Методы обеспечения безопасности персональных данных в электронном образовании

Гюляра Мамедова[1], Лала Зейналова[2], Рена Меликова[3]
[1,2,3]Институт Информационных Технологий НАНА, Баку, Азербайджан
[1]*gyula.ikt@gmail.com*, [2]*lalamaillala@bk.ru*

***Аннотация*— В последние годы популярность электронного образования набирает обороты. В связи с этим возникает проблема обеспечения его безопасности, которая должна осуществляться с использованием методов безопасности и международно-признанных стандартов. В этой статье определены различные проблемы безопасности персональных данных в электронном образовании и предложены решения по обеспечению защиты учебной информации.**

Ключевые слова— электронный университет, защита учебной информации, межсайтовый скриптинг, SQL атака, безопасная аутентификация, цифровая подпись

I. ВВЕДЕНИЕ

В высшем учебном заведении используется разнообразная информация, требующая защиты. Это – персональные данные студентов, преподавателей, администрации и других категорий пользователей. Сюда также можно отнести сведения, составляющие коммерческую тайну университета (образовательные программы и учебные материалы, результаты научно-исследовательских работ и т.д.), позволяющие ему опережать другие ВУЗы в области предоставления более качественного образования, более прогрессивных методов обучения, лучших образовательных программ.

Исследовательская и консалтинговая компания Gartner [1], специализирующаяся на рынках информационных технологий, прогнозирует, что расходы на информационную безопасность в мире превысят 124 миллиарда долларов в 2019 году и будут влиять на различные сегменты, такие как, управление идентификацией и доступом (IAM – identity and access management), управление идентификацией и администрирование (IGA – identity governance and administration), предотвращение потери данных (DLP – data loss prevention).

Выполнение требований безопасности в системе электронного обучения является чрезвычайно сложной проблемой, поскольку, необходимо защищать контент, услуги и личные данные не только для внешних пользователей, но и для внутренних пользователей, включая системных администраторов. Обучающая система должна реализовать такие службы безопасности, как аутентификация, шифрование, контроль доступа, целостность данных, защиту контента и управление пользователями. В этой статье мы рассмотрим некоторые ключевые проблемы безопасности, которые необходимо учитывать при разработке и использовании электронного обучения.

II. СИСТЕМА ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ИНФОРМАЦИИ ЭЛЕКТРОННОГО УНИВЕРСИТЕТА

Основными методами обеспечения безопасности информации в электронном образовании являются [2-4]:

- Организационные средства защиты. Используются для ограничения доступа (исключает доступ к информации посторонних лиц); разграничения доступа - разделение информации на части и организация доступа к ней в соответствии с функциональными обязанностями и полномочиями пользователя; контроль доступа – определение подлинности субъекта, имеющего доступ к информации.
- Аппаратные средства защиты. К ним относятся – защита от сбоев работы сервера, защита от сбоев устройств для хранения информации, защита от утечек информации, электромагнитных излучений.
- Программные средства защиты – для выявления технических устройств и программ, представляющих опасность для нормального функционирования электронного образования.

Безопасная обучающая платформа должна включать следующие основные аспекты безопасности:

- доступность учебной информации (возможность за разумное время получить требуемую информацию);
- целостность (защищенность учебного контента от разрушения и несанкционированного изменения);
- конфиденциальность (защита персональных данных, учебного контента и менеджмента системы от несанкционированного доступа.

Основными элементами реализации угроз учебным данным в компьютерной сети университета могут быть

DOI: 10.25045/NCInfoSec.2019.29

объекты или субъекты, создающие эти угрозы, коммуникационная среда распространения персональных данных, носители (материальный объект, в котором персональные данные находят свое отражение в виде текста, видео и звуковой информации).

Защищенность данных тесно связана с целостностью программ и операционных систем. Если нарушается целостность операционной системы, тогда контрольный монитор может перестать работать должным образом. Контрольный монитор – это механизм, который гарантирует, что только уполномоченные субъекты могут получить доступ к данным и выполнять операции. Очевидно, что защита информации не может быть гарантирована, если не работает механизм проверки и ограничения доступа к данным. По этой причине, чтобы защищать сами данные, важно защитить целостность операционных систем. [5].

Безопасная аутентификация требуется для идентификации пользователя и определения его прав доступа при использовании веб-приложений. Этот механизм не позволяет злоумышленникам получить доступ к учетной записи другого пользователя, просмотреть конфиденциальную информацию или выполнить несанкционированные операции. Кроме того, после аутентификации пользователь должен иметь возможность изменить свой пароль.

Контроль доступа во время аутентификации ограничивает доступ к системе неавторизованных пользователей и позволяет пользователю выполнять в системе только свои разрешенные операции (администратор, редактор, инструктор, студент, зарегистрированный пользователь, незарегистрированный пользователь и т. д.).

На Рис.1 представлена обобщенная схема обеспечения безопасности электронного университета.

Рис. 1. Обобщенная система обеспечения безопасности электронного университета

III. МЕТОДЫ ЗАЩИТЫ УЧЕБНОЙ ИНФОРМАЦИИ В ЭЛЕКТРОННОМ ОБРАЗОВАНИИ

При внедрении системы электронного обучения в учебном заведении она должна быть проверена на внешние проблемы вторжения, такие как:

- межсайтовый скриптинг (XSS – Cross-Site Scripting);
- удаленная инъекция с использованием файла вируса / трояна;
- SQL инъекция в адрес сайта (URL SQL инъекция);
- взлом паролей с использованием систем дешифрования;
- угадывание идентификатора сессии веб-сайта (прогноз сессии).

Межсайтовый скриптинг – одна из самых распространенных веб-атак на уровне приложений. XSS обычно предназначается для скриптов, встроенных в страницу, которые выполняются на стороне клиента (в веб-браузере пользователя) [6-8]. Сам по себе XSS - это угроза, вызванная слабостью интернет-безопасности языков сценариев. Концепция XSS заключается в том, чтобы манипулировать сценариями на стороне клиента веб-приложения, чтобы они выполнялись так, как этого хочет злоумышленник. Такая манипуляция может встраивать скрипт в страницу, который затем может выполняться каждый раз, когда страница загружается, или всякий раз, когда выполняется соответствующее событие. Атака XSS может быть использована для достижения следующих целей:

- доступ к конфиденциальной информации;
- кража личных данных;
- изменение функциональности браузера;
- порча веб-приложений;
- отказ в обслуживании.

На рис 2. показаны наиболее уязвимые участки распространения угроз учебным данным в компьютерной сети университета [9].

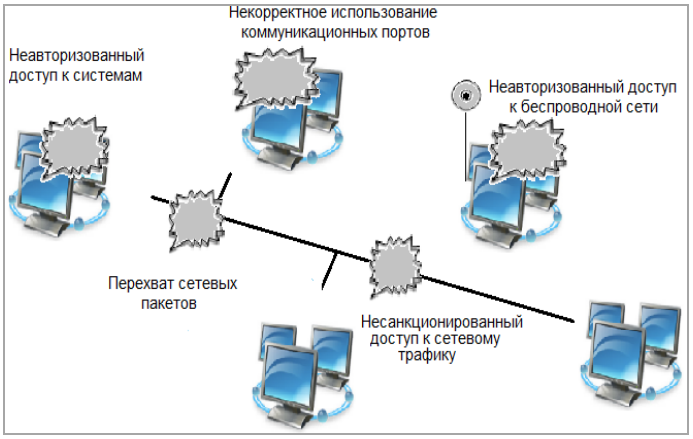

Рис.2. Наиболее уязвимые места в компьютерной сети университета для распространения угроз учебной информации.

Отказ в обслуживании означает, что пользователь (студент или преподаватель) не может выполнить в системе соответствующие действия. Допустим, что учитель удаляет результаты экзамена своего ученика. В этом случае должна предусматриваться возможность отследить, кто их удалил с помощью некоторого файла сценария. Эти файлы сценариев должны быть надежными и защищенными от подделки. Для выполнения этого требования используется механизм аудита.

Чтобы предотвратить такую атаку, необходимо, чтобы разработчик платформы электронного обучения обеспечил безопасность использования веб страницы, чтобы страницы на веб-сайте возвращали пользовательские данные только после проверки их на наличие вредоносного кода. Необходимо широко использовать инструменты тестирования на этапе проектирования, чтобы устранить возможность XSS атак в приложения электронного обучения, прежде чем оно будет введено в эксплуатацию.

Следующий вид атаки это – SQL атака [10-12]. Используя этот метод атаки, хакеры вводят SQL-запросы или символы в веб-приложение, с целью получить несанкционированный доступ к базе данных. Такие запросы могут привести к доступу к неавторизованным данным в обход аутентификации. Эту угрозу можно избежать при строгом соблюдении некоторых основных практик кодирования. Наиболее распространенные методы предотвращения такой уязвимости:

- проверка при вводе SQL-запросов пользователем на наличие опасных символов, например, одинарных кавычек;
- шифрование конфиденциальных данных;
- обеспечение того, чтобы сообщения об ошибках не уведомляли нежелательных пользователей о внутренней архитектуре приложения или базы данных.

SQL-атака может применяться также для URL-адресов [13], которые могут быть изменены злоумышленником для доступа к важной информации. Чтобы предотвратить это, желательно избегать отправки важных параметров в URL. Это достигается путем передачи уникального и трудно угадываемого значения идентификатора (идентификатора сеанса), который браузер отправляет при каждом новом запросе либо в файл cookie, либо в URL. Сеансы - это способ сохранения переменных состояния и пользователя для последующих запросов страниц. Сессия жива до тех пор, пока браузер продолжает отправлять идентификатор с каждым новым запросом. Прогнозирование сеанса означает угадывание действительного идентификатора сеанса с использованием различных инструментов и методов (например, техника грубой силы). Атака возможна, когда идентификатор сессии слабо зашифрован, слишком короткий или назначен последовательно.

Сессии, которые не истекают на сервере HTTP, могут позволить злоумышленнику неограниченное количество времени угадать или перебрать действительный аутентифицированный идентификатор сеанса и в конечном итоге получить доступ к веб-учетным записям этого пользователя. Кроме того, идентификатор сеанса может быть зарегистрирован и кэширован на прокси-серверах. При передаче через URL адреса, GET-запросы могут сохраняться в истории браузера, кэше и закладках, которые можно увидеть. Для предотвращения проблем, связанных с безопасностью сеанса, следует придерживаться следующих рекомендаций:

- идентификатор сессии должен быть достаточно длинным и непредсказуемым;
- проверить правильность идентификатора сеанса;
- избежать опции «запомнить меня» (постоянные входы в систему);
- остановить сеанс при обнаружении ошибки безопасности;
- остановить сеанс после периода бездействия;
- удалить cookie сессию, когда сессия уничтожена.

Хорошей практикой для обеспечения безопасности и целостности данных является межсайтовая репликация [14], которая также повышает скорость обработки данных.

ЗАКЛЮЧЕНИЕ

В этой статье мы описали некоторые аспекты безопасности платформ электронного обучения и, в частности, проанализировали наиболее важные проблемы, как, межсайтовый скриптинг, SQL атаки, взлом паролей и т.д. Разработка систем электронного обучения должна осуществляться с использованием методов безопасности и международно- признанных стандартов. Система должна реализовать службы безопасности, такие как аутентификация, шифрование, контроль доступа, управление пользователями и их разрешениями. Передача данных между системой и администраторами или операторами контента должна осуществляться по

зашифрованным каналам SSL через интерфейс веб-администрирования.

ЛИТЕРАТУРА

[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] В. В. Гафнер, Информационная безопасность / В.В. Гафнер. - М.: Феникс, 2017. 336 с.

[3] Урбанович, П. П. Информационная безопасность и надежность систем – Минск: БГТУ, 2007. 90 с.

[4] Васильков, А. В. Безопасность и управление доступом в информационных системах / А.В. Васильков, И.А. Васильков. - М.: Форум, 2017. 368 с.

[5] G. Gagne, P. B. Galvin, A. Silberschatz? Operating System Concepts, Publisher: John Wiley & Sons, 2012, p. 312.

[6] Носиров З. А., Ажмухамедов И. М. Обнаружение XSS-уязвимостей на основе анализа полной карты веб-приложения. Системы управления, связи и безопасности. №1, 2018, с. 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] Защита информации и надежность информационных систем «Белорусский государственный технологический университет». Методические указания и контрольные задания для студентов, Минск 2012. https://elib.belstu.by/bitstream/123456789/3372/1/zashhita-informacii-i-nadezhnost_-urbanovich-dlya-z.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] [14Романенко, Д. М. Основы сетевого администрирования. Минск: БГТУ, 2015. 135 с.

PERSONAL DATA SECURITY METHODS IN ELECTRONIC EDUCATION

Gyulara Mammadova[1], Lala Zeynalova[2], Rena Malikova[3]

[1,2,3]Institute of Information Technology of ANAS, Baku, Azerbaijan

gyula.ikt@gmail.com, lalamaillala@bk.ru

Abstact – In recent years, the popularity of e-learning is gaining momentum. In this regard, there is a problem to ensure its security, which must be carried out using safety practices and internationally recognized standards. This article identifies various security issues in e-education and proposes solutions to ensure security measures.

Key words – *e-university, educational information protection, crossite scripting, SQL attack, secure authentication, digital signature*