Technologies and Innovative Research (www.jetir.org). Track Your Paper Link Track Your Paper https://www.jetir.org/trackauthorhome.php?a_rid=309162 Your Review Report is as follows:

An International Scholarly Open Access Journal, Peer-Reviewed, Refereed Journal Impact Factor 7.95
Review Results

Registration ID	JETIR309162
Email ID	varshavenkatesh99@gmail.com
Paper Title	REVIEW ON DETECTION OF SQLI and XSS ATTACKS
Review Status	Accepted
Impact Factor & Licence:	Open Access, Peer-Reviewed, Refereed, Indexing,ISSN Approved,DOI and Creative Common Approved & 7.97 Calculated by Google Scholar
Unique Contents	95 %
Comments	Paper Accepted. Complete Phase 2 Payment and Phase 3 Documets Process so within 1 to 2 day it will publish

C. Details of Publication

1. **Name of the Journal/Conference:** Journal of Emerging Technologies and Innovative Research
2. **Impact Factor (if applicable):** 7.95
3. **Date of Publication: (dd/mm/yyyy):** 12/05/2021

Abstract of Published Paper:

© 2021 JETIR May 2021, Volume 8, Issue 5 www.jetir.org (ISSN-2349-5162)

REVIEW ON DETECTION OF SQLi AND XSS ATTACKS

[1]Varsha Venkatesh, [2]B.U. Kavya, [3]Sri Harsha A, [4]Architha J, [5]Deepthi V S
[1]UG student, [2] UG student, [3]UG student, [4]UG student, [5]Assistant Professor,
[1]Department of Information Science and Engineering,
[1]Global Academy of Technology, Bengaluru, India.

Abstract : Now a days, people are mostly dependent on internet for many things such as online shopping, bank transactions, internet surfing and many more. Also, adoption of web in areas like communications and productivity via the Internet has outpaced user security awareness. Technologies like smart devices and high-speed mobile networks have allowed for an always-connected vector of malware, fraud, virus, spyware and other complications. The rapid digitalization of the world has increased the usage of online services due to which vast amount of information is shared over the internet. The web-based applications that accept critical information from users stock this information in databases. These applications and the databases are susceptible to all kinds of information security threats due to being accessible through the Internet. Regardless of intent or cause, the consequences of a web threat may vandalize both individuals and organizations. The threats include attacks such as Cross Site Scripting (XSS), Denial of Service Attack, SQL Injection attacks, Phishing attacks, Man in the Middle attack, Brute force attacks, water hole attacks and many more. Among these, SQLi and XSS are the two major web application attacks. This paper focuses on the survey of various approaches used to detect SQLi and Cross Site Scripting (XSS)attacks.

IndexTerms **- Malware, virus, spyware, Web application attacks, SQL Injection attacks, Cross Site Scripting (XSS), Denial of Service Attack, Phishing attacks, Man in the Middle attack, Brute force attacks, water hole attacks.**

Certificates of Published Paper:

Journal of Emerging Technologies and Innovative Research
An International Open Access Journal Peer-reviewed, Refereed Journal
www.jetir.org | editor@jetir.org An International Scholarly Indexed Journal

Certificate of Publication

The Board of
Journal of Emerging Technologies and Innovative Research (ISSN : 2349-5162)
Is hereby awarding this certificate to
Varsha Venkatesh
In recognition of the publication of the paper entitled
REVIEW ON DETECTION OF SQLi and XSS ATTACKS
Published In JETIR (www.jetir.org) ISSN UGC Approved (Journal No: 63975) & 7.95 Impact Factor
Published in Volume 8 Issue 5 , May-2021 | Date of Publication: 2021-05-12

EDITOR EDITOR IN CHIEF
JETIR2105284 Research Paper Weblink http://www.jetir.org/view?paper=JETIR2105284 Registration ID : 309162
An International Scholarly Open Access Journal, Peer-Reviewed, Refereed Journal Impact Factor Calculate by Google Scholar and Semantic Scholar | AI-Powered Research Tool, Multidisciplinary, Monthly, Multilanguage Journal Indexing in All Major Database & Metadata, Citation Generator

Journal of Emerging Technologies and Innovative Research
An International Open Access Journal Peer-reviewed, Refereed Journal
www.jetir.org | editor@jetir.org An International Scholarly Indexed Journal

Certificate of Publication

The Board of
Journal of Emerging Technologies and Innovative Research (ISSN : 2349-5162)
Is hereby awarding this certificate to
B.U. Kavya
In recognition of the publication of the paper entitled
REVIEW ON DETECTION OF SQLi and XSS ATTACKS
Published In JETIR (www.jetir.org) ISSN UGC Approved (Journal No: 63975) & 7.95 Impact Factor
Published in Volume 8 Issue 5 , May-2021 | Date of Publication: 2021-05-12

EDITOR EDITOR IN CHIEF
JETIR2105284 Research Paper Weblink http://www.jetir.org/view?paper=JETIR2105284 Registration ID : 309162
An International Scholarly Open Access Journal, Peer-Reviewed, Refereed Journal Impact Factor Calculate by Google Scholar and Semantic Scholar | AI-Powered Research Tool, Multidisciplinary, Monthly, Multilanguage Journal Indexing in All Major Database & Metadata, Citation Generator

Journal of Emerging Technologies and Innovative Research
An International Open Access Journal Peer-reviewed, Refereed Journal
www.jetir.org | editor@jetir.org An International Scholarly Indexed Journal

Certificate of Publication

The Board of
Journal of Emerging Technologies and Innovative Research (ISSN : 2349-5162)
Is hereby awarding this certificate to
Sri Harsha A
In recognition of the publication of the paper entitled
REVIEW ON DETECTION OF SQLi and XSS ATTACKS
Published In JETIR (www.jetir.org) ISSN UGC Approved (Journal No: 63975) & 7.95 Impact Factor
Published in Volume 8 Issue 5 , May-2021 | Date of Publication: 2021-05-12

EDITOR EDITOR IN CHIEF
JETIR2105284 Research Paper Weblink http://www.jetir.org/view?paper=JETIR2105284 Registration ID : 309162
An International Scholarly Open Access Journal, Peer-Reviewed, Refereed Journal Impact Factor Calculate by Google Scholar and Semantic Scholar | AI-Powered Research Tool, Multidisciplinary, Monthly, Multilanguage Journal Indexing in All Major Database & Metadata, Citation Generator

Journal of Emerging Technologies and Innovative Research
An International Open Access Journal Peer-reviewed, Refereed Journal
www.jetir.org | editor@jetir.org An International Scholarly Indexed Journal

Certificate of Publication

The Board of
Journal of Emerging Technologies and Innovative Research (ISSN : 2349-5162)
Is hereby awarding this certificate to
Architha J
In recognition of the publication of the paper entitled
REVIEW ON DETECTION OF SQLi and XSS ATTACKS
Published In JETIR (www.jetir.org) ISSN UGC Approved (Journal No: 63975) & 7.95 Impact Factor
Published in Volume 8 Issue 5 , May-2021 | Date of Publication: 2021-05-12

EDITOR EDITOR IN CHIEF
JETIR2105284 Research Paper Weblink http://www.jetir.org/view?paper=JETIR2105284 Registration ID : 309162
An International Scholarly Open Access Journal, Peer-Reviewed, Refereed Journal Impact Factor Calculate by Google Scholar and Semantic Scholar | AI-Powered Research Tool, Multidisciplinary, Monthly, Multilanguage Journal Indexing in All Major Database & Metadata, Citation Generator

Journal of Emerging Technologies and Innovative Research
An International Open Access Journal Peer-reviewed, Refereed Journal
www.jetir.org | editor@jetir.org An International Scholarly Indexed Journal

Certificate of Publication

The Board of
Journal of Emerging Technologies and Innovative Research (ISSN : 2349-5162)
Is hereby awarding this certificate to
Deepthi V S
In recognition of the publication of the paper entitled
REVIEW ON DETECTION OF SQLi and XSS ATTACKS
Published In JETIR (www.jetir.org) ISSN UGC Approved (Journal No: 63975) & 7.95 Impact Factor
Published in Volume 8 Issue 5 , May-2021 | Date of Publication: 2021-05-12

EDITOR
EDITOR IN CHIEF

JETIR2105284 Research Paper Weblink http://www.jetir.org/view?paper=JETIR2105284 Registration ID : 309162

An International Scholarly Open Access Journal, Peer-Reviewed, Refereed Journal Impact Factor Calculate by Google Scholar and Semantic Scholar | AI-Powered Research Tool, Multidisciplinary, Monthly, Multilanguage Journal Indexing in All Major Database & Metadata, Citation Generator