DOI: https://doi.org/10.53052/9788367652124.03

Michaela BODINGEROVÁ[1], Vladimíra BIŇASOVÁ[2]

Supervisor: Patrik HRKÚT[3]

BADANIE MECHANIZMÓW OCHRONY UŻYTKOWNIKÓW W WYBRANYCH APLIKACJACH INTERNETOWYCH

Streszczenie: Głównym celem pracy było zbadanie czynników wpływających na bezpieczeństwo cyfrowe aplikacji internetowych. W artykule przedstawiono różne aspekty etycznego hakowania i bezpieczeństwa aplikacji internetowych. Na podstawie analizy wyników zaproponowano rozwiązania mające na celu poprawę bezpieczeństwa z perspektywy użytkownika.

Słowa kluczowe: cyberprzestrzeń, bezpieczeństwo cyfrowe, aplikacje internetowe

AN EXAMINATION OF USER SECURITY MECHANISMS IN SELECTED WEB APPLICATIONS

Summary: The purpose of this paper is to examine the factors that influence the digital security of web applications. The paper presents various aspects of ethical hacking and web application security. Based on the analysis of the results, solutions have been suggested to improve security from the user's perspective.

Keywords: cyberspace, digital security, web applications

1. Introduction

Information and communication technology is presently one of the industries experiencing the most rapid expansion. We rely heavily on information and communication technologies in our daily existence. Web applications not only enhance productivity but also substantially improve daily comfort. Although many of us spend the majority of our days connected to the Internet, whether for work or

[1] Ing., University of Žilina, Faculty of Mechanical Engineering, Department of Industrial Engineering, e-mail: bodingerova@fstroj.uniza.sk
[2] Ing., PhD., DiS., University of Žilina, Faculty of Mechanical Engineering, Department of Industrial Engineering, e-mail: vladimira.binasova@fstroj.uniza.sk
[3] doc. Ing., PhD., University of Žilina, Faculty of Management Science and Informatics, Department of Software Technologies, e-mail: patrik.hrkut@fri.uniza.sk.

recreation, few users are mindful of the dangers associated with web application usage. Cyberspace is an increasingly common target for attacks by various groups to gain competitive advantage, damage or acquire funds. As a result, more and more companies operating in the online space are seeking to protect their systems. One way to effectively prevent attacks in cyberspace is to use the services of ethical hackers to help expose weaknesses in web applications. The aim of the study is to conduct a baseline survey of the current state of security features in selected web shops and based on the results of the analysis, propose appropriate solutions to enhance security, especially from a user interface perspective.

2. CASE STUDY - Web applications

A web application is a computer program that uses web browsers and web technologies to perform tasks over the Internet. Web applications use a combination of server-side scripts to handle the storage and also retrieval of information. On the client side, they present information to users, which allows them to interact using online forms, shopping carts, or various content management systems. Similarly, web applications allow employees to share information or collaborate on joint projects and documents regardless of their location or the device on which they are viewed [1].

Web applications use the WWW service or the World Wide Web to function. The service was created between 1989 and 1990. At that time, Tim Berners Lee became a software engineer at CERNE (European Organization for Nuclear Research) in Switzerland, where scientists came from all over the world for research. It was there that Berners Lee noticed the difficulties they were having in sharing information; even then, millions of computers were connected via the rapidly developing internet. Berners Lee realized the potential of sharing information through an emerging technology called Hypertext. In 1989, Tim Berners Lee presented his vision in a paper entitled "Information management: A proposal". In September 1990, he started working with the NeXT computer, one of Steve Jobs' first products. In the same year, he created the three basic technologies that became the foundation of the web as we know it today [2].

These are HTML – the markup language for the web, URI – Uniform Resource Identifier a type of address that is unique and is used to identify each resource found on the web, and finally HTTP – Hyper Text Transfer Protocol, which allows you to retrieve linked resources from across the web. Originally, this service was intended to be used for easy exchange of documents and work results between CERNE staff. However, over time Tim and his colleagues realized the potential of the service and pushed for the underlying code to be made available free of charge. In 2014, celebrating the 25th anniversary of the site, two out of five people worldwide were already using the site. However, he himself has said that if the technology had only been under his supervision and control, it would probably never have taken on the proportions it has today because it is impossible to design something that is meant to be a universal space and still have complete control over the technology at the same time. We can therefore summarize that the root causes of the problems in the security

of current web applications as well as the web itself are rooted in this early stage of the web's development [2].

Principle of web applications – Different programming languages are used to create web applications, such as Java, JavaScript, PHP, Python, Ruby, C++, C# or Perl. Markup languages such as HTML can only be used to create documents, but we can use the aforementioned programming languages to create complex web applications that will perform the required functionality [3].

Most applications are dynamic and require this server-side processing. Those applications that are static, on the other hand, do not require any server-side processing. For a web application to run, it requires the web server to manage client requests and the application server to perform the required tasks or manage the database to store information (if required). Application server technologies include ASP.NET, for example, or the PHP [1].

A typical web application flow looks like a user launches a web server using the Internet, either through a web browser or by using the user interface of the application in question. The web server then sends this request to the application server and it performs the requested task, such as querying a database or processing data, then generates the results of the requested data [1].

The application server sends the results with the requested or processed data to the web server, which then responds to the client and the requested information is displayed to the user. Web applications run identically on multiple platforms regardless of operating system or device and are not installed on a personal computer's hard drive, eliminating space constraints for the user. Another advantage is the lower computer requirements of the end user [1].

Web application security – is the process of protecting websites and online services against a variety of security threats, which mainly exploit various vulnerabilities in the application code. The most common targets of web application attacks are content management systems such as WordPress and database management tools such as PhpMyAdmin. For attackers, web applications are priority targets because of the underlying complexity of the code. It is this that increases the likelihood of vulnerabilities and manipulation of malicious code, which is attractive to attackers because of the data they can obtain. With most attacks, automation is possible, and so an attacker can launch his attack against thousands or even tens of thousands of targets at once. This is why organizations need to secure their web applications against similar attacks to prevent information theft, damaged client relationships or even lawsuits [4].

Web application vulnerabilities are usually the result of inadequate protection of inputs/outputs that are used to manipulate source code or gain unauthorized access. Vulnerabilities allow the use of various forms of attacks [4].

Types of attacks – Cyberspace is a virtual environment that has no beginning and no end, knows no borders between states, and cannot be clearly determined how large it

is. Thus, it is currently the most effective and dangerous weapon in the hands of cyber criminals. Cybercrime is classified as a new type of criminal or criminal activity. It differs considerably from other types of criminal activity, primarily due to the possibilities of its dynamic development and instantaneous change [5].

Cybercrime – is typically manifested mainly through so-called cyber-attacks. There is no doubt that cybercrime is on the rise and is a global problem. Different statistics offer us different information on the damage caused by cybercrime. These are mainly primary damages, such as the malfunctioning of a computer system, the failure of infrastructure or of the services offered. And also secondary damages such as the recovery of systems, the rescue of data or the reconnection of end users. We will name some of the attacks that will be discussed in more detail in the next chapter. These include, for example, social engineering, Botnet, Malware, Phishing, Dos, DDos, DrRDoS [5].

Without information and communication technologies, life for our society has been not only unimaginable but also impossible for a few years now. This is evidenced by the consequences from the 2017 WannaCry ransomware attacks or the Petya malware, or the Petwrap mutation of this malware [5].

The attacks described are some of the most common attacks within cybercrime:

- Social Engineering (Sociotechnics).
- Botnet.
- Phishing.
- Ransomware.
- Dos, DDos, DrRDoS T.

3. Ethical hacking in practice

Both ethical hacking and unethical hacking involve the compromise of computer systems and are therefore equivalent. Nevertheless, their objectives, legal standing, and results are diametrically opposed [6].

Ethical Hacking:

- Ethical hacking is a legal practice authorized by the company or individual[1].
- Ethical hackers, also known as white-hat hackers, work on principles of ethical hacking.
- They hack systems to identify vulnerabilities and propose solutions to enhance security.
- Ethical hackers often work with different government agencies and big tech companies.
- They create firewalls and security protocols.
- Ethical hacking is performed to protect the system or websites from malicious hackers and viruses.

Unethical Hacking:

- Unethical hacking is an illegal practice and considered a crime.
- Unethical hackers, also known as black-hat hackers, do not work on principles of ethical hacking.
- They steal valuable information of companies and individuals for illegal activities.
- Unethical hackers try to access restricted networks through illegal practices and reduce the security of data.
- They work for themselves for personal gains.

An ethical or white hacker is one who uses his or her skills to enhance security and keep other attackers out of an organization's systems, servers, networks, or other software. Ethical or also "white" hacking is the process of penetrating a system or network to find vulnerabilities. These system vulnerabilities could be found by other attackers and subsequently exploited to steal data, causing significant damage to companies. The priority purpose of ethical hacking is to increase the level of security. Malware samples and vulnerabilities are many times removed directly during their testing. The tools and methods used by ordinary hackers are almost identical to those of ethical hackers. However, the difference is that ethical hackers work with the authorized permission of the specific entity being tested and follow all management rules as well as all laws pertaining to the field [7].

Ethical hackers adhere to three main principles that form the so-called CIA or AIC triangle from the English (Confidentiality, Integrity and Availability), which translates to confidentiality, integrity and availability. It is these principles that serve to increase the level of security of an organization [7].

According to Peter Chah, founder of DrPete Technology Experts, ethical hackers must have a great deal of skill and knowledge in the field of information and communication technology, especially knowledge of exploiting vulnerabilities that are present in a given system. There are several certifications required to pass a penetration test, such as the EC-Council Certified Ethical Hacker Certification, or CESG - Communication Electronics Security Group. There are also a number of courses that target beginners with no previous experience. Many of them can be found on popular portals like Udemy or Coursera. Although an ethical hacker does not need to follow a precise set of steps in penetration attacks, there is a list of five main testing steps namely reconnaissance, scanning, gaining access, maintaining access and covering your tracks [7].

Web application security is a vast area that would be beyond the scope of this paper to examine, just one sub-area has been chosen that is a significant part of today's world, namely e-commerce. Therefore, the next part of the article will be devoted to security features that can help protect eshops.

4. Online shops and their security

The cornerstone of every online store - eshop or any website is hosting, i.e., the virtual space on which the eshop is operated. When choosing hosting, it is important to choose a reliable provider that can protect the eshop from attacks from both internal and external infrastructure and will use up-to-date security measures. The next step is to choose a suitable system or platform for the online sale of products. There are a number of solutions on which an online store can be built. These include eCommerce platforms, CMS systems or custom-built solutions. Well-known eCommerce platforms include Shopify, PrestaShop or Magento. Content Management Systems (CMS) allow their users to build an online store on top of an existing CMS system, such as WordPress with the WooCommerce extension, quite easily by using various extensions (plugins) [8].

Custom-built solutions are often the costliest. It is not possible to clearly assess which of the mentioned solutions for online shops has the highest/lowest level of security, because it depends on many other factors (hosting, ssl certificate, system version, etc.). For example, according to experts, the Magento platform, which is also used by large corporations such as Nike, Coca-Cola, or Nestlé, is more secure than the WooCommerce system. New features are also constantly being added to these systems. However, with the arrival of new features, come new threats. Therefore, the next step when implementing new features is to think about their security level so that the security of the entire system is not compromised with the addition of a new feature. Such features are often the source of various security vulnerabilities and weaknesses through which the entire site can be hacked. Also, among the extensions, there are some that directly enhance the security of the online store [8].

Within WooCommerce, these are plugins such as SecuriSecurity or WordFence. Other basic protection features include Captcha, for example, but also more sophisticated solutions to protect against Dos and DDoS attacks. An essential part is the use of a WAF, i.e. a web application firewall, such as mod_security [8].

Integration of third-party services, such as payment gateway, which is nowadays an essential part of most e-shops, deserves separate attention. Its conscientious selection is in place, it should be localized into Slovak language and provide sufficient security for the customer. The recommended payment method is a payment gateway that processes customer data independently and offers only information about the transaction to the eshop founder. With this type of payment, the founder will to some extent transfer the legal responsibility for his customers' payment information to the payment gateway operator. This type of payment will also relieve the establishment from PCI DSS (Payment Card Industry, Data Security Standard) standards, which are time-consuming and costly [8].

Nowadays, it is also essential to offer encrypted connectivity. The key is an SSL certificate, which provides just such a connection for the user when they are on your site or store. The HTTP protocol is wrapped in SSL/TLS (HTTPS) security connections for the customer this protocol gives the impression of security and they

tend to trust such a secured eshop, and they also tend to come back to the eshop again [8].

Another very important point for owners of eshops or websites is backup, which is a recommended practice not only in the field of websites and e-commerce, but in general when working with the computer or the Internet and data. Backup is a fundamental pillar of security that offers the ability to return the system to its original state after a failure, hacker attack, or aggressive virus.

As part of a comprehensive analysis of WordPress and WooCommerce key points, several security issues were found. If we were looking at the core platform in WordPress, there are generally no significant security issues. The core of this system has undergone a long evolution and can therefore be considered relatively secure. One of the strengths of WordPress is the ease of updating and the short development cycle. A large part of the security problems arise due to the careless actions of end-users in choosing themes and plugins with unsafe codes, as well as the use of inappropriate or poorly secured hosting. According to the statistics on hacked websites, up to 41% of websites were hacked or attacked by vulnerabilities in the hosting account. Using a security issue in the WordPress theme that the website used, 29% were hacked. Due to a security issue in the WordPress add-ons that were used 22% were hacked and 8% of users were hacked due to the use of a weak password [9].

5. Security features of selected e-shops

In the following section, we will focus on some security features of selected e-shops. We will focus on the elements that can be examined without having access to the admin part of the eshop or access to the hosting itself. Based on this survey, we can quite quickly identify the basic level of security and appropriately specify the subsequent penetration testing, which is no longer part of the article. Performing a penetration attack or so-called bug bounty testing is a rather complex testing method, which unfortunately goes beyond the scope of this article. In fact, penetration testing cannot be performed without the official permission of the owner of the online store or website.

It is also not recommended to perform penetration testing in normal operation, because it can very easily lead to the disabling of services and thus the disabling of a particular e-shop. Within the scope of this paper, those elements that can be examined from the external environment have been examined in order to identify possible vulnerabilities of specific selected eshops.

For the article, eshops that offer similar services and goods - specifically fashion and accessories - were selected. In the table below we can see the tested entities (eshops) as well as the results of testing various security features, which we will describe in more detail in this section. All the tested e-shops are mainly aimed at female customers and offer goods from the fashion, beauty and accessories category.

Table 1. Security features of selected e-shops[Source: Authors]

URL address of the shop	Available admin URL	SSL	System and version	Simple password	Captcha
www.tusaoblaciem.sk	yes	yes	Wordpress 5.3.3	no	no
www.elishafox.sk	yes	yes	Wordpress 5.4.1.	no	no
www.imoda.sk	no	yes	Magento 1.9.3.4	no	no
www.leminimacaron.sk	yes	yes	Wordpress 5.0.9	no	no

Admin URL – the risk we will address is the login URL. For example, Wordpress uses www.nazovdomeny.sk/wp-admin.php or www.nazovdomeny.sk/wp-login.php for the admin login page. When using these well-known and publicly searchable login addresses, the risk of attack increases significantly. By modifying your login address to a unique form that only you will know, you will be more protected, or your eshop will be protected from one of the most common attacks, namely brute force attack. Such attacks involve "breaking" login credentials by randomly trying different combinations [10].

Of the four eshops audited, three eshops use Wordpress and one eshop uses Magento. Within the three mentioned e-shops, none had a customised URL. Even a normal user can therefore access the admin login form directly. For a skilled attacker, there are several ways to obtain the password. One of them, for example, is the aforementioned Phising, in which the attacker creates a form that is identical to the eshop's form and then tries to lure the user into filling in the details, for example by using email. If the user (administrator) fills out such a form or logs in through it, the attacker gains full control over the administration of the e-shop at that moment.

Brute force attack is an attempt to crack usernames and passwords through trial and error. This method is quite outdated, but given that most users still use overly simple passwords, this hacking method is quite effective and popular. Depending on the length and complexity of the password, it can take anywhere from a few seconds to years to crack. IBM reports that some hackers target the same systems every day, for months and sometimes even years. Hackers have even developed tools to simplify the attack, and these are dictionaries. Hackers go through these dictionaries and augment words with special characters and numbers, so the hacker chooses a target and executes possible passwords against a specific user account. This is why this attack is often referred to as a "dictionary attack" [11].

Protection against brute force attacks is provided, for example, by limiting the number of login attempts, called Password or Login Throttling. This method consists of counting the number of failed login attempts a user makes. When a user or attacker reaches a predetermined number of failed login attempts (for example, 5), we block the user from future login attempts for a certain amount of time (for example, 60 seconds) or we can block the user completely [12].

Protection against brute force attacks is provided, for example, by limiting the number of login attempts, called Password or Login Throttling. This method consists of counting the number of failed login attempts a user makes. When a user or attacker reaches a predetermined number of failed login attempts (for example, 5), we block the user from future login attempts for a certain amount of time (for example, 60 seconds) or we can block the user completely [12].

We can find out the login address of the administrator account quite easily by editing the URL. As we have already mentioned, for Wordpress this is a modification of the type www.nazoovdomeny.sk/wp-admin.php or www.nazovdomeny.sk/wp-login.php.

However, one of the tested e-shops does not use Wordpress, but Magento. Specifically, the e-shop www.imoda.sk. For this system the situation is different, because directly on the official website of the company they warn users or administrators to use a unique, i.e. their own admin URL. The company states that although using a unique URL alone will not directly protect your website from an attacker, it will at least reduce the chances of an attack. Further, the company describes how specifically it is possible to implement a custom admin URL into the Magento system, making it easier for users, or eshop administrators, to implement these changes [13].

For the last e-shop www.imoda.sk we were not able to access the address of the admin account in the above way, so we can assume that the e-shop is using the unique URL option, which is recommended directly by Magento.

SSL certificate – the second security element tested is the SSL certificate (from the English Secure Socket Layer). We detected the presence of SSL certificate in three of the four e-shops we focused on. This certificate is primarily used to secure data transmission and credit card transactions. The certificate encrypts the information, making it readable only by the party for whom it is intended. The absence of an SSL certificate on an e-shop can give the customer the impression of untrustworthiness [14].

We verified the presence of the certificate using the freely available SSL Server Test service at https://www.ssllabs.com/ssltest. This test showed that each of the mentioned e-shops has a valid SSL certificate, which we evaluate positively. The results of the tests can be seen in Appendix C to F.

System and version – the third security element is the system on which the e-shop runs, as well as its current version. As we described above, the importance of choosing and updating the system can be crucial in many cases in terms of security. This is the reason why we have focused our attention on finding out the specific system as well as updating it. Three of the four eshops we examined run on Wordpress, but only one of them, namely www.elishafox.sk, is using the latest version of Wordpress from April this year. Each updated version of Wordpress brings the latest features and better security options. Unupdated versions, bring with them the risk of weak security. On

the official site www.wordpress.org we also find a warning that no version other than the currently released version, labeled 5.4.1, is safe to use because only the latest version is actively maintained [15].

Eshop www.imoda.sk, which is the only one using Magento, also has an outdated version of this system. The current version of this system is 2.3.5 and offers performance improvements as well as security changes. Specifically, there are 180 functional fixes and more than 25 security enhancements, which again proves that you should always give preference to the current version whatever the system [13].

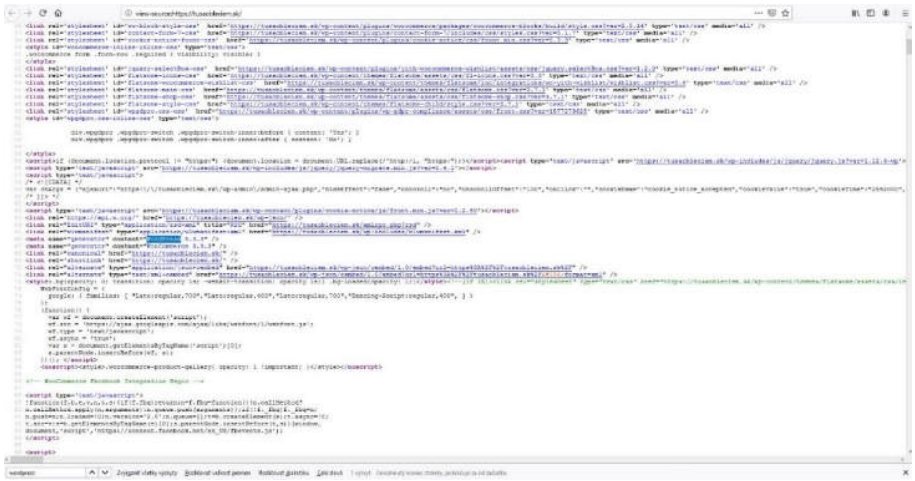

Figure 1. System and version of www-tusaobleciem.sk - source code - processed by [Source: Authors]

We can find out the system on which the e-shop is running, as well as the version of the system, by right-clicking on the selected e-shop and selecting the option "Show page source code". Then use the keyboard shortcut CTRL+F to find the text on the page. In this search box, type a keyword such as "Wordpress" or "version". In the source code, we will see the version currently in use, as well as the system on which the eshop is running. Another option is to use an online service to search for the system and version, such as www.magescan.com, which will display the details you are looking for when you enter the address of the selected eshop.

6. Conclusion

Web application security in cyberspace is becoming an important aspect, not only for large but also for small companies. The theoretical part of the study was devoted to the principles of web applications that allow communication, whether using online forms, shopping carts, or various content management systems.

The aim of the study was not only to analyze but also to summarize the aspects influencing the security of web applications with regard to ethical hacking and its use

in improving security. The theoretical part also summarized the knowledge in the field of ethical hacking and its contribution to the security of web applications. Another part of the study was to conduct a baseline survey of the current state of security features in the selected web stores. Based on the results of the analysis, practical recommendations for practice were then developed to enhance security from the user's perspective

In the practical part of the article, the security features of the selected online shops were analyzed, such as the presence and quality of the SSL certificate, the up to date of the operating system or the complexity of the password. Based on this analysis, it can be concluded that the overall security within the monitored elements is at a relatively good level, which also indicates the digital literacy of the operators or suppliers of system solutions of the tested eshops. However, there are other aspects of the digital security of web applications that would need to be examined (e.g. penetration testing) in order to declare the security of the selected eshops as sufficient.

ACKNOWLEADGMENT

This work was supported by VEGA 22/016/00 and KEGA 032ŽU-4/2021.

REFERENCES

1. GIBB Robert: What is a Web Application. In: *blog.stackpath.com* [online]. 2016 [cit. 2023-09-13]. Available at: *https://blog.stackpath.com/web-application/*
2. WORLD WIDE WEB FOUNDATION, ©2008-2020. History of the Web. In: *webfoundation.org* [online]. ©2008-2020 [cit. 2023-08-18]. Available at: *https://webfoundation.org/about/vision/history-of-the-web/*
3. IONOS, 2019. Web programming languages: the best languages for web development In: *ionos.com* [online]. 2019 [cit. 2023-09-25]. Available at: *https://www.ionos.com/digitalguide/websites/web-development/web-programming-languages/*
4. Imperva, © 2020. Web Application Security. In: *imperva.com* [online]. © 2020 [cit. 2023-09-18]. Available at: *https://www.imperva.com/learn/application-security/application-security/*
5. KOLOUCH Jan: *CyberCrime,*Praha: Edice CZ.NIC,2016. ISBN 978-80-88168-15-7.
6. GeeksforGeeks.org, 2022 Difference between hacking and ethical hacking [online]. 2022 [cit. 2023-11-27]. Available at: *https://www.geeksforgeeks.org/difference-between-hacking-and-ethical-hacking/* (accessed Nov. 27, 2023).
7. DANES Lucia: Co byste měli vědět o etickém hackování. In: *odstranitvirus.cz* [online]. 2019 [cit. 2023-09-28]. Available at: *https://odstranitvirus.cz/co-byste-meli-vedet-o-etickem-hackovani/*
8. HACKTROPHY: 20 steps how to improve the security of your e-shop. In: *hacktrophy* [online]. 2017 [cit. 2023-10-01]. Available at: *https://hacktrophy.com/en/20-steps-how-improve-eshop-security/*

9. PYLYPCHUK Ivan: WooCommerce: How Secure Is IT? [ANALYSIS]. In: *premmerce.com*[online]. 2018 [cit. 2023-09-27]. Available at: *https://premmerce.com/complete-woocommerce-security-review-issue-analysis/*
10. SINGER David: Securing Your CMS Admin Login. In: *liquidweb.com*[online]. 2016 [cit. 2023-09-27]. Available at: *https://www.liquidweb.com/kb/changing-your-cms-login-url/*
11. Kaspersky, © 2020. What's a Brute Force Attack? In: *kaspersky.com* [online]. © 2020 [cit. 2023-09-28]. Available at: *https://www.kaspersky.com/resource-center/definitions/brute-force-attack*
12. MIFTYISBORED: A Complete Tutorial on Login Throttling and reCAPTHA with Laravel 5.3. In : *miftysbored.com* [online].[bez dátumu] [cit 2023-09-22]. Available at: *http://miftyisbored.com/a-complete-tutorial-on-login-throttling-and-recaptha-with-laravel-5-3/*
13. Magento ©2020: Magento Commerce 2.3.5 Release Notes. In: *devdocs.magento.com* [online]. 2016 [cit. 2023-09-26]. Available at: *https://devdocs.magento.com/guides/v2.3/release-notes/release-notes-2-3-5-commerce.html*
14. RADIX: 4 Reasons Why An SSL Certificate Is Important For Your Company Website. In: *medium.com* [online]. 2018 [cit. 2023-09-26]. Available at: *https://medium.com/@RadixRegistry/4-reasons-why-an-ssl-certificate-is-important-for-your-company-website-de9527e8be5d*
15. WordPress.org: Releases. In: *wordpress.org* [online]. [bez dátumu] [cit. 2023-09-28]. Available at: *https://wordpress.org/download/releases/*