Security threats and methods of protecting websites of paid educational services of educational institutions

A.R. Gazizov[1*], *E.R.* Gazizov[2], and *S.E.* Gazizova[3]

[1] Don State Technical University, Rostov on Don, Russia
[2] Kazan state agrarian University, Kazan, Russia
[3] Kazan (Volga region) Federal University, Kazan, Russia

Abstract. With the increase in the number of paid educational services of educational institutions, the percentage of fraudulent actions committed, both in relation to web services and in relation to service purchasers, also increases. Therefore, all participants in the process of banking transactions, i.e. the totality of operations that accompany remote interaction between the user and the payment system, must be protected from such actions, which determines the introduction and development of anti-fraud technologies used in the virtual space of the global Internet. Errors in the protection of websites, including websites of paid educational services of educational institutions, continue to be one of the most common shortcomings in ensuring the protection of information. Such errors, i.e. vulnerabilities, are exploited by attackers who attack websites in order to steal valuable information. It also increases the likelihood of subsequent penetration into the corporate information systems of educational institutions. Therefore, there is a need to use specialized tools and methods to protect web applications.

1 A problem statement

An analysis of research conducted by the analytical center PT Research, as well as the company PositiveTechnologies, which conducts penetration tests and information security audits, shows that errors in the protection of websites, including websites of paid educational services of educational institutions, continue to be one of the most common shortcomings in ensuring information protection. Such errors, i.e. vulnerabilities, are exploited by attackers who attack websites in order to steal valuable information. It also increases the likelihood of subsequent penetration into the corporate information systems of educational institutions.

The most common threats to the security of websites are:

1) Cross-site scripting (XSS attacks). Cross-site scripting is one of the types of attacks on web systems, which involves the introduction of malicious code on a specific page of the site and the interaction of this code with a remote server of attackers when the user opens the page.

* Corresponding author: prof-ped.gpa@mail.ru

2) SQL injection. The essence of this attack is the introduction of arbitrary SQL code into the data (transmitted via GET, POST requests or Cookie values) in order to gain access to the site database.

3) No exception handling. An exception is the result of executing an incorrect statement that resulted in an error.

4) Cross-site request Forgery (CSRF) is a type of attack that exploits the shortcomings of the HTTP protocol. When the browser opens a page, it executes malicious code that forces it to send a certain request to the attacker's server (for example, under the guise of uploading an image), and thereby performs certain actions that the attacker needs.

5) Remote code Execution (RCE) is a computer vulnerability in which remote code execution occurs on a hacked computer, server, etc. Such a vulnerability is the maximum threat of class A1 according to the classification of the open web application security project OWASP, which means it is a guaranteed way to hack sites and web applications. RCE attacks are among the most dangerous vulnerabilities.

6) Attacks on the authentication process. One of the most prominent representatives of such attacks is bruteforce. Bruteforce (brute force attack) is a method for solving mathematical problems, the complexity of which depends on the number of all possible solutions. The term bruteforce is usually used in the context of hacker attacks, when an attacker tries to find a username/password for an account or service.

7) DDoS attacks-distributed network attacks, which are also called distributed denial of service attacks (from the English Distributed Denial of Service, DDoS). This type of attack uses certain bandwidth limitations that are typical for any network resources.

8) The result of successful implementation of security threats to web applications and malicious attacks can be the leakage or destruction of confidential data, infection of users ' computers with malicious software, unavailability of services, financial and reputational losses.

1.1. The objective of the work

A significant part of all websites on the Internet are the websites of paid educational services of educational institutions. In addition to all these problems, they also have an acute problem of fraud with bank cards.

Thus, the volume of unauthorized transactions using payment cards in 2020 increased by 44 percent, to 1.38 billion rubles, the number of such transactions increased by almost a third: criminals 417 thousand times managed to get money from individuals in different ways.

Fraud with bank cards, the so-called fraud (from the English fraud), becomes possible due to the use of the data of a bona fide client by fraudsters, due to their theft through phishing, skimming, click jacking, direct data leakage:

Phishing-a type of Internet fraud, which is an illegal act committed in order to force a person to share their confidential information, such as a password or credit card number. Often, such fraud looks like fake notifications from banks, providers, payment systems and other organizations that for some reason the recipient urgently needs to transfer or update personal data.

Skimming – a type of fraud with bank cards, representing criminal actions, which consists in the fact that hidden devices are installed in ATMs that allow reading information from payment cards during the transaction.

Click jacking is a fraudulent technology for deceiving Internet users, based on the fact that on the page, in addition to visible elements, there are invisible ones. Invisible buttons, links are placed on top of visible buttons and links – in places where users click. Accordingly, the click is an action that the user did not expect and which should not have

been. This technique can be used, for example, to collect personal data of site visitors without their knowledge.

In online sales of educational services, it is the educational institution that suffers the most from this kind of fraud, because if its protection is insufficient and such transactions occur more than 1%, then the payment system can blacklist this website and stop providing money transfer, or apply any sanctions.

Such vulnerabilities should be detected and fixed at the stage of website development: static, dynamic, interactive analysis should be carried out, and anomalies in the application logic should be detected.

2 Results of the research

However, only manual detection and elimination of vulnerabilities, as well as tracking fraudulent transactions in the site or application for paying for educational services, also often does not give positive results – the development team can find and fix thousands of vulnerabilities, but an attacker needs to detect just one to conduct a successful attack. Therefore, there is a need to use specialized tools and methods to protect web applications.

Thus, protection should be based on three main areas:

1) Avoiding errors in the code when developing a website. This can be achieved by special techniques for writing and testing program code, such as in Future Driven Development or Extreme Programming.

2) The use of specialized technologies and mechanisms to prevent possible external attacks, such as application-level firewall, intrusion detection system (solutions such as ApplicationFirewall), intrusion detection system (network level and node level), Anti-DDoS system, antivirus, cryptographic package for encryption. Such technologies have built-in intrusion prevention and prevention functionality and provide protection against targeted web attacks, such as buffer overflows, SQL injection, Css-Site-Scripting, changing query parameters, and others. Solutions of this class filter requests for access to the application and block all actions that are not related to the allowed user activity. It is also recommended to use a specific password policy and conduct regular audits of the website components.

3) Use of special technologies and services to filter out fraudulent transactions.

In the selected areas, an integrated approach should be used to solve the problems of protection against fraud threats, unauthorized access to user payment data and protection against web application vulnerabilities.

A method for protecting paid educational service websites from fraudulent transactions

This method requires the use of additional technologies that can be used to identify and distinguish the real buyer of the service from the fraudster.

The most common ways to protect against bank card fraud are 3-D Secure technology and fraud monitoring (anti-fraud) systems.

3-D Secure (Three-Domain Secure) is an XML user authorization protocol for securing online payments using bank cards, developed in 1999. For the first time, such a protocol appeared in the international payment system VISA and is called Verified by Visa, after which a similar protocol appeared in other payment systems with some changes.

"3D "means" 3 domains " in which the protocol works, and which include the issuer's domain (the domain of the bank that issued the card), the acquirer's domain (the domain of the seller and the bank to which the money is transferred) and the compatibility domain (the domain provided by the payment system to support the 3D Secure protocol).

3-D Secure technology is essentially a two-factor authentication of the cardholder, which allows the bank and the online store to make sure that the transaction is made directly by the cardholder. It is carried out in such a way that after entering the card data,

the buyer is sent for additional verification by the issuing bank. The check can be implemented as:

1) Introduction of the security code that was sent in the sms message.
2) One-time code card or device (token).
3) Can be permanent, set by the user himself.

The main advantage of this technology for a trade and service company is that all responsibility for the transactions is transferred to the issuing bank, as well as the fact that it does not need to spend resources on the development and implementation of its own fraud protection technologies, since 3-D Secure is a third-party service of international payment systems and requires only the correct connection to the online store.

But it is worth considering that adding such steps that require additional actions from the user in some cases leads to a decrease in the number of successfully completed transactions. Studies conducted in the United States have found that the number of pending transactions can exceed 50% due to 3-D Secure authorization. In Russia, this problem is not so acute and the number of successfully completed transactions is reduced by only 20-25%.

An alternative or addition to the 3-D Secure technology can be fraud monitoring of the system.

Fraud monitoring (anti-fraud) system – an automated system designed to evaluate financial transactions on the Internet for suspicion from the point of view of fraud and offer recommendations for their further processing. It checks each payment in real time, running them through filters for compliance with certain requirements.

Fraud monitoring systems filter fraudulent transactions based on the collected information about the buyer, for example, data about the browser and operating system, country and city of residence, email address, first and last name of the payer, etc. With its help, filters are created, with the help of which the anti-fraud system detects fraudulent transactions. It checks the legality of the transaction by many parameters in the form of filters, ranging from the behavioral factors of the buyer and ending with the technical aspects of a particular order, thus minimizing the risk of fraud with bank cards. The most popular filters are such filters as validator filters, geographic filters, stop list filters, parameter match filters, authorization limit filters, and so on.

These filters can be divided into global and local filters. Global filters are black lists of bank cards, IP addresses, regions and countries where plastic card fraud is common. Statistics show that some African countries have a high level of card skimming and compromise, and as a result, payments made from these countries are highly likely to be fraudulent. If the transaction profile contains information related to the stop list, any further checks are stopped and the transaction is rejected.

If this transaction passes global checks, it goes to the stage of checking by local filters. These are customizable filters-conditions for specific merchant tasks.

The advantage of an anti-fraud service is determined by its ability to quickly and with the maximum degree of probability recognize a fraudster. Another advantage of fraud monitoring is the ability to evaluate the behavior of the buyer during the payment process based on the behavior patterns of other users.

However, the creation and implementation of anti-fraud systems against the background of 3-D Secure technology is quite expensive, but they are more advantageous because they do not require any additional actions from the buyer, which means a large number of completed transactions.

The process of education informatization is characterised by active information and communication technologies usage of increased criticality and high interactivity. This creates a whole range of new security threats that the standard methods of protecting websites may not be able to handle. This proves once again that protecting an online store from web vulnerabilities requires a comprehensive approach.

This approach consists of several points:

1) Choosing a reliable provider.
2) Implementation of a content management system.
3) Create a password policy.
4) Application-level security.
5) Use of cryptographic packages.
6) Security audit.

One of the initial requirements is to choose a reliable hosting provider. Important aspects of choosing a hosting provider are maintaining regular backups, maintaining comprehensive activity logs, and monitoring network activity on their part. Also, one of the important factors is the system of notifications about abnormal actions on the account, possible infection of the site, etc.

The best way to implement the administration of an online store is to implement a content management system.

A content management system is an information system used to support and organize the collaborative process of creating, editing, and managing content. This system allows you to limit the administrative zone, automatically update plugins and modules to maintain their current versions, and also allows you to actively use additional mechanisms for data protection, such as a firewall, an anomaly detector, an attack blocker, etc. (Figure 1).

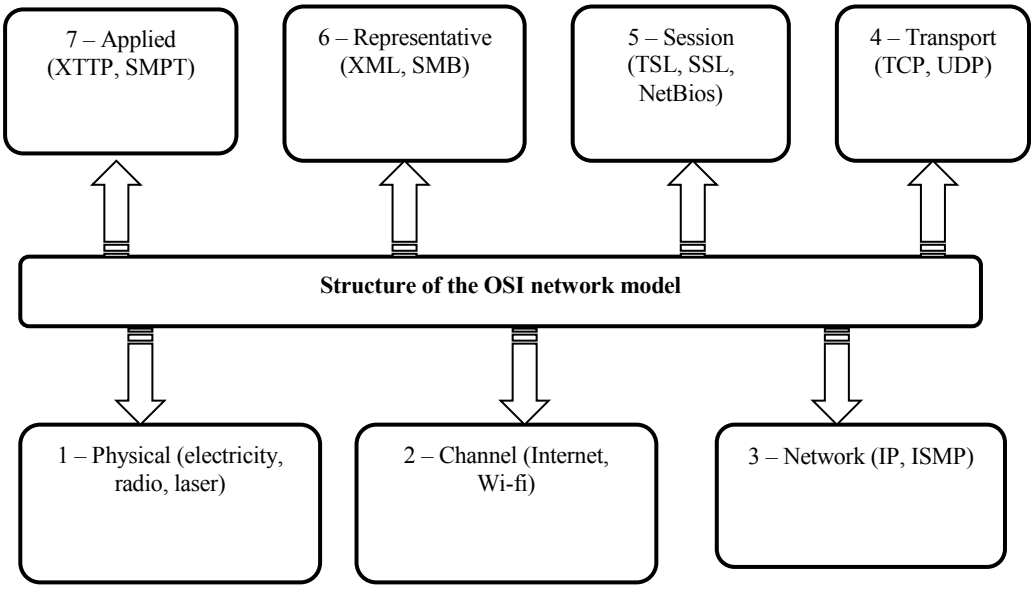

Fig 1. Structure of the OSI network model.

A strong password policy must also be implemented – it is necessary to use complex combinations with the definition of the minimum length when creating a password to protect user data. However, every year the computing power is growing and just a password is not enough, even if it is complex. To increase the security of user data, it makes sense to implement two-factor authentication.

The password policy of the technical staff (site administrators) should be even stricter – in addition to certain requirements for password generation, it is necessary to carry out routine procedures for changing passwords. It is also necessary to delete unused accounts, change passwords after the dismissal of key employees.

Undoubtedly, one of the key tasks is also the protection of the protocols of the application layer of the OSI network model (Figure), which implements the interaction of the network and the user, i.e., the use of the "client-server" architecture.

The main principle of site protection at the application level is verification and filtering of request data transmitted by the GET, POST, etc. methods. Spoofing or modifying a request is the basic basis for almost all methods of hacking and attacks on websites.

It is also advisable to use the secure data transfer protocol HTTPS, which supports encryption of the transmitted data by the cryptographic protocol TLS (Transport Layer Security), instead of HTTP.

For external protection of this layer, the application layer firewall is used.

A Web Application Firewall is a special mechanism that imposes a certain set of rules on how the server and client interact with each other when processing HTTP packets. This technology is based on a set of rules that detect the fact of an attack by signatures – signs of user activity that can mean an attack.

It is also necessary to use a cryptographic package to encrypt personal data in the event that an attacker is still able to bypass the firewall and gain unauthorized access to the database of the educational institution. The attacker will not be able to use the encrypted data for their own purposes without the use of cryptanalysis tools and a lot of time.

The last but not least important point in ensuring the protection of a website is a security audit.

3 Conclusions

Information security audit is a study and assessment of the current state of security and security of information resources and corporate systems of an organization, for compliance with certain standards. Information security audit allows management to see the real state of information assets and assess their security.

A routine procedure (for example, once a quarter) for conducting an information system security audit allows you to assess the maturity of the information security management system and identify vulnerabilities for their prompt elimination. One of the main stages is conducting external Blackbox penetration testing, i.e., checks are implemented without using authentication and any other information about the web application.

An analysis of research conducted by the analytical center PT Research, as well as the company PositiveTechnologies, which For websites that operate with payment data and process online transactions, there are specialized requirements for compliance with the PCI DSS standard. Payment Card Industry Data Security Standard (PCI DSS) is a payment card industry data security standard developed by the Payment Card Industry Security Standards Council (PCI SSC), established by the international payment systems Visa, MasterCard, American Express, JCB and Discover. The standard is a set of 12 detailed requirements for ensuring the security of data about payment card holders that are transmitted, stored and processed in the information systems of educational institutions. There are 4 levels of certification for institutions.

If more than one million transactions are processed per year, then it belongs to the first or second level. If the annual total number of transactions is less than one million, then this is the third or fourth level. Depending on how the card numbers are processed in the store's information systems, there are four types of SAQ self-assessment sheets:

1) SAQ type A is used if the store has given the processing of payment data to a certified service provider and does not participate even in their transfer.

2) SAQ type B is used if the store transmits payment data to the service provider exclusively via a telephone line, without using the Internet, and also does not have electronic card data stores.

3) SAQ type C is used if the store transmits payment data through its systems and does not have electronic card data stores.
4) SAQ type D is used if the store itself stores and processes payment data.

So, depending on the type of self-assessment sheet, the number of tests for certification will depend – from 13 to 288. All of them are divided into 12 groups:

1) Protection of the computer network.
2) Configuration of information infrastructure components.
3) Protection of stored cardholder data.
4) Protection of transmitted cardholder data.
5) Anti-virus protection of the information infrastructure.
6) Development and support of information systems.
7) Manage access to cardholder data.
8) Authentication mechanisms.
9) Physical protection of the information infrastructure.
10) Logging of events and actions.
11) Monitoring the security of the information infrastructure.
12) Information security management.

The audit is performed by an auditor with the status of QSA (Qualified Security Assessor).

However, just getting a PCI DSS certificate is not enough. Further, during the entire existence of the institution, regular confirmation of compliance with this certificate is required. It is necessary to pass such certification every year.

International card payment systems have their own requirements for it (Table). If a paid educational services website belongs to level 1 or 2, then it must pass an external QSA or internal ISA audit annually, for level 3 or 4, it will be enough to fill out the SAQ self-assessment sheet. Regardless of the level, it is necessary to conduct an external vulnerability scan of the ASV (Approved Scanning Vendor) information infrastructure components on a quarterly basis (Table 1).

Table 1. PCI DSS Compliance Confirmation.

Level	Criteria (per year)	PCI DSS Compliance Confirmation	
		MasterCard	Visa
Level 1	More than 6 million transactions	AVS quarterly, QSA or ISA annually	AVS quarterly, QSA or ISA annually
Level 2	From 1 to 6 million transactions	AVS quarterly, QSA or ISA annually	AVS quarterly, SAQ annually
Level 3	From 20 thousand to 1 million. transactions	AVS quarterly, SAQ annually	AVS quarterly, SAQ annually
Level 4	All the others	AVS quarterly, SAQ annually	AVS quarterly, SAQ annually

Without passing the required certifications, the website of paid educational services does not have the right to operate with the payment data of counterparties.

In Russia, there are also additional legal restrictions, such as Federal Law No. 152-FZ "On Personal Data", according to which the buyer's personal data and payment data must be concealed.

Also, in accordance with this law, three documents must be posted on the websites of paid educational services:

1) User Agreement.
2) Privacy Policy.
3) Public offer for online transactions.

According to the law, the signing of a contract for the processing of personal data must precede their acceptance.

References

1. A.I. Zotov, V.V. Gritsenko, A.V. Cherpakov, Engineering Bulletin of the Don, **4** (2018) ivdon.ru/uploads/article/pdf/IVD_156N4y18_Gricenko.pdf_935280522c.pdf
2. A.I. Zotov, V.V. Gritsenko, Engineering Bulletin of the Don, **1** (2019) http://www.ivdon.ru/uploads/article/pdf/IVD_144_Zotov_N.pdf_5ce4a02e25.pdf
3. Khattab, A. Abdelgawad, K. Yelmarthi, *Int. Conf. on Microelectr (ICM)*, 201-204 (2016)
4. M. Dholu, K.A. Ghodinde, *Int. Conf. on Trends in Electr. and Inform (ICOEI)*, 339-342 (2018)
5. M.R. Yousefi, A.M. Razdari, Int. J. of Advanc. Biolog. and Biomed. Res, **2(4)**, 473-476 (2014)
6. R. Inglés, P. Perek, M. Orlikowski, A. Napieralski, *Mixed Design of Integrated Circuits & Systems (MIXDES)*, 153-157 (2015)
7. G. Craessaerts, J. De Baerdemaeker, W. Saeys, *Biosystems Engineering*, 106, 26-36 (2010)
8. D.D. Bochtis, C.G.C. Sørensen, P. Busato, *Biosystems Engineering,* 126, 69-81 (2014)
9. Z. Zhai, J. Fernán Martínez, V. Beltran, N. Lucas Martínez, *Computers and Electronics in Agriculture*, 170 (2020)
10. B. Drury, R. Fernandes, M.-F. Moura, A. de Andrade Lopes, Information Processing in Agriculture, **6**, 487-501 (2019)
11. H. El Bilali, M. Sadegh Allahyari, Information Processing in Agriculture, **5**, 456-464 (2018)
12. R. Miodragović, M. Tanasijević, Z. Mileusnić, P. Jovančić, Expert Systems with Applications, **39**, 8940-8946 (2012)
13. D. Bochtis, C. Aage Gron Sorensen, D. Kateris, *Operations Management in Agriculture*, 79-115 (2019)
14. Ronkainen, IFAC Proceedings, **46**, 259-263 (2013)
15. Chen Chu, Zhao Zuo-xi, K.E. Xin-rong, Guo Yun-zhi, IFAC-PapersOnLine, **51**, 346-352 (2018)
16. J.W. Jones, J.M. Antle, B. Basso and others, *Agricultural Systems*, 155, 269-288 (2017)
17. S. O'Neill Somers, L. Stapleton, IFAC-PapersOnLine, **48**, 213-218 (2015)