Assessing the Adoption of HTTP Security Headers

Ana Țurcan [1], Dumitru Ciorbă [1], Dinu Țurcanu[1], Răzvan Rughiniș[2]
[1]Technical University of Moldova, ana.turcan@fcim.utm.md, dumitru.ciorba@fcim.utm.md, dinu.turcanu@adm.utm.md, ORCID: 0000-0002-9334-7606, 0000-0002-3157-5072, 0000-0001-5540-4246, https://utm.md
[2]National University of Science and Technology POLITEHNICA, razvan.rughinis@upb.ro, ORCID: 0000-0003-2794-280X https://upb.ro

Keywords: Web security, Security assessment, HTTP headers

Abstract. Recent cybersecurity evaluations reveal that many user vulnerabilities are linked to web technologies, mainly stemming from inadequate or improper usage of HTTP headers. [1]

Security headers in HTTP responses provide an essential layer of protection against common web vulnerabilities such as cross-site scripting (XSS), clickjacking, and MIME-type sniffing attacks. These headers, including Content-Security-Policy, X-Content-Type-Options, Strict-Transport-Security, and X-Frame-Options, among others, serve as safeguards by enforcing stricter communication policies between web servers and browsers. [2]

The availability of various tools indicates the increasing significance of using HTTP headers. [3] Although they provide valuable analyses, they are either overly complex and inaccessible, or the simplistic approach lacks comprehensiveness in various aspects of web security.

Therefore, this paper proposes a complex methodology to provide a balanced framework for assessing a website's security. This framework encompasses both traditional web security practices and modern cross-origin protections.

The Web Security Index (WSI) scoring methodology evaluates website security with 150 points. Core HTTP security headers (CSP, HSTS, X-Frame-Options, etc.) contribute 65 points, emphasizing foundational protections.

Cross-origin protections are heavily weighted (40 points) to combat data theft, while HTTP/2 standards account for 20 points. Additional features, including cookies and DNSSEC, add 25 points, reflecting modern security needs.

The research aimed to identify the presence of security headers and calculate the WSI score for specific European nations within the subregions of Europe according to the UN geoscheme. The countries were selected based on a combined index proposed by the ITU, the Global Cybers Security Index 2024 [1], and the evaluation score for each country according to the National Cyber Security Index (NCSI) [4].

The analysis of WSI scores reveals that lower-performing websites universally lack essential security headers, highlighting their inadequate security configurations and susceptibility to various cyber threats. Among the subregions, Northern Europe excels in adopting modern security practices, while Eastern Europe exhibits the most significant deficiencies in security implementations.

This context reinforces the relevance of HTTP security headers in providing a robust shield for users against the pervasive threats that proliferate across the web.

References

[1] International Telecommunication Union (ITU), “Global Cybersecurity Index, 5th edition,” Geneva, 2024. Accessed: Sep. 10, 2024. [Online]. Available: https://www.itu.int/gci

[2] A. Zineddine *et al.*, “A systematic review of cybersecurity assessment methods for HTTPS,” *Computers and Electrical Engineering*, vol. 115, p. 109137, Apr. 2024, doi: 10.1016/j.compeleceng.2024.109137.

[3] W. J. Buchanan, S. Helme, and A. Woodward, “Analysis of the adoption of security headers in HTTP,” *IET Information Security*, vol. 12, no. 2, pp. 118–126, 2018, doi: 10.1049/iet-ifs.2016.0621.

[4] “National Cyber Security Index,” National Cyber Security Index. Accessed: Sep. 15, 2024. [Online]. Available: https://ncsi.ega.ee/ncsi-index/