

Personal data security techniques in e-education

Firudin Aghaev¹, Gyulara Mamedova², Rena Melikova³
 AMEA, Institute of Information Technologies, Baku, Azerbaijan
 gyula.ikt@gmail.com, rena22@rambler.ru, lalamaillala@bk.ru

Abstract: In recent years, the popularity of electronic education is gaining momentum. In this regard, there is a problem of ensuring its safety, which should be carried out using safety methods and internationally recognized standards. This article identifies various problems of personal data security in electronic education and suggests solutions to ensure the protection of educational information.

Keywords - ELECTRONIC UNIVERSITY, PROTECTION OF EDUCATIONAL INFORMATION, CROSS-SITE SCRIPTING, SQL ATTACK, SECURE AUTHENTICATION, DIGITAL SIGNATURE

1. Introduction

The institution uses a variety of information that requires protection. This is the personal data of students, teachers, administration and other categories of users. This also includes information constituting a commercial secret of the university (educational programs and study materials, results of research work, etc.), which allows it to stay ahead of other universities in the field of providing better education, more advanced teaching methods, and better educational programs.

Research and consulting company Gartner [1], specializing in information technology markets, predicts that the cost of information security in the world will exceed \$ 124 billion in 2019 and will affect various segments, such as identity and access management (IAM), identity governance and administration (IGA) and data loss prevention (DLP).

Compliance with security requirements in the e-learning system is an extremely difficult problem, because it is necessary to protect content, services and personal data not only for external users, but also for internal users, including system administrators. The training system should implement security services such as authentication, encryption, access control, data integrity, content protection and user management. In this article, we will look at some key security issues that need to be considered when designing and using e-learning.

2. Electronic university information security system

The main methods for ensuring the security of information in electronic education are [2-4]:

- Organizational remedies. Used to restrict access (excludes access to information of unauthorized persons); access control - the separation of information into parts and the organization of access to it in accordance with the functional responsibilities and authority of the user; access control - determining the authenticity of a subject who has access to information.

- Hardware protection. These include protection against server malfunctions, protection against malfunctions of information storage devices, protection against information leaks, electromagnetic radiation.

- Software protection - to identify technical devices and programs that pose a danger to the normal functioning of electronic education.

A secure training platform should include the following key aspects of security:

- the availability of training information (the ability to obtain the required information in a reasonable amount of time);
- integrity (protection of educational content from destruction and unauthorized changes);
- confidentiality (protection of personal data, educational content and system management from unauthorized access).

The main elements of the implementation of threats to educational data in the computer network of the university can be

objects or entities that create these threats, the communication environment for the distribution of personal data, media (a material object in which personal data is reflected in the form of text, video and sound information).

Data security is closely related to the integrity of programs and operating systems. If the integrity of the operating system is violated, then the control monitor may stop working properly. A control monitor is a mechanism that ensures that only authorized entities can access data and perform operations. Obviously, information security cannot be guaranteed if the mechanism for checking and restricting access to data does not work. For this reason, in order to protect the data itself, it is important to protect the integrity of the operating systems. [5].

Secure authentication is required to identify the user and determine their access rights when using web applications. This mechanism does not allow attackers to gain access to another user's account, view confidential information or perform unauthorized operations. In addition, after authentication, the user should be able to change his password

Access control during authentication restricts access to the system of unauthorized users and allows the user to perform only their allowed operations in the system (administrator, editor, instructor, student, registered user, unregistered user, etc.).

3. Methods of protection of educational information in electronic education

When introducing an e-learning system in an educational institution, it should be checked for external intrusion problems, such as:

- Cross-Site Scripting XSS;
- Remote injection using a virus / trojan file;
- SQL injection to the site address (URL SQL injection);
- Hacking passwords using decryption systems;
- Guessing the identifier of the website session (session forecast).

Cross-Site scripting is one of the most common application level web attacks. XSS is usually intended for scripts embedded in the page, which are executed on the client side (in the user's web browser) [6-8]. XSS itself is a threat caused by the weakness of the Internet security of scripting languages. The concept of XSS is to manipulate client-side scripts on a web application so that they run as an attacker wants them to.

Such manipulation can embed a script in a page, which can then be executed each time the page is loaded, or whenever the corresponding event is executed. An XSS attack can be used to achieve the following objectives:

- access to confidential information;
- identity theft;
- change browser functionality;

- damage to web applications;
- denial of service.

Figure 1. shows the most vulnerable areas of the spread of threats to educational data in the computer network of the university [9].

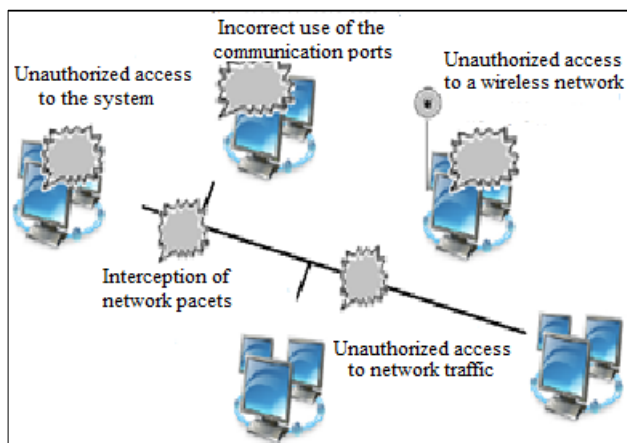


Fig. 1. The most vulnerable places in the computer network of the university for the spread of threats to educational information.

Denial of service means that the user (student or teacher) cannot perform the corresponding actions in the system. Suppose a teacher deletes his student's exam results. In this case, it should be possible to track who deleted them using some script file. These script files must be reliable and tamper-proof. An audit mechanism is used to fulfill this requirement.

To prevent such an attack, it is necessary that the developer of the e-learning platform ensures the safety of using the web page so that the pages on the website return user data only after checking for malicious code. It is necessary to make extensive use of testing tools at the design stage in order to eliminate the possibility of XSS attacks in e-learning applications before they are put into operation.

The next type of attack is SQL attack [10-12]. Using this attack method, hackers inject SQL queries or characters into a web application in order to gain unauthorized access to the database. Such requests may result in access to unauthorized data, bypassing authentication. This threat can be avoided by strictly following some basic coding practices. The most common methods to prevent this vulnerability are:

- checking when entering user SQL queries for dangerous characters, for example, single quotes;
- encryption of confidential data;
- ensuring that error messages do not notify unwanted users about the internal architecture of the application or database.

An SQL attack can also be applied to URLs [13], which can be modified by an attacker to access sensitive information. To prevent this, it is advisable to avoid sending important parameters to the URL. This is achieved by transmitting a unique and hard to guess value of the identifier (session identifier), which the browser sends with each new request either to the cookie or to the URL. Sessions are a way to store state and user variables for subsequent page requests. The session is alive as long as the browser continues to send an identifier with each new request. Session prediction means guessing a valid session identifier using various tools and methods (e.g. brute force technique). An attack is possible when the session identifier is weakly encrypted, too short, or assigned sequentially.

Sessions that do not expire on the HTTP server can allow an attacker to guess or try out a valid authenticated session identifier for an unlimited amount of time and ultimately gain access to that user's web accounts. In addition, the session identifier can be

registered and cached on proxy servers. When transmitted via URLs, GET requests can be stored in browser history, cache and bookmarks that can be seen. To prevent session security issues, you should follow these guidelines:

- The session identifier should be long enough and unpredictable;
- verify the correctness of the session identifier;
- avoid the option "remember me" (permanent logins);
- stop the session when a security error is detected;
- stop the session after a period of inactivity;
- delete cookie session when the session is destroyed.

Cross-site replication, which also improves data processing speed, is a good practice for ensuring data security and integrity [14].

4. Conclusion

In this article, we described some aspects of the security of e-learning platforms and, in particular, analyzed the most important problems, such as Cross-site Scripting, SQL attacks, password cracking, etc. The development of e-learning systems should be carried out using safety methods and internationally recognized standards. The system must implement security services such as authentication, encryption, access control, manage users and their permissions. Data transfer between the system and administrators or content operators must be done via encrypted SSL channels through the web administration interface.

5. References

- [1] <https://www.gartner.com/en/newsroom/press-releases/2018-08-15-gartner-forecasts-worldwide-information-security-spending-to-exceed-124-billion-in-2019>.
- [2] V.V. Gafner, *Informazionnaya bezopasnost / V.V. Gafner. - M.: Feniks, 2017. 336 s.*
- [3] P.P.Urbanovich. *Informazionnaya bezopasnost i nadejnost sistem - Minsk: BGTU, 2007. 90 s.*
- [4] A.V.Vasilkov. *Bezopasnost I upravleniye dostupom v informazionnix sistemax / A.V.Vasilkov, I.A. Vasilkov. - M.: Forum, 2017. 368 s.*
- [5] G. Gagne, P. B. Galvin, A. Silberschatz? *Operating System Concepts, Publisher: John Wiley & Sons, 2012, p. 312.*
- [6] Z.A.Nosirov, I.M.Ajmutexamedov. *Obnaruzheniye XSS-uyazvimostey na osnove analiza polnoy karti web-prilojeniya. Sistemi upravleniya, svyazi I bezopasnosti. №1, 2018, s. 78-92.*
- [7] S. Fogie, J. Grossman, R. Hansen, A. Rager, P.Petkov. *XSS attacks: Cross Site Scripting exploits and defense - Seth Fogie, Oxford: Elsevier Limited, 2007. 448 p.*
- [8] M. Denis, C. Zena, T. Hayajneh, "Penetration Testing: Concepts, Attack Methods, and Defense Strategies", ISBN: 978-1-4673-8490-2, DOI: 10.1109/LISAT. 2016.
- [9] Zashita informazii i nadejnost informazionnix sistem "Beloruskiy gosudarstvenniy texnologicheskiy universitet". *Metodicheskiye ukazaniya i kontrolniye zadaniya dlya studentov, Minsk, 2012.*
https://elib.belstu.by/bitstream/123456789/3372/1/zashhita-informacii-i-nadezhnost_-urbanovich-dlya-z.o.o.pdf.
- [10] K. Ahmad, J. Shekhar, K.P. Yadav. *Classification of SQL Injection Attacks. VSRD Technical & Non-Technical Journal Vol. I (4), 2010, pp. 236-242.*
- [11] Maraj, G.Jakupi, E.Rogova, Xh.Grajqevci, "Testing of network security systems through DoS attacks", "Mediterranean Conference on Embedded Computing (MECO 2017), IEEE/Scopus conference, Montenegro, June 2017.
- [12] Z. S. Alwan , M. F. Younis. *Detection and Prevention of SQL Injection Attack: A Survey. International Journal of Computer Science and Mobile Computing, Vol.6 Issue.8, August- 2017, pp. 5-17.*
- [13] J. Clarke. *SQL Injection Attacks and Defense. Elsevier, 2012, p.761.*
- [14] D.M. Romanenko. *Osnovi setevogo administrirovaniya. Minsk: BGTU, 2015. 135 s.*