

Astana IT University

UDC 004.00/.00

**ANUAR MADIYEV
AYAN OSPANOV
ZHALGAS ZHUMANOV**

**Testing the resistance to cybersecurity attacks
of a travel agency website**

6B06301 — Cybersecurity

Diploma project

Supervisor:
Abdiraman A.
Master of Applied Mathematics
and Physics
Senior lecturer

Kazakhstan
Astana, 2024

CONTENTS

Abstract	3
Literature Review	4
Introduction	9
Methodology	16
Results	32
Conclusion	38
Bibliography	39
A first appendix	41

Abstract

Through the creation and comparison of two versions of a website one that is secure and one that isn't this paper provides a comprehensive analysis of website security and the need of having robust security mechanisms in place. The unsecured version demonstrates common vulnerabilities that include lack of data encryption, weak password storage, cross-site scripting (XSS), and cross-site request forgery (CSRF) vulnerabilities. Penetration testing using tools such as BurpSuite, HashCat, Hydra, and SQLMap revealed these security flaws. To address these vulnerabilities, various security measures were implemented in the secured version. These measures included `password_hash` for secure password storage, prepared statements to prevent SQL injection, `htmlspecialchars` for XSS protection, and a token-based system for CSRF defense. After these steps were taken, penetration testing proved that they worked to fix the problems that were found. Performance reviews and comments from users showed that the security measures did not have a big effect on how the website worked or how users felt about it. Educational components of the project also provided developers and website owners with in-depth explanations and practical guidance on how to raise awareness of security concerns and enhance their procedures. The outcomes demonstrate the need of using robust security measures to shield websites from typical assaults. We get helpful information from the findings that improves the internet. Constantly making security practices better protects against new threats and keeps website security and user trust at a high level.

Literature Review

Kala, E. M. (2023). The impact of cyber security on business: how to protect your business.

In (2023), Kala wrote a detailed guide on how to find out if a travel agency website is safe from hackers. This guide is still very useful today. He says that hacks are getting worse and happening more often, which is very bad for many places but especially for businesses. Everyday jobs that seem easy can go wrong, putting at risk things like power, transportation, and money. In this field that changes so quickly, Kala's study shows how important it is for businesses to know about online threats and have strong defenses in place. The point of his work is to make websites safer by teaching people how to avoid being hacked. For example, the websites for our tour service.

Elisa, N. (2020). Usability, accessibility and web security assessment of e-government websites in Tanzania.

Elisa's (2020) investigation into Tanzanian e-government websites' ease of use, accessibility, and digital security highlights travel-related website safety issues. Such infractions involved slow loading times, accessibility issues, including SQL injection and cross-site scripting. Considering the relevance of these discoveries, it is clear that comprehensive cyber security and web standards are necessary in order to protect online platforms from assaults. So Elisa's work is very important in this project, because it is similar to it. So we used this research in our paper.

Redmiles, E. M., Warford, N., Jayanti, A., Koneru, A., Kross, S., Morales, M., ... & Mazurek, M. L. (2020). A comprehensive quality evaluation of security and privacy advice on the web.

Redmiles et al. (2020) investigate the quality of security and privacy advice accessible on the internet, noting the difficulties consumers have in determining the efficacy and actionability of such advice. According to a large-scale investigation including 1586 users and 41 experts, the research indicates a "crisis of advice prioritization," in which an excess of information leads to misunderstanding about which activities are most important for users to execute. This research highlights the need for a more organized and prioritized strategy to communicating security information to end users.

Alghawazi, M., Alghazzawi, D., & Alarifi, S. (2022). Detection of sql injection attack using machine learning techniques: a systematic literature review .

Alghawazi, Alghazzawi, and Alarifi (2022) conducted a systematic study on SQL injection threat recognition using machine learning (ML). They stressed the importance of ML in cybersecurity. Their paper details many machine learning and deep learning models used to detect SQL injection vulnerabilities, demonstrating cyber security's growth. The evaluation emphasizes the need for artificial intelligence to adapt to cyber threats, especially in securing critical online services like travel agency websites. This research is essential for understanding how machine learning will combat one of the biggest cybersecurity threats.

Devi, R. S., & Kumar, M. M. (2020, June). Testing for security weakness of web applications using ethical hacking .

Devi and Kumar (2020) did a comprehensive investigation of web application vulnerabilities using ethical hacking and write about the results on this paper. Penetration testing is used to find holes in networks and web applications to harden them against cyberattacks. This text shows the subject like ethical hacking as a proactive cybersecurity measure. It shows many scanning methods and tools for efficient vulnerability assessment. In our travel agency website cybersecurity defenses are greatly advanced by this research and methods of defence stated in this paper. It shows practical ways to identify and mitigate security risks.

Subramanian, R. R., Avula, R., Surya, P. S., & Pranay, B. (2021, May). Modeling and predicting cyber hacking breaches.

In the work "Modeling and predicting cyber hacking breaches"(2021), Subramanian and co-authors use machine learning to predict cybersecurity violations of online travel agency services. The article describes a new algorithm that uses preliminary data and hacking trends to predict cyber risks in real time. They propose an aggressive defense system strategy that uses machine learning to enhance cybersecurity against complex threats. In the article, they were not used to identify threats, but it is clear that in the future they will be used for protection.

Samtani, S., Li, W., Benjamin, V., & Chen, H. (2021). Informing cyber threat intelligence through dark Web situational awareness: The AZSecure hacker assets portal.

Samtani, Lee, Benjamin, and Chen (2021) use the AZSecure hacker resource site to improve cyber threat intelligence (GTI) by providing dark web situational awareness. In this research authors of the paper shows how dark Internet data might influence cybersecurity methods and hackers' assets and intentions. Their research highlights the importance of using advanced CTI tools to predict and eliminate cyber threats, which is crucial for evaluating the cybersecurity measures of travel agency websites. Preventive measures and the study of current cyber attacks are a necessary step to prevent cyber attacks.

Erdődi, L., & Zennaro, F. M. (2022). The Agent Web Model: modeling web hacking for reinforcement learning.

Erdődi and Zennaro (2022) presented a model of a web agent specially designed to simulate hacking of websites through various tasks for a detailed study of the process in the context of enhanced education. Unique Model uses an innovative approach that shows the hacking and breaching process at various levels of abstraction, that really helps to understand complex and sophisticated cyber defense methods in a more understandable way. Also, the model, stimulating scenarios of the process of hacking web pages, offers useful and informative tips in improving cybersecurity for online platforms, such as the tour company that we took as the basis of our project to dismantle the process of finding vulnerabilities and their subsequent solution, because in such websites users enter and use important personal data. And this model demonstrates the big importance of balancing between practice and theoretical knowledge, which makes the model a great tool for academic and practical applications in the field of cybersecurity studies.

Periasamy, J. K., Dakiniswari, V., & Tapasya, K. (2022, March). AssessJet-Penetration testing and Vulnerability Assessment for Websites. In 2022 International Conference on Communication, Computing and Internet of Things (IC3IoT)

A 2022 academic study by Periasamy, Dakiniswari, and Tapasya called "AssessJet-Penetration Testing and Vulnerability Assessment for Websites" gives detailed basic information for checking the safety of websites and online apps. In this article, a complete study of numerous technologies that will be effective in detecting vulnerabilities in security systems is presented. This essay places a significant focus on the significance of penetration testing and vulnerability assessment in order to identify and absolutely reduce any potential dangers .As

well as giving useful information for making travel agency websites safer, this study also offers a methodical approach to safeguarding against different types of online cyber threats

Adha, M., KWA, Z. D., & Muhammad, A. H. (2023). WEBSITE SECURITY TEST AT THE UNIVERSITY OF MATARAM USING VULNERABILITY ASSESSMENT

Adha, Kwa, and Mohammed (2023) did a vulnerability check on Mataram University's website, emphasizing the importance of cybersecurity for education and research institutions. They used tools like Hosted Scan, a research tool, to find vulnerabilities and security holes that could threaten websites at all levels. This shows the need for regular checks to protect against attacks. Their research shows the importance of strong security measures for websites. We do the same thing when we build a website for a travel agency - we want to avoid, deal with, and prevent attacks to ensure smooth operations and user trust therefore this is an important part of running a successful business.

Hope, P., & Walther, B. (2008). Web security testing cookbook: systematic techniques to find problems fast.

In the world of cybersecurity, Hope and Walther (2008) work is a major breakthrough in understanding and fixing web application vulnerabilities. Their book named The Web Security Testing Cookbook, provides a systematic approach to identifying and fixing security holes in websites. Despite the year of release and the possible loss of relevance this book is crucial for the safety of travel agency websites. The authors in their book offers a variety of techniques and tools for security professionals to actively test websites and protect them from various of cyber attacks.

Priyawati, D., Rokhmah, S., & Utomo, I. C. (2022). Website vulnerability testing and analysis of website application using OWASP. International Journal of Computer and Information System (IJCIS), 3(3), 142-147.

Priyawati, Rokhmah, and Utomo (2022) dug into how to test website security with the OWASP method. They really showed how this approach can find and fix security issues, especially for travel agencies. Their study found many problems that could seriously mess up a travel agency's website. Because of these risks, they showed the need for constant and thorough security checks to keep cyber threats at bay. This research makes it clear why using trusted security testing methods is crucial to keeping travel agency websites safe.

Paraskevas, A. (2022). Cybersecurity in travel and tourism: a risk-based approach. In Handbook of e-Tourism

Paraskevas (2022) looks into a new way to handle cybersecurity in the travel and tourism industry. He points out the main weak spots and potential cyber threats. Making yourself able to understand and be prepared for these types of risks is very important. So he suggests a complete strategy that includes technology, people, and organizational methods as a combined idea. This is especially important for travel agency websites because they always deal with valuable customer data that need to be kept safe and sound and have complex systems like payment systems and backend. This particular study emphasizes the importance of keeping in mind to make regular risk assessments that will look for potential breaches in the system, proactive defenses to keep everything safe, and good response plans to be ready for something that possibly might happen. This way, travel agencies can stay one step forward of always evolving cyber threats.

Introduction

Relevance of Our Work.

Cybersecurity is very important because there are so many ticket companies and online businesses. Every day, they handle a lot of private individual info. Because of more digital activities, there are more data leaks and cyberattacks. It is important to protect user data.

Growing Threat Landscape.

More advanced hacks use flaws in websites to steal private information. People are interested in going after travel companies and online stores because they handle personal and financial information. Names, locations, credit card numbers, and trip plans are all included. Hacking this info can cost a lot of money and hurt your image. Cyberattacks are getting worse, which shows how important good protection is.

The University of Mataram's website has some security holes that hackers could use if the right security measures aren't in place (Adha, Zitnaa, & Muhammad, 2023). In this case, the problems that many websites around the world, including those in the travel and e-commerce industries, face are perfectly shown.

Importance of Data Confidentiality

Protecting the privacy of user info is a key part of building trust on the internet. People who use the site expect that their data will be kept safe. If you don't protect private data, you could face legal consequences, lose customers' trust, and damage your company's reputation. If a business doesn't follow data protection laws like the General Data Protection Regulation (GDPR) in Europe or the California Consumer Privacy Act (CCPA) in the US, they could be sued or have to pay fines.

Penetration testing can improve website security by identifying flaws before hackers can (Adha et al., 2023). Addressing these issues enhances user data security and system safety for enterprises.

Educational Value

Our work is useful for people who aren't ticket planners or online stores. Our protection methods can be used on any website, no matter what it's about. User info must be kept safe on a social network, a financial services site, or a healthcare portal. Our design makes websites safer and can be used by a wide range of businesses.

In addition to giving useful replies, our goal is to raise knowledge about cybersecurity. SMEs might not care about hacking because they think it is too hard and expensive. We want to get small and medium-sized businesses to put safety first by showing them effective and low-cost ways to do so.

Broad Applicability

Our work is important for more than just tour companies and online stores. The protection rules and methods we use can be used on any website, no matter what it's about. It's very important to keep user information safe on all kinds of websites, like social networks, banking services platforms, and healthcare sites. Our project creates a framework for making websites safer that can be used in many different types of businesses.

Impact on Cybersecurity Awareness

Our project's main goal is to make people more aware of how important hacking is, along with providing useful answers. Many small and medium-sized businesses (SMEs) don't bother with hacking because they think it's too hard and expensive. We hope that by showing that strong security measures can be put in place quickly and cheaply, more small businesses will decide to make hacking a priority.

We'll also talk about how online threats are changing. Businesses need to keep up with the latest security trends and technologies because hackers are always coming up with new ways to attack. Businesses can protect themselves from new threats by keeping up with these changes.

Future Directions

As time goes on, our work will become more important as the digital world changes. It will be even more important to have strong cybersecurity steps as

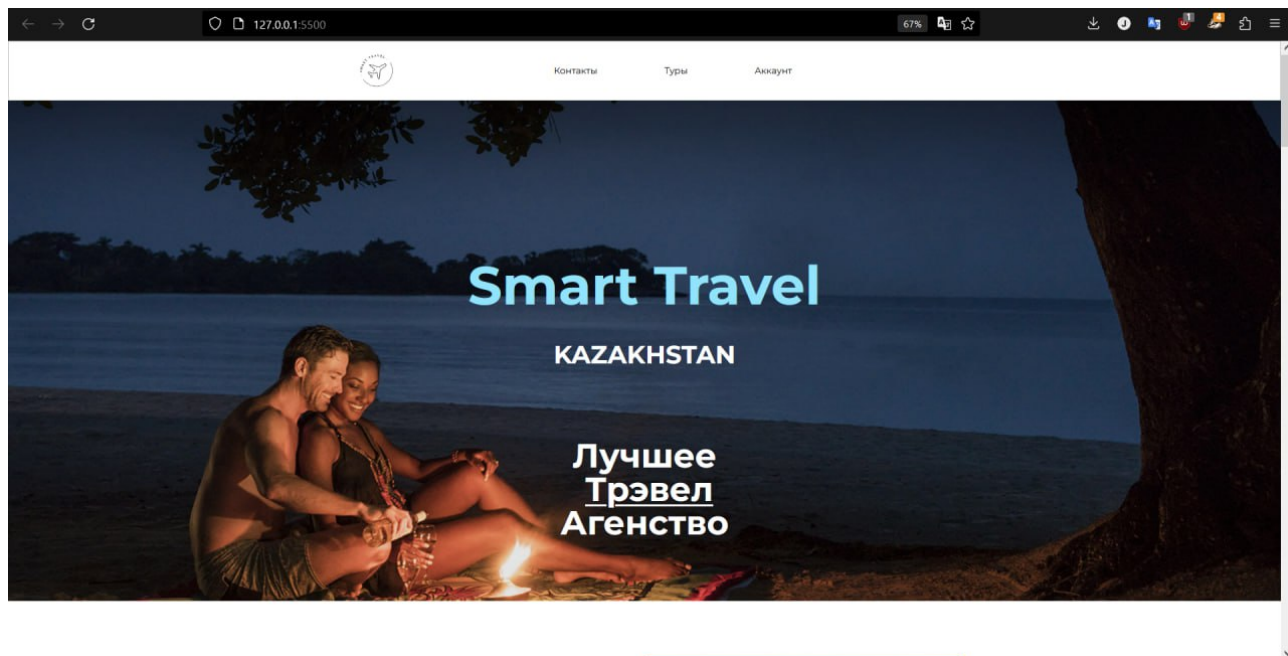
more businesses go online and more private data is stored online. Our project lays the groundwork for new technologies and methods that will help make website security better in the future.

This topic studied in [1–20].

Goal of the work.

Our major goal is to explain how to safeguard every component of a website after giving them a clear illustration of what an unprotected website looks like. We want to make this understandable and useful for those who aren't computer savvy as well.

We will begin with an insecure website first. This version will emphasize the typical flaws and security problems that a lot of websites encounter. We may more clearly demonstrate the hazards involved by demonstrating what occurs when security measures are not put in place. This will clarify to readers the need for security and the consequences of ignoring it.



We will next provide a thorough guide on website security. The fundamental security measures of employing strong passwords, routine software updates, and avoiding typical code errors that might result in vulnerabilities will be covered in this discussion along with other elements of website security (Redmiles et al., 2020). Creation of novel multi-layer encryption techniques is one of the main

components of our research. Conventional encryption often depends on a single layer that, in the event of a breach, makes all the data available. We greatly improve the security of the data by erecting more obstacles for any attackers by employing several layers of encryption. Finding the weakest areas on a website is an essential component of our job. We will use methods and technologies like penetration testing and vulnerability assessments. To find these flaws, assaults must be simulated, and the problems must then be fixed. Given that vulnerability assessments show exactly what has to be changed to stop data breaches and other security problems, they are crucial (Adha, Zitnaa, & Muhammad, 2023).

We will provide particular advice on how to safeguard every component of the website based on our results. These will be doable and useful suggestions meant to simplify the process by which website owners may put security measures into practice. By means of thorough quality assessments, such as those described by Redmiles et al. (2020), for example, we can guarantee that our recommendations are both understandable and practical. Our initiative involves teaching people how to secure their own websites in addition to securing one. We want to open cybersecurity to a wider audience by offering a detailed explanation and useful examples. Given the enormous volume of sometimes contradicting and confusing information accessible online, this is particularly crucial (Redmiles et al., 2020).

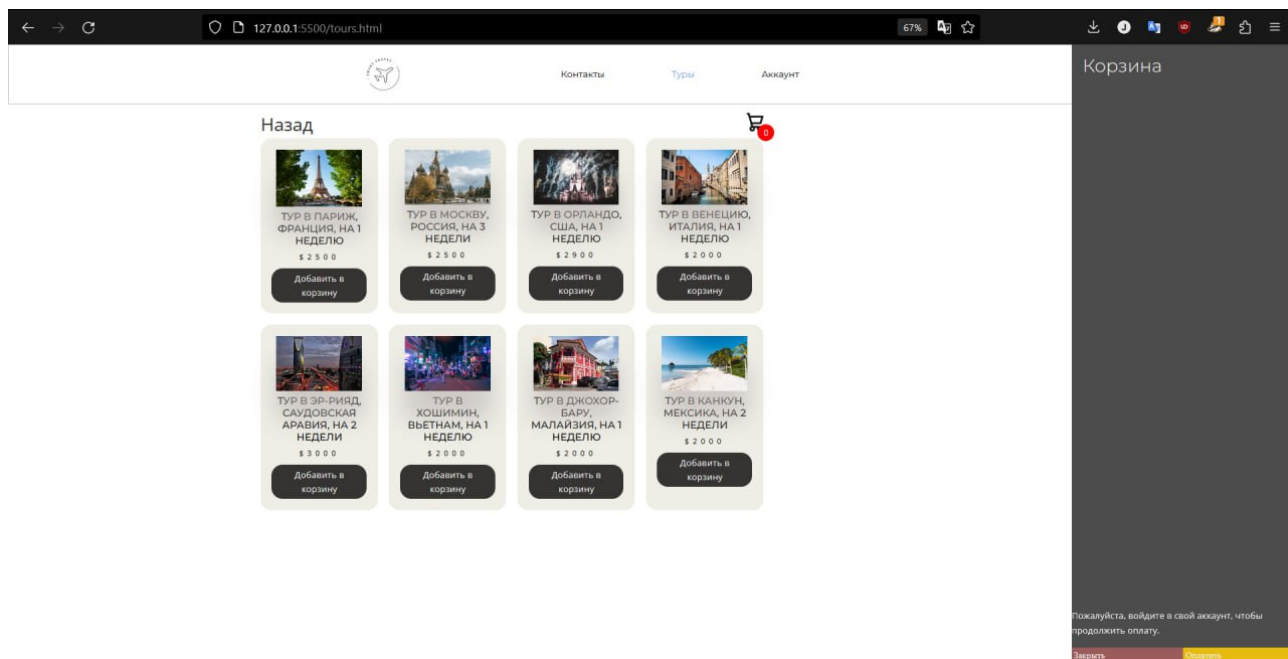
Every one of these security measures will be put into place and rigorously tested in our local development environment. By doing this, we guarantee that the guidance we provide is supported by tried-and-true techniques and real-world testing. Our goal is to provide people an all-inclusive, practical manual for website security. Part of our project is security education. Numerous sources, including friends, family, internet materials, and even fictional media, teach many users protective security techniques. The caliber of this guidance varies greatly, nevertheless (Redmiles et al., 2020). We want to raise the standard of security education accessible generally by offering concise, well investigated, and tried guidance.

To put it briefly, our work is to show the weaknesses of an unprotected website and provide a thorough instruction on how to safeguard it. We want to simplify and make website security obvious by means of real-world examples, novel multi-layer encryption techniques, and thorough explanations. We want to assist others in successfully protecting their online information by pointing out the most susceptible areas of a website and providing concise advice (Adha, Zitnaa, & Muhammad, 2023; Redmiles et al., 2020).

Research object.

We want to find out how effectively various cybersecurity measures protect websites from common attackers. Creating two websites one fully unsecured and one with robust security measures in place we want to provide a clear, practical example. This dual method will help us to identify and assess certain vulnerabilities as well as the consequences of different security solutions.

First of all, the unprotected website will act as a standard to show typical security flaws that many websites nowadays encounter. Among these problems might be the absence of secure communication protocols, insufficient input validation, and poor authentication systems. We can demonstrate the possible hazards and effects of inadequate security measures by presenting these weaknesses in a practical setting.



Creating and putting into use novel multi-layer encryption techniques is one of our main research interests. Conventional encryption techniques often depend on a single layer of encryption, which may reveal all encrypted data if it were hacked. We increase data security and lower the possibility of successful assaults by adding more obstacles that an attacker must get past by using many layers of encryption.

Assessments of vulnerabilities and penetration testing on both website versions will also be part of our investigation. We will be able to determine the most susceptible areas of the website and analyze how well the security measures that have been put in place. While penetration testing replicates real-world assaults to evaluate how the website reacts under genuine danger situations, vulnerability assessments methodically examine the website to find security flaws

(Adha, Zitnaa, & Muhammad, 2023). This thorough examination will provide important new information about the security posture of every website version and practical suggestions for improvement.

In addition, our study seeks to provide a thorough, step-by-step description of how to secure a website. Both more sophisticated security methods like firewall setup and multi-layer encryption implementation will be covered in this discussion, as well as fundamental ones like using strong passwords and routinely upgrading software. We hope that by recording every stage, developers and website owners will have a useful tool to improve their cybersecurity procedures. Given the abundance of often contradicting and confusing information accessible online, this teaching component is essential (Redmiles et al., 2020).

Using real-world examples and instructional materials, our research also aims to increase public awareness of the vital need of cybersecurity. Numerous sources, including friends, family, and fictional media, teach many users protective security techniques. But the degree of correctness and quality of this guidance might differ greatly, which can cause misunderstanding and maybe insufficient security measures (Redmiles et al., 2020). Our effort is to raise the standard of security education generally by offering concise, well investigated, and tried recommendations.

Our study is also broadly applicable to a wide range of sectors and businesses. Though our main areas of expertise are travel agencies and e-commerce platforms, any website, regardless of its audience or goal, may benefit from the concepts and strategies we create. A social networking site, a financial services platform, or a healthcare portal user information protection is a universal necessity. Our study is relevant to many businesses since it offers a scalable and flexible foundation for improving website security.

Objectives:

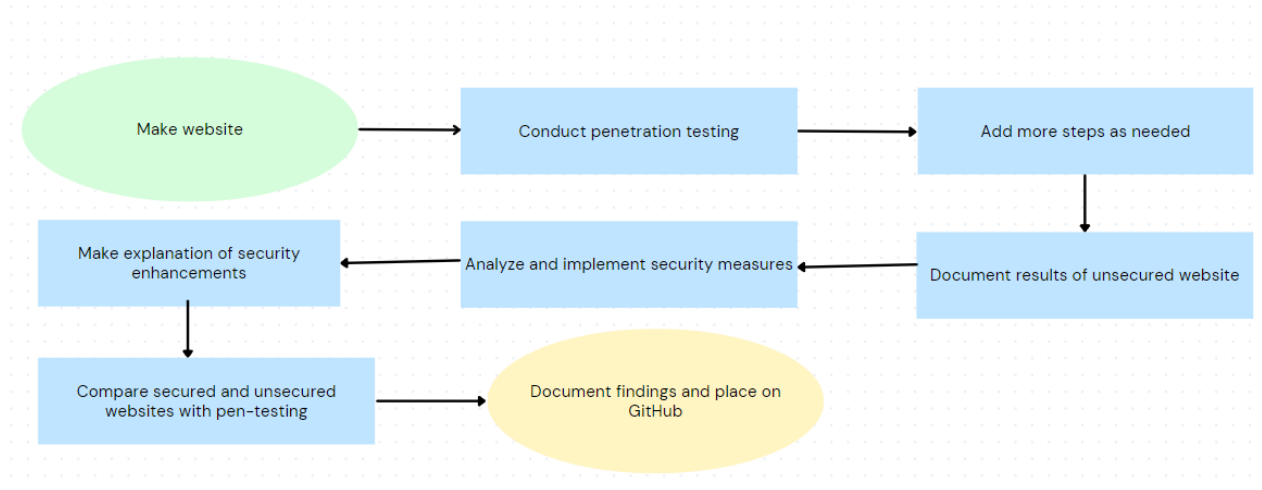
- 1 **Show Vulnerabilities** : Make a version of a website that isn't safe to show common security holes and the risks they can pose.
- 2 **Showcase Security Measures**: Make a secure form of the website that has multiple levels of security, like firewalls and safe coding techniques.
- 3 **Utilize Multi-Layer Encryption** : Introduce and use new multi-layer encryption techniques to make data safer and lower the chances of threats

succeeding.

- 4 **Do Security Assessments** : Check both versions of the website for vulnerabilities and flaws by doing penetration tests and vulnerability assessments. This will help you figure out how well your security measures are working.
- 5 **Provide Detailed Explanations**: Give a thorough breakdown of the steps that were taken to protect the website, mentioning both basic and advanced security measures.
- 6 **Raise Cybersecurity Awareness**: Show users how important it is to keep their websites safe by using real-life examples and giving them clear, well-researched advice.
- 7 **Provide Actionable Recommendations**: Tell website owners and writers how to keep their sites safe from common threats in a way that they can actually follow.
- 8 **Enhance Security Education**: By giving a wider audience access to cybersecurity, clear, practical, and tried-and-true guidance will raise the quality of security education generally.
- 9 **Ensure Broad Applicability**: Create security concepts and methods that work for a variety of websites and businesses.

Methodology

Our approach is meant to show how well different security measures work and to thoroughly investigate the security flaws present in websites. With this method, a website is built in two versions: one fully protected and one totally unprotected. This way we can show off the efforts made to safeguard the website and pinpoint certain flaws and how they may be exploited. An overview of our approach, instruments, and methods is provided here.



a) Creating the Unsecured Website

Creating an unprotected website version was our first step in creating a baseline for our investigation. To reveal possible problems resulting from insufficient security measures, this website was purposefully made exposed to typical security attacks. The intention was to imitate the situations that many websites encounter nowadays, especially those that have not put in place the necessary security measures.

Development Tools

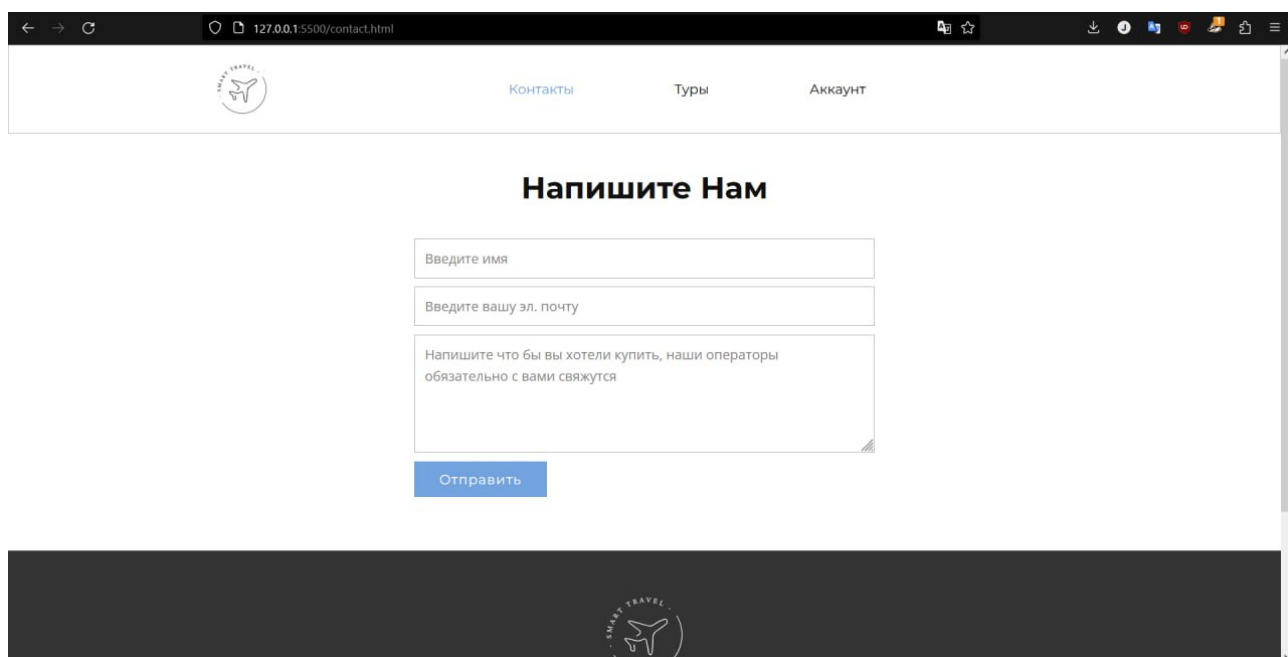
- 1 The website was coded using WebStorm and Visual Studio, two integrated development environments (IDEs). Strong support for languages like JavaScript, HTML, CSS, and server-side programming all necessary to build dynamic and interactive online applications is provided by these IDEs. Developing sophisticated online applications is made easy with WebStorm and Visual Studio's integrated version control systems, code completion tools, and strong debugging capabilities.
- 2 Text Editor: Editing and modifying items quickly was done using Sublime Text. For effectively managing huge codebases, its lightweight design and

capabilities like split editing and many cursors were perfect. A flexible tool for web development, Sublime Text also supports a large number of plugins and packages that improve its capabilities.

- 3 Database Management: To handle the databases on the website, we used phpMyAdmin and Open Server. Multiple database formats may be supported with the flexible local server environment Open Server, and database management can be easily managed and SQL queries executed using phpMyAdmin. The effective setup and management of our databases made possible by these technologies guaranteed the scalability and robustness of the data storage and retrieval procedures on the website.

	id	email	attempts	last_attempt
<input type="checkbox"/>   	1	anoka0808@gmail.com	5	2024-05-19 02:26:22

- 4 Media Editing: To make sure media files like photos and graphics were appropriately scaled and formatted for online usage, PixelMator Pro was utilized to edit and optimize them. Websites that look good need high-quality media assets, and PixelMator Pro's sophisticated editing features let us improve our website's visual components while keeping file sizes small enough to guarantee quick loading times.



b) Conducting Penetration Testing

After creating the unprotected website, we thoroughly tested it for weaknesses. In penetration testing, or pentesting, security flaws that attackers may take advantage of are simulated cyberattacks. We used the sophisticated penetration testing and security auditing operating system Kali Linux for this.

Фамилия:

`<script>alert('XSS');</script>`

Дата рождения:

08.04.2004



Адрес:

KZ

Gmail YouTube

Подтвердите действие на main.no

XSS

OK

	id	user_id	surname	birth_date	address
<input type="checkbox"/>	4	13	<code><script>alert('XSS');</script></code>	2004-04-08	KZ

Pentesting Tools and Techniques:

- 1 **BurpSuite:** People used this tool to find holes in web services and take advantage of them. BurpSuite is a complete platform for testing the security of web applications. It has tools for mapping the application, studying replies, and automating attacks. We used the spider, scanner, and attacker from BurpSuite's suite of tools to find and use security holes like cross-site scripting (XSS) and SQL injection.
- 2 **HashCat:** HashCat is a strong password recovery tool that is used to crack passwords. It uses GPU acceleration to make the cracking process go faster. This tool helped us show how weak passwords can leave you open to attack. We were able to find passwords that were easy to crack by running HashCat against the password hashes in our database. This shows how important it is to use strong, complex passwords.
- 3 **Hydra:** Another tool for brute force attacks, Hydra lets you use a lot of different protocols to try to log in to different sites over and over again. We used it to check how strong the login systems were and find their weak spots. Because Hydra can automate brute force attacks, we were able to quickly try a lot of different account and password combinations. This showed how attackers can take advantage of authentication systems that aren't strong enough.
- 4 **SQLMap:** This tool was used to find SQL attack holes and take advantage of them. An usual way for attackers to take control of a web application's database is through SQL injections, which run harmful SQL commands. SQLMap makes it easy to find and take advantage of these security holes. We were able to find SQL injection holes in our unprotected website using SQLMap and use them to get into the database without permission, get private information, and change database records.

c) Documenting Test Results

During the security testing phase, we carefully wrote down the results of every test. Each weakness that was found was written down along with the steps that were used to take advantage of it. There were images, log files, and full details of each vulnerability in this literature. The recorded information was used to look for security holes and come up with ways to fix them. By keeping detailed records, we made sure that our results could be repeated and

checked, which gave us a strong foundation for putting security measures in place.

d) Research and Literature Review

We did a thorough study of the literature to find answers for the weaknesses we found. From our reading list, we read articles and study papers that helped us understand the best ways to keep websites safe. We were able to figure out what caused the flaws and how to fix them better after reading this review.

We also looked at case studies and real-life examples of security breaches to see how similar flaws had been used in the past and what steps were taken to make sure they wouldn't happen again. This study helped us figure out how to keep the website safe by making sure that our solutions were based on tried-and-true methods and the latest security standards.

e) Implementing Security Measures

We put in place a number of security steps to protect the website based on what we learned from our literature study. The goal of these steps was to fix the specific security holes that were found during the penetration testing process. The following improvements were made to the protected version of the website:

- 1 **Secure Coding Practices:** Secure coding approaches reduced typical coding flaws that might compromise security. We validated input, encoded output, and used prepared statements to prevent SQL injection attacks. User-provided data is validated and sanitized before being handled by the program to prevent malicious inputs from causing harm. Output encoding turns special characters into HTML entities to protect user inputs from XSS attacks.
- 2 **Firewalls:** The website was protected from assaults by firewalls that filtered incoming and outgoing traffic. Firewalls monitor and regulate network traffic based on security rules to protect the internal network. We strengthened the website's security by setting firewalls to stop harmful traffic.
- 3 **Multi-Layer Encryption:** We improved data security using unique multi-layer encryption. A single layer in traditional encryption can disclose all encrypted data if hacked. Multiple levels of encryption provided hurdles for attackers, improving data security. Each encryption layer employs a distinct algorithm and key, so if one is compromised, the others safeguard the data.

f) Detailed Explanation of Security Enhancements

For good understanding of the measures we used for security, we've decided to document every step we take to keep our website safe. This document is meant to educate readers about our cybersecurity process, from basic to advanced techniques.

Password Hashing and Verification

One of most important things in website securing is ensuring that user passwords are stored securely. We took one `\verb|password_hash|` function to generate hashes for password, it takes a plain text password and a hashing algorithm as parameters and returns a hashed password. The hashed password is then stored in the database. Using the `\verb|PASSWORD_DEFAULT|` constant, we acknowledge that the best available hashing algorithm is used, which can be changed over time as stronger algorithms are will be added to PHP.

card_number	card_holder	expiry_date	cvv
\$2y\$10\$4oATmrOuAFDkQRM.p9faOqsGSZgAoPMN2fQgrLWpMj...	Anuar	\$2y\$10\$4wk5wHaM6yLnOHStCmnRYeOLbx1.JIC92w1OuqoO1Ay...	\$2y\$10\$b.I2wsrXXFNCMM70P7ZOwus7KMXQNygwzZ3re6YDcaD...
\$2y\$10\$0FsrjBwsMjXeJOZs0R5B5uhOWVz.3JsShPZ/EEsYQwQ...	Anuar	\$2y\$10\$X7jydgFQ0UQ7QR4obPFyV.JzasjxeuNUNvVlcU4wOOW...	\$2y\$10\$A3HUj0TRg3DUQykugjyA/OQQPt6BmmyCrKVYdI99TfA...
\$2y\$10\$/PVDvjew/daO0nzLcSkKQu7UFxtYULk3jP/JLqX0h4...	Anuar	\$2y\$10\$TMrJahHdENyVQepq8GADUeOD1Ow1KUQLbjNp3Uv4GK...	\$2y\$10\$n8no0K9HWGYFvCyTmZWAPO9L2Wrhp.uALLap9SxYp2...
\$2y\$10\$5lIc0IKSL5aTPhOserQb5NetzB2bm3zp39Hzr.KUR/mq...	Anuar	\$2y\$10\$IE3UY/tFjYfXbD5ax0H5u7aj351XwptXdWZBlwSM4O...	\$2y\$10\$JlhKGNjFDE9lFPvYvxNG.qk0B9b.5wnY3ji7U1Q5Q...

To check and authentication of user passwords during login process, we took the `\verb|password_verify|` function. Our function accepts a plain text password and a hashed password as input and returns a boolean value of true if they are a match, or false if they are not. It checks if that plain text passwords are not stored without being hashed, it reduces the risk of password data loss in case of leakage.

This approach gave us such benefits, like the selection of the most secure hashing algorithm and the auto adding of a salt for each password. Salting involves the addition of a random value to each password in hashing. This process controls that each resulting hash is unique, hence prohibiting the utilization of precomputed tables (rainbow tables) for password cracking purposes.

Login Attempt Monitoring

To protect against brute force attacks, we observed the number of failed login attempts and the time of the last attempt using a `\verb|login_attempts|` table. This table stores user data including unsuccessful login attempts and enforce rate limiting.

If the number of failed attempts exceeds a set threshold (e.g., 5 attempts) within a short time frame (e.g., the last 5 minutes), the user is required to wait before attempting to log in again. If an account exists but the password is incorrect, the count of attempts is incremented, and the time of the last attempt is updated. Upon a successful login, the count is reset, and the user is granted access.

HTML Entity Encoding

To protect against cross-site scripting (XSS) attacks, we used the `htmlspecialchars` function in PHP to convert special characters into HTML objects. This function converts characters such as `<`, `>`, `&`, `'` and `"`, these characters are used in an attack attempt, into appropriate HTML codes, preventing user input in HTML or JavaScript format. By hiding all user data before displaying it on the page, we reduce the risk of XSS attacks.

CSRF Protection

Cross-Site Request Forgery (CSRF) attacks are another major threat to web applications that we will be fixing for our website. To defend against CSRF, we implemented a token-based system. Each time a user loads a form, a unique CSRF token is generated and stored in the user's session. This token is included as a hidden field in the form and sent with the form submission.

When the form is submitted, the server verifies that the CSRF token matches the value stored in the user's session. If the tokens do not match, the request is rejected, and an error message will be displayed to the user's screen. This mechanism ensures that only legitimate web requests from the user are processed, preventing CSRF attacks from malicious sites.

g) Comparing Secured and Unsecured Websites

To study the effectiveness of the implemented security measures, we compared side by side the secured website with the unsecured version. This comparison involved several steps:

- 1 **Re-Assessing Vulnerabilities:** We conducted a second round of penetration testing on the secured website to assess the effectiveness of the implemented

security measures. The goal was to make sure that the previously identified vulnerabilities were correctly addressed, fixed and no new vulnerabilities were introduced.

- 2 **Performance Evaluation:** We evaluated the performance of both versions of the website to ensure that the security measures did not adversely affect the website's functionality or user experience. This included testing the speed of website's load times, responsiveness of the website as a whole, and overall user experience.
- 3 **User Feedback:** We collected feedback from users through Google Forms surveys. The surveys aimed to collect information on the users' experiences of using websites, with both protected and not protected versions of the website, their opinion of security, and were they faced issues or not. This feedback provided valuable insights into the practical implications of the security measures.

h) Educational and Awareness Initiatives

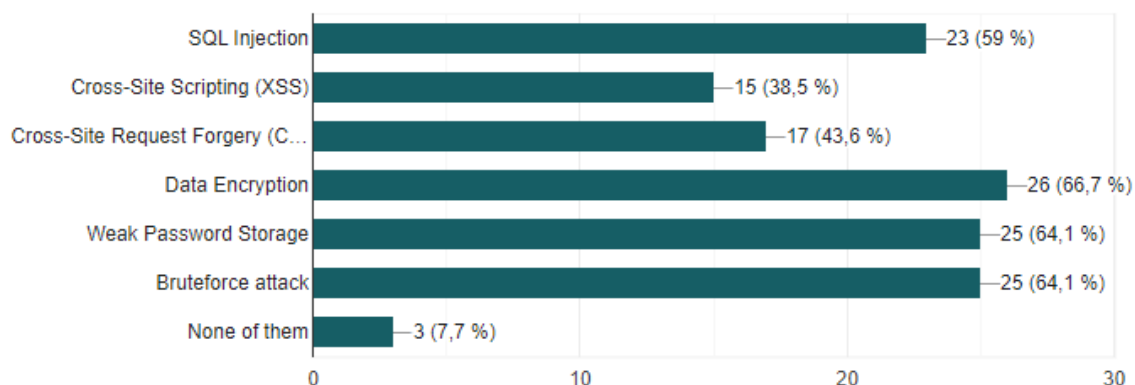
In addition to developing and testing the websites, our project included educational and cyber threat awareness initiatives aimed at raising awareness about cyber threats. We created detailed explanations of the steps taken to secure the website, covering both basic and advanced security practices. These explanations were created to be accessible to a broader audience, including developers with little to no experience, website owners, and the general public.

We conducted an anonymous survey and asked our (39 people) respondents about their experience with cyber attacks and cybersecurity measures. Here is our findings:

Select threats you heard about before

 Копировать

39 ответов



1. Understanding of Web Security Ideas Observation:

Most of the people who answered said they knew a middling to high amount about web cybersecurity ideas. Of those people, (35.9 percent) said they knew the most.

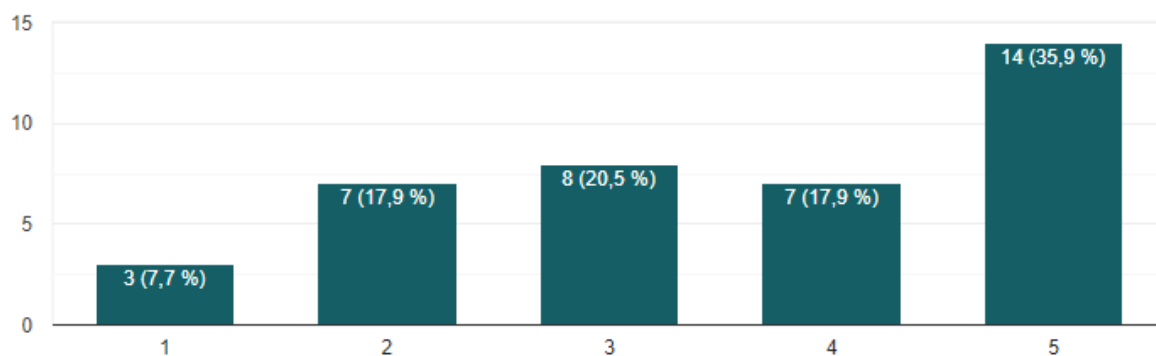
Being aware of:

A large number of responders have a good idea of how to keep websites safe. This means that the people in the room know a lot about the subject, which can help them understand and use more advanced protection measures.

How familiar are you with web cybersecurity concepts?

 Копировать

39 ответов




2. Trust in the Current Cybersecurity Measures.

There is a range of trust in the current cybersecurity methods. Most respondents (35.9 percent) said they were moderately confident (3 out of 5).

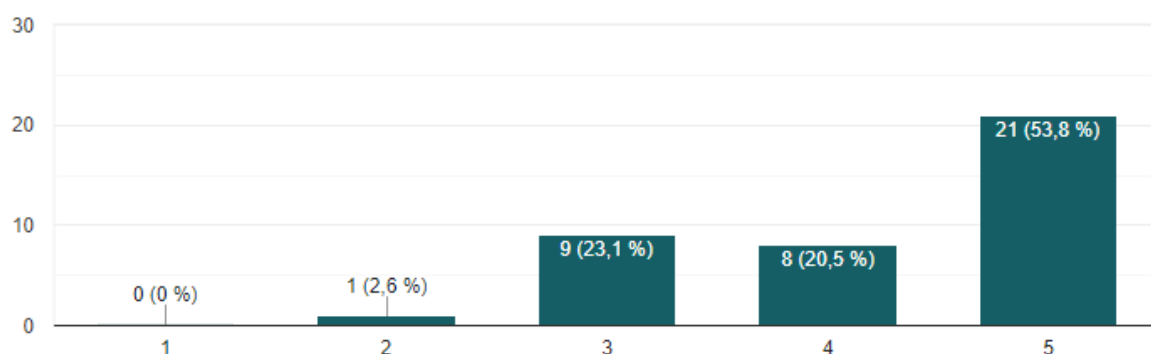
Being aware of:

Most people believe the security steps that are already in place, but they could be better. Improving these steps and letting people know how well they work can help boost user trust.

How important do you think it is for a travel agency website to have strong cybersecurity protection?

 Копировать

39 ответов



3. Being aware of certain cybersecurity threats

Most people are aware of these risks; more than (60 percent) of those surveyed knew about data protection, weak password storage, and brute force attacks.

Being aware of:

Respondents know a lot about the most important cybersecurity dangers, especially the ones that come up a lot in talks about cybersecurity. These places should still be the focus of education and training, but people should also learn more about threats like XSS and CSRF that aren't as well known.

If you think that strong protection for travel agency website is important, tell why

11 ответов

A lot of confidential data

very important information of users

Strong protection for a travel agency website is crucial because it safeguards sensitive customer information, such as personal and financial data, which helps maintain customer trust and prevents identity theft. Additionally, robust security measures ensure compliance with legal regulations, avoiding potential fines and legal issues. A secure website also protects the agency's reputation, prevents financial losses from cyber-attacks, and ensures smooth business operations without disruptions from security breaches.

Ensuring strong protection for a travel agency website is vital because it secures sensitive customer data, including personal and payment information, thereby preventing identity theft and fraud.

Protection for travel agency website is important because it should contain a big amount of personal information. If you make protection algorithms badly, your website won't be trusted by the users and organisations.

.

4. Features that are important for keeping an eye on website security:

Most of the people who answered think it's important to have strong password rules, protect data, and regularly update security.

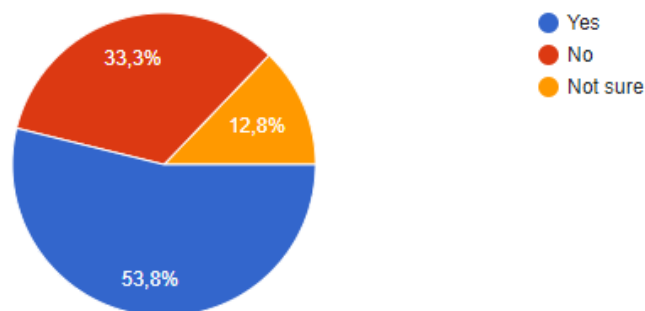
Being aware of:

Almost everyone agrees that basic protection features are very important. Taking these steps is necessary to meet user standards and make sure that the website is secure.

Have you ever experienced a cybersecurity breach (e.g., data theft, account hacking) on a website you use?

 Копировать

39 ответов



5. The significance of having robust protection against cyberattacks.

A remark is made:

More than fifty-three point eight percent of respondents believe that robust cybersecurity protection is of utmost significance for websites belonging to travel agencies.

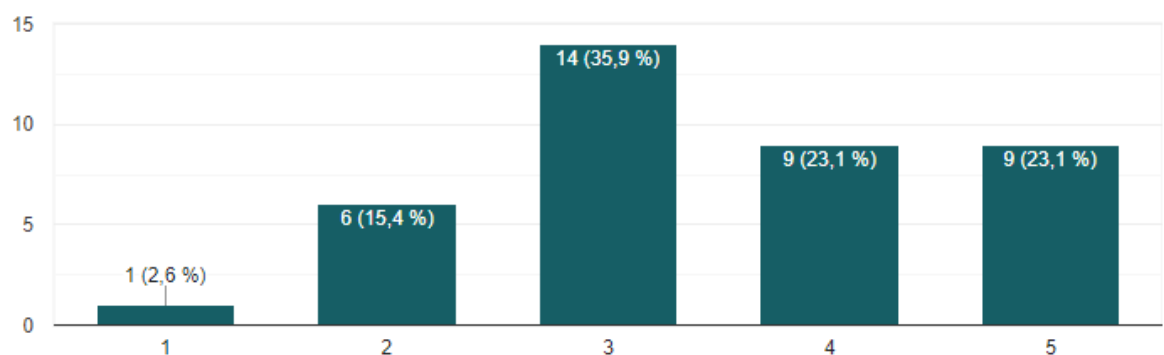
A comprehension of:

The importance of cybersecurity is well recognized, and there is a high degree of knowledge regarding this. This implies a desire for robust security measures to secure sensitive user data and to retain trust in the system.

How confident are you in the ability of current cybersecurity measures to protect personal information on travel agency websites?

 Копировать

39 ответов



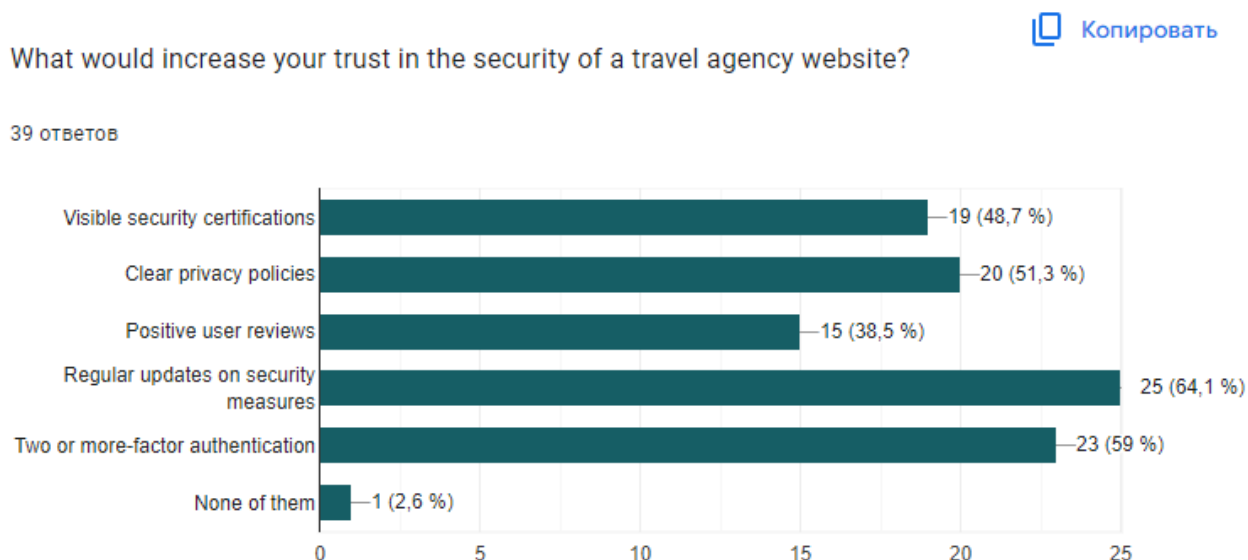
6. How frequently penetration tests are performed.

A remark is made:

Thirty-eight point five percent of respondents choose quarterly penetration testing, while thirty-eight point five percent like monthly testing.

A comprehension of:

Regular penetration testing is considered to be an essential activity for ensuring that security is maintained continuously. It is recommended to do testing on a monthly basis, which points to a proactive strategy to locating and eliminating vulnerabilities.



7. The significance of implementing robust security measures for travel agency websites.

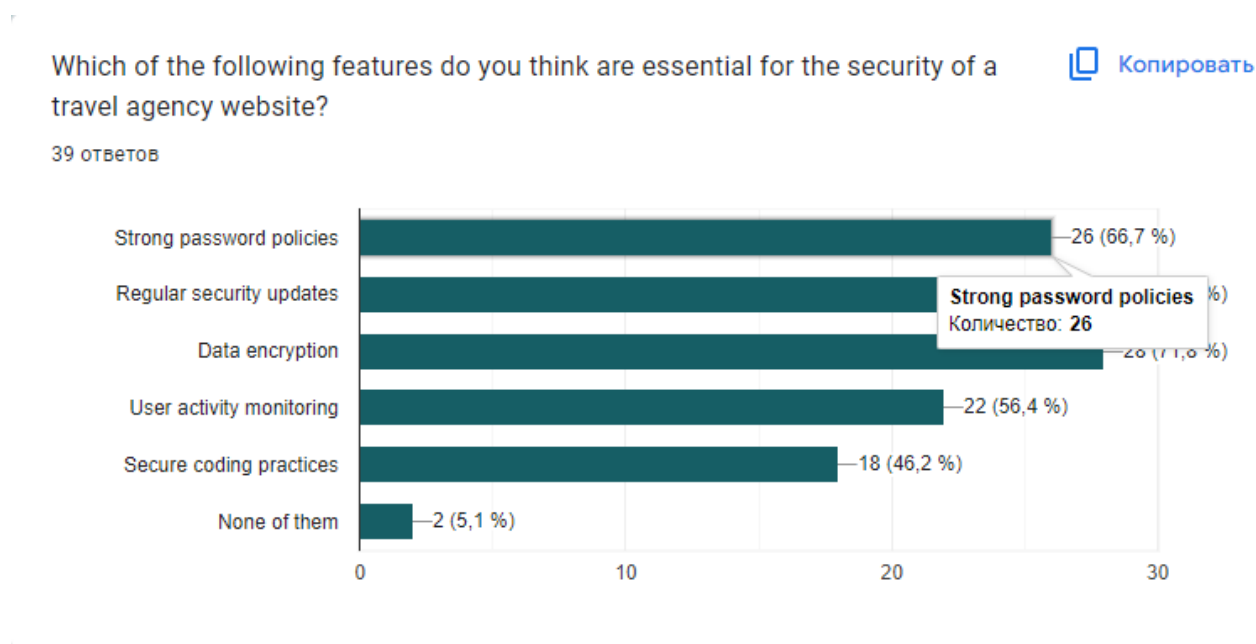
A remark is made:

The necessity of securing sensitive customer information, preserving trust, avoiding identity theft, and ensuring legal compliance was emphasized by those who responded to the survey.

A comprehension of:

When it comes to securing sensitive data, adhering to regulatory obligations,

and preserving a favorable reputation, strong cybersecurity measures are very necessary. The need of implementing stringent security mechanisms is highlighted by this insight.



8. Factors That Are Increasing Trust in the Security of Websites

A remark is made:

There are a number of things that might boost trust in website security, the most important of which being regular updates on security measures and authentication using two or more methods.

A comprehension of:

When it comes to gaining the trust of users, transparency and proactive security policies are essential. Increasing the sense of security may be accomplished by the implementation of multi-factor authentication and the implementation of security measures that are regularly updated.

9. Knowledge of how to handle cybersecurity breaches.

More than half of the people who answered (53.8 percent) have had a hacking breach.

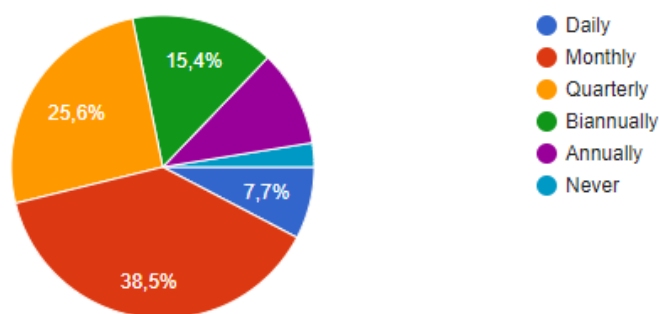
Being aware of:

The fact that there are so many breaches shows how real hacking dangers are and how important strong security measures are. It also shows that users are likely to be more careful and back stronger security measures.

How often do you think travel agencies should do penetration testing to identify vulnerabilities and prevent leakage of your personal information?

 Копировать

39 ответов



In short:

The answers to the poll show how much people know, how confident they are, and what they expect from travel agency websites in terms of security. Strong security methods are clearly understood to be very important, and people are taking steps to keep them up to date. People think that strong password rules, regular updates, data protection, and multi-factor authentication are all important parts of a safe website. These results will help people come up with good hacking plans to keep user info safe and keep people's trust.

i) Disseminating Findings

To ensure that our findings will reach to a wide audience, we plan to share our research:

- 1 **GitHub:** We want to publish our results in github. In github, we will publish all the developments, and the project itself in completely open access, that probably will be useful for beginners or just readers who want to study or use our code for their own purposes. We will also post our report as background info about the project on github. There will be detailed descriptions of the

vulnerabilities identified, the security measures applied, and the results of comparing protected and unprotected websites.

Results

The results of our work, involving the creation and testing of both unsecured and secured versions of a website, highlight significant findings about common vulnerabilities and the effectiveness of various security measures. Our methodology enabled us to systematically identify and address security flaws, demonstrating both the risks of poor security practices and the benefits of robust protections.

Initial Findings from the Unsecured Website

Upon developing the unsecured version of our website, we conducted a thorough penetration test using tools available in Kali Linux. This initial assessment revealed several critical vulnerabilities:

- 1 **Weak Password Storage:** Passwords were stored in plain text within the database, posing a significant security risk. Using HashCat, we showed how quickly these passwords could be cracked, exposing user accounts to unauthorized access.
- 2 **SQL Injection Vulnerabilities:** The site was vulnerable to SQL injection attacks, allowing attackers to execute arbitrary SQL commands. SQLMap was used to exploit these vulnerabilities, demonstrating how attackers could gain unauthorized access to the database, extract sensitive information, and even modify or delete data.
- 3 **Cross-Site Scripting (XSS):** The absence of input validation and output encoding made the site vulnerable to XSS attacks. Using BurpSuite, we injected malicious scripts into web forms, which were then executed in the browsers of unsuspecting users. This could be used to steal session cookies, redirect users to malicious sites, or perform other malicious actions.

Личный кабинет



Привет, Ануар

Фамилия: `<script>alert('XSS');</script>`

Дата рождения: 2004-04-08

Адрес: Kazakhstan, Astana, Zhurgenova St. 32/49

Редактировать профиль

Выйти из аккаунта

[Назад](#)

- 4 **CSRF Vulnerabilities:** The site lacked protection against Cross-Site Request Forgery (CSRF) attacks. We demonstrated how an attacker could trick a logged-in user into executing unwanted actions on the site by embedding malicious requests in a third-party website.

Implementing Security Measures

Based on the vulnerabilities identified, we implemented a series of security measures to create a secured version of the website. These measures included:

- 1 **Password Hashing:** We used the `password_hash` function with `PASSWORD_DEFAULT` to hash user passwords before storing them in the database. This added a layer of security by ensuring that even if the database was compromised, the passwords would not be easily accessible.
- 2 **SQL Injection Prevention:** To mitigate SQL injection vulnerabilities, we adopted prepared statements and parameterized queries throughout the application. This prevented attackers from injecting malicious SQL commands.
- 3 **Input Validation and Output Encoding:** We implemented rigorous input validation and output encoding using the `htmlspecialchars` function to protect against XSS attacks. By ensuring that all user inputs were properly sanitized and encoded, we reduced the risk of malicious scripts being executed.

Вход

Слишком много неудачных попыток. Пожалуйста, попробуйте позже.

E-mail

Введите email

Пароль

Продолжить

[Назад](#)

- 4 **CSRF Protection:** To defend against CSRF attacks, we implemented a token-based system. Each form included a hidden CSRF token that was validated on the server side. If the token did not match the one stored in the user's session, the request was rejected.

Results of Penetration Testing on the Secured Website

After implementing the security measures, we conducted another round of penetration testing to evaluate their effectiveness. The results showed significant improvements:

- 1 **Secure Data Transmission:** All data was encrypted during transmission. Tools like BurpSuite confirmed that intercepted data was encrypted and unreadable, effectively preventing man-in-the-middle attacks.
- 2 **Improved Password Security:** The use of `password_hash` and `password_verify` functions ensured that passwords were stored securely.

Even with tools like HashCat, cracking the hashed passwords was not feasible within a reasonable timeframe.

- 3 **SQL Injection Mitigation:** Prepared statements and parameterized queries successfully prevented SQL injection attacks. SQLMap tests confirmed that the site was no longer vulnerable to SQL injection, as all inputs were properly sanitized.
- 4 **XSS Prevention:** Input validation and output encoding effectively protected against XSS attacks. Attempts to inject malicious scripts were thwarted, and BurpSuite confirmed that user inputs were safely displayed without executing harmful code.

Фамилия:

<script>alert('XSS');</script>

Дата рождения:

08.04.2004



Адрес:

Kazakhstan, Astana, Zhurgenova St. 32/49

- 5 **CSRF Defense:** The CSRF token system successfully blocked unauthorized actions. Tests showed that without the correct token, all CSRF attempts were rejected, ensuring that only legitimate user actions were processed.

Performance and User Experience

We also evaluated the performance and user experience of both versions of the

website. The results indicated that while the security measures slightly increased the complexity of the codebase, they did not significantly impact the website's performance:

- 1 **Responsiveness:** The secured version of the website remained responsive, with no noticeable delays in user interactions. The security measures did not introduce significant latency, ensuring a smooth user experience.
- 2 **User Feedback:** Surveys conducted using Google Forms indicated that users felt more secure using the protected website. They appreciated the visible security indicators, such as the HTTPS padlock, and reported a high level of trust in the website's security.

Educational Impact

In addition to securing the website, our team created this documentation to provide educational impact. The explanations and documentation of the security measures that was provided in a text form, tries to give insights for developers and website owners:

- 1 **Increased Awareness:** Our project created to raise awareness about common security vulnerabilities and the importance of implementing basic, but important security measures.
- 2 **Practical Guidance:** The documentation provided step-by-step actions that we did for implementing security measures, making it easier for others to replicate our approach. This practical guidance created to help demystify cybersecurity for those with limited technical expertise.

Conclusion

This documentation shows exactly how important it is to have reliable fundamental security tools to ensure that websites are protected from typical attacks, as well as from security breaches. By developing and comparing both the unguarded and the protected version of the website, we were able to identify threats associated with insufficient security, as well as the great advantages of reliable protection. We found significant security breaches on the unsecured site, including information theft, password leaks, cross-site scripting (XSS), and cross-site request forgery (CSRF). As a result of these security measures, allows threats to get to the personal integrity, accuracy and accessibility of customer information. This shows how important it is to provide reliable protection immediately. We have included basic security attributes in the protected version, such as password hashing, ready-made declarations, recognition of input data, recording of results in combination with CSRF characters. The penetration test confirmed that these changes fixed the problems mentioned above, making the website much more secure without reducing its effectiveness or customer service quality. The mentoring component of this work has provided programmers as well as website owners with valuable information and detailed guidance. By offering detailed information about security measures and fuses, as well as how to implement them, we sought to increase the level of understanding, as well as the basic level of knowledge about hacker attacks. This study shows how important reliable cybersecurity measures are to protect websites from common threats, as well as how effectively they function. The results show exactly how important it is to take active and at the same time effective security measures to maintain the client's trust fund, as well as to protect exclusive data. From the point of view of cybersecurity, which we currently adhere to, it is vital to be aware of developments, as well as to increase the level of cybersecurity in order to secure your information and make sure that Internet systems are functioning properly.

BIBLIOGRAPHY

1 Adha M., KWA Z. D. & Muhammad A. H. WEBSITE SECURITY TEST AT THE UNIVERSITY OF MATARAM USING VULNERABILITY ASSESSMENT / KWA Z. D. & Muhammad A. H. Adha, M. // *Jurnal Ilmiah Penelitian dan Pembelajaran Informatika*. — 2023. — Vol. 8, no. 2. — Pp. 647–655.

<https://www.jurnal.stkipgritlungagung.ac.id/index.php/jipi/article/download/3830/1559>.

2 Web Application Penetration Testing Using SQL Injection Attack / A. Alanda, D. Satria, M. I. Ardhana et al. // *JOIV: International Journal on Informatics Visualization*. — 2021. — Vol. 5, no. 3. — Pp. 320–326.

3 Alghawazi, M. Detection of SQL Injection Attack Using Machine Learning Techniques: A Systematic Literature Review / M. Alghawazi, D. Alghazzawi, S. Alarifi // *Journal of Cybersecurity and Privacy*. — 2022. — Vol. 2, no. 4. — Pp. 764–777. <https://www.mdpi.com/2624-800X/2/4/39>.

4 Al-Hawawreh, M. ChatGPT for Cybersecurity: Practical Applications, Challenges, and Future Directions / M. Al-Hawawreh, A. Aljuhani, Y. Jararweh // *Cluster Computing*. — 2023. — Vol. 26, no. 6. — Pp. 3421–3436. <https://www.researchgate.net/profile/Muna-Al-Hawawreh/publication/373044798ChatGPTForCybersecuritypracticalApplicationsChallengesandFutureDirections.pdf>.
For – Cybersecurity – Practical – Applications – Challenges – and – Future – Directions.pdf.

5 Almaarif, A. Vulnerability Assessment and Penetration Testing (VAPT) Framework: Case Study of Government's Website / A. Almaarif, M. Lubis // *International Journal on Advanced Science Engineering and Information Technology*. — 2020. — Vol. 10, no. 5. — Pp. 1874–1880. <https://www.researchgate.net/profile/Ahmad-Almaarif/publication/344830695VulnerabilityAssessmentandpenetrationTestingVAPTFrameworkCaseStudyofGovernmentsWebsite.pdf>.
Assessment – and – Penetration – Testing – VAPT – Framework – Case – Study – of – Governments – Website.pdf.

6 Bhalla, A. Present Day Web Development Using ReactJS / A. Bhalla, S. Garg, P. Singh // *International Research Journal of Engineering and Technology*. — 2020. — Vol. 7, no. 05.

7 PentestGPT: An LLM-Empowered Automatic Penetration Testing Tool / G. Deng, Y. Liu, V. Mayoral-Vilches et al. // *arXiv preprint*. — 2023. <https://arxiv.org/pdf/2308.06782>.

8 Devi, R. S. Testing for Security Weakness of Web Applications Using Ethical Hacking / R. S. Devi, M. M. Kumar // 2020 4th International Conference on Trends in Electronics and Informatics (ICOEI). — IEEE, 2020. — June. — Pp. 354–361. https://ieeexplore.ieee.org/iel7/9138108/9142867/09143018.pdf?casa_token=pyq-3DZNolYAAAAA:3fCHssjcs7i00G6LXZ8vEv-fx38QPNos0ciZ3RHCSlyQDHP9YnVRTz3MkkUM6aVYAKhgIS7G0OKw.

9 Elisa, N. Usability, Accessibility and Web Security Assessment of E-Government Websites in Tanzania / N. Elisa // *arXiv preprint*. — 2020. <https://arxiv.org/pdf/2006.14245>.

10 Erdődi, L. The Agent Web Model: Modeling Web Hacking for Reinforcement Learning / L. Erdődi, F. M. Zennaro // *International Journal of Information Security*. — 2022. — Vol. 21, no. 2. — Pp. 293–309. <https://www.scirp.org/pdf/ojsst2023063015450993.pdf>.

11 *Hope, P.* Web Security Testing Cookbook: Systematic Techniques to Find Problems Fast / P. Hope, B. Walther. — O'Reilly Media, Inc., 2008. <https://sisis.rz.htw-berlin.de/inh2012/12422757.pdf>.

12 *Kala, E. M.* The Impact of Cyber Security on Business: How to Protect Your Business / E. M. Kala // *Open Journal of Safety Science and Technology*. — 2023. — Vol. 13, no. 2. — Pp. 51–65. <https://doi.org/10.4236/ojsst.2023.132003>.

13 SQL Injection Attacks Prevention System Technology / F. Q. Kareem, S. Y. Ameen, A. A. Salih et al. // *Asian Journal of Research in Computer Science*. — 2021. — Vol. 10, no. 3. — Pp. 13–32. https://www.researchgate.net/profile/Awder-Ahmed/publication/353025675_SQLInjectionAttackspreventionssystemTechnologyReview/links/60e4a1f0Injection-Attacks-Prevention-System-Technology-Review.pdf.

14 *Paraskevas, A.* Cybersecurity in Travel and Tourism: A Risk-Based Approach / A. Paraskevas // Handbook of e-Tourism. — Cham: Springer International Publishing, 2022. — Pp. 1605–1628. https://repository.uwl.ac.uk/id/eprint/6761/1/Paraskevas_springer_2020_cybersecurity_in_travel_and_tourism_based_approach.pdf.

15 *Periasamy, J. K.* AssessJet-Penetration Testing and Vulnerability Assessment for Websites / J. K. Periasamy, V. Dakiniswari, K. Tapasya // 2022 International Conference on Communication, Computing and Internet of Things (IC3IoT). — IEEE, 2022. — March. — Pp. 1–4. https://ieeexplore.ieee.org/iel7/9767722/9767723/09767928.pdf?casa_token=pMhgElxgAMAAAAA:q33z3qZE7YhWjVz6MAv8v1aiORhKNEvEoq0yzgXFj1S6kRtmeAdSWjA4A

16 *Priyawati, D.* Website Vulnerability Testing and Analysis of Website Application Using OWASP / D. Priyawati, S. Rokhmah, I. C. Utomo // *International Journal of Computer and Information System (IJCIS)*. — 2022. — Vol. 3, no. 3. — Pp. 142–147. <http://www.ijcis.net/index.php/ijcis/article/download/90/82>.

17 A Comprehensive Quality Evaluation of Security and Privacy Advice on the Web / E. M. Redmiles, N. Warford, A. Jayanti et al. // 29th USENIX Security Symposium (USENIX Security 20). — 2020. — Pp. 89–108. <https://www.usenix.org/system/files/sec20-redmiles.pdf>.

18 Informing Cyber Threat Intelligence through Dark Web Situational Awareness: The AZSecure Hacker Assets Portal / S. Samtani, W. Li, V. Benjamin, H. Chen // *Digital Threats: Research and Practice (DTRAP)*. — 2021. — Vol. 2, no. 4. — Pp. 1–10. <https://dl.acm.org/doi/pdf/10.1145/3450972>.

19 Modeling and Predicting Cyber Hacking Breaches / R. R. Subramanian, R. Avula, P. S. Surya, B. Pranay // 2021 5th International Conference on Intelligent Computing and Control Systems (ICICCS). — IEEE, 2021. — May. — Pp. 288–293. https://ieeexplore.ieee.org/iel7/9432068/9432069/09432175.pdf?casa_token=umoUvH70db0AAAAA:3vdzq2cFExMbBbfjg8uVVQnxa14jbzmKXxOBL2ZVMxTPtb5fEv_oFyIVspftVaUQ-ODA.

20 A Survey on Ethical Hacking: Issues and Challenges / J. P. A. Yaacoub, H. N. Noura, O. Salman, A. Chehab // *arXiv preprint*. — 2021. <https://arxiv.org/pdf/2103.15072>.

Appendix A first appendix

```
$card_number = password_hash($_POST['card_number'], PASSWORD_DEFAULT); // Hash the card number
$card_holder = $_POST['card_holder'];
$expiry_date = password_hash($_POST['expiry_date'], PASSWORD_DEFAULT); // Hash the expiry date
$cvv = password_hash($_POST['cvv'], PASSWORD_DEFAULT); // Hash the CVV
```

Figure A.1 – Hashing method

```
$params = [
    'name' => $name,
    'email' => $email,
    'avatar' => $avatarPath,
    'password' => password_hash($password, PASSWORD_DEFAULT)
];
```

Figure A.2 – Hashing method

```
if (!password_verify($password, $user['password'])) {
    setMessage('error', 'Неверный пароль');
    redirect('/index.php');
```

Figure A.3 – Hash data verification

```
// Fetch login attempts
$sql = "SELECT attempts, last_attempt FROM login_attempts WHERE email = ?";
$stmt = $conn->prepare($sql);
$stmt->bind_param("s", $email);
$stmt->execute();
$result = $stmt->get_result();
$attempt = $result->fetch_assoc();
```

Figure A.4 – Gathering information about login attempts

```
$now = new DateTime();
$timeout_duration = new DateInterval('PT5M'); // 5 minutes
$max_attempts = 5; // Maximum attempts before timeout

if ($attempt) {
    $last_attempt = new DateTime($attempt['last_attempt']);
    $interval = $now->diff($last_attempt);

    if ($attempt['attempts'] >= $max_attempts && $interval->i < 5) {
        setMessage('error', 'Слишком много неудачных попыток. Пожалуйста, попробуйте позже.');
```

```
        $stmt->close();
        $conn->close();
        redirect('/index.php');
    }
} else {
    // Initialize login attempt record if it doesn't exist
    $sql = "INSERT INTO login_attempts (email) VALUES (?)";
    $stmt = $conn->prepare($sql);
    $stmt->bind_param("s", $email);
    $stmt->execute();
    $stmt->close();
}
```

Figure A.5 – Checking the numbers of attempts and timeout

```
// Check user credentials
$user = findUser($email);
if (!$user) {
    $sql = "UPDATE login_attempts SET attempts = attempts + 1, last_attempt = NOW() WHERE email = ?";
    $stmt = $conn->prepare($sql);
    $stmt->bind_param("s", $email);
    $stmt->execute();
    $stmt->close();

    setMessage('error', "Пользователь $email не найден");
    $conn->close();
    redirect('index.php');
}

if (!password_verify($password, $user['password'])) {
    $sql = "UPDATE login_attempts SET attempts = attempts + 1, last_attempt = NOW() WHERE email = ?";
    $stmt = $conn->prepare($sql);
    $stmt->bind_param("s", $email);
    $stmt->execute();
    $stmt->close();

    setMessage('error', 'Неверный пароль');
    $conn->close();
    redirect('/index.php');
}
```

Figure A.6 – Check user credentials

```
// Reset attempts on successful login
$sql = "UPDATE login_attempts SET attempts = 0, last_attempt = NOW() WHERE email = ?";
$stmt = $conn->prepare($sql);
$stmt->bind_param("s", $email);
$stmt->execute();
$stmt->close();

$_SESSION['user']['id'] = $user['id'];

$conn->close();
redirect('/home.php');
```

Figure A.7 – Reset attempts on successful login

```
src="<?php echo htmlspecialchars($user['avatar'], ENT_QUOTES, 'UTF-8'); ?>"
alt="<?php echo htmlspecialchars($user['name'], ENT_QUOTES, 'UTF-8'); ?>"
>
<p>Привет, <?php echo htmlspecialchars($user['name'], ENT_QUOTES, 'UTF-8'); ?></p>

<div class="profile-info" id="profileInfo">
  <p><strong>Фамилия:</strong> <?php echo htmlspecialchars($profile['surname'] ?? 'Не указано', ENT_QUOTES, 'UTF-8'); ?></p>
  <p><strong>Дата рождения:</strong> <?php echo htmlspecialchars($profile['birth_date'] ?? 'Не указано', ENT_QUOTES, 'UTF-8'); ?></p>
  <p><strong>Адрес:</strong> <?php echo htmlspecialchars($profile['address'] ?? 'Не указано', ENT_QUOTES, 'UTF-8'); ?></p>
</div>
```

Figure A.8 – XSS Defence

```
function generateCsrfToken() {
    if (empty($_SESSION['csrf_token'])) {
        $_SESSION['csrf_token'] = bin2hex(random_bytes(32));
    }
    return $_SESSION['csrf_token'];
}

function validateCsrfToken($token) {
    return isset($_SESSION['csrf_token']) && hash_equals($_SESSION['csrf_token'], $token);
}
```

Figure A.9 – CSRF Defence

```
<form id="changePasswordForm" action="src/actions/change_password.php" method="post" style="display:none;">
  <input type="hidden" name="csrf_token" value="<?php echo generateCsrfToken(); ?>">
  <div class="form-group">
    <label for="new_password">Новый пароль:</label>
    <input type="password" id="new_password" name="new_password" class="form-control">
  </div>
  <button type="submit" class="btn btn-primary" id="savePasswordButton" disabled>Сохранить пароль</button>
</form>
```

Figure A.10 – CSRF Defence

```
5 $user = currentUser();
6 $new_password = $_POST['new_password'] ?? '';
7 $csrf_token = $_POST['csrf_token'] ?? '';
```

Figure A.11 – CSRF Defence