IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

Content Integrity as Counter-Measure to Site Content Attacks

Dr. J. Sridhar[1] T. Charan sai [2] Adarsh Dubey [3] P. Dinesh Reddy [4] T. D. Gowtham Kumar[5]

[1]Associate Professor, [2345]UG Student, Department of Computer Science and Engineering, Siddharth Institute Of Engineering & Technology, Puttur , Andhra Pradesh, India.

ABSTRACT

This article discusses the Content Security Policy (CSP) header, which is now the most popular defence against Cross-Site Scripting (XSS) assaults. It is stressed that the CSP header implementation is a comparatively easy way to raise the security level of Internet-based communication between people and devices. This makes it possible to precisely define the communication parties and web service assets utilised in the environments where secure web services are essential, such as web applications and Internet of Things (IoT) networks. As straightforward and efficient reporting is a natural element of the CSP design, administrators can be alerted to active attacks practically immediately. On real-world situations, the advantages of implementing CSP for communication are shown, as well as how simple it is to spread CSP.

keywords: *Information security, organisation personnel, security planning and control.*

INTRODUCTION

The topic of secure communication is constantly hot, and new security risks are found daily. Although the topic of safeguarding communication between a web server and a browser is not entirely new, new security tools are now available. These tools, called HTTP Security Headers, have

discovered new methods of securing communication between the aforementioned parties. Although using the HTTPS protocol for communication between people and devices is now widely recognised, restricting communication to authorised domains or subdomains is a relatively new security requirement. Cross Site Scripting (XSS) assaults are becoming more prevalent as a result of online apps and Internet of Things (IoT) networks. securing HTTPS protocol connection and limiting communication to permitted domains and subdomains, brings the desired outcomes. Despite the fact that the HTTPS protocol is generally safe, it is important to consider any risks that could arise from the improper usage of URIs in HTML source code. Even in well-managed code, it is possible to skip HTTP protocol usage in favour of HTTPS. The second example is dynamic HTML pages, where anyone with access to the Internet can include links to malicious third-party targets, and these harmful assets might result in unanticipated web application or web service behaviour. The primary focus of this paper is the implementation of Content Security Policy (CSP) as an HTTP Security Header. CSP is one of a number of HTTP Response Headers that have recently been

used to protect communication using HTTP and HTTPS protocols. It increases the level of security in IoT network communications between devices as well as between web servers and web browsers. Although CSP header is not yet required, it is advised in contexts where communication parties (people and devices) want to ensure that they only access resources (source code and services) within authorised domains and subdomains.

LITERATURE SURVEY

CONTENT SECURITY POLICY

Similar to HTTP Strict Transport Policy, the goal of Content Security Policy (CSP), another type of HTTP Security Header, is to transmit security policy from the web server to the web browser in the form of an HTTP Response Header. Assets, or sources of content that a web browser may load, are included in this policy. It is a successful defence against Cross Site Scripting (XSS) assaults and the leading web browsers, including Chrome, Firefox, Opera, Safari, Internet Explorer, and Edge, all accept this technique. However, they all support SCP headers differently, as do the browser versions.

Do I need a content security policy?

Because the source code of the web page ordered them to, web browsers also load the assets indicated in the code, such as stylesheets, Java scripts, fonts, images, etc. There is no way for web browsers to tell whether or not those assets will be loaded. An attacker can direct browsers to download malicious malware from a third party by placing a specific snippet of code on a web page. traditional fashion, There is no justification for web browsers not to load the resources from rogue domains or subdomains. This is where the Cross Site Scripting (XSS) assault security problem is addressed elegantly by the Content Security Policy.

Accepting reliable sources

The CSP header specifies the sources from which a web browser may load content. It is feasible to defend web browser against a variety of security vulnerabilities by identifying the allowed sources that web browser use for page rendering. The CSP Response Header is a rather straightforward mechanism for allowing a web browser to load, for instance, a script solely from its own domain. An example of this is the HTTP Response (CSP) header.

ADVANCED STUDIES

A unified information space that offers timely, comprehensive information security, full-scale protection from computer terrorism and terrorism in general, socio-economic stability of economic entities of all types and forms of ownership, society as a whole, and each individual from various threats and risky situations in market conditions is objectively necessary at the current stage of socio-economic development. Applying a logistics approach to the problems of enhancing the effectiveness and security of the processes of functioning of information flows (IE) of an organisation on the basis of micro- and macro-level human management is therefore fascinating and socially and economically rewarding. The management of information security ensures the availability, confidentiality, and integrity of an organization's assets. data, information, and services. The processing of paper documents, building access, phone conversations, etc. for the entire business are all included in an organisational approach to security management that has a wider scope than the service provider [2]. Information security management is typically a component of this strategy. ISM's primary objective is to make sure that all services and activities within service management

are managed effectively in terms of information security. Information security is intended to defend against attacks on the integrity, confidentiality, and availability of data, systems, and communications.

1. Information is in a confidential condition when only those with the proper authorization can access it.

2. Integrity is the condition of information when no changes are made to it or when changes are not made.
3. Accessibility is the quality of information that allows those with access rights to use it freely. If: 1. Information is accessible when needed, and information systems are resilient to attacks, can avoid them, or can recover rapidly, the goal of assuring information security is achieved. 2. Only those with the necessary rights can access information. 3. The data is accurate, full, and shielded from unauthorised changes.

4. Information exchange with partners and other organisations is secure.Several antivirus solutions are being used to check the content, but they only look for specific infections according to their viral databases. The integrity of the website's content is what our proposal aims to reflect. We are primarily focused on ensuring security for the existing systems. If the security was breached, hackers would be able to change the data on the web pages stored on the web servers. The current system is completely secure.

Internet web pages may include data that has been altered by hackers or other unauthorised parties.The web servers might not provide us with accurate statistics.

It can be challenging for the Administrator to find the alterations in the current system.

PROPOSED METHOD

To check the accuracy of web contents before the server sends an HTTP response to a user request, we recommend using the WM-PDA (Web Server based MD5 Page Digest Algorithm). Our Java implementation of the WSPDA, known as the Dynamic Security Surveillance Agent, adds additional security protections over and above the standard ones. in terms of Web-based systems' content integrity. Its purpose is to stop client machines from being used by hostile attackers and intruders to modify Web contents from being displayed.

Integrity Checking Techniques.

Here, we go over the methods that can be used to verify the validity of web contents while maintaining the integrity of web pages. There are four ways to determine a Web document's legitimacy. A method that can conduct the checking procedure at the maximum speed with the least amount of server-side processing time qualifies as one of the solutions provided in this thesis. The following discussion of these techniques takes into account these prerequisites. The last approach, the proposed way, is more appropriate for usage on the server side whereas the other three methods are better suited for use on the client side. A digital signature is used to authenticate (sign) each page as a separate document. This requires a lot of computation. According to the literature, 200 signatures can be verified or two communications can be signed every second. This is inappropriate for the kind of server-side activity that we are proposing. When Web pages are signed or verified at the server, this causes the server to operate slower than normal. Also, the client-side procedure of a user having to confirm the legitimacy of the Web pages they are viewing takes time.

A number of pages are read through and signed as Although this is more effective than the prior approach, verification is still carried out at the conclusion of the path. This takes too much time and serves no useful purpose. The website has a page tree structure. The use of a digital signature is then necessary in order to check the integrity in a more flexible and natural manner.

Only use the hash functions when you need them to access a web page's entire content, including any embedded objects. The page is legitimate and the Web server will respond to clients if the determined hash value matches the previously calculated and stored value. If not, it is assumed that security breaches on the page will require corrective action. This project's algorithm solely relies on hash functions. Due to its 1000x quicker generation and 100x faster verification speeds than RSA signature systems, the use of a hash function is preferable over digital signatures. In a secure database server that is write protected, hash values are encrypted and kept there. Due to its particular function and the fact that it is a different server from the Web server, the access control on the secure database server is stronger. Moreover, SSL security is used to protect the communication channel between the two servers (Secure Socket Layer).

HASHING PRACTICES

Our thesis proposes the Safe Hash Algorithm to calculate hash functions (SHA-1).

Together with this SHA-1 method, we also have PGP34 and Message Digest (MD5). These strategies have benefits and drawbacks as well. These two techniques are also covered.

MESSAGE DIGEST:

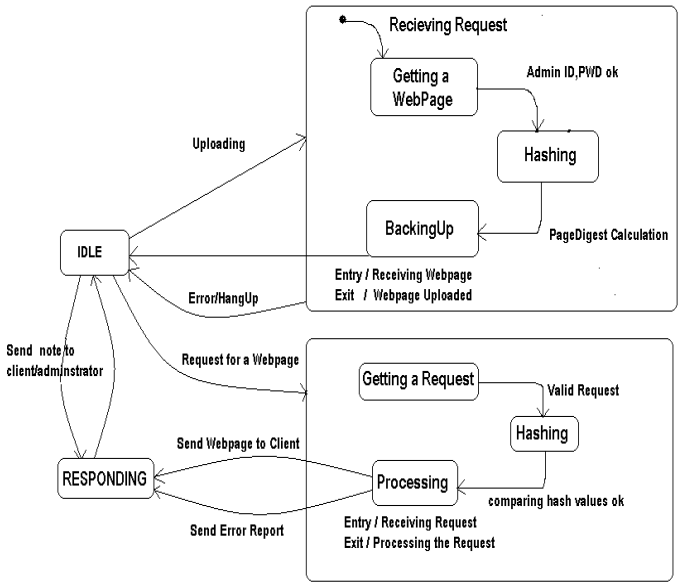
An MD5 message digest for Web pages was created to study the two-way exchange of information when resources metadata was embedded into WebPages using the HTML META element. The checksum of the resource, for which the metadata is listed as one of the metadata elements, was placed in the webpage in order to ascertain whether the resource had been updated.

The checksum algorithm used here is restricted to the extraction of particular Web page components such embedded objects like resource photos and HTML "META" elements. The document's body, which may contain tab spaces, white spaces, etc., is ignored. It then generates the message digest of each of the aforementioned portions using the MD5 hash function. A message-digest (hash value), which has a constant size and represents messages with variable sizes p, is called a hash value. In order of occurrence on the page, it then rehashes the previously hashed message-digests for each segment of the content. The resource for which the metadata was created has not been changed since its creation if the generated hash value matches the stored hash value embedded in the page.

WE HAVE CONTRIBUTED:

- Data integrity will be upheld.
- The web servers can provide accurate information about web environments.
- The Administrator can quickly identify changes in the planned system.
- recording the list of safety controls, the procedures for using and managing them, as well as the dangers connected to them;
- oversee vendors and agreements that call for system and service access.
- It is carried out in conjunction with the supplier management process, as well as monitoring all security incidents and breaches involving systems and services, proactively enhancing security measures.
- lowering information security risks, and incorporating information security considerations into all service management processes.

Architecture Diagram



ALGORITHM:

Page Digest verfication ALGORITHM:

Input: present digest
Output: original digest
Algorithm:
Start
Step 1: hc=getHashCode(pc)
Step 2: Ppd=makeDigest(hc)
Step 3: Opd=oget Digest ()
Step 4:callDigestEngine ()
Step 5:VerifyIntegrity ()
Step 6: dofilter ()
Stop

MODULE DESCRIPTION

Digest gen: - The Digest Generator class recognises the user's request, computes the digest, and updates the database with the URL requested, the request's digest value, and the identity of the administrator who uploaded the page to the server. The class DWA SHA is used to calculate the digest value. This module provides the digest value, which is then used to verify the website's integrity.

DWA Varifier: When a web page request is made, the DWA Varifier compares the current calculated page digest value with the previous database page digest value. To obtain the url for which the page digest should be calculated, this module depends on the DigestGen class. Based on a comparison of the old and new digest values, this verifier module returns a Boolean value. It uses DigestGen and Dwa Connection, two additional modules, for this function. By means of the DWA Connection class, a connection String is obtained, and this is used to retrieve a database digest value. It obtains a digest value—the present value—by using Digestgen. As a result of the comparison, the Verifier now compares the old value to the current value and returns a Boolean value.

DWA Connection: In accordance with the Backend Specification being utilised, this module loads the necessary driver. We retrieve a SHA instance and the requested page's hash value from this class.

DWA_MD5:

DWA SHA performs the Page Digest calculation and returns the Page Digest value. This module receives the requested Web page as input and generates a page digest value for it. The Digest Gen module updates the database with the URL and PAGE DIGEST updates, respectively, and depends on the DWA MD5 for the digest value. The connection string can only be obtained by using DWA Connection.

Filtering Pages: DWA Varifier is required by the PageFilter module. The DWA Varifier returns a Boolean value, and the filter responds to the client based on this Boolean value.

The requested web page is sent to the client if the Boolean value returned by the Varifier is TRUE; else, an error note and an error mail are sent to the administrator.

INDICATORS OF INFORMATION SECURITY MANAGEMENT'S PERFORMANCE

As examples of markers that can be utilised as key performance indicators for the management of personnel information security, consider the following:

1. safeguarding the company's information security and its employees: Use is only permitted at San Francisco State University with a licence. downloaded from IEEE Xplore on June 18, 2021 at 10:25:23 UTC. There are constraints. 109 a percentage decrease in the Service Desk's communications concerning "gaps"; a percentage decrease in the impact that "gaps" and incidents have on the company; and a percentage increase in the SLA's information security requirements.
2. decreasing the number of inconsistencies between ISM procedures and corporate information security processes and policies, that is, developing a clear and consistent information security policy that takes into account the demands of the company and staff.
3. Security measures that the management of the company has justified, agreed upon, and approved:

• enhancing the suitability and consistency of security protocols; • gaining more management backing. Reducing the number of discrepancies found during testing and audit; and Proposing more enhancements to controls and processes are the other two improvement techniques.

CONCLUSION

When it comes to maintaining information security, the science and practise of people management face numerous challenges and dangers. Very frequently, management and administration think that only IT should handle information security-related concerns. Because management is the one who decides whether to fund something, they should be aware of the substantial expenses involved in developing an efficient information security system. Maintaining a balance is crucial; the expense of information security should not outweigh the cost of protecting the most sensitive data.

REFERENCES

[1] HUIWEN WANG, LIANGLIANG WANG, KAI ZHANG, JINGUO LI, AND YIYUAN LUO, "A Conditional Privacy-Preserving Certificateless Aggregate Signature Scheme in the Standard Model for VANETs" in IEEE Access Jan 2021.

[2] SUHYEON LEE AND SEUNGJOO KIM, "Blockchain as a Cyber Defense: Opportunities, Applications, and Challenges" in IEEE Access Dec 2021.

[3] ABEL YEBOAH-OFORI 1, SHAREEFUL ISLAM2, SIN WEE LEE2, ZIA USH SHAMSZAMAN 3, (Senior Member, IEEE), KHAN MUHAMMAD 4, (Member, IEEE), METEB ALTAF 5, AND MABROOK S. AL-RAKHAMI 6, (Member, IEEE), "Cyber Threat Predictive Analytics for Improving Cyber Supply Chain Security", in IEEE Access Jul 2021.

[4] YAKUB KAYODE SAHEED 1,2, (Member, IEEE), AND MICHEAL OLAOLU AROWOLO3,4, (Member, IEEE), "Efficient Cyber Attack Detection on the Internet of Medical Things-Smart Environment Based on Deep Recurrent Neural Network and Machine Learning Algorithms", in IEEE Access Nov 2021.

[5] ANA KOVACEVIC 1, NENAD PUTNIK, AND OLIVER TOSKOVIC, "Factors Related to Cyber Security Behavior", in IEEE Access Jul 2020.

[6] DAMJAN FUJS 1, SIMON VRHOVEC 2, AND DAMJAN VAVPOTIC 1, "Know Your Enemy: User Segmentation Based on Human Aspects of Information Security", in IEEE Access Nov 2021.

[7] Sanjeetha. R, K.N Ajay Shastry, H.R Chetan, Anita Kanavalli, "Mitigating HTTP GET FLOOD DDoS attack using an SDN controller" in IEEE Access Nov 2020.

[8] Agung Wijayanto, Ema Utami, Agung Budi Prasetio, "Analysis of Vulnerability Webserver Office Management of Information And Documentation Diskominfo using OWASP Scanner", in IEEE Jan 2020.

[9] Marek Sikora, Andrej Krivulcik, Radek Fujdiak, Petr Blazek, "Design of Advanced Slow Denial of Service Attack Generator," in ICUMT Mar 2020.

[10] Vaibhavi Deshmukh, Swarnima Deshmukh, Shivani Deosatwar, Reva Sarda, Lalit Kulkarni, "Versatile CAPTCHA Generation Using Machine Learning and Image Processing," in ICCCA Oct 2020.

[11] Rizgar R. Zebari, Subhi R. M. Zeebaree, Amira Bibo Sallow, Hanan M. Shukur, Omar M. Ahmad, Karwan Jacksi, "Distributed Denial of Service Attack Mitigation using High Availability Proxy and Network Load Balancing", in ICOASE Feb 2021.

[12] Krishna Chaitanya Nunna, Ramakalavathi Marapareddy, "Secure Data Transfer Through Internet Using Cryptography and Image Steganography", in IEEE Access May 2022.

[13] EONGSU KIM 1 AND AARAM YUN 2, "Secure Fully Homomorphic Authenticated Encryption", in IEEE Access Jul 2021

[14] GABRIEL ARQUELAU PIMENTA RODRIGUES1, ROBSON DE OLIVEIRA ALBUQUERQUE 1, GABRIEL DE OLIVEIRA ALVES1, FÁBIO LÚCIO LOPES DE MENDONÇA1, WILLIAM FERREIRA GIOZZA1, RAFAEL TIMÓTEO DE SOUSA, JR. 1, (Senior Member, IEEE), AND ANA LUCILA SANDOVAL OROZCO 1, "Securing Instant Messages with Hardware-Based Cryptography and Authentication in Browser Extension", in IEEE Access May 2020.

[15] KOOKJIN KIM 1,2, SUKJOON YOON3, DONGHWAN LEE1,2, JISOO JANG1,2, HAENGROK OH4, AND DONGKYOO SHIN 1,2,3, (Member, IEEE)," Study on Prioritization of Actions by Classifying and Quantifying Cyber Operational Elements Using 5W1H Method", in IEEE Access Jul 2022.

[16] HOSSEIN ABROSHAN 1, JAN DEVOS 2, GEERT POELS 1, AND ERIC LAERMANS 2, (Member, IEEE), "Phishing Happens Beyond Technology: The Effects of Human Behaviors and Demographics on Each Step of a Phishing Process", in IEEE Access Mar 2021.

[17] LAKSHMANA RAO KALABARIGE1, ROUTHU SRINIVASA RAO 2, AJITH ABRAHAM 3, AND LUBNA ABDELKAREIM GABRALLA 4, "Multilayer Stacked Ensemble Learning Model to Detect Phishing Websites" in IEEE Access Jul 2022.

[18] HOSSEIN ABROSHAN 1, (Member, IEEE), JAN DEVOS 2, GEERT POELS 1, AND ERIC LAERMANS 2, (Member, IEEE), "COVID-19 and Phishing: Effects of Human Emotions, Behavior, and Demographics on the Success of Phishing Attempts During the Pandemic", in IEEE Access Aug 2021.

[19] THOMAS SUTTER, AHMET SELMAN BOZKIR, BENJAMIN GEHRING, AND PETER BERLICH, "Avoiding the Hook: Influential Factors of Phishing Awareness Training on Click-Rates and a Data-Driven Approach to Predict Email Difficulty Perception," in IEEE Access Sept 2022.

[20] JAEIL LEE1, YONGJOON LEE2, DONGHWAN LEE3, HYUKJIN KWON4, AND DONGKYOO SHIN, "Classification of Attack Types and Analysis of Attack Methods for Profiling Phishing Mail Attack Groups", May 2021.

[21] MIKIO FUJIWARA1, RYO NOJIMA1, TOYOHIRO TSURUMARU2, SHIHO MORIAI1, MASAHIRO TAKEOKA1, AND MASAHIDE SASAK, "Long-Term Secure Distributed Storage Using Quantum Key Distribution Network With Third-Party Verification", In IEEE Access Dec 2021.

[22] GENQING BIAN1, RUI ZHANG 1, AND BILIN SHAO, "Identity-Based Privacy Preserving Remote Data Integrity Checking With a Designated Verifier", in IEEE Access Apr 2022.

[23] IMRAN MAKHDOOM 1,2, (Member, IEEE), KADHIM HAYAWI 3, (Member, IEEE), MOHAMMED KAOSAR 4, (Senior Member, IEEE), SUJITH SAMUEL MATHEW 3, (Member, IEEE), AND PIN-HAN HO 5, (Fellow, IEEE), "D2Gen: A Decentralized Device Genome Based Integrity Verification Mechanism for Collaborative Intrusion Detection Systems", in IEEE Access Oct 2021.

[24] HWAJUNG KIM1, INHWI HWANG1, JEONGEUN LEE1, HEON Y. YEOM 1, (Member, IEEE), AND HANUL SUNG, "Concurrent and Robust End-to-End Data Integrity Verification Scheme for Flash-Based Storage Devices", in IEEE Access Mar 2022.

[25] Qingxuan Wang, Chi Cheng, Member, IEEE, Rui Xu, Jintai Ding, and Zhe Liu, "Analysis and Enhancement of a Lattice-Based Data Outsourcing Scheme With Public Integrity Verification", in IEEE Access Aug 2022.