HTTP Security Headers Analysis of Several Categories Macedonian Websites

Bojana Taseva, Aleksandra Brashnarova, Aleksandra Mileva, Dushan Bikov
Faculty of Computer Science, Goce Delcev University, Stip
N. Macedonia

bojana.102558@student.ugd.edu.mk; aleksandra.102553@student.ugd.edu.mk;
aleksandra.mileva@ugd.edu.mk; dusan.bikov@ugd.edu.mk

Abstract

In recent years, with the growth in the number and importance of various Internet services, there has been a deficiency in the implementation of security measures. Many website services are susceptible to cyberattacks and have various vulnerabilities. This assertion is supported by monitoring conditions and reports regarding the status of several government websites that have experienced large-scale attacks, resulting in their temporary unavailability. Some of them were compromised, leading to the theft of confidential data.

For websites' security, it is critical to understand and implement properly HTTP security headers to prevent or limit the dangers that can cause website attacks such as Denial of Service (DoS), Cross-Site Scripting (XSS), SQL Injection, Clickjacking, and more. HTTP security headers include Strict Transport Security, Content Security Policy, X-Frame-Options, Cross-site Request Forgery Tokenization, X-Content-Type-Options, X-XSS-Protection, Referrer Policy, Cookies, etc.

This research covers the security analysis and evaluation of HTTP implementation and configuration in several categories of Macedonian websites, based on HTTP security headers, security performance metrics, gathering statistics, and examining other security properties using Mozilla Observatory. Mozilla Observatory is a set of web security tools that scans websites, analyzes HTTP response headers, evaluates TLS configurations, checks for the implementation of security best practices, etc. By inputting the website's URL, users receive a detailed report with overall grade (from F to A+) and score (from 0 to current maximum of 135), details about implemented HTTP security headers, recommendations for enhancing its security, etc. All websites start with a baseline score of 100 and receive penalties or bonuses from there. The tool is split in three separate projects: scanner/grader, command line interface and web interface.

Our study aims to answer the following research question: How do different examined Macedonian website categories perform in terms of security, based on an analysis of multiple HTTP security metrics?

The dataset for this research includes websites of all 88 municipalities and centers for regional development, 93 government bodies and institutions, 75 universities and faculties and 72 high schools.