

**Отчет о результатах анализа защищенности информационной инфраструктуры ПАО "Сургутнефтегаз"**

<

Веб-приложение «ИС Avanpost IDM»

**КАЗАНЬ**

**2024**

**ОГЛАВЛЕНИЕ**

[Обозначения и сокращения 2](#_Toc178942879)

[Термины и определения 3](#_Toc178942880)

[1. Общие сведения 4](#_Toc178942881)

[2. Область исследования 5](#_Toc178942882)

[2.1. Объект исследования 5](#_Toc178942883)

[2.2. Модель нарушителя 5](#_Toc178942884)

[2.3. Ограничения проведения работ 5](#_Toc178942885)

[3. Методика исследования 6](#_Toc178942886)

[4. Основные результаты работ 8](#_Toc178942887)

[5. Оценка уровня защищенности 9](#_Toc178942888)

[6. Детальное описание хода работ и результатов 10](#_Toc178942889)

[6.1. undefined 10](#_Toc178942890)

Обозначения и сокращения

| ИТ | – | Информационные технологии |
| --- | --- | --- |
| ПО | – | Программное обеспечение |
| СУБД | – | Система управления базами данных |
| УЗ | – | Учетная запись |
| CVSS | – | Common Vulnerability Scoring System |
| HTTP | – | HyperText Transfer Protocol |
| HTTPS | – | HyperText Transfer Protocol Secure |
| IP | – | Internet Protocol |
| ISSAF | – | Information Systems Security Assessment Framework |
| NIST | – | National Institute of Standards and Technology |
| OSSTMM | – | Open-Source Security Testing Methodology Manual |
| OWASP | – | Open Web Application Security Project |
| PTES | – | Penetration Testing Execution Standard |
| RCE | – | Remote Code Execution |
| SAST | – | Static Application Security Testing |
| SCA | – | Software Composition Analysis |
| SMTP | – | Simple Mail Transfer Protocol |
| SQL | – | Structured Query Language |
| URL | – | Uniform Resource Locator |
| SSI | – | Server Side Injection |

Термины и определения

| Злоумышленник | – | Субъект, оказывающий на информационный процесс воздействия с целью вызвать его отклонение от условий нормального протекания |
| --- | --- | --- |
| Сервис | – | Идентифицируемая уникальным веб-адресом программная система со стандартизированными интерфейсами |
| Уязвимость | – | Недостаток программного (программно-технического) средства или информационной системы в целом, который может быть использован для реализации угроз безопасности информации |
| Чувствительная информация | – | Информация, которая может позволить злоумышленнику выстроить дальнейший вектор атаки |
| Эксплойт | – | Компьютерная программа, фрагмент программного кода или последовательность команд, использующие уязвимости в программном обеспечении и применяемые для проведения атаки на вычислительную систему |
| Remote Code Execution (RCE) | – | Критическая уязвимость, которая позволяет злоумышленнику дистанционно запустить вредоносный код в целевой системе по локальной сети или через Интернет |

# Общие сведения

Данный отчет составлен по результатам анализа защищенности информационной инфраструктуры ПАО "Сургутнефтегаз".

**Заказчик:** ПАО "Сургутнефтегаз"

**Исполнитель:** ООО «Телеком интеграция»

**Даты проведения работ:** 21.10.2024 г. – 25.10.2024 г.

Целью проведения исследования является:

* выявление недостатков в применяемых Заказчиком мерах информационной безопасности и оценка возможности их использования нарушителем;
* получение на основе объективных свидетельств анализа текущего уровня защищённости инфраструктуры Заказчика;
* выявление уязвимостей и ошибок конфигурации, проведение попыток их эксплуатации для получения привилегий в инфраструктуре Заказчика;
* выработка рекомендаций по устранению выявленных уязвимостей для повышения уровня защищённости инфраструктуры Заказчика.

В ходе проведения анализа защищенности информационной инфраструктуры были выполнены следующие работы:

* выявление уязвимостей ресурсов внешней инфраструктуры Заказчика, способных привести к возможности осуществления несанкционированного воздействий на них;
* попытки получения несанкционированного доступа к внутренним ресурсам Заказчика;
* попытки получения учетных записей и паролей пользователей и администраторов информационных систем Заказчика.

Отчет содержит данные об области исследования, методику исследования, описание процесса проведения работ, результаты анализа, в том числе экспертную оценку уровня защищенности и перечень выявленных уязвимостей.

# Область исследования

## Объект исследования

Объектом исследования являлись публично доступные сервисы информационной системы Заказчика в сети Интернет, а именно Веб-приложение «ИС Avanpost IDM».

Работы проводились на территории Исполнителя путем удаленного подключения к инфраструктуре Заказчика.

## Модель нарушителя

В ходе проведения анализа защищенности информационной инфраструктуры рассматривался внешний нарушитель 1.

## Ограничения проведения работ

В ходе проведения работ по анализу защищенности информационной инфраструктуры не предполагалось обнаружение всех существующих на настоящий момент проблем безопасности тестируемых систем Заказчика. Акцентирование внимания выполнялось на наиболее критичных уязвимостях, эксплуатация которых может привести к серьезным негативным последствиям для Заказчика.

# Методика исследования

Анализ защищенности информационной инфраструктуры выполняется путем имитации действий потенциального злоумышленника по выявлению уязвимых мест тестируемого ресурса и анализа последствий эксплуатации обнаруженных уязвимостей.

Исследование проводится по модели «Черный ящик», которая подразумевает отсутствие   
какой-либо информации у потенциального злоумышленника о внешнем или внутреннем устройстве сети Заказчика.

Анализ защищенности проводится с учетом международных стандартов и лучших практик:

* Penetration Testing Execution Standard (PTES);
* NIST Special Publications 800-115 Technical Guide to Information Security Testing and Assessment;
* Open-Source Security Testing Methodology Manual (OSSTMM);
* Information Systems Security Assessment Framework (ISSAF);
* Common Vulnerability Scoring System (CVSS);
* Open Web Application Security Project (OWASP) Testing Guide;
* Web Application Security Consortium (WASC) Threat Classification;
* Software composition analysis (SCA);
* Static Application Security Testing (SAST).

В ходе проведения работ используются как ручные проверки возможных уязвимостей, так и проверки с использованием инструментов автоматизации поиска уязвимостей.

В процессе исследования используются следующие программные средства:

* средства инструментального сканирования как общего назначения, так и специализированные (Nmap, Nikto и другие);
* комплексное решение для анализа защищенности (Kali Linux);
* интернет-браузер Google Chrome;
* общедоступные эксплойты;
* ПО собственной разработки различного назначения;
* ПО для подбора паролей (Hydra, Hashcat, и другие);
* специализированные решения для анализа защищенности веб-приложений (gobuster, BurpSuite и другие);
* Прочее специализированное ПО (Proxychains, SQLMap, и другие).

При оценке уровня защищенности информационной инфраструктуры Заказчика учитываются минимально необходимые компетенции злоумышленника для реализации вектора направленного на преодоление сетевого периметра или на получение доступа к критичному объекту сетевой ИТ‑инфраструктуры.

Квалификация злоумышленника:

* **Низкая квалификация:** базовые знания о проведении атак на информационную инфраструктуру. Использование автоматизированных средств проведения атак, применение публично доступных эксплойтов без модификаций.
* **Средняя квалификация:** использование узко специализированного ПО для проведения атак, навыки модификации публично доступных эксплойтов.
* **Высокая квалификация:** глубокие знания об особенностях работы информационной инфраструктуры. Навыки написания эксплойтов для выявляемых уязвимостей.

Критичность ресурса:

* **Низкая:** компрометация не влечет за собой значительных негативных последствий для информационной инфраструктуры Заказчика.
* **Высокая:** компрометация ресурса влечет за собой значительные финансовые и/или репутационные потери.

Оценка уровня защищенности информационной инфраструктуры Заказчика осуществляется исходя из сводной таблицы (Таблица 3.1).

Таблица 3.1 – Сводная таблица оценки уровня защищенности

|  |  |  |  |
| --- | --- | --- | --- |
| **Квалификация**  **злоумышленника**  **Критичность**  **ресурса** | **Низкая** | **Средняя** | **Высокая** |
| **Не скомпрометировано** | Высокий | Высокий | Высокий |
| **Низкая** | Низкий | Средний | Выше среднего |
| **Высокая** | Крайне низкий | Ниже среднего | Средний |

# Основные результаты работ

В рамках работ по анализу защищенности информационной инфраструктуры методом «черного ящика» были получены следующие результаты:

* в ходе перебора директорий по URL-адресу **<Адрес>** была обнаружена страница отладочной панели «Yii Debugger», доступная без предварительной авторизации;
* была обнаружена чувствительная информация об используемой СУБД и SMTP-сервере в ресурсах отладочной панели «Yii Debugger»;
* была обнаружена утечка персональных данных сотрудников, включая ФИО, номера телефонов, электронные почты и другую чувствительную информацию;
* была выявлена уязвимость Remote Code Execution (RCE), позволяющая удаленно запустить произвольный код или команды в целевой системе.

Основные результаты анализа защищенности информационной инфраструктуры методом «черного ящика» приведены в таблице ниже (Таблица 4.1).

Таблица 4.1 – Результаты анализа защищенности информационной инфраструктуры

| **№** | **URL-адрес** | **Критичность** | **Сложность эксплуатации** | **Обнаруженные уязвимости** | **Описание и рекомендации** |
| --- | --- | --- | --- | --- | --- |
| **1** | **2** | **3** | **4** | **5** | **6** |
|  | <Адрес> | Высокая | Низкая | * Публичный доступ к отладчику | п. 6.1 |
|  | <Адрес №1>  …  <Адрес №N> | Высокая | Низкая | * Уязвимость Remote Code Execution (RCE) | п. 6.2 |

Детальное описание проведения атак указано в 6.

# Оценка уровня защищенности

Методика оценки уровня защищенности с учетом критичности ресурса и квалификации злоумышленника приведена в п.3.

Уровень защищённости ресурса **Веб-приложение «ИС Avanpost IDM»** от внешнего нарушителя оценивается как **ниже среднего**, так как в ходе тестирования методом «черного ящика» выявлена уязвимость, позволяющая удаленно запустить произвольный код или команды в целевой системе, в результате чего был получен контроль над уязвимой системой. Дополнительно в ходе работ были обнаружены персональные данные сотрудников организации в открытом виде и чувствительная информация об используемой СУБД.

**От внешнего нарушителя ресурса Веб-приложение «ИС Avanpost IDM»**

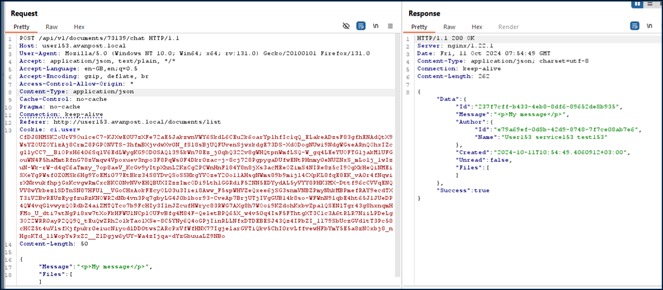
# Детальное описание хода работ и результатов

## Проверка подверженности уязвимости «IDOR» в обсуждениях заявок

**CVSS балл:** ()

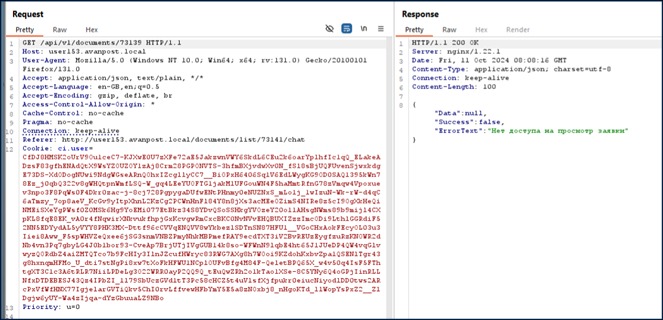
**Описание:**

С целью выявления нарушений контроля доступа на странице обсуждения заявок специалистами Исполнителя был выполнен POST-запрос типа **/api/v1/documents/{document\_id}/chat** , который позволяет отправлять сообщения в обсуждение других заявок (см. Запрос на отправку сообщения в обсуждение другой заявки).

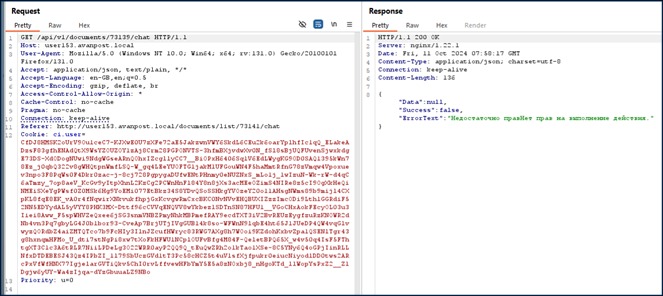


Запрос на отправку сообщения в обсуждение другой заявки

Однако при попытке получения доступа к заявкам и её содержимого с помощью GET-запроса формата **GET /api/v1/documents/73139/chat**, веб-сервер возвращает сообщения об ошибке «Недостаточно прав» или «Нет доступа на просмотр» (см. Запрос на просмотр другой заявки - см. Запрос на просмотр обсуждения другой заявки) .



Запрос на просмотр другой заявки



Запрос на просмотр обсуждения другой заявки

**Наблюдения:**

**Ссылки:**

**Доказательства:**

**Затронутые активы:**

**Рекомендации:**

Уровень трудности устранения: средний

Приоритет:

* рекомендуется использовать уникальные идентификаторы, например, UUID, GUID, для идентификации защищенных объектов. Избегать использования идентификаторов, которые можно угадать или перебрать;
* использовать косвенные ссылки, вместо прямых ссылок на объекты;
* убедиться, что каждый запрос на доступ к объекту сопровождается проверкой, что пользователь имеет право выполнять запрашиваемое действие;
* убедиться, что пользователи имеют доступ только к тем ресурсам и функциям, которые необходимы для их работы;
* использовать механизмы контроля доступа;
* доступ к любым частям системы, особенно к функциям администрирования, должен быть закрыт, если не установлено иное, отказ в доступе должен быть установлен по умолчанию.