DETECTION AND PREVENTION OF VARIOUS ATTACKS ON DATABASE IN BANKING WEB APPLICATION

[1]Shekhar Dhangar, [2]Ayushi Yadav, [3]Shubham Kadam, [4]Priya Mandhare, [5]Chandrama Thorat
[1]Students,
[1]Computer Engineering RSCOE,
[1]Savitribai Phule Pune University, Pune, India

Abstract-- This is a Banking web application which provides various functionalities to User and Admin. Admin can approve or reject user application. Admin can search customers by account number or customer name. Admin can see logs of attacks. User can do online transactions like Fund Transfer, Bill Payments (electricity bill, income tax, mobile recharge).we are using unsupervised machine learning, pattern matching & honeypot system. The application is protected by detecting different attacks such as SQL injection, URL injection, Cross site Scripting attack and Brute Force attack. User will get randomly generated username, password and pin number on his SMS. After every transaction user will get notification by message. User can see his account details and mini statement. AES-128 bit encryption and decryption is used for storing user details.

Index Terms— Unsupervised machine learning, Pattern matching, Honeypot system, AES 128 bit encryption and decryption technique.

I. INTRODUCTION

The extremely widely-used World Wide Web environment provides a rich set of targets for motivated attackers. The main goal of the attack is the disruption of service. To prevent these attacks and protect web applications from attacks we are implementing system which are going to use 'AES-128 bit algorithm'. In this we are using Banking application can do online transaction, and can detect attacks like SQL injection, Brute force attack, URL injection, Cross site scripting attack. Personal information of user get stored in database in encrypted format. Dynamic password and pin generates and send to user on his SMS. After every transaction user get notification by message. User can see his account details and mini statements. Because of attack on Database following things are happens with web server, and to avoid such problems we proposing this system. Because of attacks network performance getting down. Sometimes particular websites could not be open, unavailability of a particular web site, Inability to access any web site, increase in the number of spam emails received, sometimes a wireless or wired internet connection get disconnects.

II. RELATED WORK

SQL Injection Attack (SQLIA) has been consistently ranked among the top security threats against web applications for more than a decade. Nowadays, attackers use sophisticated tools to launch automated injection attacks. The problem of prevention and detection of SQLIA has been long attended by the research community, but hardly any solution exists for protecting multiple websites in a shared hosting environment. In this paper, we present a novel method to detect malicious queries using a twin Hidden Markov Model (HMM) ensemble and validate it with large set of benign and malicious queries collected from five sample web applications written in PHP and MySQL. Following the Multiple Classifier System (MCS) paradigm, we combine the output of individual HMMs to arrive at the final decision, which provides better accuracy and lower false alarms. The system is intended to work at the database firewall layer, therefore it can protect multiple web applications hosted on a shared server. The initial experimental results are very encouraging and indicate that the approach can effectively identify wide varieties of SQLIA with negligible impact on performance. The technique can be easily ported to other languages and database platforms without requiring major modifications.

III. OUR APPROACH

SQL Injection:-

SQL injection is a code injection technique, used to attack data-driven applications, in which nefarious SQL statements are inserted into an entry field for execution, so we are creating one database for SQL query which is going to store all the queries which attacker is going to enter and also some more queries we are going to store in database. If attacker type of query or data, then we are going to detect that query or data is authorised or not by scanning the database.

We are going to prevent this type of attack by using AES 128 Bit Encryption and Decryption . When database is scanned and we found that entered data is valid then we provide access to their account . In case Sql injection is detected then user will be blocked for 24 hrs.

Brute Force:-

We are detecting Brute Force Attack throw Loop detection method in which attacker will enter password multiple time by guessing. In this scenario we will provide user to enter their password only 3 times and this cycle of entering wrong is detected by loop detection method.

Mostly our Data is in AES 128 Bit Encrypted Format. To prevent Brute Force Attack, If user is Entering password for multiple time then loop Detection Technique is going to detect it and also it is going to check type of passwords which is entered is present in our database. If password is entered is wrong for 3 times then, we will block that account for 24 hours and will send message and email to user on registered number that his account is blocked for 24 hrs.

URL Injection:-

Mostly URL injection Attack is Done throw URL Information in which User name and password is visible so One initial option is to use Google to determine whether our website is harbouring spam links in the first place. For instance, we can search for our domain alongside keywords for spam by entering a site query such as: "site:www.websitename.com casino."

For Avoidance of URL injection Attack we create database and also all passwords and usernames are already there in database .URLs are stored in database in encrypted format using AES 128 Encryption and Decryption algorithm so that user is not able to get information of username and password throws URL injection Attack.

Cross Site Scripting Attack:-

In cross site scripting attacker can check user mostly visited time and website throw that he will use some HTML page to take user inputs attacking on website database so we generate on type scanner which detect this type of HTML pages.

In cross site scripting mostly user can get username and password directly, so here we are using AES 128 bit Encryption technique throw which user input will be totally Encrypted.

IV.CONCLUSION

Attack is conducted on a sufficiently large scale, entire geographical regions can be compromised. To prevent these attacks and protect web server we are implementing system which are going to use Unsupervised machine learning, Pattern matching, AES 128 bit encryption and decryption technique We presented a system, which is using a AES 128 bit encryption decryption Algorithm and Honeypot system. We also discussed various potential optimizations for improving performance .Using such techniques we can avoid web server from attacks. Effective Can detect and prevent attack efficiently. User get notification by SMS. No complicate hardware required.

V. REFERENCES

[1] "Silk." [Online]. Available: https://tools.netsa.cert.org/silk/

[2] "Cisco 2014 annual security report," Cisco, Tech. Rep., 2014. [Online]. Available: http://www.cisco.com/web/offer/gist_ty2_asset/Cisco_2014_ ASR.pdf

[3] "Ponemon 2014 ssh security vulnerability report," Venafi, Tech. Rep., 2014.

[4] N. Das and T. Sarkar, "Survey on host and network based intrusion detection system," International Journal of Advanced Networking and Applications, vol. 6, no. 2, pp. 2266–2269, Dec. 2014.

[5] T. Scholte, D. Balzarotti, and E. Kirda, "Have Things Changed Now? An Empirical Study on Input Validation Vulnerabilities in Web Applications," Computers & Security, 2012.

[6] TrustWave, "Trustwave 2015 Global Security Report." https://www2.trustwave.com/rs/815-RFM-693/images/2015_ TrustwaveGlobalSecurityReport.pdf, 2015. Accessed: 2015-04-10. [8] OWASP, "Top 10 Security Threats 2013." https://www.owasp.org/index. php/Top_10_2013-A1-Injection, 2013. Accessed: 2013-11-15

LITERATURE SURVEY:

YEAR OF PUBLICATION	PUBLICATION	METHODOLOGY	ATTACKS	FUTURE SCOAP	DRAWBACKS	TITLE	AUTHOR
2015	IEEE	Host-based detection, Machine learning	Brute Force	Using machine learning algorithm build the predictive model for detection of attacks	Traditional intrusion techniques have limitations for detecting sophisticated Attacks like DOS.	Detection of SSH Brute Force Attacks Using Aggregated Net flow Data	Maryam M. Najafabadi, Taghi M. Khoshgoftaar, Chad Calvert
2016	IEEE	Novel method to detect malicious queries using a twin Hidden Markov Model	SQL injection	Reducing the false alarm rate and improving the performance by running HMM evaluation on parallel threads	System has minimal performance impact which is imperceptible over the Internet	Detection of SQL Injection Attacks using Hidden Markov Model	Debabrata Kar, Khushboo Agarwal, and Suvasini Panigrahi
2016	IEEE	vulnerability test, web application test, test pattern generation, feature matrix	SQL injection	improve testing accuracy and efficiency effectively with considerable effectiveness and practicability	HTTP requests overall with little loss of accuracy under this kind of trade-off situation	An Effective Penetration Test Approach based on Feature Matrix for Exposing SQL Injection Vulnerability	Lei Liu1, Jing Xu1, Hongji Yang2, Chenkai Guo1, Jiehui Kang
2015	IEEE	vulnerability scanner	SQL injection, cross site scripting	a generic web vulnerability scanner that analyzes web sites for exploitable SQL and XSS vulnerabilities specially.	web application security vulnerabilities result from generic input validation problems.	Detection of Web Application Vulnerability Based on RUP Model	Deven Go,Nisha Shah
2013	IEEE	stack-smashing protector	Brute Force	protection against attacks several, specially when combined with other commonly used protection techniques, several orders of magnitude with a negligible cost	If it modify the coverage protection of the SSP technique. SSP technique fail to detect attacks.	Preventing brute force attacks against stack canary protection on networking servers	Hector Marco-Gisbert, Ismael Ripoll
2012	IEEE	Web Vulnerabilities, Authentication Bypass, Input Validation, Database Mapping	SQL injection, cross site scripting	products which are rising and likely to become essential parts of comprehensive online data protection strategies	Inherent limitations, Incomplete implementations, Complex frameworks, Runtime overheads	A Survey On Web Application Vulnerabilities(SQLIA,XSS)Exploitation and Security Engine for SQL Injection	Rahul Johari, Pankaj Sharma
2012	IEEE	Randomization, Vulnerability	SQL injection	Web application specific randomized encryption algorithm to detect and prevent.	Needs an additional proxy and computational overhead and keys.	Application Specific Randomized Encryption Algorithm to prevent SQL injection	Srinivas Avireddy

2015	IEEE	XSS vulnerabilities, black-box scanners	SQL injection, cross site scripting	Black-box scanner XSS has recently improved and the scanners are able to provide higher detection rate for stored XSS vulnerabilities	Want improved to correctly analyze server's response on SQL syntax error and to detect server's response.	Analysis of Effectiveness of Black-Box Web Application Scanners in Detection of Stored SQL Injection and Stored XSS	Muhammad Parvez, Pavol Zavarsky, Nidal Khoury
2012	IEEE	Piggy-backed Queries, Blind Injection	SQL injection	compare effctiveness, efficiance, stability, flexibility an performance of tools to show th strength and weackness of the tool.	Latest technologies not used.	Comparison of SQL Injection Detection and Prevention Techniques	Atefeh Tajpour, Maslin Massrum
2012	IEEE	Machine learning, scripting languages security	cross site scripting	The search for features that represent new attacks is a good opportunity for new experiments seeking for extending knowledge and conclusions	Not deal with large databases, this work does not reach all attacks possibilities	Automatic Classification of Cross-Site Scripting in Web Pages Using Document-based and URL-based Features	Angelo Eduardo Nunan, Eduardo Souto, Eulanda M. dos Santos, Eduardo Feitosa
2015	IEEE	Tier Web Application, Web Security Vulnerability	SQL injection, cross site scripting	This approach applies mapping model to detect SQL injection and XSS attacks	Want to use Latest technologies to detect and prevent attacks.	A Novel Approach for Detection of SQL Injection and Cross Site Scripting Attacks	Piyush A. Sonewar, Nalini A. Mhetre.
2015	IEEE	Machine Learning Aggregated Netflows	Brute Force	compare the performance of the aggregated features and Netflow features for the detection of brute force attacks.	Aggregated Netflows can discriminate between brute force attacks and normal SSH traffic	Detection of SSH Brute Force Attacks Using Aggregated Netflow Data	Maryam M. Najafabadi, Chad Calvert, Clifford Kemp
2016	IEEE	Supervised Machine Learning, Text Classification, Pattern Matching	SQL injection	Kibana queries, using other machine learning methods to reduce manual log classification efforts	Want improvement on Kibana queries	Detecting Web Attacks Using Multi-Stage Log Analysis	Melody Moh, Santhosh Pininti, Sindhusha Doddapaneni
2014	ACM	output filtering, application security	SQL injection	output filtering is another option to defend an application against classic and blind SQLi attacks.	different platforms and web application frameworks not Used.	Measuring the Effectiveness of Output Filtering Against SQL Injection Attacks	Mark E. Fioravanti, Liam M. Mayron
2016	ACM	Web protocol security, Web Server Log Files,	cross site scripting	Mod Security web application firewall and code filtering will be use for both detection and	XSS attacks use known vulnerabilities in existing Internet tools and technologies	NEUTRALIZING CROSS-SITE SCRIPTING	G.Rama Koteswara

		Mod Security, open source tools		prevention of attack	to disrupt web services impacting their users	ATTACKS USING OPEN SOURCE TECHNOLOGIES	Rao, R.Satya Prasad, M.Ramesh
2014	ACM	Web application security, Machine learning	cross site scripting	this work can be extended by identifying more features and adding them to the currently created dataset	it gave comparatively better performance with respect to FPR	Prediction of Cross-Site Scripting Attack Using Machine Learning Algorithms	Vishnu. B. A, Ms. Jevitha. K. P
2013	ACM	Scanning; SSH,Distributed	Brute Force	In this work we propose a general approach for detecting distributed, potentially stealthy activity at a site	instances of stealthy attacks that would have proven very difficult to detect other than in aggregate	Detecting Stealthy, Distributed SSH Brute-Forcing	Mobin Javed and Vern Paxson