УДК [004.56+003.26] (075.8)

Stud. Mateusz Wojno
Supervisor prof. P. Urbanovich
(the John Paul II Catholic University of Lublin, Poland)

INCREASED SECURITY "SOCIAL NETWORK" WEB-APPLICATION WITH MYSQL DATABASE

The security problem is one of the most important in the development and operation of information systems [1]. The aim of the work is to analyze the basic methods and technologies of creating safe web applications and, on the basis of this analysis, create an original web application for the Social Portal. The client-server model is an architecture based on the division of roles. The client's task is to request access to a given service. The server's job, on the other hand, is to offer resources. The advantage of the client-server model is that all data is stored on the server, which results in better data security. On the other hand, the disadvantage of such a model is that the server receives a large number of requests from clients, which causes bandwidth and technical problems. E-mail servers, web servers and application servers are based on the client-server model [2].

The first step in creating a web application is designing it. The UML language is used for this. In UML we can create 13 diagrams. They are divided into 3 main groups. The first group includes diagrams that represent the static structure of the application. The second group consists of diagrams responsible for the application's behavior. Includes use case diagram, activity diagram, and state machine diagram. The last group includes diagrams corresponding to the interaction. These are the sequence diagram, communication diagram, timing diagram, and interaction overview diagram [2]. After designing the application, you need to create a backend layer. The most popular language is PHP. The PHP language powers tools such as Laravel, Drupal, and Word Press. In order to speed up the work, you can use the most popular PHP framework; Laravel. The final step is to create the frontend layer. Technologies such as HTML, CSS, Bootstrap or JavaScript are used for this.

Databases are the most important component of applications [3]. That is why databases are subject to various attacks. The first type of attack is SQL-Injection. It involves injecting malicious code using the input field of a web application. Athens is very dangerous because a hacker can do damage such as deleting a database or stealing data from a database. To prevent SQL-Injection attacks, you should validate the input data, use specially prepared statements or stored procedures [4].

Fig. 1 shows the SQL-Injection attack. The question should return a row with the login name 'admin'. However, the attacker wrote the malicious code 'OR' 1 '=' 1 ', which will cause the query to always return all the rows from the table as 1 is always 1.

```
$query = "SELECT * FROM user where login = 'admin' OR '1' = '1'";
```

Figure 1 – SQL-Injection attack

Another type of attack is the XSS (Cross-site-scripting) attack. This attack consists in entering code such as HTML, CSS or JavaScript in the input field. There are three types of XXS attacks; reflected, stored and DOM based. In order to prevent this type of attack, you should perform a detailed validation of all input fields of the system [5]. Fig. 2 shows a stored XSS attack carried out using JavaScript. After publishing a post that contains malicious code, any user entering the page where the post is published will execute the malicious code. In this case, an alert will be displayed.

```
<script>alert('This is XSS attack')</script>
```

Figure 2 – XSS attack

It is also worth mentioning the attacks of the Distributed Denial of Service. Its purpose is to drain the server's resources by sending data packets across multiple computers. According to CISCO Visual NetwortingInex, the number of DDoS attacks will increase every year.

The main function of the portal is communication between users. Six technologies were used to create the application. HTML elements were styled with SASS. Bootstrap made the application fully responsive. A MySQL database was used for data storage. The main technology used in the application is PHP. With its help, the entire application logic was based. The application also uses JavaScript language to dynamically create content on the website.

The structure of portal consists of five modules. The first module is called "*Logging and registration*". It enables to get a registration and a logging. The data provided during registration are put into the database in the users table, where they will later be used for the proper functioning of the application. When logging in, it is first checked whether the given login exists. If it exists, the password is checked. If the password matches the login, the user is redirected to the main page. All posts and photos will be displayed on the home page, but only people who are in the group of friends. In the top menu, the user has five options to choose from. On the left side, it can search for other users. Then he has the option to go to his main profile. On the main profile page, basic information about the user is displayed

on the dashboard, such as photo, first name, surname, date of birth, telephone number, etc. Below the board is a form where you can post on your own timeline. Posts can be rated, commented and shared. t should be noted that the user can only comment on his own posts. The user also has the option to send an invitation to a group of friends to each user. The user receiving the invitation has two options to choose, decline the invitation or accept. You can send messages to people who are among your friends. The conversation module is used for this. In addition to posting, the user can also add photos. As in the case of posts, he can rate or comment on photos. In addition, the user can select a photo from among his / her photos and set it as a profile photo. In the upper right corner there is an option where you can change settings such as personal data or password. It is also possible to delete the account. If the user wants to leave the portal, he should press the "log out" button.

During the development of the application, special attention was paid to the security of the application. The focus was on two types of attacks; XSS and SQL-Injection. In order to protect the application against XSS attacks, a detailed validation of all input fields in the application was performed. To avoid SQL-Injection attacks, the PDO library offered by PHP was used. This library minimizes the chance of a successful SQL-Injection attack to a minimum. The application was developed in three stages. In the first stage, the application was designed using UML diagrams. Then a backend layer was created. The main language used here is PHP. Finally, the frontend layer was implemented.

From the above analysis, it can be concluded that creating a web application is a long and complicated process. The analysis suggests that the most important issue when creating a web application is application security.

REFERENCES

1. Ochronainformacji w sieciachkomputerowych / pod red. prof. P. Urbanowicza. – Lublin: Wydawnictwo KUL, 2004. – 150 s.

2. Kliet-serwer, URL: https://pl.wikipedia.org/wiki/Klient-serwer, [access: 10.03.2021].

3. Urbanowicz, P. Bazydanych: teoriaipraktyka / PawełUrbanowicz, Marcin Płonkowski, Dmitry Urbanowicz. – Lublin: KUL, 2010. – 382 s.

4. Gupta R., Kamra R. Web Security against SQL Injection Attack. – Munich:BookRix GmbH &Ko, 2019.

5. Gupta B. B., Chaudhary P. Cross-Site Scripting Attacks: Classification, Attack, and Countermeasures. – CRC Press, 2020.