Detection of Website Security Headers and Leaked Version along with Remedies

Rutvi Changela[1], Dr. Ravi Sheth[2]
[1]*MTech Student, School of Information Technology & Cyber Security, Raksha Shakti University, Dahegam, Gandhinagar, Gujarat*
[2]*Guide, Assistant Professor, School of Information Technology & Cyber Security, Raksha Shakti University, Dahegam, Gandhinagar, Gujarat*

***Abstract*- In this fast IT development process, almost many processes are automated by several open sources. While develop anything using open-source to trust their tools which may have many vulnerabilities in the website likewise configuration, actual security code requirements, headers, filters security misconfiguration, unused pages, unnecessary services, unprotected files, and directory, etc. To identify the first level of vulnerability here develops a tool to measure the security headers and website version along with remedies.**

***Index terms*- HTTP Security Headers, Liked Version, Remedies, and Tools**

I.INTRODUCTION

The main goal of this research is to assess the contemporary adoption rate of safety policies primarily based on HTTP reaction headers at the most popular Internet websites. Declarative net safety through HTTP reaction headers constitutes an effective and easy way to enhance internet site safety, at the same time as the surprisingly little attempt is required from internet site operators. It has been a recurrent research topic, aided by way of the reality that the nature of the World Wide Web makes facts publicly available to any interested party and that the World Wide Web itself is unendingly growing and evolving.

Besides measuring protection headers adoption in popular websites, we set out to understand it in a deeper way via trying to and correlations among adoption quotes and variables like HTTPS usage and recognition rank position. We need to benefit perception into why and the way policies based totally on HTTP headers are adopted. As can be shown, the most popular a website is, the much more likely it'll apply safety through HTTP headers. Those sites also tend to be more prone to favoring HTTPS protocol over HTTP.

II. BACKGROUND

The web infrastructure continues to be exploited by attackers, with wide unfold implications that have an effect on each aspect of society. Over the years, Researchers and Industry have responded in kind by develop- opting browser mechanisms that mitigate popular website attacks such as cross-site scripting, click jacking, and others. The browse has become the main battleground, and many recent proposals have sought to strengthen the browser by leveraging and extending existing features. In particular, HTTP Headers have become a popular channel for implementing defense mechanisms. Effective website security defense mechanisms have emerged in the form of declarative security in HTTP headers, which provide explicit security parameters that instruct browsers to enforce specific security functionality against common web vulnerabilities. This requires close coordination between the browser and the server.

Headers	Example Attacks Mitigated
Set-Cookie	Session hijacking, Cookie stealing.
X-Frame-Options	Clickjacking
Access-Control-Allow-Origin	Cross-site access
X-XSS-Protection	Cross-site scripting
Strict-Transport-Security	Man-in-the-middle
X-Content-Type-Options	MIME sniffing.
Content-Security-Policy	XSS, CSRF

Table1- List of security header analyses

III. HTTP SECURITY HEADERS

When a person visits a website through his/her browser, the server responds with HTTP Response Headers. These headers tell the browser a way to behave during communication with the website. These headers especially incorporate metadata.

You can use those headers to outline conversations and improve network security. Let's have a examine five security headers in an effort to deliver your web page some much-wanted protection.

A. HTTP Strict Transport Security (HSTS)

Let's say you've got an internet site named example.Com and you installed an SSL/TLS certificate and migrated from HTTP to HTTPS. This is good, right? That changed into rhetorical. It sincerely is. But this isn't in which the work stops. What if your internet site is nonetheless available over HTTP? It could be utterly pointless, right? Many internet site admins migrate to HTTPS and then forget about it without understanding this. This is in which HSTS enters the picture. If a domain is geared up with HTTPS, the server forces the browser to speak over steady HTTPS. This way, the possibility of an HTTP connection is eliminated entirely.

B. Content Security Policy (CSP)

The HTTP Content Security Policy reaction header gives internet site admins an experience of manipulating by means of giving them the authority to limit the assets a consumer is permitted to load within a web site. In other words, you may white list your web page's content sources.

Content Security Policy protects against Cross-Site Scripting and different code injection attacks. Although it doesn't eliminate their possibility entirely, it can positively reduce the damage. Compatibility isn't a problem as the maximum of the predominant browsers assist CSP.

C. Cross-Site Scripting Protection (X-XSS)

As the name suggests, X-XSS header protects in opposition to Cross-Site Scripting attacks. XSS Filter is enabled in Chrome, IE, and Safari by means of default. This filter out doesn't let the page load whilst it detects a cross-website scripting attack.

D. X-Frame-Options

In the Orkut era, a spoofing method called 'Clickjacking' changed into pretty popular. It nonetheless is. In this technique, an attacker fools a user into clicking something that isn't there. For example, a user may suppose that he's on the authentic Orkut website, however, something else is running within the background. A person may screen his/her confidential records within the process.

X-Frame-Options help defends these varieties of attacks. This is executed by way of disabling the iframes present at the web site. In different words, it doesn't allow others to embed your content.

E. X-Content-Type-Options

The X-Content-Type header gives a countermeasure against MIME sniffing. It instructs the browser to follow the MIME sorts indicated inside the header. Used as a feature to find out an asset's file format, MIME sniffing can also be used to execute cross-website scripting attacks.

IV. TOOL ANALYSIS

A. Hacker Target

Use open-source gear and network intelligence to help organizations with attack surface discovery and identification of security vulnerabilities.

Hacker device is an Online Vulnerability Scanners to map the attack surface and pick out vulnerabilities.

Hacker Target Tool will Display the HTTP headers of any web site. Use the simple web interface or access the Free API to check the HTTP headers. Information can be accrued in a check of the HTTP Headers from an internet server. Server-side software can be identified frequently down to the precise version running. Cookie strings, web application technologies and other statistics can be gathered from the HTTP Header.

HTTP Header Security Analysis

In our evaluation of the era used by the world's pinnacle websites, we queried the statistics on using HTTP Header protection controls.

This is a breakdown of the HTTP Header safety functions which have been developed by using different businesses. These controls can utilize features within the net browser to guard the user from browser-based exploits. Unfortunately, it's far clean from the consequences the application of those security controls is at exceptional minimal and toward non-existent inside the top websites.

B. Geekflare

Secure Headers Test

Mitigate the security vulnerabilities by enforcing important steady HTTP response headers in the internet server, network device, etc.
Currently, it checks the subsequent OWASP recommended headers.
HTTP Strict Transport Security
Public Key Pinning Extension for HTTP
X-Frame-Options
X-XSS-Protection
X-Content-Type-Options
Content-Security-Policy
X-Permitted-Cross-Domain-Policies
Referrer-Policy
Expect-CT
Feature-Policy

C. Pentest-Tools

The website vulnerability scanner is one in every of a complete set of gear offered by Pentest-Tools that incorporates a solution for records gathering, net utility testing, CMS testing, infrastructure testing,and SSL testing. In particular, the website scanner is designed to discover commonplace internet utility vulnerabilities and server configuration issues.

D. Ipvoid

This HTTP Security Response Headers Analyser lets you check your internet site for OWASP endorsed HTTP Security Response Headers, which encompass HTTP Strict Transport Security (HSTS), HTTP Public Key Pinning (HPKP), X-XSS-Protection, X-Frame-Options, Content-Security-Policy (CSP), X-Content-Type-Options, etc.

E. Up Guard

Up Guard Web Scan is an external hazard assessment device that makes use of the publicly available facts to grade.
Test results are labelled into the following groups.

- Website risks
- Email risks
- Network protection
- Phishing and Malware
- Brand protection

Good to get a short protection posture of your internet site.

F. Site Guarding

Site Guarding lets you scan your domain for malware, website blacklisting, injected spam, defacement, and plenty more. The scanner is well-matched with WordPress, Joomla, Drupal, Magento, osCommerce, Bulletin, and another platform.

Tool	Directory Listing	HTT Security Headers	Leaked Version Show	Remedies Show
Hacker Target	NO	NO	YES	NO
Geek flare	NO	YES	NO	NO
Pentest-Tools	Yes	YES	Yes	NO
IPVOID	NO	NO	Yes	NO
Up Guard	NO	No	NO	NO
Site Guarding	NO	NO	Yes	NO

Table2- Tools Comparison

V. PROPOSED WORK

A. Implementation

I have make an online scanner, when you enter any URL or domain name in input then scanner will scan your website and as output show results like malware detection, HTTP Security Headers detection, Detect liked version of website and show the Remedies.

Figure 1 Input Section

Figure 2 what is site Check

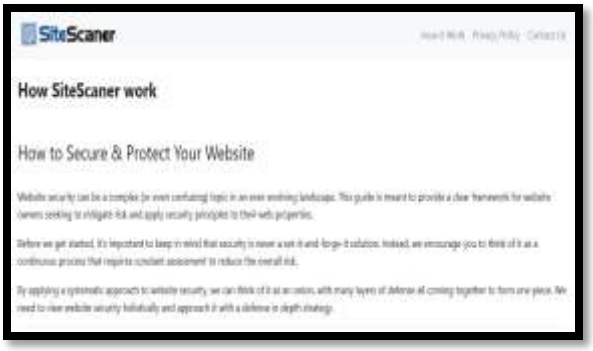

Figure 3 How Site Scanner Work

Figure 4 Privacy Policy

Figure 5 Contact Us

B. Results

Figure 1 Enter the Domain Name

Figure 2 Malware Detection

Figure 3 Detect Rating and Version

Figure 4 Detect HTTP Security Headers

VII. CONCLUSION

From the implementation of the tool, we can conclude that:

1 It detects the domain is vulnerable to host header attack or not. The host header specifies which application and websites should process an incoming HTTP request.

2 It displays the list of files contained in this directory.
3 It also scans websites and detects malware is present or not.
4 It also show Leaked version of website and give the solution of vulnerability.

VIII. ACKNOWLEDGMENT

The author like to thanks IT department of Raksha Shakti University for giving all support and guidance which have enhanced the quality of the paper.

REFERENCES

[1] Fielding, R., Gettys, J., Mogul, J., et al.: 'RFC 2616 – hypertext transfer protocol – HTTP/1.1'. Society [Internet], 1999, no. 2616, pp. 1–114. Available at: http://www.ietf.org/rfc/rfc2616.txt
[2] Klensin, J.: 'RFC 5321 – simple mail transfer protocol'. IETF RFC, 2008
[3] Postel, J., Reynolds, J.: 'RFC 959 – file transfer protocol'. Rfc 959 [Internet], 1985, pp. 1–69. Available at: https://www.ietf.org/rfc/rfc959.txt
[4] Mockapetris, P.: 'Domain names – implementation and specification [Internet]'. Request for Comments, 1987, pp. 1– 55. Available at: https:// www.ietf.org/rfc/rfc1035.txt
[5] Rescorla, E.: 'RFC 2818 – HTTP over TLS'. Network Working Group, IETF, 2000. p. pp. 1–8
[6] Sterne, B., Barth, A.: 'Content security policy 1.0 [Internet]. W3C. 2012'. Available at http://www.w3.org/TR/CSP/
[7] Bash, E.: 'RFC7469 public key pinning extension for HTTP'. PhD Propos, 2015, vol. 1, pp. 1–28
[8] Hodges, J., Jackson, C., Barth, A.: 'HTTP strict transport security'. Available at http//tools.ietf.org/html/rfc6797. 2012
[9] Gondrom, T.: 'HTTP header field X-frame-options', IETF Standard, 2013. Available at: https://tools.ietf.org/html/rfc7034
[10] Hodson, H.: 'A little privacy, please'. New Sci [Internet], 2014, vol. 224, no. 2997, p. 24. Available at: http://www.sciencedirect. com/science/article/ pii/ 0262407914622843