Computer Science Journal of Moldova, vol.**33**, no.1(97), 2025

HTTP Security Headers Analysis of Several Macedonian Website Categories

Aleksandra Mileva, Dushan Bikov, Bojana Tasheva, Aleksandra Brashnarova

Abstract

The present research focuses on the security of Macedonian websites. It involves the analysis of HTTP Security header responses for 756 websites in the country, of which 246 are the most popular. This analysis is conducted across 13 different categories of websites, including government bodies and institutions, public institutions and enterprises, educational, commercial, news and media, entertainment, sports, etc. We intend to create a comprehensive security profile for the country's websites, which will help raise their overall security level.

It is critical to understand and implement proper HTTP security headers to prevent or limit the dangers that can cause website attacks such as Denial of Service (DoS), Cross-Site Scripting (XSS), Cross-Site Request Forgery (CSRF), SQL Injection, clickjacking, etc.

Our analysis was performed with the help of the Mozilla Observatory tool. We have discovered a significant lack of implementation and/or misconfiguration of HTTP security headers in all categories. Almost half of the websites (n=375; 49.60%) have an F grade, while more than a quarter of all websites (n=214; 28.31%) have a minimal security score of 0.

Keywords: Websites security, HTTP security headers, Mozilla Observatory, XSS, clickjacking.

MSC 2020: 68M10, 68M25, 68M11, 68M12.

doi:10.56415/csjm.v33.01

1 Introduction

In today's modern digital world, it is unimaginable without websites and the myriad of services they provide, influencing every aspect of our lives. Digital services play a crucial role in shaping our daily activities. Therefore, we must emphasize the importance of web trust and security. It is important to note that websites classified as e-Commerce, shopping, or payment services, which involve financial transactions, have even higher security requirements. The daily activities of people using digital services, regardless of whether the interface is a standard website or a mobile application, have significantly increased internet traffic. This trend has not only been accelerated, but is also a result of changes in people's lifestyles influenced by modern trends and, more recently, the global COVID-19 pandemic.

In recent years, with the growth in the number and importance of various 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 on the status of several government websites that have experienced large-scale attacks (e.g., the Health Insurance Fund of the Republic of North Macedonia [1], the Ministry of Education and Science [2]), resulting in their temporary unavailability. Some of them were compromised, leading to the theft of confidential data.

Different techniques, tools, and good practices have been developed to improve the security of websites [5], [6], [9], [12], [15], but their implementation is not consistent. How security techniques are developed, so do attackers adapt and exploit others and different vulnerabilities [16], [18].

Today, web servers and browsers offer support for many security HTTP headers that, if properly configured, can improve web application security against different types of attacks, such as cross-site script-

[1] https://www.slobodenpecat.mk/en/hakeri-go-napagjaat-fondot-za-zdravstvo-nadlezhnite-uveruvaat-pacientite-se-lekuvaat-neprecheno/

[2] https://balkaninsight.com/2022/02/07/north-macedonia-ministry-confirms-new-hacking-attack/

ing (XSS), clickjacking, cross-domain information leakage, man-in-the-middle (MiTM) attacks, insecure cookies, Content Delivery Network (CDN) compromises, and improperly issued certificates. In fact, they can be extremely powerful for blocking entire classes of attacks by restricting the behaviors permitted by the browser and server while the web application is running. Still, security HTTP headers depend on dynamic nature of current research and specifications, together with the browser vendor support, so sometimes we have a situation where some security headers are deprecated and replaced by others. In addition, its implementation should be tested before their approval to use, so that security and functionality can be balanced across the application environment.

This research will cover the security evaluation of 756 websites, divided into 13 categories, which includes an analysis of their current state based on HTTP security response headers, security performance metrics, collection of statistics, and examination of other security properties using Mozilla Observatory tools [10]. Mozilla Observatory was developed in 2016 by the security engineer April King. Its popularity can be observed from the fact that more than 6.9 million websites are being scanned a total of 47 million times up to July 2024 [4].

The dataset created for this research encompasses a diverse landscape, including the most significant Macedonian websites in the world. These websites cover various aspects of digital daily life, including education, research, state government services, local government services, services from the public sector, law, etc.

Concerning the organization of this article, in Section 2, we provide an overview of the related work. In Section 3, we present our methodology, while the results obtained and the discussion are given in Section 4. The last Section 5 is a conclusion of our work.

2 Related Works

There are several studies that can be found in the literature on analysis of deployment of HTTP security headers in the world. In 2017, Felt, et al. [5] evaluated how HTTPS adoption has grown over time, while Buchanan, et al. [1] analyzed Alexa Top One Million sites in May 2017 for several HTTP security headers (Content Security Policy (CSP), public key pinning extension for HTTP, HTTP Strict Transport Security (HSTS), and X-Frame-Options) within their HTTP responses. Lavrenovs and Melón [12] in September 2017 conducted an HTTP security header analysis (HSTS, CSP, X-XSS-Protection, X-Frame-Options, Cookies, and X-Content-Type) of the top one million websites. Kishani and Das [11] performed a similar analysis using the Mozilla Observatory tool with a list of the 10.000 most popular websites, categorized into 27 categories, using natural language processing.

The resilience of a website against various types of attacks is crucial and closely linked to the prevention of cybercrimes, which can be costly to address. Numerous studies have explored different aspects of website security. The authors Zhao J. and Zhao S. [25] assessed the e-commerce security of Fortune 500 organizations. Although all organizations used SSL to encrypt traffic between their websites and users, only 16% of them limited access attempts to a maximum of three attempts, and all sites had a firewall to secure their perimeter. Another investigation related to the Fortune 500 can be found in the Rapid7 report [23], which examines cybersecurity exposure, highlights improvements, and points out ongoing vulnerabilities, such as insufficient use of Domain-based Message Authentication, Reporting, and Conformance (DMARC) and HSTS. The WhiteHat website security statistics report [22] found that 86% of the scanned web applications had vulnerabilities, with an average of 56% per application, including at least one critical issue. In [24], an analysis of e-government platforms was performed to identify vulnerabilities on Web servers. The findings revealed that 67% of the platforms had broken links, 43.8% stored passwords without encryption, 35% were vulnerable to XSS attacks, and one in four platforms was susceptible to SQL injection and cookie manipulation. The study in [21] investigated inconsistencies in HTTP headers in desktop and mobile versions of websites, analyzing their impact on security, privacy, and user experience. A security assessment of Saudi Arabian websites [20], conducted using open source tools, revealed that a significant percentage of these websites were vulnerable to SQL injection, shell injection, and clickjacking. Content Management Systems (CMS), particularly WordPress, are widely used for building web applications. A study on the security assessment of WordPress backup plugins was conducted in [19].

3 Methodology

For this study, we used a methodology that involves three main phases: dataset creation, security evaluation using the Mozilla Observatory tool, and analysis of the results. Our methodology is similar to that of [11].

Dataset creation. For the creation of the dataset, we use the List of Information Holders [7], maintained by the Macedonian Agency for the protection of the right to free access to public information, where you can find all information holders in N. Macedonia with their officials and websites, categorized in several categories. On this website, you can find that information holders "are the bodies of the state government and other bodies and organizations determined by law; the bodies of the municipalities, the City of Skopje and the municipalities in the City of Skopje, institutions and public services, public enterprises, legal and natural persons exercising public authorities determined by law and activities of public interest and political parties in the area of revenues and expenditures".

For our study, we first selected 558 websites which we classified into 7 different categories: Municipalities and Centers for Regional Development, High Schools, Higher Educational Institutions (HEIs) and Educational Research Institutes, Judicial Authorities, Public Enterprises, Public Institutions, and Government Bodies and Institutions. Most of these entities have one website, but some of them have more. For example, most universities and faculties have several websites for e-learning platforms, information systems, e-repositories, e-libraries, etc. However, for our study, we used only their main websites, presented in the list [7].

Furthermore, we extend the dataset using Macedonian websites found in the Alexa Top 1 Million Sites[3]. We found 262 Macedonian websites on 05.07.2024. Of them, 16 were inactive and 23 were in-

[3] `https://www.kaggle.com/datasets/cheedcheed/top1m`

cluded in the previous classification. The rest 223 websites were categorized into 7 additional categories: News and Media, Classifieds and E-Commerce, Sport, Entertainment and Lifestyle, Business, Finance and Economy, Technology and Innovation, and Others. The 25 websites of Others were excluded from the dataset. So, we enlarge the original dataset with 198 additional websites, working with a total of 756 Macedonian websites.

Security evaluation using Mozilla Observatory tools. Several studies exist that use Mozilla Observatory tools for the security evaluation of websites (e.g., [5], [12]). The Mozilla Observatory is a set of tools for automatic security analysis of a given website, which also provides recommendations of different available measures and methods that can be used to secure the website, by their proper configuration and implementation in the web server itself. These measures are grouped into 10 different categories: Content Security Policy, Cookies, Cross-origin Resource Sharing, HTTP Strict Transport Security, Redirection, Referrer Policy, Subresource Integrity, X-Content-Type-Options, X-Frame-Options, and X-XSS-Protection. If the web administrator implements the recommendations obtained, the security of the website will be improved. However, web administrators should be aware that even in the case when the website has obtained an A+ grade (the highest score), this does not mean that the website is secure. The reason behind this is that the tool does not test for other security issues, like SQL injection vulnerabilities, not installing the latest security updates of different software packages, vulnerable plugins, improper authentication, etc.

Mozilla Observatory is divided into three projects [10]: 1) http-observatory – scanner/grader; 2) http-observatory-cli – command line interface (CLI) for evaluation of many websites at once (using scripts); and 3) http-observatory-website – web interface for evaluation of one particular website, which can be used online on [13]. There is also a third-party Java library and command-line interface[4]. On 2 July 2024, the HTTP Observatory was launched on MDN[5], and on 31 October 2024, its new version was launched, but our experiments were

[4] `https://github.com/stoennies/java-http-observatory-api`

[5] `https://developer.mozilla.org/en-US/observatory`

done before this date, so our results are based on the previous testing methodology.

In Mozilla Observatory, all websites start with a baseline score of 100 and receive penalties or bonuses from there. Bonuses are only awarded if the site's score without them is greater than or equal to 90. Although the minimum score is 0, there is no maximum score. In the old version, the highest possible score obtained is 135. Per each examined security measure, the score modifiers change the score of the specific measure, and the site's score is a sum of scores per measure. Each site's score has an associate grade given to the website. The possible grades are: F(0-24), D-(25-29), D(30-39), D+(40-44), C-(45-49), C(50-59), C+(60-64), B-(65-69), B(70-79), B+(80-84), A-(85-89), A(90-99), and A+(100+)[6]. Details about each measure and its score modifiers, together with details about the scan and the site score and grade obtained, are provided in a full report generated by the online tool. CLI tool offers 3 types of reports: JSON format with details about score modifiers, and CSV and report formats, without the details.

For our study, we used the official node.js CLI[7]. The websites in our dataset were scanned for 10 days, from 10.07.2024 to 19.07.2024. We created a Python script, which accepts a CSV file with a list of websites, and produces the Excel file with details about each category, site's score, and grade.

Analysis of the results. For our research, we first analyze the distribution of grades between the websites categories, together with minimal, maximal, and average score per category, so we can understand the overall picture about the security of examined Macedonian websites.

4 Results and Discussion

This section is devoted to our findings, their analysis, and implications. The elevation of security criteria for the websites is conducted through

[6] `https://github.com/mozilla/http-observatory/blob/main/httpobs/docs/scoring.md`

[7] `https://github.com/mozilla/observatory-cli`

an analysis of the HTTP headers received from the web server. Depending on the content of the HTTP header, instructions are provided for the browser to protect the application against security threats. However, the HTTP header, unintentionally, may carry information about the application that can be exploited by an attacker.

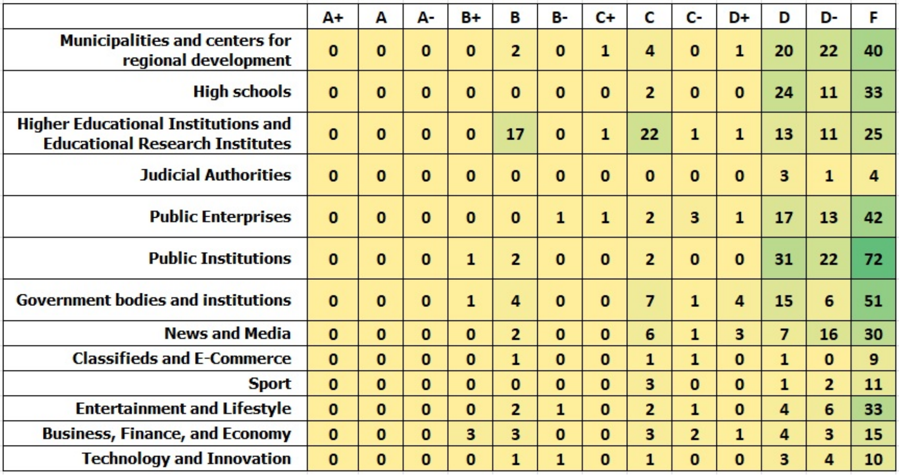
4.1 Distribution of Security Scores and Grades Between Website Categories

Table 1 gives an overview of the general results for the categories evaluated from Macedonian websites, by giving the number of websites in each category, the minimum, maximum, and average score per category, and the average grade per category.

Table 1. General results for evaluated categories of Macedonian web sites

Category	No. of websites	HTTP only	Min score	Max score	Average score	Average grade
Municipalities and Centers for Regional Development	90	3	0	75	19.94	F
High Schools	70	11	0	50	18.21	F
HEIs and Educational Research Institutes	91	12	0	75	35.55	D
Judicial Authorities	8	5	0	30	16.88	F
Public Enterprises	80	3	0	65	18.38	F
Public Institutions	130	13	0	80	16.96	F
Government Bodies and Institutions	89	7	0	80	19.89	F
News and Media	65	0	0	70	19.46	F
Classifieds and E-Commerce	13	1	0	70	19.23	F
Sport	17	0	0	50	14.12	F
Entertainment and Lifestyle	49	2	0	75	14.59	F
Business, Finance and Economy	34	1	0	80	29.41	D-
Technology and Innovation	20	1	0	70	19.75	F
Total	756	59	0	80	20.83	F

Furthermore, Figure 1 presents a heatmap with the distribution of site counts for grades and category websites.



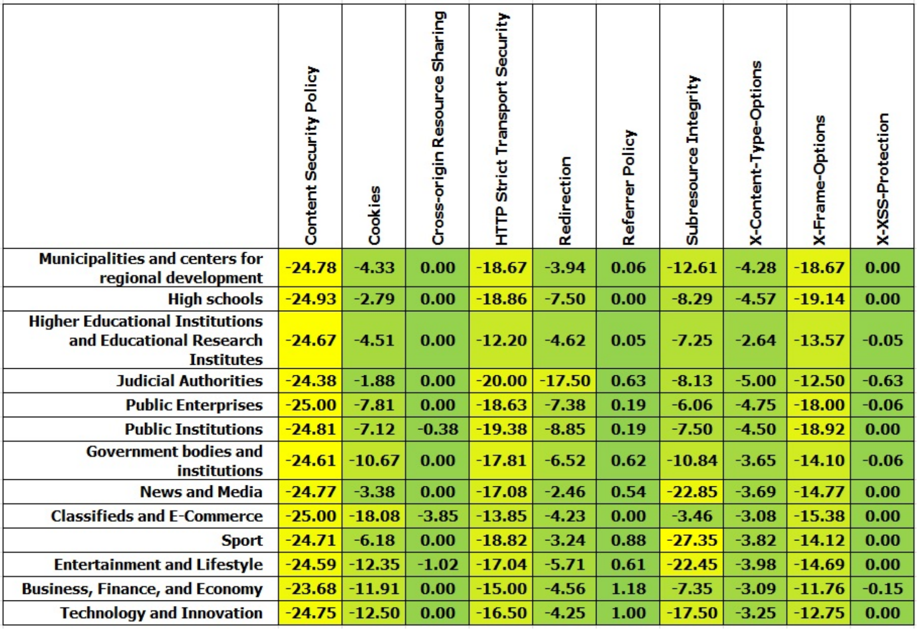
	A+	A	A-	B+	B	B-	C+	C	C-	D+	D	D-	F
Municipalities and centers for regional development	0	0	0	0	2	0	1	4	0	1	20	22	40
High schools	0	0	0	0	0	0	0	2	0	0	24	11	33
Higher Educational Institutions and Educational Research Institutes	0	0	0	0	17	0	1	22	1	1	13	11	25
Judicial Authorities	0	0	0	0	0	0	0	0	0	0	3	1	4
Public Enterprises	0	0	0	0	0	1	1	2	3	1	17	13	42
Public Institutions	0	0	0	1	2	0	0	2	0	0	31	22	72
Government bodies and institutions	0	0	0	1	4	0	0	7	1	4	15	6	51
News and Media	0	0	0	0	2	0	0	6	1	3	7	16	30
Classifieds and E-Commerce	0	0	0	0	1	0	0	1	1	0	1	0	9
Sport	0	0	0	0	0	0	0	3	0	0	1	2	11
Entertainment and Lifestyle	0	0	0	0	2	1	0	2	1	0	4	6	33
Business, Finance, and Economy	0	0	0	3	3	0	0	3	2	1	4	3	15
Technology and Innovation	0	0	0	0	1	1	0	1	0	0	3	4	10

Figure 1. Heatmap with distribution of website counts for grades and website categories

The average grade for all categories, except two, is the lowest grade F. Only the categories *HEIs and Educational Research Institutes* and *Business, Finance, and Economy* have an average grade D (35.55 security score) and D- (29.41 security score), respectively. The overall average security score for all websites is 20.83 (F grade) and the maximum score obtained is 80 (B+ grade). Almost half of the websites (n=375; 49.60%) have an F grade, and even more, more than a quarter of all websites (n=214; 28.31%) have a minimal security score of 0. Only 42 websites (5.56%) have a score from 65 to at most 80, which corresponds to grades B-, B, and B+. The security score of 80 is achieved only by 5 websites. Furthermore, 68 websites (8.99%) have a score of 45 to 64, which corresponds to grades C-, C, and C+ (Figure 1). Moreover, 59 websites are using HTTP only.

4.2 HTTP Security Headers Analysis

The current version of Mozilla Observatory provides 10 different security measures per website. Figure 2 gives a heatmap with the distribution of the average score between the categories of the website and the security measures.



	Content Security Policy	Cookies	Cross-origin Resource Sharing	HTTP Strict Transport Security	Redirection	Referrer Policy	Subresource Integrity	X-Content-Type-Options	X-Frame-Options	X-XSS-Protection
Municipalities and centers for regional development	-24.78	-4.33	0.00	-18.67	-3.94	0.06	-12.61	-4.28	-18.67	0.00
High schools	-24.93	-2.79	0.00	-18.86	-7.50	0.00	-8.29	-4.57	-19.14	0.00
Higher Educational Institutions and Educational Research Institutes	-24.67	-4.51	0.00	-12.20	-4.62	0.05	-7.25	-2.64	-13.57	-0.05
Judicial Authorities	-24.38	-1.88	0.00	-20.00	-17.50	0.63	-8.13	-5.00	-12.50	-0.63
Public Enterprises	-25.00	-7.81	0.00	-18.63	-7.38	0.19	-6.06	-4.75	-18.00	-0.06
Public Institutions	-24.81	-7.12	-0.38	-19.38	-8.85	0.19	-7.50	-4.50	-18.92	0.00
Government bodies and institutions	-24.61	-10.67	0.00	-17.81	-6.52	0.62	-10.84	-3.65	-14.10	-0.06
News and Media	-24.77	-3.38	0.00	-17.08	-2.46	0.54	-22.85	-3.69	-14.77	0.00
Classifieds and E-Commerce	-25.00	-18.08	-3.85	-13.85	-4.23	0.00	-3.46	-3.08	-15.38	0.00
Sport	-24.71	-6.18	0.00	-18.82	-3.24	0.88	-27.35	-3.82	-14.12	0.00
Entertainment and Lifestyle	-24.59	-12.35	-1.02	-17.04	-5.71	0.61	-22.45	-3.98	-14.69	0.00
Business, Finance, and Economy	-23.68	-11.91	0.00	-15.00	-4.56	1.18	-7.35	-3.09	-11.76	-0.15
Technology and Innovation	-24.75	-12.50	0.00	-16.50	-4.25	1.00	-17.50	-3.25	-12.75	0.00

Figure 2. Heatmap with distribution of average score between website categories and security measures

Content Security Policy. This header allows control of the resources that the user agent is allowed to load for a given page from external sources. If it is properly configured, it improves website's security mainly against the XSS attacks, but also against the clickjacking, data injection, and MITM attacks. Many different directives are available for it, such as *frame-ancestors* (which specifies valid parents that can embed a page using <frame>, <iframe>, <object>, or <embed>); *image-src*, *media-src*, *script-src*, *frame-src*, *default-src*, *style-src*, *object-src*, etc.

This security measure has six security modifiers: 10 for CSP with *default-src* 'none' and without 'unsafe-inline' or 'unsafe-eval'; 5 for CSP without 'unsafe-inline' or 'unsafe-eval'; 0 for CSP with unsafe values inside *style-src*; -10 for CSP implemented but allows 'unsafe-eval' or resources loaded over HTTP; -20 for CSP implemented but unsafely or resources loaded over HTTP; and -25 for CSP not implemented or invalid header.

Table 2. Distribution of security modifiers for CSP between Macedonian websites

Category	10, 5, 0, -10	-20	-25
Municipalities and Centers for Regional Development	0	4	86
High Schools	0	1	69
HEIs and Educational Research Institutes	0	6	85
Judicial Authorities	0	1	7
Public Enterprises	0	0	80
Public Institutions	0	5	125
Government Bodies and Institutions	0	7	82
News and Media	0	3	62
Classifieds and E-Commerce	0	0	13
Sport	0	1	16
Entertainment and Lifestyle	0	4	45
Business, Finance and Economy	0	9	25
Technology and Innovation	0	1	19
Total (%)	0 (0%)	42 (5.56%)	714 (94.44%)

This security measure is the least implemented measure on Macedonian websites. Only the two worst security modifiers appear in the scan results (Table 2). We have 94.44% (n=714) websites with CSP not implemented or invalid header (value -25) and the rest (n=42) with CSP implemented but unsafely or resources loaded over HTTP (value -20).

Cookies. Cookies are small pieces of data (cookie name and value) used by the web servers to provide session management, to track user's actions, to personalize user's experience, etc. They are set in the user agents (e.g., browsers) by deploying the Set-Cookie header in the HTTP response, and the user agents can send them back to the server later. Several attributes can be set in this header that influence website security, such as *Secure*, which tells browsers to send cookies to the server only when HTTPS is used; *HttpOnly* to prevent JavaScript from accessing the cookies and to stop some XSS attacks; *Expires* and *Max-Age* to provide expiration time for cookies; *SameSite* to control the sending of the cookie with cross-site requests, which provide some protection against CSRF attacks; etc.

Cookies as a security measure have 7 different security modifiers: 5 when *Secure*, *HttpOnly* and *SameSite* are configured properly; 0 for no cookies detected or *Secure* and *HttpOnly* are properly configured; -5 for cookies without *Secure* flag, but transmission over HTTP is prevented by HSTS; -10 for session cookies without *Secure* flag, but transmission over HTTP is prevented by HSTS; -20 for anti-CSRF tokens set withut *SameSite* flag, or cookies set without *Secure* or set over HTTP or cookies use *SameSite* flag, but set to something other than *Strict* or *Lax*; -30 for session cookies without *HttpOnly* flag; and -40 for session cookies without *Secure* flag or set over HTTP.

Only 4.50% (n=34) of the Macedonian websites have properly configured attributes *Secure*, *HttpOnly*, and *SameSite* and have received the highest score for this security measure. Most of the websites (n=537, 71.03%) have received 0, and 12.83% (n=97) have received the worst score of -40 (Table 3). The worst categories for this security measure are *Classifieds and E-Commerce* and *Technology and Innovation*, while the best is *Judicial Authorities.*

Cross-Origin Resource Sharing. Cross-Origin Resource Sharing (CORS) header indicates any origins (identified by domain, scheme, or port) other than its own, from which a browser should allow loading resources. It supports secure cross-origin requests and data transfers between browsers and servers by several mechanisms, such as, invocations of *fetch()* or *XMLHttpRequest*, Web Fonts, WebGL textures, CSS Shapes from images, etc. For that purpose, several options can be used, like *Access-Control-Allow-Origin* and *Access-Control-Allow-Methods.*

Three security modifiers are defined for this measure: 0 for public content visible via CORS *Access-Control-Allow-Origin*, or is restricted to specific domains, or CORS is not implemented; -20 when crossdomain.xml or clientaccesspolicy.xml cannot be parsed; and -50 for content visible via CORS file or headers.

Table 3. Distribution of security modifiers for Cookies between Macedonian websites

Category	5	0	-5	-10	-20	-30	-40
Municipalities and Centers for Regional Development	1	76	1	0	4	1	7
High Schools	1	63	0	0	2	0	4
HEIs and Educational Research Institutes	5	60	15	0	4	0	7
Judicial Authorities	1	6	0	0	1	0	0
Public Enterprises	2	59	1	0	4	1	13
Public Institutions	7	91	2	0	10	5	15
Government Bodies and Institutions	10	49	0	1	7	3	19
News and Media	0	58	0	0	2	2	3
Classifieds and E-Commerce	0	3	1	0	5	3	1
Sport	1	13	0	0	0	1	2
Entertainment and Lifestyle	1	30	0	0	4	3	11
Business, Finance and Economy	3	18	2	0	1	1	9
Technology and Innovation	2	11	0	0	1	0	6
Total (%)	34 (4.50%)	537 (71.03%)	22 (2.91%)	1 (0.13%)	45 (5.95%)	20 (2.65%)	97 (12.83%)

Macedonian websites perform well for this security measure. Only 3 websites have visible content via the CORS file or headers (-50), and all the others obtained the score 0, which is the maximum score for CORS.

Redirection. The default HTTP port is 80 on the server side (when someone tries to connect to the web server using the URI that starts with http://), and traffic on this port is not encrypted. For better security, the recommendation is to use HTTP over SSL/TLS – HTTPS (encrypted and authenticated traffic with provided integrity) on port 443, and this is the case when someone tries to connect to the URI of the website that starts with https://. Web servers usually listen on both ports (so that users do not get connection errors when typing http://), and they need to be configured to redirect HTTP traffic to the same resource on HTTPS.

HTTP has a special kind of response, called an HTTP redirect, to trigger redirection. These responses have status codes that start with 3, and a Location header that contains the targeted URL for redirection.

When browsers receive a redirect response, they immediately load this targeted URL. The cost for redirection is only a small performance hit of an additional round-trip, which is rarely noticed by the users.

Four security modifiers are defined for this score (-5 when initial redirection to an HTTPS is to a different host, preventing HSTS; -10 for initial redirection to an HTTP URL, but finally – to HTTPS; -20 for no redirection to HTTPS or invalid certificates during redirection; and 0 for proper configuration).

Table 4. Distribution of security modifiers for Redirection between Macedonian websites

Category	0	-5	-10	-20
Municipalities and Centers for Regional Development	64	11	0	15
High Schools	43	1	0	26
HEIs and Educational Research Institutes	65	6	1	19
Judicial Authorities	1	0	0	7
Public Enterprises	47	4	1	28
Public Institutions	67	6	2	55
Government Bodies and Institutions	51	8	6	24
News and Media	54	4	0	7
Classifieds and E-Commerce	9	1	1	2
Sport	12	3	0	2
Entertainment and Lifestyle	29	6	3	11
Business, Finance and Economy	21	7	0	6
Technology and Innovation	13	3	1	3
Total (%)	476 (62.96%)	60 (7.94%)	15 (1.98%)	205 (27.12%)

The distribution of security modifiers between Macedonian websites is given in Table 4. Although 62.96% (n = 476) of the websites scored zero (Table 4), which is good, all Macedonian website categories have an average negative score for this security measure. The worst category for this security measure is *Judicial Authorities* with an average score of -17.14, while the best is *News and Media* (-2.46).

HTTP Strict Transport Security. This HTTP header, if properly configured, informs the browser to connect to the website only using HTTPS and protects users from having their connection with the web server downgraded to the HTTP version. The header includes an option *max_age* that sets the expiration time of this header to a number of seconds, after which time the browser will be able to connect over HTTP again. Also, there are two optional directives: *preload* (which tells browser developers that the domain is allowed to be preloaded as an HSTS site) and *includeSubDomains* (which tells the browser to enforce HTTPS usage on the main domain and all its subdomains).

Four security modifiers are also defined for this score (5 when *preload* is set; 0 for *max_age* set to at least 6 months; -10 for *max_age* set to less than 6 months; and -20 for HSTS not implemented or invalid certificates or without HTTPS).

Table 5. Distribution of security modifiers for HSTS between Macedonian websites

Category	5	0	-10	-20
Municipalities and Centers for Regional Development	0	5	2	83
High Schools	0	4	0	66
HEIs and Educational Research Institutes	0	35	0	55
Judicial Authorities	0	0	0	8
Public Enterprises	0	4	3	73
Public Institutions	0	4	0	126
Government Bodies and Institutions	1	8	1	79
News and Media	0	8	3	54
Classifieds and E-Commerce	0	4	0	9
Sport	0	1	0	16
Entertainment and Lifestyle	1	6	0	42
Business, Finance and Economy	0	8	1	25
Technology and Innovation	0	3	1	16
Total (%)	2 (0.26%)	90 (11.90%)	12 (1.59%)	652 (86.24%)

Only 2 websites obtained the highest security modifier for this header, while 86.24% (n = 652) have the lowest value (Table 5). The worst categories for this security measure are *Judicial Authorities* and *Public Institutions*, while the best are *HEIs and Educational Research Institutes* and *Classifieds and E-Commerce.*

Referrer Policy. This header tells the browser what to include in the Referrer header (origin, path, and/or query string) when making requests. Usually, the Referrer header includes the URL of the page the user came from. There are several options for this header: *no-referrer* for omitted Referrer header; *same-origin* for sending the origin, path, and query string for same-origin requests; *no-referrer-when-downgrade*, *origin*, *origin-when-cross-origin*, *unsafe-url*, etc.

The best security modifier is 5, used when the Referrer Policy is set to *no-referrer*, *same-origin*, *strict-origin*, or *strict-origin-when-cross-origin.* When the Referrer Policy is set to *no-referrer-when-downgrade* or is not implemented, the security modifier is 0; and -5 is when the Referrer Policy is unsafely set or the header is invalid.

The Referrer Policy is the only security measure for which all categories have a zero or positive average score. Only 1.06% (n=8) of websites received the worst score of -5, while 7.67% (n=58) received the best score of 5 (Table 6), and all others received 0. The highest average score is obtained by the categories *Business, Finance, and Economy* and *Technology and Innovation.*

Subresource Integrity. When a website uses external JavaScript code, the web administrator can first verify its content and then calculate its hash result and insert it in the HTML code. Subresource Integrity (SRI) is not a header, but a feature that specifies a base64-encoded cryptographic hash of a specific resource, placed in the value of the *integrity* attribute of a <script> or a <link> element. It allows browsers to recalculate the hash result of the specific script and compare it with what is in the HTML code. If the hash results are the same, the script will run; otherwise, no.

Five security modifiers are defined for this score (5 when SRI is implemented and all scripts are loaded from a similar origin or securely; 0 for SRI not implemented but scripts are loaded from a similar origin; -5 for SRI not implemented but external scripts are loaded over HTTPS or site did not return 200; -20 when SRI is implemented but external scripts are loaded over HTTP or HTML can not be parsed; and -50 for

Table 6. Distribution of security modifiers for Referrer Policy between Macedonian websites

Category	5	0	-5
Municipalities and Centers for Regional Development	2	87	1
High Schools	1	68	1
HEIs and Educational Research Institutes	4	84	3
Judicial Authorities	1	7	0
Public Enterprises	4	75	1
Public Institutions	5	125	0
Government Bodies and Institutions	11	78	0
News and Media	9	54	2
Classifieds and E-Commerce	0	13	0
Sport	3	14	0
Entertainment and Lifestyle	6	43	0
Business, Finance and Economy	8	26	0
Technology and Innovation	4	16	0
Total (%)	58 (7.67%)	690 (91.27%)	8 (1.06%)

SRI not implemented and external scripts are not loaded over HTTPS).

The worst categories for this security measure are *Sport*, *News and Media*, and *Entertainment and Lifestyle*, while the best is *Classifieds and E-Commerce*. Only 3 websites obtained the highest security modifier, while 19.05% (n = 144) have the value -50 and 36.38% (n = 275) have the value -5 (Table 7).

X-Content-Type-Options. Usually, a website has several resources that need to be requested by the browser and loaded into it when the website is open. So, the browser needs to know what to do with a resource (display it as an image, run it as a script, play the video, etc.), and for that purpose, it relies on MIME types (Multipurpose Internet Mail Extensions) sent with the file from the web server as Content-Type. The browser has to figure out how to use the file correctly when this MIME type is not configured correctly or is not present, which, on the other hand, can introduce some security issues.

Table 7. Distribution of security modifiers for Subresource Integrity between Macedonian websites

Category	5	0	-5	-20	-50
Municipalities and Centers for Regional Development	0	34	37	0	19
High Schools	0	44	16	0	10
HEIs and Educational Research Institutes	0	49	32	0	10
Judicial Authorities	0	4	3	0	1
Public Enterprises	1	44	28	0	7
Public Institutions	1	77	36	0	16
Government Bodies and Institutions	1	38	34	0	16
News and Media	0	11	27	0	27
Classifieds and E-Commerce	0	4	9	0	0
Sport	0	5	3	0	9
Entertainment and Lifestyle	0	9	20	0	20
Business, Finance and Economy	0	11	20	0	3
Technology and Innovation	0	4	10	0	6
Total (%)	3 (0.40%)	334 (44.18%)	275 (36.38%)	0 (0%)	144 (19.05%)

So, the X-Content-Type-Options header indicates that the MIME types advertised in the Content-Type headers should be followed and not be changed. This is done to avoid MIME type sniffing by saying that the MIME types are deliberately configured. There is only one option *nosniff*, and when it is set, the browser should follow the content type set by the web server and not change that or try to guess if it is missing. Only 2 security modifiers are defined for this security metric (0 if *nosniff* is set, and -5 if the header is not implemented or it is invalid).

Only about a fifth of all websites (n=159; 21.03%) have properly set *nosniff* in the X-Content-Type-Options header. The worst categories for this security measure are *Judicial Authorities*, *Public Enterprises*, and *High schools*, while the best is *HEIs and Educational Research Institutes*.

X-Frame-Options. The main purpose of this header is to improve the security of the website against clickjacking. It indicates whether a browser should be allowed to render a page in a <frame>, <iframe>, <embed>, or <object> elements, which is usually content from remote sources. It has two options: *DENY*, which completely denies the content rendered within a frame, regardless of the site attempting to do so, and *SAMEORIGIN*, which only allows the content if all ancestor frames are of the same origin as the page itself. This header can be skipped if the CSP *frame-ancestors* directive is used, and this corresponds to the first security modifier with value 5. There are 2 additional security modifiers: the header is implemented (0) and not implemented at all, or it is invalid (-20).

Only seven websites obtained the highest security modifier for this security measure, while 81.48% (n = 616) have not implemented any protection against clickjacking through this header or CSP header. The best category here is *Business, Finance, and Economy* (where 38.24% of websites have implemented protection against clickjacking), while the worst are *High schools*, *Public Institutions*, *Municipalities and Centers for Regional Development*, and *Public Enterprises*, with 95.71%, 94.62%, 93.33%, and 90.00% of websites without implemented security header for clickjacking, respectively.

X-XSS-Protection. This header is a non-standard feature of some browsers (Internet Explorer, Chrome, and Safari) that stopped pages from loading when reflected cross-site scripting (XSS) attacks were detected. This is unnecessary if a strong CSP is implemented. Novel suggestions are not to use this feature on production websites, so, we excluded the discussion for it.

4.3 Discussion

Generally, all categories of Macedonian websites have underestimated the importance of the implemented and properly configured HTTP security headers for website security. We present our discussion according to the security measures with negative average scores for most of the categories:

- Content Security Policy – This is the most under-implemented security measure in Macedonian websites, despite widely recognized high-security benefits in the protection of the XSS, click-jacking, data injection, and MITM attacks. The average score for each category is negative and below -23. The protection is achieved by a combination of an allowlist of origins from which third-party content can be included, and disallowing potentially dangerous code such as eval, inline scripts, and event handlers by default. The deployment of CSP policies should be done, but very carefully, because in 2016, Weichselbaum, et al. [18] showed that while CSP deployment is increasing, the majority of policies used in practice are insecure. Also, according to [17], third parties that provide code are major roadblocks to this measure, because they can introduce new delegated hosts or similar, and most first parties are unable to outsource noncore business needs and deploy security mechanisms at the same time.

- Cookies – Proper configuration and protection of cookies is very important for security because with little effort, you achieve more resistance to XSS and CSRF attacks, session hijacking, and similar; while if you do not perform that, the website is quite insecure. Less than 5% of the Macedonian websites analyzed have properly configured this security measure, and more than 70% are at least not insecure about it. Still, it is quite a problem that sites that belong, for example, to E-Commerce, do not perform well here, taking into account that they work with payments.

- HTTP Strict Transport Security and Redirection – Proper implementation of HSTS (standardized in 2012 [8]) eliminates the vulnerability associated with unsecured HTTP connections, ensuring encryption of sensitive information during transfer. This highly beneficial security measure is under-implemented in all Macedonian website categories, which can be seen from the fact that, even if only 59 websites do not use HTTPS at all, the rest 593 out of 652 with the worst score of -20 do not implement HSTS or have invalid certificates. Even more, the implementation effort of HSTS is very low. In addition, even 221 websites that use HTTPS do not have properly implemented Redirection.

- Subresource Integrity – Chapuis, et al. [3] conducted a longitudinal analysis of SRI deployment in 3.5 years, starting from the first recommendation of its use in 2016. They observed an increasing deployment of SRI, but also that this is mostly related to widely-used libraries such as jQuery having example code with SRI. The Mozilla Observatory identified SRI as a measure with a medium benefit and a medium implementation difficulty. All Macedonian website categories have a negative average score for this security measure, with even 6 categories with an average below -10. Only 3 websites have properly implemented this, while 144 have the worst score of -50.

- X-Content-Type-Options – This low beneficial security measure, with low implementation effort, is under-implemented in 597 websites.

- X-Frame-Options – Clickjacking protection is commonly enforced via server-sent, yet client-side security mechanisms, like the X-Frame-Options and CSP headers. Even 81.48% (n = 616) of Macedonian websites fail this security measure, standardized in 2013 [14], which offers a high security benefit for a low implementation effort. One research [2] showed that even if these framing controls are well implemented because protection is delegated to web browsers, there are some inconsistencies in the security guarantees offered to users of different browsers.

We can compare our results with the results obtained by Kishani and Das [11] in 2023, because they performed a similar analysis using the Mozilla Observatory tool, with a list of the 10.000 most popular websites from Tranco's list [8]. Comparison can be done only for some of the categories (Table 8). Their category *Law and Government* covers three categories in our classification: *Municipalities and Centers for Regional Development*, *Judicial Authorities* and *Government Bodies and Institutions.* It can be seen that all of our three categories are one grade below the grade in *Law and Government*, and while its average score is 35.67, the average score for the three Macedonian categories

[8] `https://tranco-list.eu/list/3VJNL/full`

is below 20. Taking into account the importance of these categories of websites, it is clear that their security needs to be greatly improved.

Table 8. Comparison of the results for some Macedonian websites with those from [11]

Category	Average score (MK)	Average score [11]	Average grade (MK)	Average grade [11]
Municipalities and Centers for Regional Development	19.94	35.67	F	D
High Schools	18.21	23.78	F	F
HEIs and Educational Research Institutes	35.55	23.78 24.89	D	F D-
Judicial Authorities	16.88	35.67	F	D
Government Bodies and Institutions	19.89	35.67	F	D
News and Media	19.46	20.21	F	F
Classifieds and E-Commerce	19.23	27.64	F	D-
Sport	14.12	20.13	F	F
Business, Finance and Economy	29.41	32.30 28.42	D-	D D-
Technology and Innovation	19.75	31.97 27.87	F	D D-

The category *Jobs and Education* partially covers our categories *High Schools* and *HEIs and Educational Research Institutes*, but also *HEIs and Educational Research Institutes* is covered by *Science.* Whereas our category *High Schools* has the same grade and a lower average score than *Jobs and Education*, our category *HEIs and Educational Research Institutes* performs much better than both categories of [11]. Categories *Sport* and *News and Media* have the same average grade and a lower average score than their counterparts *Sport* and *News.* Macedonian category *Business, Finance, and Economy* is covered by two categories in [11] – *Finance* and *Business & Industrial*, with the category *Finance* outperforming our category for half a grade. *Technology and Innovation* is covered by two categories: *Computers & Electronics* and *Internet & Telecom*, both of which outperform our websites in average score and grade. *Classifieds and E-Commerce* can be compared with *Shopping*, and it demonstrates a lower average grade and score.

Entertainment and Lifestyle is difficult to compare, because several categories correspond to it, such as *Games* (26.46, D-), *Hobbies & Leisure* (26.67, D-), *Beauty & Fitness* (29.21, D-), *Travel & Transportation* (29.49, D-), and *Arts & Entertainment* (19.94, F), all with a much better average score. In addition, we cannot compare the last two categories: *Public Enterprises* and *Public Institutions*.

If we try to locate the root causes for the bad performance of Macedonian websites, we can identify several reasons. Most Macedonian information holders do not have enough cybersecurity awareness, funds, and people to improve their websites, infrastructure, and information systems. In addition, the proposal for the legislation on network and information security has been in development for several years and is still in a draft version. This law proposal will enforce better cybersecurity in most information holders.

5 Conclusion

We hope that the analysis we performed will help raise awareness of better security in Macedonian websites. The proper implementation of HTTP security headers is only one part of their overall security. More security properties can be evaluated for Macedonian websites, such as the proper implementation of the TLS protocol and its cipher-suites, correctly performed logouts, etc. Additionally, Mozilla Observatory is only one tool, so cross-checking with additional security analysis tools can be performed for future work.

Starting from 31 October 2024, a new version of HTTP Observatory was launched, with the same security measures, except now the obsolete X-XSS-Protection and some changed security modifiers per measure [9]. It would be good to redo the analysis for the same set, and even more categories of Macedonian websites, together with the health sector, in one year at least, to see if something has changed.

[9] `https://developer.mozilla.org/en-US/observatory/docs/tests_and_scoring`

References

[1] 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.

[2] S. Calzavara, S. Roth, A. Rabitti, M. Backes, and B. Stock, “A tale of two headers: a formal analysis of inconsistent Click-Jacking protection on the web,” in *29th USENIX Security Symposium (USENIX Security 20)*, 2020, Article No. 39, pp. 683–697.

[3] B. Chapuis, O. Omolola, M. Cherubini, M. Humbert, and K. Huguenin, “An empirical study of the use of integrity verification mechanisms for web subresources,” in *Proceedings of The Web Conference 2020*, April 2020, pp. 34–45.

[4] H. Condei, “Introducing the MDN HTTP Observatory,” 2024. [Online]. Available: `https://developer.mozilla.org/en-US/blog/mdn-http-observatory-launch/#a_brief_history_of_the_mdn_http_observatory`. Accessed 02.09.2024.

[5] A. P. Felt, R. Barnes, A. King, C. Palmer, C. Bentzel, and P. Tabriz, “Measuring HTTPS adoption on the web,” in *26th USENIX security symposium (USENIX security 17)*, 2017, pp. 1323–1338.

[6] J. Fonseca, M. Vieira, and H. Madeira, “Evaluation of web security mechanisms using vulnerability & attack injection,” *IEEE Transactions on Dependable and Secure Computing*, vol. 11, no. 5, pp. 440–453, 2013.

[7] “List of information holders,” Agency for protection of the right to free access to public information. 2024. [Online]. Available: `https://aspi.mk/en/list-of-information-holders/`, Accessed 02.03.2024.

[8] J. Hodges, C. Jackson, and A. Barth, “Http strict transport security (hsts),” Request for Comments: 6797, Internet Engineering

Task Force (IETF), 2012. [Online]. `https://www.rfc-editor.org/rfc/pdfrfc/rfc6797.txt.pdf`, Accessed 02.03.2024.

[9] L. Jiang, H. Chen, F. Deng, and Q. Zhong, "A Security Evaluation Method Based on Threat Classification for Web Service," *J. Softw.*, vol. 6, no. 4, pp. 595–603, 2011.

[10] A. King, Mozilla observatory, 2016. [Online]. `https://github.com/mozilla/http-observatory-website/`, Accessed 02.03.2024.

[11] U. Kishnani and S. Das, "Securing the Web: Analysis of HTTP Security Headers in Popular Global Websites," *arXiv preprint*, arXiv:2410.14924. [Online]. `https://arxiv.org/abs/2410.14924`, Accessed 02.12.2024.

[12] A. Lavrenovs and F. J. R. Melón, "HTTP security headers analysis of top one million websites," in *2018 10th International Conference on Cyber Conflict (CyCon)*, (Tallinn, Estonia), May 2018, IEEE, pp. 345–370.

[13] Mozilla, "HTTP Observatory," Mozilla observatory website, 2016. [Online]. `https://observatory.mozilla.org/`, Accessed 02.03.2024.

[14] D. Ross and T. Gondrom, "Http header field x-frame-options," Request for Comments: 7034, Internet Engineering Task Force (IETF), 2013. [Online]. `https://www.rfc-editor.org/rfc/pdfrfc/rfc7034.txt.pdf`, Accessed 02.03.2024.

[15] H.Z. Shi, B. Chen, and L. Yu, "Analysis of web security comprehensive evaluation tools," in *2010 Second International Conference on Networks Security, Wireless Communications and Trusted Computing*, (Wuhan, China), vol. 1, IEEE, April 2010, pp. 285–289.

[16] S. Stamm, B. Sterne, and G. Markham, "Reining in the web with content security policy," in *Proceedings of the 19th international conference on World wide web*, April 2010, pp. 921–930.

[17] M. Steffens, M. Musch, M. Johns, and B. Stock, "Who's hosting the block party? Studying Third-Party Blockage of CSP and SRI," in *Network and Distributed Systems Security (NDSS) Symposium*, 2021. DOI: 10.14722/ndss.2021.24028.

[18] L. Weichselbaum, M. Spagnuolo, S. Lekies, and A. Janc, "CSP is Dead, Long Live CSP! On the Insecurity of Whitelists and the Future of Content Security Policy," in *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*, October 2016, pp. 1376–1387.

[19] I. Cernica, N. Popescu, and B. ţigănoaia, "Security evaluation of wordpress backup plugins," in *2019 22nd International Conference on Control Systems and Computer Science (CSCS)*, (Bucharest, Romania), May 2019, IEEE, pp. 312–316. DOI: 10.1109/CSCS.2019.00056.

[20] M. S. Al-Sanea and A. A. Al-Daraiseh, "Security evaluation of Saudi Arabia's websites using open source tools," in *2015 First International Conference on Anti-Cybercrime (ICACC)*, (Riyadh, Saudi Arabia), IEEE, November 2015, pp. 1–5. DOI: 10.1109/Anti-Cybercrime.2015.7351928.

[21] A. Mendoza, P. Chinprutthiwong, and G. Gu, "Uncovering HTTP Header Inconsistencies and the Impact on Desktop/Mobile Websites," in *Proceedings of the 2018 World Wide Web Conference*, April 2018, pp. 247–256. DOI: https://doi.org/10.1145/3178876.3186091.

[22] J. Grossman, "WhiteHat Website Security Statistics Report," Founder and CTO, WhiteHat Security, 2007. Retrieved March 8, 2010, [Online]. Available: `http://hhs.janlo.nl/articles/Whitehatstat.pdf`.

[23] T. Beardsley, B. Rudis, T. Sellers, C. Barnard, and K. Lin, "2021 Industry Cyber-Exposure Report (ICER): Fortune 500," RAPID7. [Online]. `https://www.rapid7.com/research/report/2021-industry-cyber-exposure-report/`, Accessed 09.12.2024.

[24] O. M. Awoleye, B. Ojuloge, and M. O. Ilori, "Web application vulnerability assessment and policy direction towards a secure smart government," *Government Information Quarterly*, vol. 31, pp. S118–S125, 2014.

[25] J. J. Zhao and S. Y. Zhao, "Retail e-commerce security status among Fortune 500 corporations," *Journal of Education for Business*, vol. 87, no. 3, pp. 136–144, 2012. DOI: https://doi.org/10.1080/08832323.2011.582191.

Aleksandra Mileva, Dushan Bikov,
Bojana Tasheva, Aleksandra Brashnarova

Received December 10, 2024
Revised February 25, 2025
Accepted March 04, 2025

Aleksandra Mileva
ORCID: https://orcid.org/0000-0003-0706-6355
Goce Delcev University, Faculty of Computer Science
str. Krste Misirkov No. 10-A P.O box 201, Stip, 2000, Macedonia
E–mail: aleksandra.mileva@ugd.edu.mk

Dushan Bikov
ORCID: https://orcid.org/0000-0002-5145-5297
Goce Delcev University, Faculty of Computer Science
str. Krste Misirkov No. 10-A P.O box 201, Stip, 2000, Macedonia
E–mail: dusan.bikov@ugd.edu.mk

Bojana Tasheva
Goce Delcev University, Faculty of Computer Science
str. Krste Misirkov No. 10-A P.O box 201, Stip, 2000, Macedonia
E–mail: bojana.102558@student.ugd.edu.mk

Aleksandra Brashnarova
Goce Delcev University, Faculty of Computer Science
str. Krste Misirkov No. 10-A P.O box 201, Stip, 2000, Macedonia
E–mail: aleksandra.102553@student.ugd.edu.mk