# Secure Cross Site Script Analyzer And Monitoring System

**Aryalakshmi.R[1], Josmy George[2]**
[1]Dept of computer sciences & engineering
[2]Assistant professor, Dept of computer sciences & engineering
[1, 2] MBCCET peermade 685531, Idukki, Kerala

***Abstract-*** *Protecting web application is increasingly important due to their high popularity and wide adoption. Therefore, a multitude of protection techniques emerged in effort to secure web applications, such as exploits can have a devastating impact on personal and economic levels. As for asynchronous communication between client and server xmlhttp (Ajax) were used and it can communicate only with parent server by default. If we allow multiple sever access in Ajax code that is enabling cross site scripting it leads to breach the security among multiple clients. The proposed method tries to solve this problem by developing a technique which can monitor the web in real time and deny unauthorized foreign clients. Thus, we can provide service for concerned client.*

## I. INTRODUCTION

Due to the immense popularity of the internet, usage of web application has expanded. Since extremely sensitive information are being exchanged via web applications every day, they have become a playground for cyber criminals to steal data and to use them for malicious purposes [4].

Ajax is a Web application client technology, which is a combination of JavaScript, CSS, HTML, the XMLHttp Request object, and Document Object Model (DOM). Ajax applications running in the browser communicate with a Web server in an asynchronous manner, and update only a part of the page. By using Ajax technology, we can enrich the browser-based user experience. [4] Ajax can capture rich user action events, and the Ajax applications only send to the server and retrieve the necessary data. It uses some of the XML-based web service interface, and processes responses from the server by JavaScript on the client side. Because of a significant reduction in the data exchanged between browser and server, the application will respond faster. [3] Also, a lot of work can be completed on the requesting client machine, the Web server's processing time is also reduced. Due to the advantages of interaction, Ajax has been widely used.

The core technology in Ajax is XMLHttp Request, XMLHttp Request provides a kind of communication method with the server within the page for JavaScript operating in browser. One of the biggest Ajax characteristic is be able to transmit or read data to the server without refreshing page, also called update pages without refresh. This characteristic mainly benefits from XMLHTTP components and XMLHttp Request objects, which is just the same with desktop applications, only need data exchange with server, instead of refreshment each time or processing data. This not only reduces the burden of server and accelerates the response speed, but also shortens the time for customers and improve the user experience. [1]

Asynchronous communication between client and server use xmlhttp [Ajax].Xmlhttp can only communicate with parent server .In order to allow multiple server access in Ajax codes we need to enable the cross site scripting. When enabling xss any foreign pages can use the server pages. These reduce the confidentiality of the server pages. Because analyzing xss cannot be dynamic.

## II. PROPOSED APPROACH

The proposed technique is well-suited to discover vulnerabilities in high level. Within the current techniques the analyzing of cross site scripting cannot be dynamic .By using xmlhttp for asynchronous communication between client and server it can only communicate with parent server. There is only one solution for access multiple servers in Ajax code that is enabling cross site scripting. Enabling xss leads to allow any foreign pages can use the server pages (through Ajax).

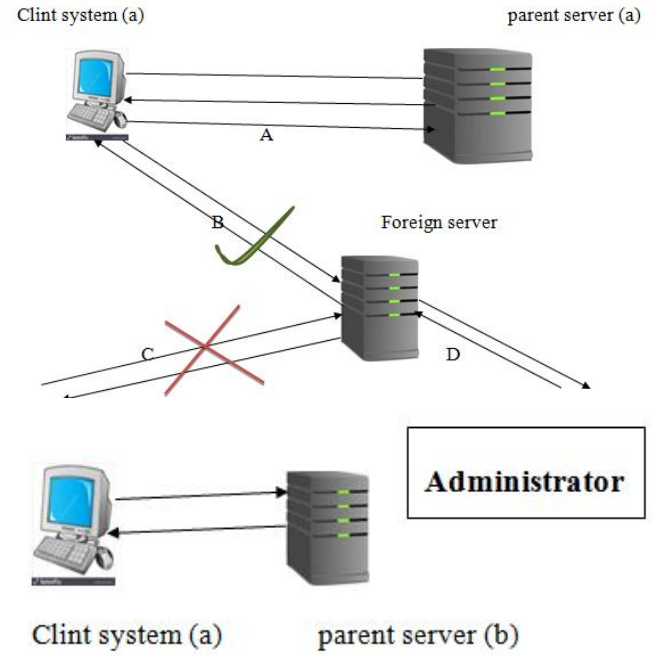


Fig: propose method

The above figure which shows the proposed method. It allowing the authorized Clint to access the foreign server and prevent the unauthorized Clint access and monitoring the malleolus script in real time. The main operations of the proposed method.

A: The client system (a) communicates with its own parent server, such as http request from the Client side and html response from the server side, then the Connection is ok.

B: communication between client system (a) and the foreign server. Here the Connection is ok because the client system (a) is authorized one it contains the access permission. The client gives the xmlhttp request to the foreign server and server gives response.

C: In the same time the unauthorized client request deny by the server, the sever not allowed access the data. Which are to be shown in the above figure.

D: The unauthorized accesses are to be monitored by the administrator. All the Attacks are to be monitored in real time and also the malleolus scripts are to be identified by it.

## III. ACCESS CONTROL SPECFICATION

The first module of the proposed approach is access control specification in this module it mainly consists with the operations:

Source
Identification
Authentication
Respond

Setting the proper access permissions are one of the important thing in the case of security. Only the authorized client can access the data and the access permission can be configured with the corresponding server.

## IV. SCRIPT EVALUATION

The second module is script evaluation it consist with:

Script source stealing
Find outing ajax scripts
Filtering the attack script

## V. ATTACK MONITORING

The last module of the proposed approach is attack monitoring. In this module attack is to be monitored in real time. It consists with:

Add to attack repository
Real time monitoring on admin panel

The proposed approach also contains an administrator it set all the configurations and monitoring the whole access of clients and prevents the malicious ones in real time.

## VI. CONCLUSION

With the characteristics of ajax technology and xmlhttp improved the communication between client and server. The xmlhttp only allowed the client to communicate with its parent server,if any communication is done in between client and a foreign server the server must enables the cross site script.when enabling the cross site script it leads to permit all the unauthorized access of the server data. The proposed method proved a secure communication between authorized clients and the foreign server and also providing real time attack and the malleolus script monitoring.

## REFERENCES

[1] Shuxia Dong1, Chen Cheng1, Yi Zhou2 "Research on AJAX Technology Application in Web Development" 978-1-4244-8694-6/11/$26.00 ©2011 IEEE.

[2] Madhurima,dr.anju kumar,saru dhir,madhulika "Difficulties and Challenges Faced in Testing AJAX Applications" 2015 International Conference on Soft Computing Techniques and Implementations- (ICSCTI) Department of ECE, FET, MRIU, Faridabad, India, Oct 8-10, 2015.

[3] Jin Yuping, "Research and Application of Ajax Technology in Web Development" 2014 IEEE Workshop on Electronics, Computer and Applications978-1-4799-4565-8/14/$31.00©2014 IEEE.

[4] Darshan G. Puranik,dennis c,james h "Real-time Monitoring using AJAX and WebSockets" 20th Annual IEEE International Conference and Workshops on the Engineering of Computer Based Systems (ECBS)" 978-0-7695-4991-0/13 $26.00 © 2013 IEEE DOI 10.1109/ECBS.2013.10.