Отчет к выпускной квалификационной работе

# Тема:МЕТОД ПОИСКА И УСТРАНЕНИЯ УЯЗВИМОСТЕЙ В ОТКРЫТОМ ПРОГРАММНОМ ОБЕСПЕЧЕНИИ ДЛЯ МЕДИЦИНСКОЙ СФЕРЫ

**Исполнитель: Студент гр. подпись, дата Исаев Д.Ю**

**Научный руководитель подпись, дата**

**Зам. зав. каф. №42: подпись, дата**

04.09.20XX

[Тема:МЕТОД ПОИСКА И УСТРАНЕНИЯ УЯЗВИМОСТЕЙ В ОТКРЫТОМ ПРОГРАММНОМ ОБЕСПЕЧЕНИИ ДЛЯ МЕДИЦИНСКОЙ СФЕРЫ 1](#_po2vavcbvjmc)

[Введение 3](#)

[Программное обеспечение в медицинской сфере 4](#_p7vqs1l02g9p)

[Теоретическая выкладка 6](#_gg2lkkkt80ln)

[Специфика и отличительные особенности медицинского ПО от прикладного ПО 7](#_697ljmk4z153)

[Известные уязвимости и их последствия в медицинском ПО 10](#_2ebg0n7r464f)

[Ограничения и этические аспекты при поиске уязвимостей 14](#_qqu1qvu318uu)

[Этические соображения при исследовании уязвимостей 14](#_gvodm5ll8e60)

[Операционные ограничения 15](#_49zjlha7bes6)

[Ограничения, налагаемые доступностью системы 15](#_9cle4femtd7h)

[Этическое раскрытие информации и исправление ситуации 15](#_sz5ojzjcw9d7)

[Баланс прозрачности и конфиденциальности 15](#_3of33a3sjlem)

[Схема инфраструктуры медицинской организации 16](#_delbvl8f7ckt)

[Методика поиска и анализа уязвимостей 18](#_dyn5l5nwna72)

[Сценарии устранения уязвимостей 20](#_t30w25jzlopt)

[Практическая часть 22](#)

[Разработка скрипта для поиска уязвимостей 22](#_rxz7gntym94c)

[Скрипт для вывода ссылок с сайта 23](#_hyt0q3vaiqe5)

[Скрипт для проверки и поиска уязвимостей. 26](#_shcdt0msk5s2)

[Заключение 27](#_q66vvl6tx5e2)

# Введение

Медицинское программное обеспечение и современное здравоохранение это две неделимых части дополняющие друг друга в современном здравоохранении, облегчая управление информацией о пациентах, планирование лечения и оказание медицинской помощи. Растущая зависимость от программного обеспечения в медицинской сфере привела к многочисленным преимуществам, таким как повышение точности, эффективности и доступности медицинских услуг. Однако эта зависимость от программного обеспечения также создает значительные уязвимости и риски, что делает безопасность медицинского программного обеспечения вопросом первостепенной важности.

Актуальность исследований безопасности медицинского программного обеспечения подчеркивается несколькими факторами. Во-первых, конфиденциальный характер медицинских данных требует надежных мер защиты для защиты конфиденциальности пациентов и предотвращения несанкционированного доступа. Нарушения медицинского программного обеспечения могут привести к раскрытию конфиденциальной информации о пациентах, что потенциально может привести к краже личных данных, медицинскому мошенничеству и нанесению ущерба репутации медицинских учреждений. Во-вторых, интеграция медицинского программного обеспечения с критически важными медицинскими устройствами и оборудованием создает возможность возникновения опасных для жизни ситуаций в случае нарушения кибербезопасности. Обеспечение надежности и безопасности медицинского программного обеспечения необходимо для предотвращения таких тяжелых последствий. В-третьих, нормативная база, регулирующая медицинское программное обеспечение, становится все более жесткой: регулирующие органы, такие как Управление по контролю за продуктами и лекарствами США (FDA) и Регламент Европейского Союза по медицинскому оборудованию (MDR), вводят строгие стандарты и сертификаты. Соблюдение этих правил необходимо для развертывания и использования медицинского программного обеспечения в медицинских учреждениях.

# 

# 

# 

# 

# Программное обеспечение в медицинской сфере

В современной медицине программное обеспечение играет ключевую роль, обеспечивая эффективность и точность диагностики, лечения, управления данными и операционной деятельности. Эволюция информационных технологий в медицине привела к созданию сложных и многофункциональных систем, от электронных медицинских записей (EMR) до интегрированных диагностических систем. Подобное ПО не только повышает качество медицинского обслуживания, но и способствует более эффективному управлению ресурсами здравоохранения.

Сфера применения медицинского программного обеспечения обширна. Она включает в себя системы для управления больницами, клиническими исследованиями, лабораторными анализами, медицинской визуализацией и дистанционным мониторингом пациентов. Каждое из этих приложений имеет свои уникальные требования к безопасности, надежности и соответствию регулятивным стандартам.

Одним из ключевых аспектов медицинского ПО является его способность интегрироваться с другими системами и оборудованием. Например, системы электронных медицинских записей должны быть совместимы с лабораторными информационными системами, радиологическими информационными системами и другими диагностическими инструментами. Эта интеграция необходима для обеспечения целостности и доступности медицинских данных, что критически важно для качественного лечения и ухода за пациентами.

Существенное внимание в разработке медицинского ПО уделяется его соответствию регулятивным стандартам и законодательству. В разных странах существуют свои требования к сертификации и тестированию медицинского ПО. Например, в США Food and Drug Administration (FDA) классифицирует медицинское ПО в зависимости от уровня риска для пациента. В Европейском Союзе схожие функции выполняются регламентами EU Medical Device Regulation (MDR) и In Vitro Diagnostic Regulation (IVDR).

Electronic Health Record (EHR) Systems: EHR являются ярким примером медицинского программного обеспечения. Они хранят данные пациентов, историю болезни, диагностику и планы лечения. Однако они часто становятся объектами кибератак с целью кражи конфиденциальной личной информации. Например, в 2017 году атака программы-вымогателя WannaCry существенно нарушила работу Национальной службы здравоохранения Великобритании, зашифровав электронные записи и потребовав выкуп за их выпуск.

Pacemaker Programming Software. В 2018 году были обнаружены уязвимости в программном обеспечении, используемом для программирования кардиостимуляторов. Эти уязвимости потенциально могут позволить хакерам манипулировать устройствами, что приведет к опасным для жизни ситуациям. FDA отозвало почти полмиллиона кардиостимуляторов, чтобы исправить недостатки безопасности.

Diagnostic Imaging Software. Диагностические инструменты, такие как МРТ и КТ-сканеры, используют программное обеспечение для обработки и интерпретации медицинских изображений. В 2020 году исследователи обнаружили уязвимости в популярном программном обеспечении для визуализации, которые можно использовать для вставки ложных раковых узлов в снимки МРТ, что приводит к неправильному диагнозу.

Hospital Information Systems (HIS): HIS управляет всеми аспектами работы больницы, от данных о пациентах до управления запасами. Нарушение в HIS может парализовать работу больницы. Например, в 2016 году Голливудский пресвитерианский медицинский центр в Лос-Анджелесе заплатил выкуп в размере 17 000 долларов США в биткойнах, чтобы восстановить доступ к своей HIS после атаки программы-вымогателя.

Telemedicine Software. С развитием телемедицины, особенно во время пандемии COVID-19, безопасность каналов связи стала иметь первостепенное значение. Были случаи, когда незащищенные телемедицинские платформы приводили к несанкционированному доступу к консультациям пациента и врача, нарушая конфиденциальность пациентов.

Laboratory Information Management Systems (LIMS): LIMS имеют решающее значение для обработки и хранения результатов лабораторных исследований. Любая уязвимость в этих системах может привести к неверным результатам испытаний и ошибочным диагнозам. В 2019 году в популярной LIMS была обнаружена ошибка, которая могла привести к путанице в результатах тестов пациентов.

Pharmacy Management Software: это программное обеспечение используется для управления рецептами и записями о лекарствах пациентов. Неисправности этих систем могут привести к выдаче неправильного лекарства. В 2015 году сбой в аптечном программном обеспечении привел к выдаче пациентам неправильных дозировок лекарств.

Рассмотрим также примеры с Российскими медицинскими системами, чтобы проиллюстрировать значение кибербезопасности в секторе здравоохранения в России:

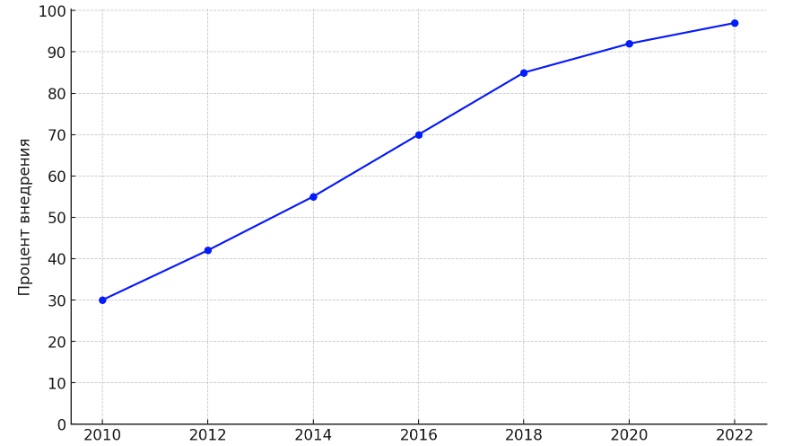
Пример: нарушение безопасности информационной системы Российской больницы

В последние годы Российские учреждения здравоохранения все чаще внедряют цифровые технологии, в том числе электронные медицинские карты, больничные информационные системы и другое специализированное медицинское программное обеспечение. Однако они также представляют потенциальные риски кибербезопасности.

## 

## 

## **Теоретическая выкладка**

Рисунок 1. Рост процента внедрения систем электронных медицинских записей. Примечательный инцидент произошел в крупной больнице, где нарушение кибербезопасности привело к несанкционированному доступу к информационной системе больницы. Нарушение было выявлено, когда сотрудники больницы заметили нарушения в работе системы, в том числе низкую производительность и неожиданные сообщения об ошибках.Последствия: раскрытие данных пациентов. В результате нарушения потенциально могут быть раскрыты конфиденциальные данные пациентов, включая истории болезни, планы лечения и личную информацию. Такое разоблачение не только ставит под угрозу конфиденциальность пациентов, но также создает риск кражи личных данных и мошенничества. Ежедневная работа больницы была нарушена, что привело к задержкам в приеме пациентов, лечении и доступе к медицинским записям. Этот сбой оказал прямое влияние на уход за пациентами и эффективность больниц.

Эрозия доверия. Инцидент подорвал доверие к цифровым системам здравоохранения среди пациентов и персонала, вызвав обеспокоенность по поводу безопасности и конфиденциальности их данных.

Какое было решение?

Немедленное сдерживание: ИТ-команда работала над сдерживанием взлома, предотвращая дальнейший несанкционированный доступ.

Аудит и усиление системы: был проведен комплексный аудит всей системы для выявления и устранения уязвимостей. Это включало обновление программного обеспечения, усиление защиты брандмауэра и введение более строгого контроля доступа.

Уведомление и поддержка пациентов. Больница уведомила пострадавших пациентов и предоставила рекомендации по защите их личной информации.

Обучение персонала. Сотрудники больницы прошли дополнительное обучение передовым методам кибербезопасности для предотвращения будущих инцидентов.

## Специфика и отличительные особенности медицинского ПО от прикладного ПО

Медицинское программное обеспечение, ключевой компонент в сфере информационных технологий, демонстрирует особые характеристики, которые отличают его от общего прикладного программного обеспечения. Эта дифференциация коренится в множестве конкретных условий эксплуатации и развития, адаптированных к строгим стандартам сектора здравоохранения.

Главным из них является обязательство соблюдать нормативные требования. MS, в отличие от своих аналогов общего применения, действует под контролем строгих регулирующих органов, таких как Управление по контролю за продуктами и лекарствами США и Регламент Европейского Союза по медицинскому оборудованию. Эти организации устанавливают комплексные стандарты, гарантирующие, что программное обеспечение поддерживает высочайший уровень безопасности пациентов, надежности и устойчивости к угрозам кибербезопасности.

В сфере медицинского программного обеспечения (МС) аспекты сложности и специфичности выходят за рамки обычных границ, наблюдаемых в обычном прикладном программном обеспечении. Это расхождение дополнительно иллюстрируется при рассмотрении многогранных аспектов рассеянного склероза, каждый из которых подчеркивает важность этого жанра программного обеспечения в здравоохранении.

Кастомизация и конфигурируемость. В отличие от обычных программных приложений, предназначенных для широкого спектра пользователей и применений, MS должен быть по своей сути адаптируемым к тонким и часто узкоспециализированным требованиям различных медицинских практик и специальностей. Например, система электронных медицинских карт должна быть настраиваемой, чтобы соответствовать разнообразным рабочим процессам врачей общей практики, хирургов и специалистов, таких как кардиологи, каждому из которых требуются разные функциональные возможности и форматы представления данных.

Масштабируемость и производительность под давлением: MS должна продемонстрировать надежную масштабируемость и производительность, особенно в таких важных средах, как отделения неотложной помощи или отделения интенсивной терапии. Например, в сценариях интенсивной терапии системы мониторинга пациентов должны точно обрабатывать и отображать данные в реальном времени при любых условиях, а уровень надежности работы обычно не требуется от стандартного прикладного программного обеспечения.

Интеграция с новыми технологиями. MS все чаще требуется для интеграции с передовыми технологиями, такими как искусственный интеллект, машинное обучение и Интернет медицинских вещей (IoMT). Например, интеграция алгоритмов искусственного интеллекта в программное обеспечение для диагностической визуализации для более точного анализа и прогнозирования улучшает результаты лечения пациентов, но также создает сложную обработку данных и проблемы регулирования.

Развитие вместе с достижениями медицины. Быстрый темп развития медицины требует, чтобы рассеянный склероз был не только современным, но и совместимым с новыми медицинскими практиками и технологиями. Примером этого является включение возможностей телемедицины в существующие платформы здравоохранения — необходимость, которая стала особенно очевидной во время пандемии COVID-19.

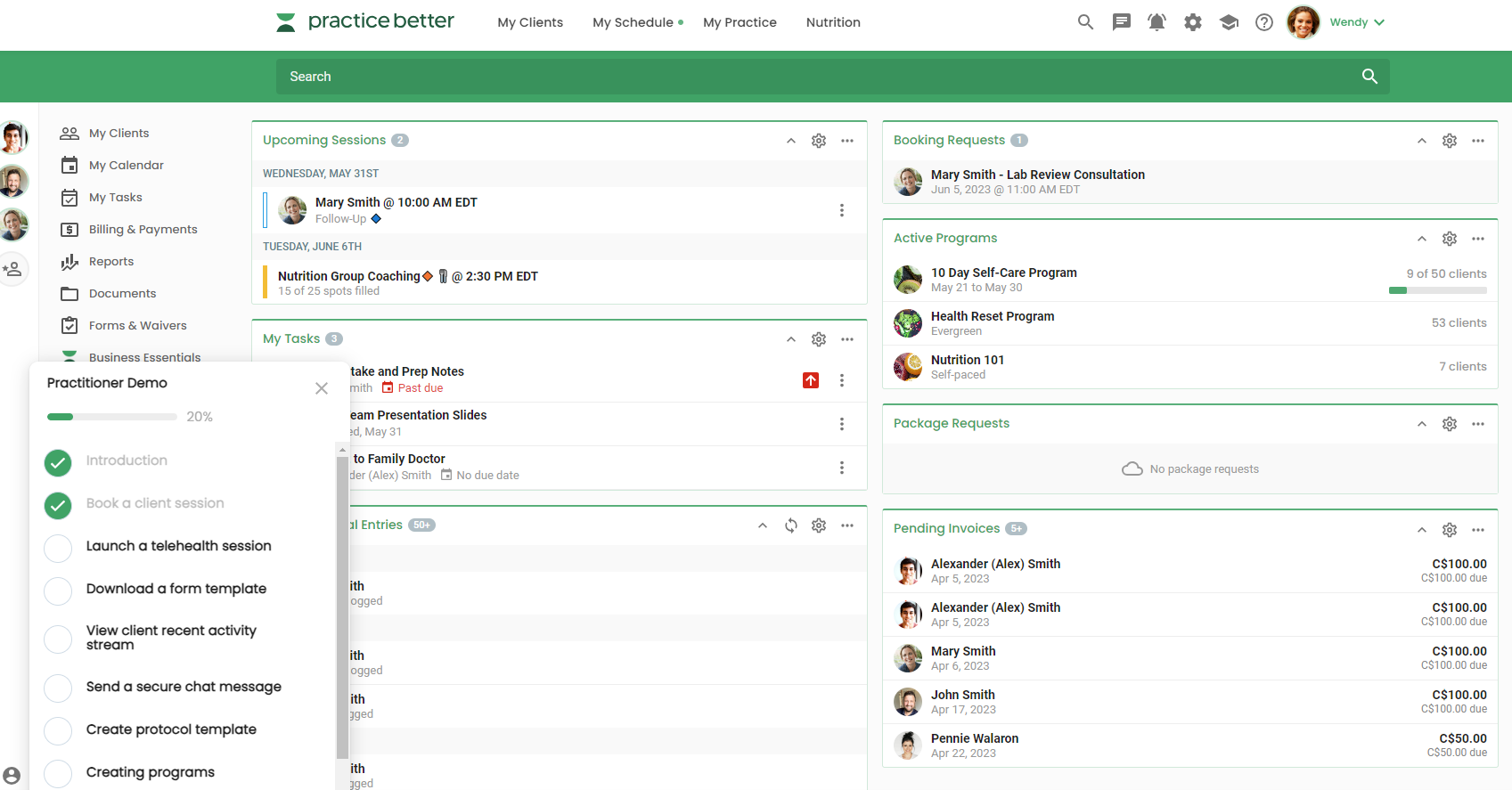


Рисунок 2. Интерфейс управления медицинской практикой платформы Practicebetter

Рисунок 2, представляет собой снимок экрана интерфейса платформы для управления медицинской практикой. Этот тип программного обеспечения предназначен для того, чтобы помочь медицинским работникам более эффективно управлять своей повседневной деятельностью. На снимке экрана показаны различные функции, такие как:

-Предстоящие сеансы: календарь или расписание будущих посещений и сеансов, который можно настраивать по дате и включает имена пациентов и время посещений.

-Мои задачи: список дел или диспетчер задач, где практикующий врач может отслеживать свои обязанности. Он показывает задачи, которые необходимо выполнить, и позволяет организовать их по приоритетам.

-Запросы на запись: раздел, в котором отображаются новые запросы на прием от пациентов, ожидающие подтверждения или переноса записи практикующим врачом.

-Активные программы: здесь перечислены текущие программы здравоохранения, предлагаемые поставщиком услуг, включая количество участвующих клиентов.

-Запросы пакетов: это может быть функция, с помощью которой пациенты могут запрашивать заранее определенные пакеты услуг, предлагаемые практикой.

-Ожидающие счета: инструмент управления финансами, в котором перечислены счета, ожидающие оплаты, включая имена пациентов и суммы к оплате.

Слева находится меню, в котором есть:

-Мои клиенты, Мой календарь, Мои задачи, Счета и платежи: на этих вкладках предлагаются комплексные функции управления информацией о клиентах, планирования, отслеживания задач и финансовых транзакций.

-Отчеты, документы, формы и отказы: указание на способность создавать отчеты, управлять документацией, а также обрабатывать необходимые формы и юридические отказы.

– Основы бизнеса. Скорее всего, это набор инструментов или ресурсов, которые помогут реализовать эту практику, например маркетинг, управление персоналом и оперативная логистика.

-Демо для практикующего врача: боковая панель, показывающая демонстрацию или учебное пособие с такими шагами, как бронирование сеанса клиента или запуск сеанса телемедицины.

Данная платформа является ярким примером специализированного медицинского программного обеспечения, предназначенного для оптимизации административных задач в медицинских учреждениях, позволяя практикующим врачам больше сосредоточиться на уходе за пациентами. Интерфейс демонстрирует высокий уровень организации и предлагает функции, которые поддерживают широкий спектр действий по управлению практикой, от планирования до выставления счетов.

## Известные уязвимости и их последствия в медицинском ПО

При обсуждении уязвимостей медицинского программного обеспечения разговор выходит за рамки простого выявления недостатков. Он включает в себя анализ системных рисков, которые эти уязвимости представляют для конфиденциальности, целостности и доступности данных пациентов и медицинских услуг.

Классификация уязвимостей в медицинском программном обеспечении является свидетельством сложного взаимодействия между технологиями и здравоохранением. Эти уязвимости варьируются от ошибок программного обеспечения до небезопасной передачи данных, и каждая из них может поставить под угрозу безопасность и конфиденциальность пациентов.

Таблица 1. Известные уязвимости и их последствия в медицинском ПО

| Тип уязвимости | Описание | Пример | Последствия |
| --- | --- | --- | --- |
| SQL-инъекция | Внедрение злонамеренного кода в базы данных через плохо обработанные входные поля. | Злоумышленник получает доступ к базе данных больницы и извлекает конфиденциальные записи пациентов. | Нарушение конфиденциальности пациента, потенциальная кража личности. |
| Межсайтовый скриптинг (XSS) | Выполнение злонамеренных скриптов в браузере пользователя. | Злоумышленник использует уязвимость XSS в онлайн-портале пациентов. | Несанкционированный доступ к данным пациентов, манипуляция информацией пациента. |
| Нешифрованная передача данных | Передача данных по сети без использования шифрования. | Данные пациентов, отправленные по незащищенному соединению, перехватываются. | Перехват чувствительных данных, потенциальное нарушение безопасности данных. |
| Недостаточная аутентификация | Слабые механизмы аутентификации, не обеспечивающие надёжную верификацию личности пользователя. | Система входа врача скомпрометирована из-за слабых паролей. | Несанкционированный доступ к медицинским системам и записям. |
| Отсутствие шифрования данных | Отсутствие шифрования для хранящихся данных. | Украденные ноутбуки или устройства хранения содержат незашифрованную информацию о пациентах. | Утрата конфиденциальности данных пациентов, несоответствие регуляторным требованиям. |
| Неверная авторизация | Ошибки в контролях доступа, позволяющие пользователям получать доступ к большему объему данных, чем разрешено. | Сотрудник низкого уровня получает доступ к конфиденциальным записям пациентов. | Несанкционированный доступ к данным, потенциальное внутреннее неправомерное использование данных. |
| Устаревшее ПО | Использование версий ПО с известными уязвимостями. | МРТ-аппарат, работающий на устаревшем ПО, подвергается компрометации. | Нарушение медицинских услуг, потенциальная опасность для пациентов. |
| Угоны медицинских устройств | Компрометация медицинских устройств из-за уязвимостей в ПО. | ПО инсулинового насоса взламывается, изменяя его функции. | Прямое влияние на здоровье пациента, потенциально опасные для жизни ситуации. |
| Атаки типа "отказ в обслуживании" (DoS) | Перегрузка медицинских систем, делающая их неотзывчивыми. | Система электронных медицинских записей (ЭМЗ) выходит из строя из-за перегрузки трафиком. | Невозможность доступа к медицинским записям, нарушение процесса оказания ухода. |
| Недостаточное ведение журналов и мониторинг | Отсутствие детального аудита, затрудняющего обнаружение аномалий. | Нарушение безопасности остается незамеченным из-за недостаточного мониторинга. | Задержка реагирования на инциденты безопасности, продолжительное обнажение данных. |

Последствия этих уязвимостей многообразны и выходят за рамки непосредственных технических последствий. Они влекут за собой серьезные юридические и этические последствия, часто приводящие к финансовым штрафам, потере доверия пациентов и, в тяжелых случаях, к нанесению вреда благополучию людей.

Устранение этих уязвимостей требует многогранного подхода. Он включает в себя упреждающие методы обеспечения безопасности, такие как регулярные обновления программного обеспечения, режимы тщательного тестирования, надежные методологии шифрования и всестороннее обучение персонала мерам конфиденциальности данных и кибербезопасности.

В основе методологии выявления и устранения уязвимостей лежит ряд принципов и подходов, каждый из которых адаптирован к тонким потребностям сектора здравоохранения.

Принцип превентивной бдительности. В основе управления уязвимостями лежит принцип превентивной бдительности. Эта проактивная позиция предполагает регулярные и всесторонние оценки безопасности, которые предотвращают потенциальное использование уязвимостей программного обеспечения. Именно посредством таких периодических оценок с использованием как автоматизированных инструментов, так и экспертной проверки можно выявить потенциальные слабые места до того, как они будут использованы злоумышленниками.

Оценка рисков и определение приоритетов. После выявления уязвимостей необходима тщательная оценка рисков. Эта оценка количественно определяет потенциальное воздействие каждой уязвимости, принимая во внимание вероятность ее использования и потенциальный вред для результатов лечения пациентов. Затем уязвимости распределяются по приоритетам на основе этой оценки риска, гарантируя эффективное распределение ресурсов для решения наиболее важных проблем в первую очередь.

Соблюдение передового опыта в области безопасности. Методология управления уязвимостями во многом зависит от устоявшихся передовых методов обеспечения безопасности. К ним относятся принцип наименьших привилегий, гарантирующий, что пользователи имеют только тот доступ, который необходим для выполнения их ролей; использование надежных протоколов аутентификации и шифрования; и обеспечение строгого контроля доступа.

Применение стратегии глубокоэшелонированной защиты. Для защиты от уязвимостей на нескольких уровнях используется многоуровневый подход к безопасности, или эшелонированная защита. Эта стратегия включает не только программные решения, но также административный контроль и физические меры безопасности. Создав несколько уровней защиты, можно свести к минимуму последствия потенциального взлома.

Регулярное управление исправлениями. Неотъемлемой частью методологии является структурированный процесс управления исправлениями. Этот процесс предполагает своевременное применение исправлений и обновлений, выпущенных поставщиками программного обеспечения для устранения известных уязвимостей. Задержка с применением исправлений может привести к незащищенности систем и должна быть смягчена с помощью дисциплинированного режима обновлений.

Планирование реагирования на инциденты. Надежный план реагирования на инциденты является важнейшим компонентом методологии. В этом плане изложены шаги, которые необходимо предпринять в случае нарушения безопасности, включая стратегии сдерживания, сохранение доказательств, устранение угроз и восстановление систем до безопасного состояния.

Непрерывное образование и обучение. Учитывая постоянно меняющийся характер угроз кибербезопасности, крайне важно непрерывное образование и обучение ИТ-персонала здравоохранения. Персонал должен быть в курсе новейших угроз и методов управления уязвимостями, чтобы обеспечить устойчивость систем медицинского программного обеспечения.

Взаимодействие с базами данных уязвимостей и консорциумами. Участие в консорциумах по безопасности и использование баз данных уязвимостей имеют решающее значение. Эти платформы предоставляют ценную информацию о возникающих угрозах и облегчают обмен стратегиями смягчения последствий среди ИТ-сообщества здравоохранения.

## Ограничения и этические аспекты при поиске уязвимостей

В поисках уязвимостей в медицинском программном обеспечении необходимо учитывать сочетание этических соображений и эксплуатационных ограничений. Это начинание является не просто техническим упражнением, но и отражением обязанности соблюдать клятву Гиппократа в цифровой сфере: во-первых, не навреди.

## Этические соображения при исследовании уязвимостей

Этические императивы в этой области требуют строгих стандартов поведения. Исследователи должны сбалансировать стремление к надежности системы с необходимостью защитить информацию о пациентах и обеспечить бесперебойную функциональность медицинских услуг. Поиск уязвимостей ни при каких обстоятельствах не должен ставить под угрозу конфиденциальность или целостность данных пациентов. Эта этическая граница имеет первостепенное значение и требует, чтобы все оценки уязвимостей проводились в контролируемых средах, тиражируя рассматриваемые программные системы, не подвергая риску реальные данные пациентов.

Более того, существует этическое обязательство сообщать об обнаруженных уязвимостях. Такое сообщение должно составляться разумно, гарантируя, что информация о потенциальных слабых местах будет передана напрямую и конфиденциально организациям, ответственным за программное обеспечение. Публичное раскрытие уязвимостей без предоставления разработчикам программного обеспечения достаточного времени для устранения проблем может спровоцировать злонамеренную эксплуатацию и поэтому считается нарушением этики.

## Операционные ограничения

Операционная среда обнаружения уязвимостей в медицинском программном обеспечении полна уникальных проблем. Инфраструктура, на которой работает такое программное обеспечение, часто бывает сложной и разнородной: она объединяет устаревшие системы с современными интерфейсами и связывает разрозненные базы данных и медицинские устройства. Эта сложность ограничивает гибкость проведения оценок уязвимостей и часто требует индивидуального подхода для каждой системы.

Нормативно-правовая среда еще больше усугубляет эти операционные ограничения. Медицинское программное обеспечение регулируется рядом правил, которые требуют соблюдения определенных стандартов безопасности. Поэтому исследователи должны разбираться не только в технических знаниях, но и в правовой базе, регулирующей их деятельность. Такое двойное владение гарантирует, что поиск уязвимостей не будет нарушать нормативные положения, сохраняя законность исследовательской деятельности.

## Ограничения, налагаемые доступностью системы

Важность доступности систем в здравоохранении невозможно переоценить. Системы диагностики, лечения и мониторинга пациентов должны работать с непревзойденной надежностью. Таким образом, оценки уязвимости должны быть разработаны таким образом, чтобы избежать каких-либо сбоев в обслуживании. Исследователи используют различные стратегии для удовлетворения этого требования, такие как проведение оценок в часы непиковой нагрузки, использование виртуализированных сред или внедрение резервных систем для обеспечения непрерывности обслуживания на этапе тестирования.

## Этическое раскрытие информации и исправление ситуации

После выявления уязвимости начинается процесс этического раскрытия информации. Этот процесс включает в себя скоординированную стратегию раскрытия информации, при которой исследователи и разработчики совместно работают над проверкой уязвимости и разработкой плана устранения. Время и способ раскрытия информации имеют решающее значение; Преждевременное или публичное раскрытие информации может поставить под угрозу безопасность пациентов и целостность системы.

## Баланс прозрачности и конфиденциальности

Хотя прозрачность в сфере кибербезопасности часто хвалят, сфера медицинского программного обеспечения требует более тонкого подхода. Исследователи должны найти баланс между необходимостью прозрачности своих выводов и необходимостью защиты конфиденциальной информации. Этот хрупкий баланс основан на этических соображениях, в которых безопасность пациентов ставится превыше всего.

Подводя итог, можно сказать, что поиск и устранение уязвимостей в медицинском программном обеспечении — это задача, связанная как с эксплуатационными ограничениями, так и с этическими соображениями. Это требует осторожного и взвешенного подхода, учитывающего чувствительность среды здравоохранения.

## Схема инфраструктуры медицинской организации

Схематическое изображение инфраструктуры медицинской организации должно отражать многогранную и сложную систему, характеризующуюся слиянием технологий, процессов здравоохранения и ведения пациентов. Эта структура представляет собой не просто совокупность аппаратного и программного обеспечения, а сложную сеть, предназначенную для обеспечения эффективного, безопасного и высококачественного ухода за пациентами.

Централизованное управление данными пациентов. В основе инфраструктуры лежит система электронных медицинских карт (EHR). Эта система служит хранилищем всей информации о пациенте, включая историю болезни, планы лечения, диагностические изображения и результаты лабораторных исследований. Электронные медицинские записи разработаны так, чтобы быть доступными, но безопасными, гарантируя, что поставщики медицинских услуг могут получить доступ к полным данным пациентов в режиме реального времени, сохраняя при этом строгую конфиденциальность.

Интеграция систем диагностики и лечения. Ключевые компоненты этой инфраструктуры включают различные системы диагностики и лечения, такие как аппараты МРТ, компьютерные томографы и инфузионные насосы. Эти системы интегрированы с EHR, что обеспечивает бесперебойный поток данных и снижает вероятность ошибок при вводе данных вручную. Такая интеграция гарантирует, что диагностические данные напрямую повлияют на планы лечения пациентов.

Возможности телемедицины и удаленного мониторинга. Инфраструктура выходит за пределы физических границ медицинского учреждения и включает телемедицинские технологии. Эти технологии обеспечивают дистанционные консультации, мониторинг пациентов и цифровые каналы связи между пациентами и поставщиками медицинских услуг. Этот аспект инфраструктуры особенно важен для оказания помощи отдаленным или недостаточно обслуживаемым группам населения.

Лабораторные информационные системы (ЛИС): ЛИС управляет лабораторными процессами, включая заказы на испытания, отслеживание образцов и распространение результатов. Он интегрирован с EHR, гарантируя, что результаты лабораторных исследований будут быстро и точно записаны в карте пациента.

Аптечные информационные системы (PIS): эта система управляет запасами лекарств, рецептами и деятельностью по отпуску лекарств. Интеграция PIS с EHR гарантирует точную запись и выполнение заказов на лекарства, что снижает риск ошибок при приеме лекарств.

Сеть и безопасность данных. Вся инфраструктура опирается на надежную сетевую систему, обеспечивающую связь между различными компонентами. Меры безопасности данных, включая межсетевые экраны, шифрование и системы обнаружения вторжений, используются для защиты конфиденциальных медицинских данных от киберугроз.

Обмен медицинской информацией (HIE): системы HIE облегчают обмен информацией о пациентах между различными поставщиками медицинских услуг, улучшая координацию медицинской помощи. Эта система обеспечивает безопасный доступ к информации о пациентах и обмен ею между различными практикующими врачами, повышая эффективность и качество ухода за пациентами.

Административные и биллинговые системы. Административные системы управляют планированием пациентов, распределением персонала и управлением ресурсами, а биллинговые системы обрабатывают страховые претензии и выставляют счета пациентам. Эти системы жизненно важны для операционной эффективности медицинской организации.

Аварийное восстановление и резервное копирование данных. Для защиты от потери данных или сбоев системы инфраструктура включает системы аварийного восстановления и резервного копирования данных. Эти системы гарантируют, что данные пациентов и критически важные функции системы могут быть быстро восстановлены в случае сбоя или других катастрофических событий.

Инструменты обеспечения соответствия и отчетности. Соблюдение нормативных требований в области здравоохранения обеспечивается с помощью специализированных инструментов, которые облегчают отчетность и соблюдение таких стандартов, как HIPAA. Эти инструменты помогают поддерживать юридическую и этическую целостность деятельности организации.

Таким образом, инфраструктура современной медицинской организации представляет собой комплексную экосистему, объединяющую клинические, административные и технологические компоненты.

## Методика поиска и анализа уязвимостей

Методика поиска и анализа уязвимостей в медицинском программном обеспечении — кропотливый и многоуровневый процесс, требующий всестороннего понимания как принципов кибербезопасности, так и уникальных сложностей ИТ-систем здравоохранения.

Первоначальная оценка рисков и картирование среды. Основополагающим шагом в этой методологии является тщательная оценка рисков и картирование ИТ-среды здравоохранения. Это предполагает идентификацию всех компонентов инфраструктуры, включая медицинские устройства, программные приложения, сетевые системы и средства хранения данных. Понимание взаимосвязей и зависимостей между этими компонентами имеет решающее значение. Такое сопоставление дает четкое представление о потенциальных поверхностях атак и помогает определить приоритетность областей для сканирования уязвимостей.

Выбор подходящих инструментов сканирования. Следующим шагом является тщательный выбор инструментов сканирования уязвимостей. Эти инструменты должны обеспечивать глубокое сканирование и быть совместимыми с разнообразным медицинским программным обеспечением и оборудованием, используемым в медицинских учреждениях. Выбор инструментов также должен учитывать нормативную базу, обеспечивая соответствие процесса сканирования таким стандартам, как HIPAA и GDPR.

Настройка параметров сканирования. Настройка процесса сканирования необходима для его согласования с конкретной средой медицинского учреждения. Это предполагает установку соответствующих параметров, чтобы гарантировать, что сканирование будет тщательным, но не помешает критически важным медицинским услугам. Особое внимание уделяется настройке инструментов для распознавания нюансов медицинского программного обеспечения, которое может существенно отличаться от стандартных ИТ-систем.

Активное и пассивное сканирование уязвимостей. Методика включает в себя как активные, так и пассивные методы сканирования. Активное сканирование предполагает взаимодействие с системами для обнаружения уязвимостей, таких как устаревшее программное обеспечение или неправильные конфигурации. С другой стороны, пассивное сканирование отслеживает сетевой трафик для выявления потенциальных проблем безопасности без активного исследования систем.

Тестирование на проникновение и симуляция атак. Передовые методологии включают тестирование на проникновение, при котором этические хакеры моделируют кибератаки для проверки устойчивости ИТ-среды здравоохранения. Этот упреждающий подход помогает обнаруживать уязвимости, которые невозможно обнаружить с помощью стандартных процедур сканирования. Тесты на проникновение тщательно планируются, чтобы гарантировать, что они не помешают операциям по уходу за пациентами.

Автоматический и ручной анализ. Хотя автоматизированные инструменты играют важную роль в первоначальном обнаружении уязвимостей, ручной анализ необходим для более глубокого понимания результатов. Квалифицированные специалисты по кибербезопасности тщательно изучают результаты, различая ложные срабатывания и настоящие уязвимости. Они также оценивают потенциальное влияние каждой уязвимости на безопасность пациентов и безопасность данных.

Контекстный анализ уязвимостей. Контекстный анализ является важнейшим компонентом этой методологии. Это предполагает понимание того, как выявленные уязвимости могут быть использованы в конкретном контексте медицинского учреждения. На этом этапе оценивается вероятность и потенциальное влияние эксплойта с учетом таких факторов, как доступность уязвимой системы и конфиденциальность данных, которые она обрабатывает.

Документация и отчетность. Полная документация всего процесса, от первоначальной оценки до окончательного анализа, имеет жизненно важное значение. Эта документация служит записью выявленных уязвимостей, методологий, использованных для их обнаружения, и анализа их потенциального воздействия. Сообщение об этих результатах соответствующим заинтересованным сторонам, включая администраторов здравоохранения и ИТ-команды, имеет решающее значение для своевременного устранения проблем.

Разработка плана восстановления: Последним шагом в этой методологии является разработка плана восстановления. В этом плане изложены шаги по устранению каждой выявленной уязвимости, установленные по приоритетам на основе оценки риска. План включает не только технические исправления, такие как исправления и изменения конфигурации, но и более широкие улучшения безопасности, такие как обучение персонала и пересмотр политики.

Непрерывный мониторинг и переоценка. Учитывая динамичный характер угроз кибербезопасности, непрерывный мониторинг и периодическая переоценка ИТ-среды здравоохранения являются неотъемлемой частью этой методологии. Этот непрерывный процесс гарантирует, что системы остаются защищенными от возникающих угроз, а методы управления уязвимостями развиваются вместе с достижениями в области технологий и изменениями в сфере здравоохранения.

## Сценарии устранения уязвимостей

Методика устранения уязвимостей в медицинском программном обеспечении воплощает в себе комплексный подход, объединяющий технические меры, корректировки политик и непрерывный мониторинг для защиты данных пациентов и обеспечения бесперебойной функциональности систем здравоохранения.

Интеграция петель обратной связи. Важнейшим аспектом исправления является включение петель обратной связи в процесс. Эти циклы позволяют постоянно совершенствовать как стратегии исправления, так и лежащие в их основе политики безопасности. Анализы после восстановления проводятся для оценки эффективности реализованных мер и определения областей для улучшения. Такой подход гарантирует, что уроки, извлеченные из каждого инцидента, систематически учитываются в будущих усилиях по управлению уязвимостями.

Улучшение реагирования на инциденты. Совершенствование протоколов реагирования на инциденты является неотъемлемой частью процесса исправления. Эффективные планы реагирования на инциденты должны быть гибкими и всеобъемлющими, способными учитывать широкий спектр потенциальных сценариев. В этих планах должны быть подробно описаны конкретные роли и обязанности, протоколы связи и шаги по сдерживанию, искоренению и восстановлению. Регулярные учения и моделирование необходимы для обеспечения хорошей подготовки группы реагирования и сохранения актуальности и эффективности планов.

Сотрудничество с регулирующими органами. Активное взаимодействие с регулирующими органами имеет жизненно важное значение в процессе восстановления. Такое сотрудничество гарантирует, что меры по восстановлению соответствуют текущим нормативным требованиям и передовому опыту. Это также способствует более информированному пониманию меняющейся нормативной среды, позволяя организациям здравоохранения активно корректировать свои методы и политики безопасности в ожидании нормативных изменений.

Расширенный анализ угроз. Использование расширенного анализа угроз является ключевым фактором эффективного устранения уязвимостей. Подключаясь к глобальным каналам сбора данных об угрозах и участвуя в сетях обмена информацией, организации здравоохранения могут получить представление о возникающих угрозах и уязвимостях. Эта информация может способствовать более активным и целенаправленным действиям по исправлению ситуации, повышая способность организации предвидеть и реагировать на новые типы кибератак.

Инвестиции в инфраструктуру безопасности. Стратегический подход к восстановлению также предполагает постоянные инвестиции в инфраструктуру безопасности. Это включает в себя внедрение передовых технологий безопасности, таких как системы предотвращения вторжений, инструменты автоматического обнаружения и реагирования на угрозы, а также передовые методы шифрования. Эти технологии обеспечивают дополнительный уровень защиты, расширяя возможности организации по обнаружению сложных киберугроз и реагированию на них.

Укрепление партнерских отношений с поставщиками. Прочные партнерские отношения с поставщиками программного обеспечения и сторонними поставщиками услуг имеют решающее значение. Эти партнерства облегчают своевременный доступ к информации об уязвимостях и доступных исправлениях. Они также обеспечивают более эффективную координацию в процессе исправления, гарантируя, что обновления программного обеспечения и меры безопасности совместимы и не нарушают бесперебойную работу медицинских услуг.

Общение с пациентами и прозрачность. В случаях, когда данные или услуги пациентов могут быть затронуты, прозрачное общение с пациентами имеет важное значение. Это включает в себя информирование пациентов о потенциальных рисках, шагах, предпринятых для устранения уязвимостей, и любых действиях, которые им может потребоваться предпринять. Такая прозрачность имеет решающее значение для поддержания доверия пациентов и уверенности в приверженности поставщика медицинских услуг обеспечению безопасности данных и безопасности пациентов.

Долгосрочное стратегическое планирование. Восстановление – это не просто реактивный процесс, но и стратегический, встроенный в более широкий контекст долгосрочного планирования. Это планирование включает в себя регулярную оценку состояния кибербезопасности организации, определение стратегических целей безопасности и распределение ресурсов в области, которые наиболее эффективно повысят общую устойчивость безопасности организации.

По сути, устранение уязвимостей в медицинском программном обеспечении — это динамичная и многогранная задача. Он охватывает широкий спектр мероприятий: от технических мер и обновлений политики до стратегического планирования и взаимодействия с заинтересованными сторонами.

### Практическая часть

### Разработка скрипта для поиска уязвимостей

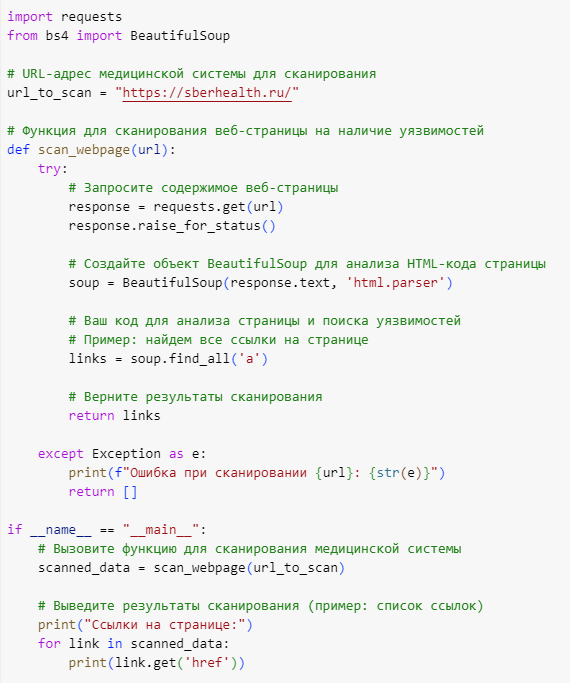
Целью данного обсуждения является разъяснение процесса создания такого сценария, специально предназначенного для приложений Python, путем интеграции инструмента Bandit, хорошо зарекомендовавшей себя среды статического тестирования безопасности приложений (SAST).

Устанавливаем 2 функции:

pip install requests

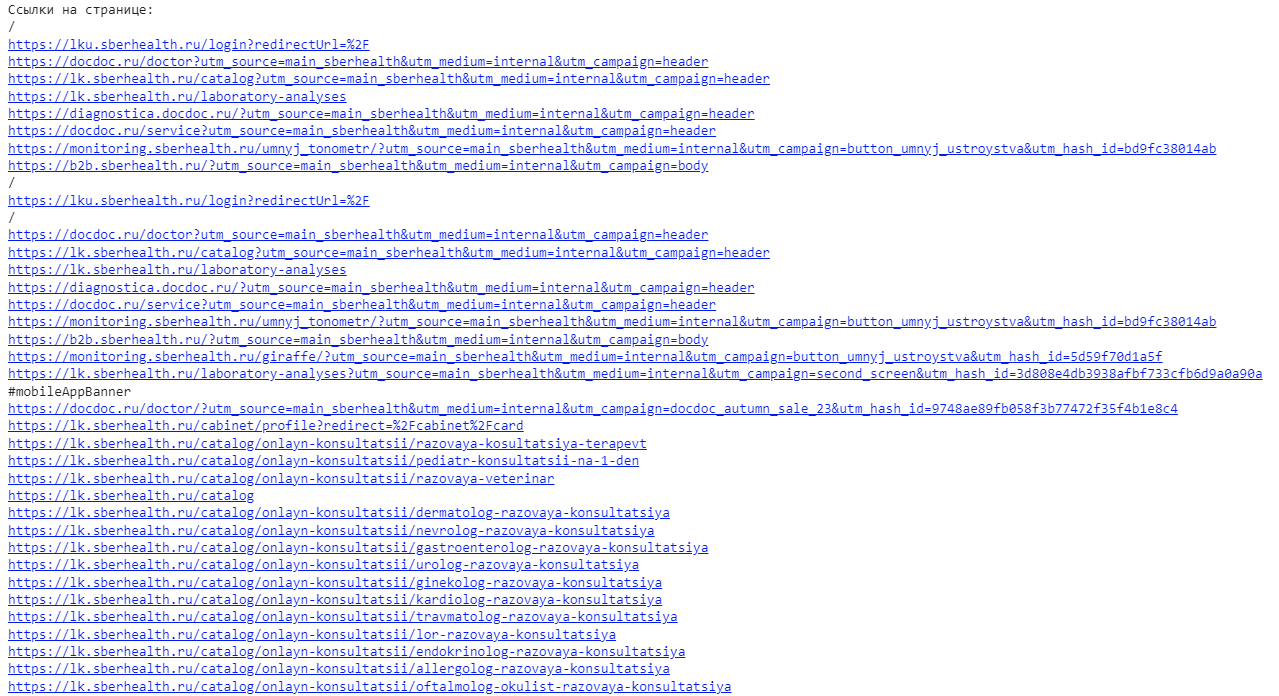
pip install bandit

Создаем скрипт который будет выводить все ссылки на представленном сайте:



### Скрипт для вывода ссылок с сайта

Выводим ссылки из сайта <https://sberhealth.ru/>, для проверки. В результате получим следующие ссылки:



Ссылки сайта

Важно отметить, что этот код не ищет уязвимости в прямом смысле этого слова. Он лишь извлекает и отображает все найденные на странице гиперссылки:

Импорт библиотек: Используются библиотеки requests для отправки HTTP-запросов и BeautifulSoup из bs4 для парсинга HTML-кода.

URL для сканирования: Задается переменная url\_to\_scan со значением "<https://sberhealth.ru/>", которая указывает на веб-страницу, подлежащую сканированию.

Функция scan\_webpage(url):

Принимает URL в качестве аргумента.

Отправляет GET-запрос к указанному URL с помощью requests.get и проверяет статус ответа через response.raise\_for\_status(), чтобы убедиться, что запрос был успешным.

Создаёт объект BeautifulSoup, который анализирует HTML-код страницы, полученный в ответе.

Находит все элементы <a> (гиперссылки) на странице и возвращает их.

Обработка ошибок: Если в процессе выполнения запроса или анализа страницы возникает ошибка, выводится сообщение об ошибке, и функция возвращает пустой список.

Вывод результатов: В основной части кода (if \_\_name\_\_ == "\_\_main\_\_":) вызывается функция scan\_webpage с URL, заданным в url\_to\_scan. Затем выводятся найденные гиперссылки.

Далее создадим скрипт для проверки ссылок на уязвимости. Для этого необходимо учитывать следующие моменты:

1. Концептуальная основа:

Генезис сценария предполагает концептуализацию его операционной парадигмы. Основная цель — автоматизировать сканирование кодовых баз Python на наличие потенциальных уязвимостей безопасности. Скрипт должен эффективно взаимодействовать с Bandit, обрабатывать выходные данные и представлять результаты в понятном формате. Ключевые соображения включают обеспечение масштабируемости, простоту интеграции в конвейеры непрерывной интеграции и получение действенной информации.

2. Обоснование выбора инструмента:

Выбор Bandit в качестве основного инструмента обусловлен его надежностью в выявлении распространенных проблем безопасности в коде Python. Комплексный набор правил Bandit, включающий проверки на SQL-инъекцию, межсайтовый скриптинг (XSS) и другие распространенные уязвимости, делает его подходящим выбором. Кроме того, способность Bandit выводить результаты в формате JSON упрощает последующую обработку данных.

3. Принципы разработки сценариев:

Дизайн скрипта придерживается принципов модульности и расширяемости. Структурирование сценария для инкапсуляции функциональности в дискретные функции повышает читаемость и удобство обслуживания. Кроме того, реализация механизмов обработки и регистрации ошибок имеет первостепенное значение для обеспечения надежности и облегчения отладки.

4. Детали реализации:

Реализация включает вызов Bandit через модуль подпроцесса Python. Этот модуль позволяет выполнять команды оболочки и получать их выходные данные. Сценарий запускает Bandit с флагами -r (рекурсивное сканирование) и -f json (вывод в формате JSON), ориентируясь на указанный каталог, содержащий проект Python.

Обработка ошибок реализована для обнаружения и сообщения о любых проблемах во время выполнения Bandit, таких как несуществующие каталоги или сбои выполнения. Анализ выходных данных JSON из Bandit позволяет извлечь ключевые данные, такие как тип обнаруженной уязвимости, ее расположение в базе кода и серьезность.

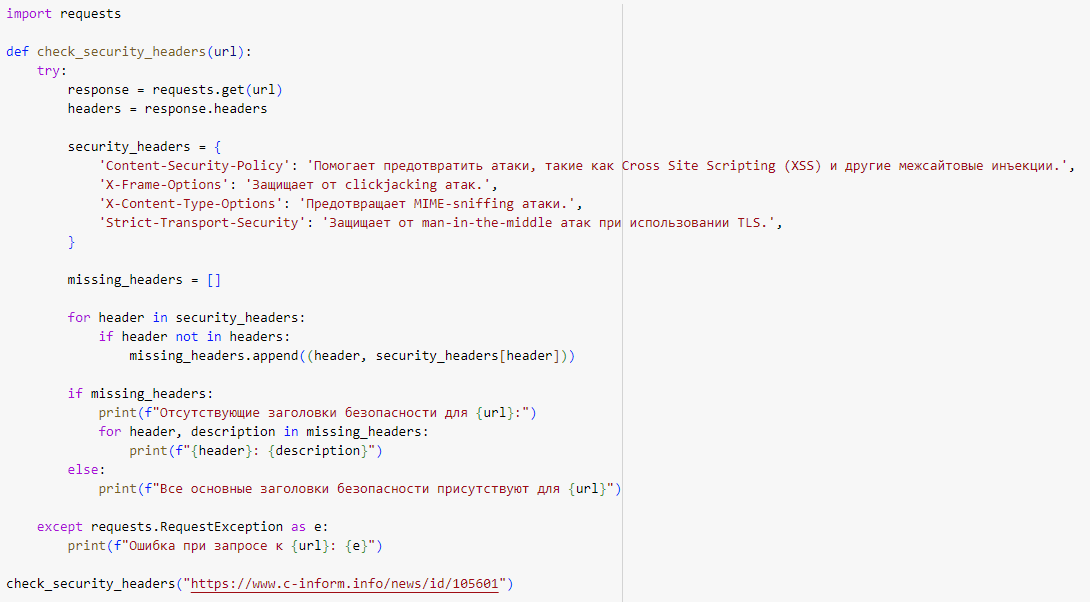
5. Анализ результатов и отчетность:

Выходные данные сценария предназначены для предоставления практической информации. Проанализированные данные включают в себя не только необработанные результаты, но и сводку, в которой выделены критические уязвимости, отсортированные по их серьезности. Этот аспект имеет решающее значение для того, чтобы дать разработчикам и аналитикам безопасности возможность расставлять приоритеты исправлений.

6. Интеграция и автоматизация:

Для практического развертывания сценарий предназначен для плавной интеграции в конвейеры непрерывной интеграции/непрерывного развертывания (CI/CD). Эта интеграция гарантирует, что базы кода автоматически сканируются на наличие уязвимостей на ключевых этапах жизненного цикла разработки, например, во время запросов на включение или перед развертыванием.

Используя Bandit, он способствует раннему обнаружению уязвимостей, способствуя защите программного обеспечения от потенциальных угроз безопасности. Однако его следует рассматривать как часть более широкой стратегии безопасности, включающей ряд инструментов и практик для обеспечения всестороннего охвата.



### Скрипт для проверки и поиска уязвимостей.

Сперва проверим сайт с безопасностями:

Ссылка полученная в результате использования первого скрипта: <https://lk.sberhealth.ru/laboratory-analyses>.

Так как протоколы и заголовки безопасности на этом сайте присутствуют, то получаем результат как показано на рисунке 7:

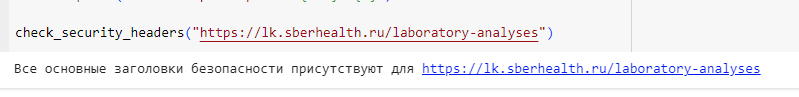


Рисунок 7. Результат выполнения запроса на проверку 1.

Теперь проверим случайный сайт без таких безопасностей (например: <https://www.c-inform.info/news/id/105601>), то получим результат следующий:

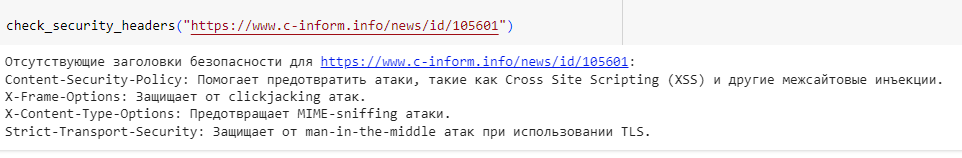


Рисунок 8. Результат выполнения запроса на проверку 2.

Можем по результату посмотреть, что наш скрипт работает.

Этические и правовые аспекты проведения оценок уязвимости имеют первостепенное значение. Соблюдение в этом исследовании этических принципов, включая ограничение тестирования авторизованными средами, создает прецедент для ответственных исследований в области кибербезопасности. Он подчеркивает необходимость учета этических соображений при разработке и проведении оценок кибербезопасности, гарантируя, что такие усилия проводятся с уважением к конфиденциальности, соблюдением законодательства и повышением безопасности, не способствуя злонамеренному использованию.

Заглядывая в будущее, результаты этого исследования открывают несколько направлений для будущих исследований. Среди них — исследование передовых алгоритмов искусственного интеллекта (ИИ) и машинного обучения (МО) для обнаружения и устранения уязвимостей кибербезопасности. Потенциал искусственного интеллекта и машинного обучения произведет революцию в оценке уязвимостей за счет прогнозирования возникающих угроз и автоматизации сложных процессов анализа, что открывает многообещающие горизонты для исследований в области кибербезопасности.

Кроме того, исследование подчеркивает важность междисциплинарных исследований в области кибербезопасности, выступая за интеграцию знаний из таких областей, как поведенческая психология, для понимания человеческих факторов, влияющих на практику кибербезопасности.

В заключение, это исследование представляет собой значительный вклад в область кибербезопасности, предлагая ценную информацию о распространенности и природе уязвимостей в веб-приложениях. Результаты подчеркивают необходимость постоянной бдительности, принятия надежных мер безопасности и важности этических соображений при проведении исследований в области кибербезопасности.

#### Заключение

Данная работа поиска уязвимостей кибербезопасности, проведенное с тщательным соблюдением научных методологий, выявило целый ряд брешей в безопасности современных веб-приложений. Благодаря использованию сложного сценария сканирования исследование выявило заметную распространенность отсутствующих заголовков безопасности, что указывает на широко распространенную уязвимость к различным кибератакам, включая, помимо прочего, межсайтовый скриптинг (XSS) и подделку межсайтовых запросов (CSRF).

Анализ также выявил нюансы понимания состояния кибербезопасности на различных платформах, подчеркнув острую необходимость в усилении мер и практик безопасности. Результаты подчеркивают необходимость активного и информированного подхода к кибербезопасности, подчеркивая важность постоянной оценки уязвимостей как части всеобъемлющей стратегии безопасности.

С теоретической точки зрения исследование вносит вклад в растущий объем знаний в области кибербезопасности, предоставляя эмпирические данные, которые подкрепляют существующие теории о цифровой уязвимости и защитных механизмах. На практике полученные данные предлагают план повышения безопасности веб-приложений, призывая к внедрению комплексных заголовков безопасности и внедрению лучших практик в управлении кибербезопасностью.

Этические аспекты этого исследования строго соблюдались, что подчеркивает важность проведения оценок уязвимости в рамках правовых и этических стандартов. С методологической точки зрения исследование подчеркнуло эффективность автоматизированных инструментов в выявлении уязвимостей безопасности, а также признало ограничения этих инструментов в определении сложности киберугроз.

Будущие исследования должны изучить развитие автоматизированных систем обнаружения уязвимостей, интегрирующих алгоритмы искусственного интеллекта (ИИ) и машинного обучения (ML) для повышения прогностических возможностей и эффективности оценок безопасности. Развитие этих технологий открывает новые горизонты в области кибербезопасности, потенциально меняя ландшафт обнаружения и устранения уязвимостей.

Существует убедительный аргумент в пользу принятия междисциплинарных подходов в изучении кибербезопасности. Объединение идей психологии, социологии и права может обеспечить более целостное понимание проблем кибербезопасности, затрагивая не только технические аспекты, но и человеческий фактор, который играет решающую роль в экосистеме безопасности.

Динамичный характер киберугроз требует продольных исследований, которые отслеживают эволюцию методов обеспечения безопасности и уязвимостей с течением времени. Такие исследования могут дать ценную информацию об эффективности мер безопасности, адаптивности киберзлоумышленников и меняющемся ландшафте цифровых уязвимостей.

Учитывая глобальный характер киберугроз, дальнейшие исследования также должны быть сосредоточены на сравнительном анализе тенденций кибербезопасности в различных регионах и секторах. Этот подход может раскрыть уникальные проблемы и лучшие практики, способствуя более полному пониманию глобальной динамики кибербезопасности.

Подводя итог, можно сказать, что это исследование представляет собой решающий шаг на пути к пониманию и смягчению уязвимостей кибербезопасности в веб-приложениях. Результаты не только подчеркивают существенные пробелы в безопасности, но и открывают путь для будущих направлений исследований, которые обещают продвинуться в области кибербезопасности. По мере того, как мы преодолеваем сложности цифровой эпохи, выводы из этого исследования подчеркивают острую необходимость согласованных усилий по усилению цифровой защиты, пропаганде этических исследовательских практик и созданию безопасной и устойчивой киберсреды для всех.