© 2016 IJSRSET | Volume 2 | Issue 6 | Print ISSN: 2395-1990 | Online ISSN : 2394-4099
Themed Section: Engineering and Technology

Survey on Preventing the Password Hacking by Using the Loss Encryption

C. Chandru Vignesh[*1], D. Sandhika [2], A. R. Suvetha[3], P.Thirumoorthy[4]
[1]Assistant Professor, Department of Computer Science and Engineering, SNS College of Technology, Coimbatore, Tamilnadu, India
[2,3,4] UG Scholar, Department of Computer Science and Engineering, SNS College of Technology, Coimbatore, Tamilnadu, India

ABSTRACT

Cyber security is playing very important role in today's world because of increasing web attacks and vulnerabilities emerging today. Cross-site scripting (XSS) is one of the common attack involves injecting malicious script into a trusted website. In existing system the Content security policy (CSP) is used to prevent web application from cross-site scripting. It will prevent the XSS attack only on client side. Various approaches to defend against attacks are available today but not a single approach solves all the loopholes .After investigating this area we have to be propose an efficient approach to prevent the password hacking by loss encryption method which prevents XSS attack in server side .In Loss encryption, we loss the encrypted password so the attacker cannot decrypt it and cannot capture original data.

Keywords : Cross-site scripting, Content Security Policy, Loss Encryption

I. INTRODUCTION

Cyber security is one of the technology which helps to analyze and prevent the victim from unauthorized users. It is designed to protect networks, data, and computer, program from unauthorized users, attack or damage. Among the many attacks on a web application, cross-site scripting (XSS) is one of the most common. It involves injecting harmful script into a website without user knowledge. It executes on visitor's browser and enables the attacker to access sensitive data like session tokens and cookies stored on the browser. With this data, an attacker can track user's confidential and personal information.

An XSS attack is of three types namely persistent, non-Persistent and document object model (DOM).Persistent XSS involves injecting virus script into a website which stores the script in its database. In non-persistent XSS attacker hides harmful script in the URL, disguising it as user input, and lures the victims by sending emails which prompt users to click on the crafted URL.DOM-based XSS is to update the structure and style of webpage content dynamically, so the web applications and websites interact with the DOM.A DOM-based, or type-0, XSS attack executes in the same manner as like the non-persistent XSS attack the attacker encodes malicious value in a URL and sends it to the victim.

II. METHODS AND MATERIAL

A. Existing System

A content security policy is one of the browser security mechanism that aims to protect websites from Cross Site Scripting attacks. The content security policy (CSP) can help web developers and server administrator's better control website content and avoid Vulnerabilities to cross-site scripting. To adopt CSP, website developers should have to manually compile a list of allowed content sources.

The content security policy (CSP) provides server administrators with a white list of accepted and approved resources. The web application or website will block any input which is not on the list and thus there is no need for sanitizing. The white list also guards against data exfiltration and extrusion the unauthorized downloading of data from a website visitor's computer.

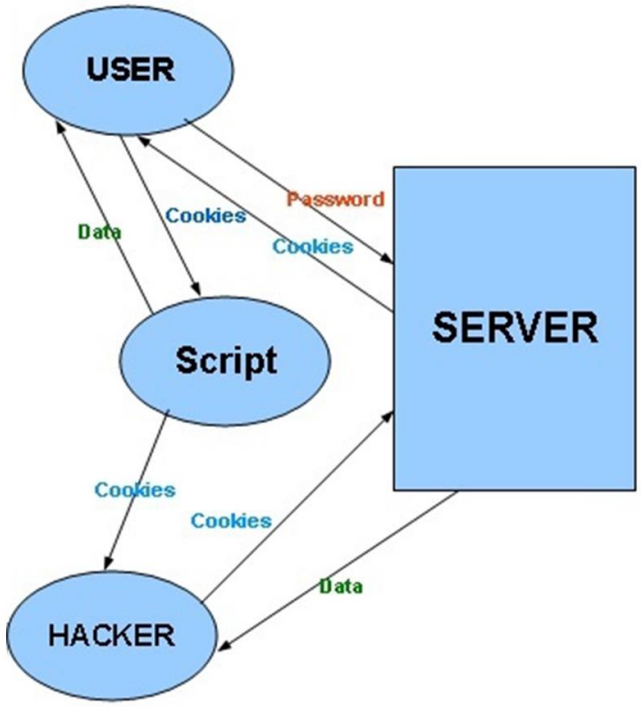

Figure 1. XSS (Cross Site Scripting)

B. Literature Survey

Several researchers investigated in cyber security In "Preventing Persistent Cross Site Scripting attack by applying pattern filtering approach "by I. Yusof ,XSS attack prevented by applying pattern filtering method which involves sanitizing user's input before storing it in the database. Input from the user is taken from a web browser as untrusted data, which go through filtering process to get a "clean" status. These clean data are stored in database to generate clean output from that output sanitization

In "Defending against Web Vulnerabilities and Cross Site Scripting" by T.Venkat Narayana Rao, XSS vulnerabilities is eliminated by using defensive coding practice which validates and sanitize inputs

In "Notes:A Client-Side Solution for Mitigating Cross-Site Scripting attack" by E.Kirda, Notes is used. It is the first client side solution to mitigating cross-site scripting attack.Notes act as a web proxy and uses both manual and automatically generated rules to mitigate cross-site scripting attempts. Notes efficiently protects against information leakage from user's environment. It requires minimal user interaction and customization effort.
In "Defeating Script Injection attacks with Browser Embedded Policies" by T.Jim and N.Swamy, XSS is prevented by using Browser enforced embedded policies. The two simple kind of policies used in this policy is white list and DOM sandbox. When the script is detected in the browser and passed to the hook function. This hook function hashes the script and matches it against a whitelist. Any script whose hash is not in the list is rejected.

In "Blueprint: Robust Prevention of Cross Site Scripting attacks for Existing Browsers" by M.T.Louw, Content filtering and browser collaboration techniques are used. Content filtering uses the filter function to remove potential malicious data or instruction from user input browser. In Browser Collaboration, the application may collaborate with the browser by indicating which scripts in a web page are authorized leaving the browser to ensure the authorization policy is updated.

III. RESULTS AND DISCUSSION

Proposed System

The existing system fully focused on client side security. It will detect the attacks possible in client side and secure the data in client side .If the database security (server side) is weak, then the attacker can easily attack the database and access confidential information. Many of the peoples are using the same password in different websites. If the attacker hacks the password in one site, then he will decrypt the password and known the original password. In our proposed system we are going to loss the encrypted password so the attacker cannot decrypt it and cannot capture original data. This method is called loss encryption. We also prevent brute force attack and guessing password attack.
Module description:

There are four modules are in proposed system

- Website creation
- Prevention
- Detection
- Loss encryption

1. Website creation

In a website creation, we are going to design a website using HTML, CSS, JavaScript, PHP and MySQL. Then host website in any free web hosting or paid hosting.

Front end

1. HTML –Hyper Text Markup Language
2. CSS-Cascading Style sheet

Backend

1. PHP-Hyper Text Preprocessor
2. SQL-Structured Query language
3. MySQL- PHPMyAdmin

2. Prevention

XSS attack is prevented by using content security policy with help of white list. There are two types of list are available.

1. White list
2. Black list

White list

Only listed peoples can access the data in the system.

Black list

The people who are listed in the black list can't access the data in the system.

The white list is more secure compare the black list. In CSV technique using whitelist mechanism to prevent the vulnerable script injections in the database.

3. Detection

The same whitelist can be used to detect the unauthorized users and attacks. If any attack has been detected then it will be sent to the administrator through email. The HTML special chars () will help to change the vulnerable scripts. Example script tag into some another entity's

4. Loss encryption

The above 3 technique are used to prevent the client side attack and sever attacks. In our proposed system is a loss encryption.

Why loss encryption?

Sometimes the database and file system security is a week on the website. The attacker can attack the website and grant access to the database and file manager. So the attacker got the encrypted password he finds the encryption technique and known the decryption method. Then find the original password.so many online users are using the same password in different websites .The attacker attack one website it means he will get another secure website access also so we are going loss encryption.

First, the plaintext (password) is got from the client. The plaintext is given to MD5 (Message Digest) method.MD5 is old and open source cryptographic hash algorithm .It's a 128bit algorithm.

Encrypt the password using MD5 hashing algorithm and concatenate (reduce) the password and store it in the database. The login mechanism by using above method verifies the login authentication.MD5 is capable of encrypting any message of any length (can be more than 8bit).

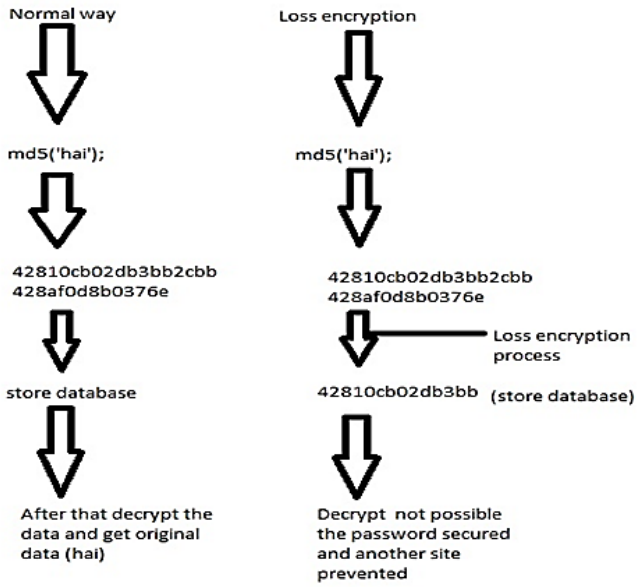

Figure 2. Loss Encryption

IV. CONCLUSION

The problem of password hacking is solved by loss encryption. It is designed to protect networks, data, and computer program from unauthorized users, attack or damage. Using XSS attack, it is possible to steal or manipulate victim's sessions and cookies, which may be used to impersonate a legitimate user of a system. The existing system the Cross-site Scripting attack is prevented by using Content Security Policy. The proposed loss encryption attack prevention model has been found to be very effective. However each time, various kinds of tricks and techniques are being devised hackers are not sitting idle, in fact, their attacks are getting more and more sophisticated as the time moves ahead. As our future work, we plan to investigate thoroughly how our prevention model can be used in any type of web application and windows application.

V. REFERENCES

[1] I. Yusof and A.S.K. Pathan, "Preventing Persistent Cross-Site Scripting (XSS) Attack by Applying Pattern Filtering Approach," Proc. 5th IEEE Conference Information and Communication Technology for the Muslim World (ICT4M14), 2014.

[2] T.Venkat Narayana Rao, "Defending against Cross-Site Scripting Attacks,"

[3] Computer, vol.45, no.3, 2012.

[4] E. Kirda et al., "Noxes: AClient-Side Solution for Mitigating Cross-Site Scripting Attacks," Proc. 21st

[5] ACM Symposium Applied Computing (SAC06), 2006.

[6] T. Jim, N. Swamy, and M. Hicks,"Defeating Script Injection Attacks with Browser-Enforced Embedded Policies," Proc. 16th Int'l ACM Conference World Wide Web (WWW07), 2007, pp. 601−610.

[7] Y. Nadji, P. Saxena, and D. Song, "Document Structure Integrity: A Robust Basis for Cross-Site Scripting Defense,"Proc.6th Ann.Network & Distributed System Security Symposium. (NDSS09), 2009;

[8] M.T. Louw and V.N. Venkatakrishnan, "Blueprint: Robust Prevention of Cross-site Scripting Attacks for Existing Browsers," Proc. 30th IEEE Symp. Security and Privacy (S&P09), 2009, pp. 331−346.

[9] R. Hansen, "XSS (cross site scripting) cheat sheet esp: for filter evasion," 2008. Online]. Available: http://ha.ckers.org/xss.html

[10] P. Saxena, D. Song, and Y. Nadji, "Document structure integrity: A robust basis for cross-site scripting defense," in 16th Annual Network & Distributed System Security Symposium, San Diego, CA, USA, Feb. 2009.

[11] M. Johns, "Code Injection Vulnerabilities in Web Applications -Exemplified at Cross-Site Scripting," PhD dissertation, Univ. of Passau, 2009;https://opus4.kobv.de/opus4unipassau/frontdoor/index/index/docId/144.

[12] Open Web Application Security Project, "OWASP Top 10 – 2013: The Ten Most Critical Web Application Security Risks," 2013;www.owasp.org/index.php/Top10#OWASP_Top_10_for_2013.F