International Journal of Engineering Research-Online
A Peer Reviewed International Journal
Articles available online http://www.ijoer.in

Vol.3., Issue.3, 2015

RESEARCH ARTICLE

ISSN: 2321-7758

ENHANCEMENT IN WEB SECURITY

MOHAMMAD ASIM[1], MANI SHARMA[2]

[1]Assistant Professor,Mgm Coet, Noida,India
[2]Department of Computer Science & Engineering
Mahatma Gandhi Mission's Engineering College, Noida, India

Article Received:12/05/2015

Article Revised on:20/05/2015

Article Accepted on:26/05/2015

ISSN:2321-7758
International Journal of Engineering Research-Online
A peer-reviewed, open access International scientific journal
www.ijoer.in

ABSTRACT

Content injection Attacks performed by hackers on websites has become a global issue now-a-days. Hackers perform attacks on websites for the purpose of information stealing. Due to increasing facilities provided by the websites and failure of web developer to sanitizing input of users, cross site scripting has become a security threat in websites. Using XSS techniques, hackers can hijack web sessions .As a result , users are facing problem in receiving content from websites. The major objective of this research paper is to describe the working of approach which we have suggested to provide security in websites by mitigating content injection attacks. This research paper extends approach to prevent XSS attack. This research paper also suggests security safeguard for users using websites for performing online operation. We hope that this extension of approach will help in preventing XSS attacks and ensures security of information of websites will be maintained in future.

INTRODUCTION

In this era of changing technologies, websites are facing problems of content injection attacks. This is because of providing additional amount of features by websites to users. Websites uses client side scripting languages to provide more services. These scripting languages are JavaScript, ActiveX, VBScript, etc. Web developers are frequently facing failure to providing sanitize input of user. Hence, Web developers are not applying security in websites due to work load or lack of security knowledge about websites. As a result, code injection attacks such as Cross-Site Scripting, SQL Injection, Cross-site Request Forgery are the most common attacks faced by websites and have become a serious issue of concern now-a-days. Out of these content injection attacks, XSS is difficult to identify and prevent. Sites which faced XSS vulnerability are HSBC, Google Search Engine, Vodafone, MySpace, etc

Information stealing in websites which is done by hackers by injecting malicious script in the webpage results in serious problems faced by websites .Various methods implemented by researchers have failed to provide security to websites because of certain drawbacks.

This research paper is divided into three sections. First section describes the detailed discussion of our approach. Second describes working of approach. Third section describes the security safeguards for users. Rest of the paper describes Conclusion and Future Work.

SECTION-1

In this research paper, to apply the security in websites, we are using encryption technique. The confidential data of the user which is stored in the database is encrypted so that the hacker would not able to identify the content. In case if hacker gets password of user by unfair means .when he will click to open the content, he will get encrypted data. Hence, uploaded data of the user will be in encrypted format so that hacker would not hack it. This can be done with the help of digital encryption algorithm.

Our approach is based on four steps:

1. Content is copied when transmitted from sender to receiver to enhance protection of data.

2. A firewall is set up to check each connection entering and leaving local machine

3. Installing of filters to detect and remove malicious content of webpage.

3. Commands are used to disable the keyboard so that only mouse will be used for objective of scroll down.

Discussion of approach

First step describes that when data is transferred from sender to receiver, it is copied. Before transferring the content, data is encrypted so that hacker will not able to identify it. Hence, he will not be able to steal the confidential data.

Second step describes that installing of filters identifies and sanitize the content of webpage which is seemed to be malicious. New version of filters overcomes the limitation of server side filters where service providers leave the users defenceless at the time of code injection attacks due to several reasons. If malicious content exits in websites , then filters successfully removes it from webpage .This filter is able to identify and remove malicious code of the various scripting languages such as JavaScript, VBScript, ActiveX etc .Hence ,it will able to overcome the limitation of JavaScript tester in SWAP[1].

Third step describes that if user is working on website to perform online operation then only selection procedure is followed .Keyboard is deactivated by using certain commands. Only mouse is used for scroll down. This is done so that no input data is entered by the user which is hacked when he is filling form of registration online. Thus, the confidential data of user is safe and privacy is maintained.

SECTION-2

Working of approach

This approach works in the following steps:

1. Client sends request to the server.
2. Server checks the request and fetches the data from database in order to respond the client's query.
3. Server sends response to the client.
4. When data is transmitted during network, it is copied for protection.
5. Data is encrypted after copying process by symmetric key cryptography technique.
6. Cipher text reaches at reverse proxy.
7. Reverse proxy forward the cipher text to script tester.
8. Script tester checks that whether a malicious script is present in webpage or not. If script does not present in webpage then it would be forward to reverse proxy and sends to the client.
9. If script is present in webpage, then it sends to filter.
10. Filter identifies the malicious content and sanitize the harmful scripts from webpage.
11. Data is forward to reverse proxy.
12. Reverse proxy sends data to the client.
13. Client receives data and it is decrypted to plain text by symmetric key cryptography.

SECTION-3

Security safeguards are necessary to protect confidential data of users. They create awareness among users to be careful while working on sites for performing online operation. Hence, they allow users to alert from malicious attacks. In this research paper, we have suggested security safeguard for users.

Safeguard For users:

1. Users should change their password regularly.
2. Installing the personal firewall and Anti-virus software. Anti-virus software will help in detecting the malwares. Personal firewall checks each and every connection leaving and entering the local machine. If any connection mismatched with the rules of

firewall, then it gives control to the user either block or allow the connection.

3. Use update version of operation system and internet explorer.
4. User should report to service providers regularly about abnormal behaviour of websites.
5. Users should not perform login and registration on critical sites.
6. At the end of the session, users must remember to log out.
7. Users should not download software or any content from unknown sources.

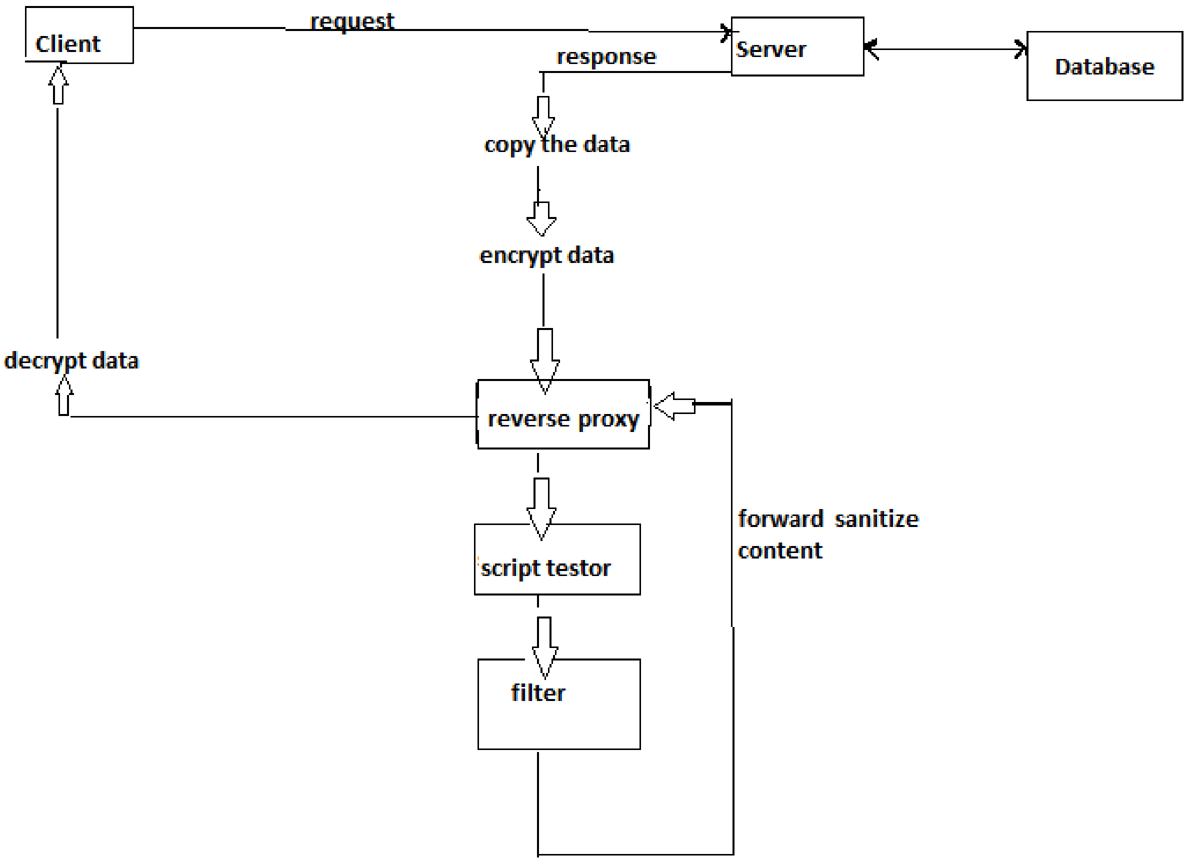

Diagram showing working of approach

CONCLUSION AND FUTURE WORK

We have discussed our approach in detail. Steps mentioned in our approach overcomes the limitation of existing techniques. Inadequate validation of user input which is the major cause of XSS attack is restricted by using certain commands to deactivate the keyboard. Only selection procedure is followed. Setting up of firewall identifies and checks each connection leaving and entering the local machine. Filters sanitize malicious content of websites. We performed a detail study on existing methods implemented by researchers and concluded that no technique is fully perfect to perform the desired function. Existing techniques suffers the limitations of complex construction of devices, performance overhead, manual work requirement etc. Hence, these methods are not capable to mitigate content injection attacks completely. Awareness must be created among the users regarding security of websites. We hope that approach suggested by us will help to mitigate code injection attacks completely and secure the websites from attacks performed by hackers. We hope that our approach will help to identify and prevent the code injection attacks completely in future.

ACKNOWLEDGEMENT

We are expressing our pleasure and thanks to our guide Mr Mohammad Asim for their guidance and all those teachers who have cooperated us in this project. We are happy to express thanks to those people who have directly or indirectly helped us to complete this research paper.

REFERENCES

[1]. WURZINGER , PLATER, LUDL , KIRDA , KRUEGAL: SWAP : mitigating XSS attacks using reverse proxy

[2]. Engin Kirda, Christopher Kruegel, Giovanni Vigna, and Nenad Jovanovic. Noxes: A client-side solution for mitigating cross site scripting attacks. In Proceedings of the 21st ACM Symposium on Applied Computing (SAC), 2006

[3]. A. Duraisamy, M.Sathiyamoorthy, S.Chandrasekar: A Server Side Solution for Protection of Web Applications from Cross-Site Scripting Attacks

[4]. Grossman, RSNAKE, PDP, Rager, and Fogie, “XSS Attacks: Cross-site Scripting Exploits and Defense,” Syngress Publishing Inc, 2007.

[5]. Y.-W. Huang, S.-K. Huang, T.-P. Lin, and C.-H. Tsai, “Web application security assessment by fault injection and Behavior Monitoring,” In Proceeding of the 12th international conference on World Wide Web, ACM, New York, NY, USA: 2003, pp.148-159.

[6]. A. Klein, “DOM Based Cross Site Scripting or XSS of the ThirdKind,”http://www.webappsec.org/projects/articles/071105.html, July 2005.

[7]. “OWASP Document for top 10 2007- cross SiteScripting,”http://www.owasp.org/index.php/Top_10_2007-Cross_Site_Scripting.

[8]. T. Pietraszek, and C. V. Berghe, “Defending against Injection Attacks through Context-Sensitive String Evaluation,” In Proceeding of the 8th International Symposium on Recent Advance in Intrusion Detection (RAID), September 2005.