Mitigating Cross-Site Scripting Attacks with a Content Security

[#1]Ganesh Gore, [#2]Pradip Khanekar, [#3]Girish Sonar, [#4]Amey Kulkarni

[1]gore.mahesh2@gmail.com
[2]pradipkhanekar@gmail.com
[3]sonargirish04@gmail.com
[4]ameykulkarni04@gmail.com

[#1234]Department of Computer Engineering.
TSSM's Bhivarabai Sawant College of Engineering and Research,
Narhe,Pune

ABSTRACT

***Abstract*—**A content security policy (CSP) can help Web application developers and server administrator's better control website content and avoid vulnerabilities to cross-site scripting (XSS). In experiments with a prototype website, the authors CSP implementation successfully mitigated all XSS attack types in four popular browsers. Among the many attacks on Web applications, cross-site scripting (XSS) is one of the most common. An XSS attack involves injecting malicious script into a trusted website that executes on a visitor browser without the visitors knowledge and thereby enables the attacker to access sensitive user data, such as session tokens and cookies stored on the browser. With this data, attackers can execute several malicious acts, including identity theft, key logging, phishing, user impersonation, and web cam activation. The project aims to determine an effective approach to detect and curb the SQL attacks in database using modified data cleaning algorithm. The project work includes sanitization of the tainted information being sent to the database and innovate a new prototype, with run time monitoring without any delay.

Keywords—SQL Injection, SQL Attack, Data Sanitization, Database Security, Security Threats, Cross Site Scripting

ARTICLE INFO

Article History

Received: 3rd June 2017

Received in revised form :

3rd June 2017

Accepted: 6th June 2017

Published online :

8th June 2017

I. INTRODUCTION

To determine an effective approach to detect and curb the SQL attacks in database using modified data cleaning algorithm. The project work includes sanitization of the tainted information being sent to the database and innovate a new prototype, with runtime monitoring without any delay. Reverse Proxy is a technique which is used to sanitize the users inputs that may transform into a database attack. In this technique a filter program redirects the users input to the proxy server before it is sent to the application server.

At the proxy server, data cleaning algorithm is triggered using a sanitizing application. New security vulnerabilities are discovered every day in todays system, networking, and application software. In the recent years, web applications have become primary targets of cyber-attacks. Analysis of the National Vulnerability Database (NVD) maintained by the National Institute of Standards and Technology (NIST) shows the rapid increase of vulnerabilities that occur mostly in web-based applications, SQL Injection. This study intends to identify Web application security is a difficult task because these applications are, by definition, exposed to the general public, including malicious users. The incorrect or missing input validation is the most frequent vulnerability type in web applications. Network firewalls, network vulnerability scanners, and the use of Secure Socket Layer (SSL) do not, by themselves, make a web site secure Group estimates that over 70 percent of attacks against a companys web site or web application come at the application level, not the network or system layer .One type of tools being employed to address these applicationlevel vulnerabilities is web application scanners

II. PROBLEM STATEMENT

To develop an application which detect Sql injection and cross site scripting attacks and sanitize users input.

III. PROPOSED SYSTEM

Mitigating Cross-Site Scripting Attack is a good way to provide scientific decision support for a SQL injection attack occurs when an attacker causes the web application to generate SQL queries that are functionally different from what the user interface programmer intended. example, consider an application dealing with author details.

Server: generate characteristics automatically for each item by using word segmentation technology; mine item characteristic association rules and store the set of rules in database.

Client: receive a set (sequence) of items and read the item characteristic association rules; return a set of items which is strongly associated to the received set (sequence). It is aimed at discovering customer purchase patterns by determining associations from point-of-sale (POS) transaction data. The item association information thus developed can be applied in such marketing activities as catalog design, product placement, promotion and cross-selling.

Reverse Proxy Server

A reverse proxy is a type of proxy server that retrieves resources on behalf of a client from one or more servers. These resources are then returned to the client like they originated from the Web server itself. Contrary to a forward proxy, which is an intermediary for its associated clients to contact any server, a reverse proxy is an intermediary for its associated servers to be contacted by any client. A reverse proxy can distribute the load from incoming requests to several servers, with each server serving its own application area. In the case of reverse proxying in the neighborhood of web servers, the reverse proxy may have to rewrite the URL in each incoming request in order to match the relevant internal location of the requested resource.

Sql injection

At the point when SQL is utilized to show information on a website page, it is normal to let web clients input their own particular pursuit values. Since SQL articulations are content just, it is simple, with a little bit of PC code, to progressively change SQL explanations to furnish the client with chose data SQL infusion is a system where malevolent clients can infuse SQL summons into a SQL proclamation, by means of site page input. Injected SQL charges can adjust SQL explanation and trade off the security of a web application.

Cross Site Scripting

Cross-Site Scripting (XSS) assaults are a kind of infusion, in which vindictive scripts are infused into generally favourable and trusted sites. XSS assaults happen when an aggressor uses a web application to send noxious code, for the most part as a program side script, to an alternate end client. Imperfections that permit these assaults to succeed are very across the board and happen anyplace a web application utilizes contribution from a client inside the yield it produces without approving or encoding it. An assailant can utilize XSS to send a vindictive script to a clueless client. The end client's program has no real way to realize that the script ought not be trusted, and will execute the script. Since it supposes the script originated from a confided in source, the malignant script can get to any treats, session tokens, or other delicate data held by the program and utilized with that site. These scripts can even rework the substance of the HTML page.

IV. LITERATURE SURVEY

1. Literature Survey on Sql Injection:
   Cross-site Scripting (XSS) refers to client-side code injection attack wherein an attackercan execute malicious scripts into a legitimate website or web application. XSS is amongst the most rampantof web application vulnerabilities and occurs when a web application makes use ofunvalidated or unencoded
   user input within the output it generates. The system isnot able to tackle the attack effectively, confusing the innocent clients and pruning them to be a victim. [1][2]
2. Basically url injections is someone who tries to manipulate your database usingthe url. This means a hacker has created new pages on your site, often containingspammy words or links. Sometimes these new pages contain code that doesthings you didnt intend, such as redirecting your users to other sites or making yourwebserver participate in a denial ofservice attack against other sites. The system isnot suitable for handling new type of attack based on application layer.[3]
3. Literature Survey on cross site scripting:
   Explains methods, principles, and techniques for conducting predictive analytics projects from start to finish Illustrates each technique with hands-on examples and includes as series of in-depth case studies that apply predictive analytics to common business scenarios.[5]
4. The product bundling problem is a challenging task in the e-Commerce domain. We propose a generative engine in order to find the bundle of products that best satisfies user requirements and, at the same time, seller needs such as the minimization of the dead stocks and the maximization of net income. The proposed system named Intelligent Bundle Suggestion and Generation (IBSAG) is designed in order to satisfy these requirements. Market Basket Analysis supports the system in user requirement elicitation task. Experimental results prove the ability of

system in finding the optimal tradeoff between different and conflicting constraints.[4]

V. PROPOSED SYSTEM

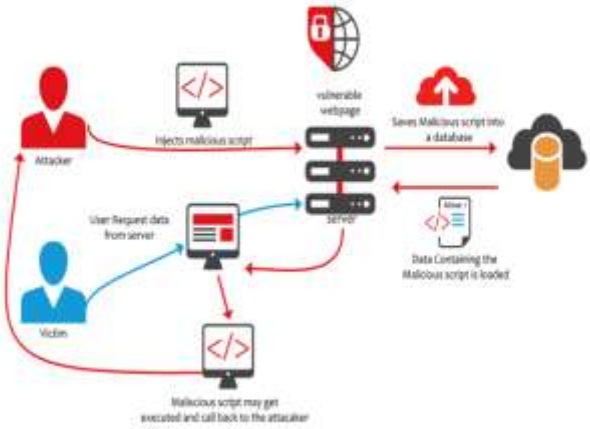

Fig: 1.1 System Architecture

CONCLUSION

we first classified the types of inputs and sinks that may cause security attacks. Then, we classified the types of sanitization methods that are commonly applied to inputs to avoid security issues. For each sensitive sink in a web program, we collect the static code attributes that characterize these classification schemes. Vulnerability prediction models are then built using the collected data and the vulnerability information of each sink. In our preliminary studies, these models predicted over 85% of SQLI and XSS vulnerabilities in different web applications. Our future work is to conduct more comprehensive experiments on a larger set of systems to further validate these results.

ACKNOWLEDGEMENT

I sincerely thank my guide Prof. L.M.Bharate and HOD Prof. N.B.Pokale TSSM's Bhivarabai Sawant College Of Engineering And Research for his guidance and encouragement in carrying out this research work

REFERENCES

1. Data Mining for Marketing in Telecommunication Industry Rokhmatul Insani, Hira Laksmiwati Soemitro, School of Electronic Egineering and Informatics, Institute of Technology Bandung, Indonesia, IEEE SENSORS JOURNAL, 2016 IEEE Region 10 Symposium (TENSYMP), Bali, Indonesia
2. A Case-Based Recommendation Approach for Market Basket Data, Anna Gatzioura and Miquel Snchez-Marr, Universitat Politcnica de Catalunya BarcelonaTechE 2015
3. Searching optimal product bundles by means of GA-based Engine and Market Basket Analysis,C. Birtolo, D. De Chiara, S.Losito, P.Ritrovato, M.Veniero, IEEE 978-1-4799-0348-1/13, 2013.
4. Applied Predictive Analytics: Principles and Techniques for the Professional Data Analyst, Dean Abbott, John Willey Son ,Inc, Indianapolis,Indiana, 2014 IEEE
5. Research on the amount of customers in telecom package preview based on data mining, Jia Danhua, Zhao Xiaoegeng, Wang Runrun, IEEE 978-0-7695-4719-0/12 DOI 10.1109/CSSS.2012.508, 2012 [2012 International Conference on Computer Science and Service System]

