УДК 004.056

МЕТОДИКА ОБНАРУЖЕНИЯ УЯЗВИМОСТЕЙ ИНТЕГРИРОВАННОЙ ИНФОРМАЦИОННОЙ СИСТЕМЫ БГУИР

Матюшкин С.И.

гр. 267241

Белорусский государственный университет информатики и радиоэлектроники, г. Минск, Республика Беларусь

Научный руководитель: Петров С.Н. – кандидат технических наук, доцент

Аннотация. В материалах доклада рассматриваются результаты анализа уязвимостей программных продуктов, использованных при реализации интегрированной информационной системы БГУИР. Уязвимости в информационной системе могут привести к несанкционированному доступу к конфиденциальной информации, ее утечке или изменению. Анализ уязвимостей играет ключевую роль в обеспечении безопасности информационной системы.

Ключевые слова: ИИС БГУИР, уязвимости, CVE, модель угроз

Введение. Интегрированная информационная система (ИИС) БГУИР ориентирована на автоматизацию учебных процессов и облегчение взаимодействия сотрудников и студентов. Использование ИИС позволяет упростить учет информации о студентах, учебных группах, учебных планах специальностей. В рамках ИИС функционирует подсистема «Студенты», в которой хранятся и обрабатываются персональные данные студентов. Согласно закону Республики Беларусь от 7 мая 2021 г. № 99-З «О защите персональных данных», оператор обязан обеспечивать защиту персональных данных в процессе их обработки. Оператор обязан принимать правовые, организационные и технические меры по обеспечению защиты персональных данных от несанкционированного или случайного доступа к ним, изменения, блокирования, копирования, распространения, предоставления, удаления персональных данных. Обнаружение уязвимостей подсистемы «Студенты» ИИС БГУИР направлено на достижение этой цели.

Основная часть. Интегрированная информационная система БГУИР содержит следующие разделы: Расписание; Расписание кафедры; Подразделения; Студенты; Рейтинг; Перечень дисциплин; Телефонный справочник; Техподдержка [1].

Подсистема «Студенты» ИИС БГУИР содержит следующие разделы: Личный кабинет; Список сотрудников; Контингент; Журнал текущей успеваемости; Отчеты; Словари; Планы; Учебная нагрузка; Учебный процесс [2].

Подсистема «Кабинет сотрудника» ИИС БГУИР содержит следующие разделы: Журнал успеваемости; Объявления; Личная страница; Должности; Настройки [3].

При реализации ИИС БГУИР используются следующие технологии:

Angular. Это открытая и свободная платформа для разработки веб-приложений, написанная на языке TypeScript, разрабатываемая командой из компании Google, а также сообществом разработчиков из различных компаний [4]. В ИИС применяется для формирования интерфейса пользователя.

Spring Framework. Это универсальный фреймворк с открытым исходным кодом для Java-платформы от компании VMware [5]. В ИИС используется при реализации логики работы системы.

Docker. Это программное обеспечение для автоматизации развертывания и управления приложениями в средах с поддержкой контейнеризации от компании Docker Inc. Позволяет «упаковать» приложение со всем его окружением и зависимостями в контейнер, который может быть развернут на любой Linux-системе с поддержкой контрольных групп в ядре, а также предоставляет набор команд для управления этими контейнерами [6]. В ИИС применяется для контейнеризации Angular и Spring Framework.

PostgreSQL. Это свободная объектно-реляционная система управления базами данных (СУБД) [7]. В ИИС используется для хранения данных системы.

Nginx. Это веб-сервер и почтовый прокси-сервер, работающий на Unix-подобных операционных системах от компании NGINX Inc [8]. В ИИС применяется в качестве реверс-прокси для отделения пользователей от среды выполнения.

Одной из основный угроз информационной безопасности для интегрированной информационной системы БГУИР является угроза утечки конфиденциальной информации, например, персональных данных студентов. Также вероятной угрозой может быть нарушение доступности информационных сервисов вследствие проведения атаки типа «отказ в обслуживании» (DoS, DDoS). Зачастую отказ в обслуживании является одним из начальных звеньев цепочки действий нарушителя, приводящей к несанкционированному доступу к конфиденциальной информации и как следствие ее утечке.

Угроза может быть реализована через уязвимости в программных продуктах, аппаратном обеспечении или недостаточно защищенные базы данных.

CVE (Common Vulnerabilities and Exposures) – это база данных, которая содержит информацию о различных уязвимостях в программном обеспечении и других компонентах информационных систем [9]. Использование CVE позволяет определить потенциальные угрозы для информационной системы, а также оценить их серьезность и возможные последствия.

Процесс использования CVE включает в себя определение уязвимостей в качестве первого шага. Используя CVE, можно идентифицировать уязвимости, которые могут быть использованы нарушителями для получения несанкционированного доступа к системе или утечки конфиденциальной информации [10].

Поиск уязвимостей в базе CVE по запросу «Angularjs» показал 8 уязвимостей за период времени с 2019 по 2024 годы: CVE-2023-26118; CVE-2023-26117; CVE-2023-26116; CVE-2022-25869; CVE-2022-25844; CVE-2020-7676; CVE-2019-14863; CVE-2019-10768.

Последняя на сегодняшний день уязвимость CVE-2023-26118. Версии пакета

angular, начиная с 1.4.9 по 1.8.3, уязвимы к Regular Expression Denial of Service (ReDoS) через элемент <input type="url"> из-за использования небезопасного регулярного выражения в функциональности input[url]. Эксплуатация этой уязвимости возможна с помощью больших продуманных входных данных, что может привести к «катастрофическому возврату», ситуации при которой регулярное выражение «подвешивает» интерпретатор и потребляет 100% ресурсов процессора. Такая уязвимость относится к категории «отказ в обслуживании». Согласно рейтингу CVSS, воздействие уязвимости на доступность низкая.

Поиск уязвимостей в базе CVE по запросу «Postgresql» показал 154 уязвимости за период времени с 2002 по 2024 годы, из них 17 уязвимостей с рейтингом CVSS выше 9 (критические уязвимости). Уязвимость CVE-2024-24213, опубликованная 8 февраля 2024, имеет рейтинг 9.8 и относится к категории Sql Injection. Имеет высокое влияние на конфиденциальность, доступность и целостность. Supabase PostgreSQL v15.1 (on x86_64-pc-linux-gnu) содержит уязвимость для внедрения SQL через компонент /pg_meta/default/query.

Поиск уязвимостей в базе CVE по запросу «Spring Framework» показал 16 уязвимости за период времени с 2020 по 2024 годы, из них 3 уязвимости с рейтингом CVSS 8 и выше (критические уязвимости). Уязвимость CVE-2022-22965, опубликованная 1 апреля 2022, имеет рейтинг 9.8 с вероятностью использования 97.46% и связана с удаленным выполнением кода. Последняя уязвимость CVE-2024-22233, связанная с тем, что специально созданные HTTP-запросы могут вызвать отказ в обслуживании (DoS), опубликована 22 января 2024.

Поиск уязвимостей в базе CVE по запросу «NGINX» показал 7 уязвимости за период времени с 2022 по 2024 годы. Уязвимость CVE-2023-44487, опубликованная 10 октября 2023, имеет вероятность использования 70.59% относится к категории «Отказ в обслуживании» и связана с тем, что отмена запроса может быстро сбросить многие потоки. Эта уязвимость активно использовалась с августа по октябрь 2023.

Использование различных средств и библиотек сторонних разработчиков, особенно популярных и с открытым исходным кодом приводит к тому, что в них злоумышленниками активно ищутся и эксплуатируются уязвимости, которые могут устраняться разработчиками в течение длительного периода. Кроме этого, возникает дополнительная сложность из-за того, что после обновления средства или библиотеки, особенно если это контейнеризировано, может возникнуть несовместимость с действующим проектом и информационная система перестанет полностью или частично выполнять свои функции. Причем определение необходимых изменений в коде проекта для корректной работы может занять много времени или быть вообще невозможна. Отказ же от обновлений приводит к высокой уязвимости. Создание «тестовой» копии проекта, на которой можно было бы отлаживать изменения, крайне сложно и малоэффективно из-за невозможности создания нагрузочных условий.

Заключение. Проведен анализ уязвимостей программных продуктов, использованных при реализации интегрированной информационной системы БГУИР, с помощью открытой базы данных уязвимостей CVE. Рассмотрены примеры критичных или распространенных уязвимостей. Более полный анализ уязвимостей непосредственно ИИС БГУИР, возможен с применением сканеров уязвимостей, что возможно лишь с разрешения владельца информационной системы.

Список литературы

1. ИИС «БГУИР: Университет» [Электронный ресурс]. – Режим доступа: https://iis.bsuir.by – Дата доступа: 15.02.2024.

2. «Студенты» ИИС БГУИР [Электронный ресурс]. – Режим доступа: https://students.bsuir.by – Дата доступа: 15.02.2024.
3. Кабинет сотрудника ИИС БГУИР [Электронный ресурс]. – Режим доступа: https://account.bsuir.by/personal-page – Дата доступа: 15.02.2024.
4. Angular. The web development framework for building the future [Электронный ресурс]. – Режим доступа: https://angular.io – Дата доступа: 18.02.2024.
5. Spring by VMware [Электронный ресурс]. – Режим доступа: https://spring.io – Дата доступа: 18.02.2024.
6. Docker: Accelerated Container Application Development [Электронный ресурс]. – Режим доступа: https://www.docker.com – Дата доступа: 18.02.2024.
7. PostgreSQL: The world's most advanced open source database [Электронный ресурс]. – Режим доступа: https://www.postgresql.org/ – Дата доступа: 18.02.2024.
8. nginx documentation [Электронный ресурс]. – Режим доступа: https://nginx.org/en/docs/ – Дата доступа: 18.02.2024.
9. Common Vulnerabilities and Exposures [Электронный ресурс]. – Режим доступа https://ru.wikipedia.org/wiki/Common_Vulnerabilities_and_Exposures – Дата доступа: 18.02.2024.
10. CVE security vulnerability database. Security vulnerabilities, exploits, references and more [Электронный ресурс]. – Режим доступа https://www.cvedetails.com – Дата доступа: 18.02.2024.

UDC 004.056

METHODOLOGY FOR DETECTING VULNERABILITIES IN THE INTEGRATED INFORMATION SYSTEM OF BSUIR

Matyushkin S.I.

gr. 267241

Belarusian State University of Informatics and Radioelectronics, Minsk, Republic of Belarus

Scientific supervisor: Petrov S.N., PhD, associate professor

Annotation. The materials of the report discuss the results of the analysis of vulnerabilities of software products used in the implementation of the integrated information system of BSUIR. Vulnerabilities in an information system can lead to unauthorized access to confidential information, its inaccessibility or modification. Vulnerability analysis plays a key role in ensuring the security of an information system.

Keywords: IIS BSUIR, vulnerabilities, CVE, threat model