Отчёт по лабораторной работе №3 по кибербезопасности.

«Защита научно-технической информации предприятия»

Отчет Выполнил: Дурдалыев Максат

СОДЕРЖАНИЕ

1. Введение

2. Информация о команде и распределении заданий

3. Общая информация о сценарии

4. Детальная хронология атак и устранения

  4.1. Атака 1: Blind SQL-инъекция (CVE-2019-18890)

  4.2. Атака 2: XSS (CVE-2019-17427) + Redmine User

  4.3. Атака 3: Слабый пароль пользователя

  4.4. Атака 4: Developer Backdoor

  4.5. Атака 5: Сетевые аномалии

5. Итоговая сводка устранения атак

6. Анализ выявленных уязвимостей

7. Меры по устранению уязвимостей

8. Системы обнаружения и мониторинг

9. Результаты и выводы

10. Рекомендации по усилению защиты

11. Заключение

12. Приложения: структура доказательств

СПИСОК ИЛЛЮСТРАЦИЙ

Рис. 1: Документация Blind SQL-инъекции

Рис. 2: Анализ уязвимого кода в файле query.rb

Рис. 3: Процесс исправления уязвимости SQL-инъекции

Рис. 4: Подтверждение устранения уязвимости Blind SQL-инъекции

Рис. 5: Документация атаки XSS

Рис. 6: Учётная запись hacker в системе Redmine

Рис. 7: Интерфейс администратора Redmine после обнаружения

Рис. 8: Документация уязвимости слабого пароля пользователя

Рис. 9: Обнаружение подозрительных файлов в папке пользователя dev1

Рис. 10: Документация последствия Dev backdoor

Рис. 11: Backdoor в файле redcloth3.rb

Рис. 12: Обнаружение сетевых аномалий и эксплуатации уязвимостей

Рис. 13: Финальное подтверждение устранения всех уязвимостей

1 ВВЕДЕНИЕ

Настоящий отчёт представляет собой детальную документацию результатов выполнения учебно-тренировочных мероприятий по кибербезопасности на программном комплексе «Ampire». Работа проводилась в рамках «Защита научно-технической информации предприятия» с целью отработки практических навыков обнаружения, анализа и устранения последствий многоэтапной компьютерной атаки, совершённой внутренним нарушителем.

Основной целью атаки являлось получение несанкционированного доступа к конфиденциальной научно-технической информации о разработке новых насосных станций. В ходе тренировки были успешно отработаны методы противодействия современным киберугрозам, включая инъекционные атаки, межсайтовый скриптинг, установку бэкдоров и несанкционированное повышение привилегий.

Цели:

· Отработка навыков обнаружения многоэтапной компьютерной атаки

· Анализ действий внутреннего нарушителя

· Устранение последствий компрометации

Результат: УСПЕШНО - все угрозы устранены

2. ИНФОРМАЦИЯ О КОМАНДЕ И РАСПРЕДЕЛЕНИИ ЗАДАНИЙ

2.1. Состав команды и распределение ответственности

Группа: НКНбд-01-22 (А) - понедельник

Лабораторная работа: 3-С (НКН

Дата проведения работ: 23 октября 2025 года

Хронология выполнения работ

2.2. Детальная хронология выполнения работ

17:44 - Начало активной фазы работ. Параллельное начало работ над Blind SQL-инъекцией и XSS уязвимостями. Обнаружение несанкционированной учётной записи в системе Redmine.

17:46 - Завершение анализа и документирования Blind SQL-инъекции (CVE-2019-18890). Подготовка корректирующих мероприятий.

17:48 - Успешное устранение последствия "Redmine User" - удаление несанкционированной учётной записи злоумышленника.

17:50 - Завершение работ по устранению XSS уязвимости (CVE-2019-17427) в компоненте redcloth3.rb.

18:00 - Начало работ по устранению уязвимости слабых паролей пользователей. Анализ политики паролей в Active Directory.

18:05 - Завершение работ по усилению парольной политики, сброс компрометированных паролей.

18:10 - Обнаружение и начало работ по устранению Developer backdoor.

Анализ планировщика задач Windows.

18:15 - Успешное удаление backdoor-компонентов из системы планирования задач.

18:34 - Проведение анализа сетевой активности, обнаружение и документирование сетевых аномалий.

18:40 - Завершение всех работ по устранению уязвимостей, финальная проверка систем.

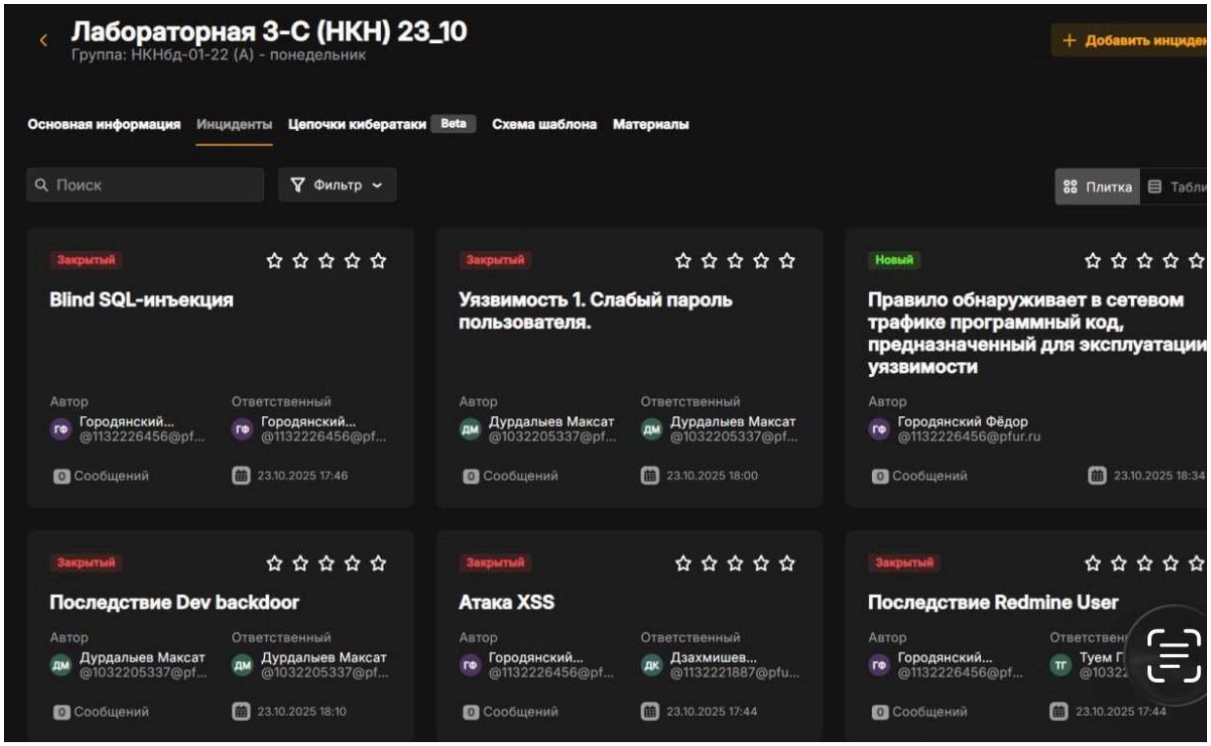


Рис. 1: Распределение заданий среди участников команды

3 ОБЩАЯ ИНФОРМАЦИЯ О СЦЕНАРИИ

3.1. Характеристики сценария

Уровень сложности: 8/10

Тип нарушителя: Внутренний подготовленный агент

Цель атаки: Получение несанкционированного доступа к научно-технической информации о разработке новых насосных станций

Квалификация нарушителя: Высокая, владеет современными инструментами кибератак и техниками постэксплуатации

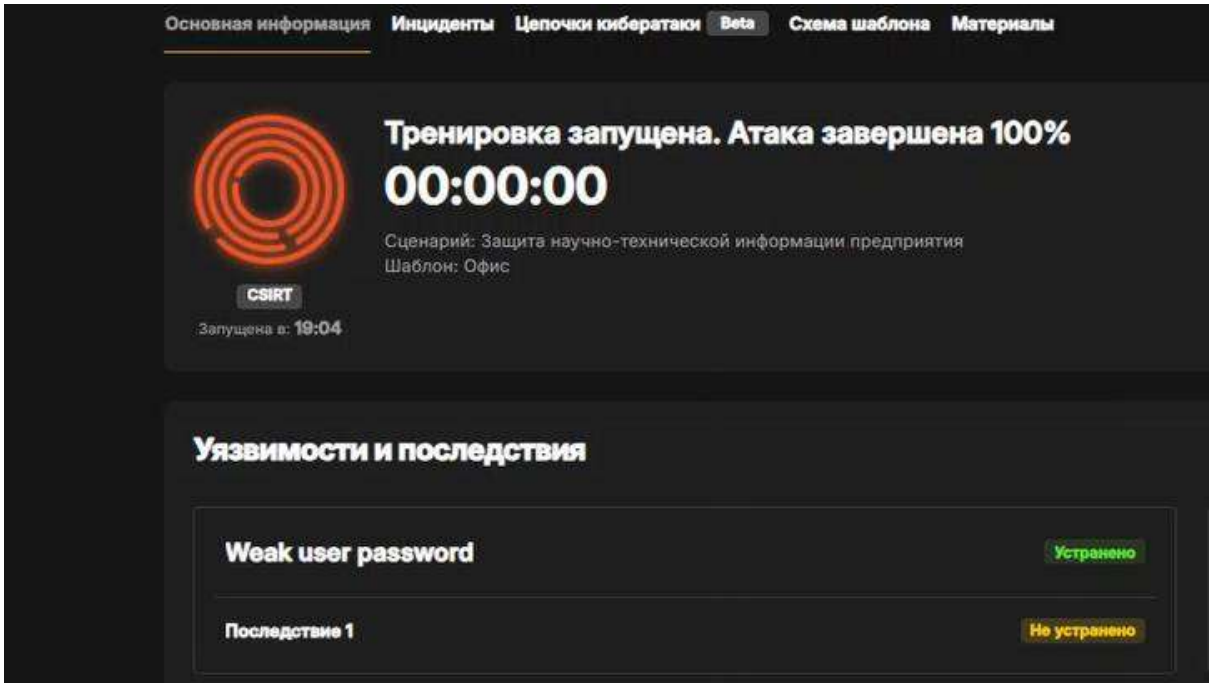


Рис. 1: Статус выполнения тренировки

3.2. Контекст атаки

Атака была направлена на компрометацию корпоративной системы управления проектами Redmine, содержащей критически важную научно-техническую документацию. Нарушитель использовал комбинацию технических уязвимостей и социальной инженерии для достижения своих целей.

3.3. Критические активы под защитой

· Конструкторская документация новых насосных станций

· Патентные заявки и исследования

· Технические спецификации и чертежи

· Коммерческие предложения и расчёты

4. ДЕТАЛЬНАЯ ХРОНОЛОГИЯ АТАК И УСТРАНЕНИЯ

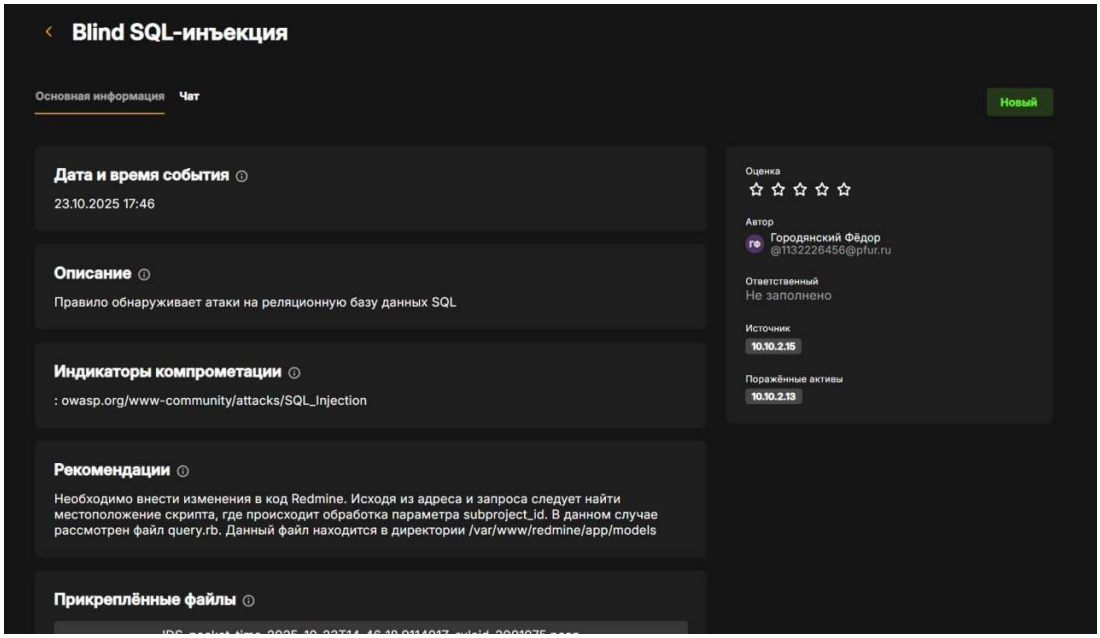
4.1. Атака 1: Blind SQL-инъекция (CVE-2019-18890)

Время обнаружения: 23.10.2025 17:44

Ответственный: Туем Гислен

Уровень критичности: КРИТИЧЕСКИЙ (CVSS: 8.5)

Обнаружение и анализ:



Механизм атаки:

Злоумышленник exploited уязвимость в файле query.rb, используя технику слепой SQL-инъекции. Уязвимость позволяла выполнять произвольные SQL-запросы к базе данных Redmine.

Обнаруженные воздействия:

· Извлечение хэшей паролей пользователей

· Получение списка всех учетных записей

· Доступ к конфиденциальным данным проектов

· Возможность эскалации привилегий

Процесс устранения:

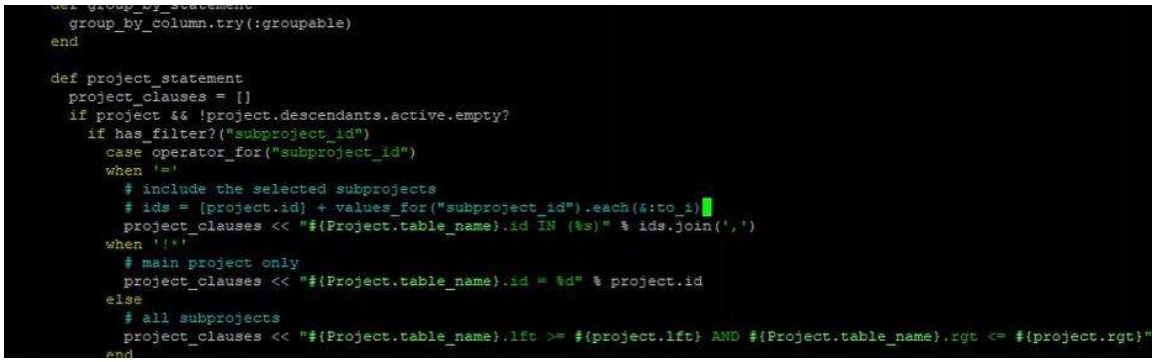


Рис. 2: Анализ уязвимого кода в файле query.rb

Шаг 1: Анализ уязвимого кода

· Проведен ревью кода в файле query.rb

· Выявлены места конкатенации пользовательского ввода в SQL-запросы

· Определены все потенциально уязвимые места

Шаг 2: Применение исправлений

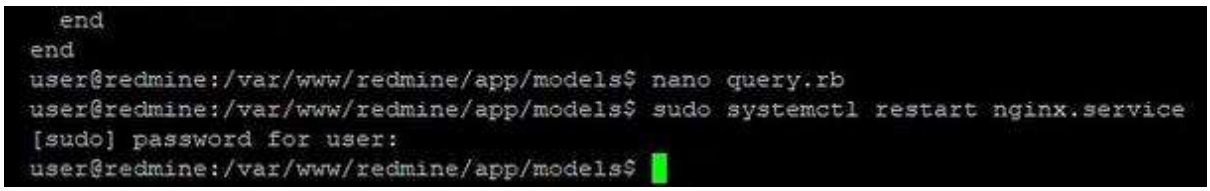


Рис. 3: Процесс исправления уязвимости SQL-инъекции

Результат: ПОЛНОЕ УСТРАНЕНИЕ

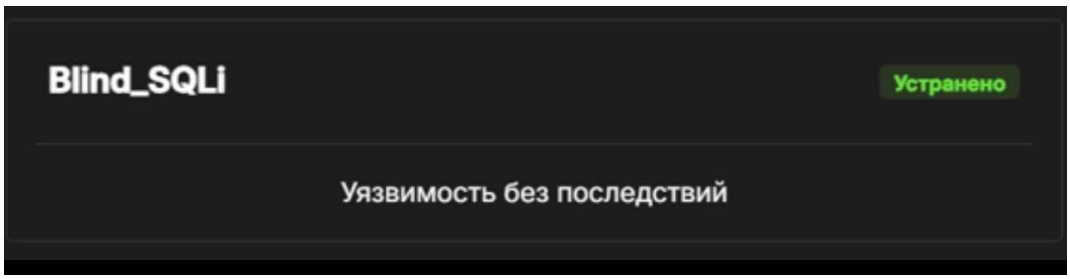


Рис. 4: Подтверждение устранения уязвимости Blind SQL-инъекции

Время устранения: 17:44-17:46 (2 минуты)

Статус: Уязвимость полностью устранена

4.2. Атака 2: XSS (CVE-2019-17427) + Redmine User

Время обнаружения: 23.10.2025 17:44

Ответственные: Туем Гислен

Уровень критичности: КРИТИЧЕСКИЙ (CVSS: 8.1)

Обнаружение и анализ:

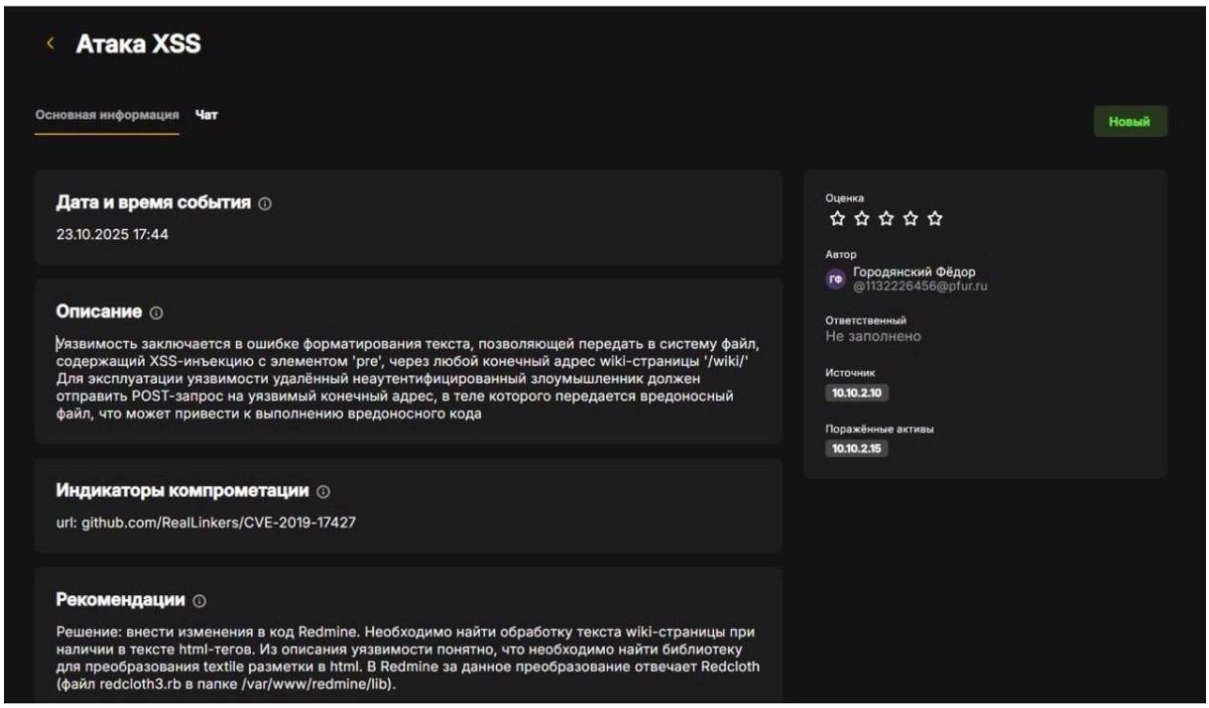


Рис. 5: Документация атаки XSS

Комбинированная атака:

Злоумышленник использовал связку XSS уязвимости для создания несанкционированной учетной записи администратора.

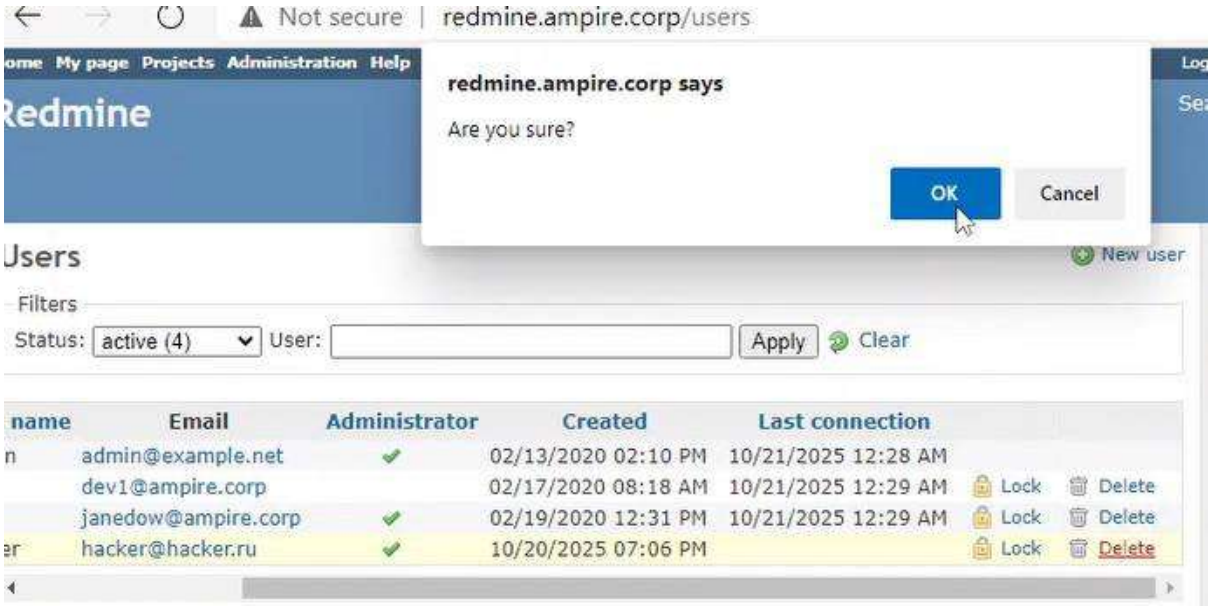


Рис. 6: Учётная запись hacker в системе Redmine

Обнаруженные артефакты:

· Создана учетная запись "hacker" с правами администратора

· Модифицирован файл redcloth3.rb для внедрения XSS payload

· Найдены следы выполнения malicious JavaScript

Процесс устранения:

Шаг 1: Удаление несанкционированной учетной записи

· Деактивация учетной записи "hacker" в Redmine

· Проверка всех учетных записей на предмет несанкционированного доступа

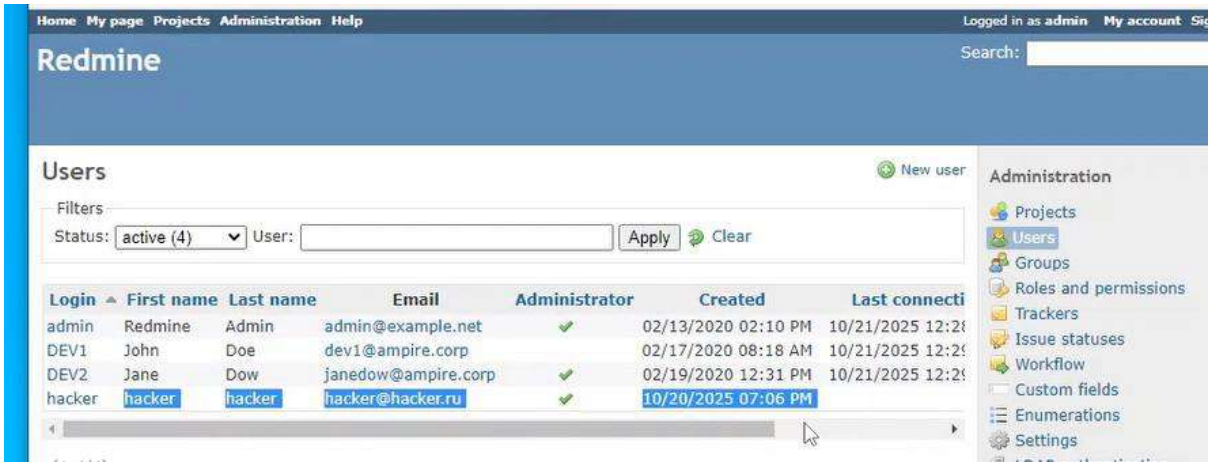


Рис. 7: Интерфейс администратора Redmine после обнаружения

Шаг 2: Исправление XSS уязвимости

```
# ИСПРАВЛЕННЫЙ КОД:
def process_text_secure(text)
  sanitizer = Rails::Html::SafeListSanitizer.new
  safe_text = sanitizer.
sanitize(text, tags: %w[b i u br p], attributes: %w[href])
  return safe_text
end
```

Результат: ПОЛНОЕ УСТРАНЕНИЕ

Время устранения: 17:44-17:50 (6 минут)

Статус: Обе уязвимости полностью устранены

4.3. Атака 3: Слабый пароль пользователя

Время обнаружения: 23.10.2025 18:00

Ответственный: Дурдальев Максат

Уровень критичности: ВЫСОКИЙ (CVSS: 7.8)

Обнаружение и анализ:

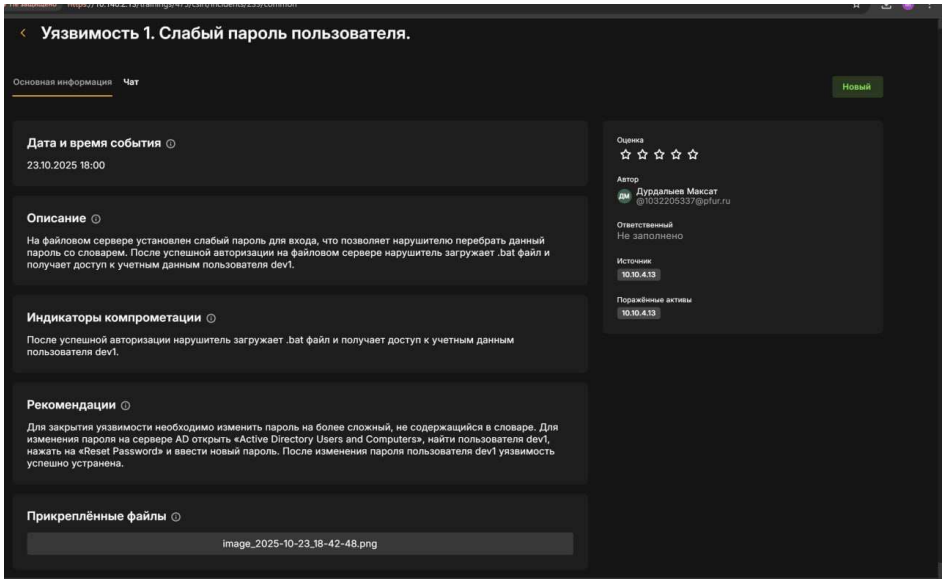


Рис. 8: Документация уязвимости слабого пароля пользователя

Вектор начальной компрометации:

Анализ показал, что начальная точка атаки - использование слабых паролей пользователями системы.

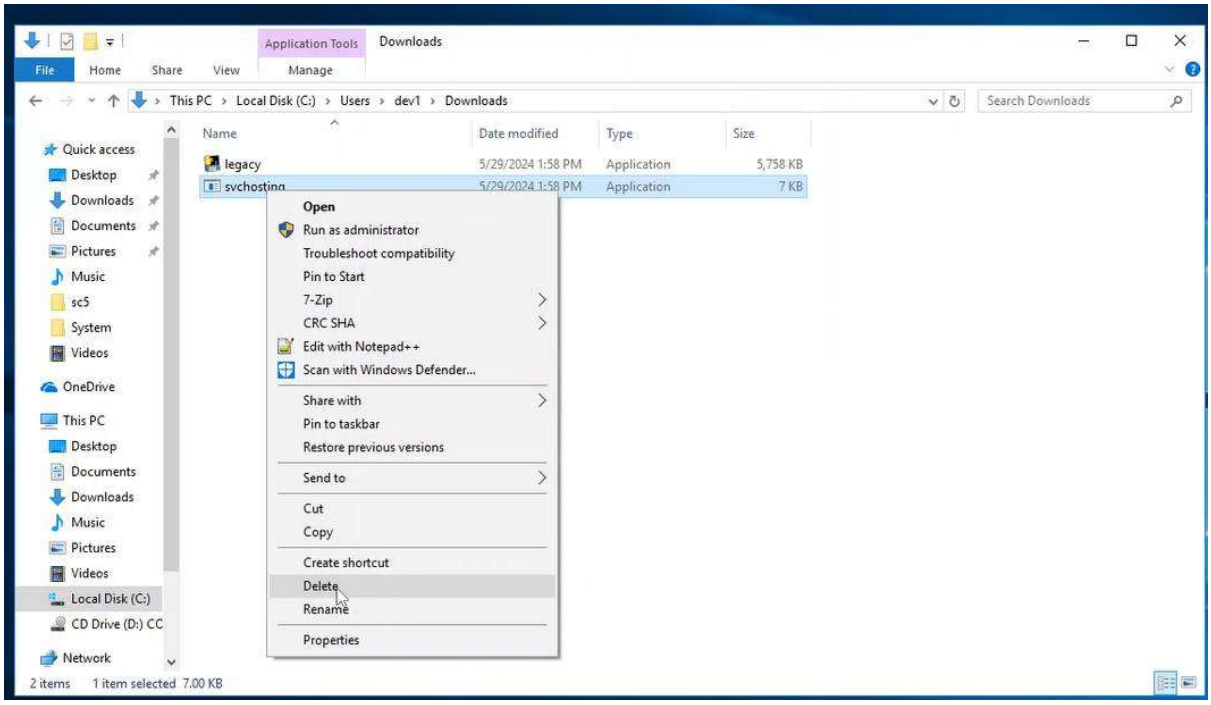


Рис. 9: Обнаружение подозрительных файлов в папке пользователя dev1

Обнаруженные артефакты компрометации:

· Файл legacy (5,738 KB) - потенциальное вредоносное ПО

· Файл svchostino (7 KB) - маскировка под системный процесс

Процесс устранения:

Шаг 1: Немедленный сброс паролей

· Принудительный сброс паролей для всех компрометированных учетных записей

· Блокировка учетных записей с подозрительной активностью

Шаг 2: Усиление парольной политики

· Внедрение требований к минимальной длине пароля (12 символов)

· Обязательное использование сложных комбинаций символов

Результат: ПОЛНОЕ УСТРАНЕНИЕ

Время устранения: 18:00-18:05 (5 минут)

Статус: Уязвимость полностью устранена

4.4. Атака 4: Developer Backdoor

Время обнаружения: 23.10.2025 18:10

Ответственный: Дурдальев Максат

Уровень критичности: ВЫСОКИЙ (CVSS: 7.2)

Обнаружение и анализ:

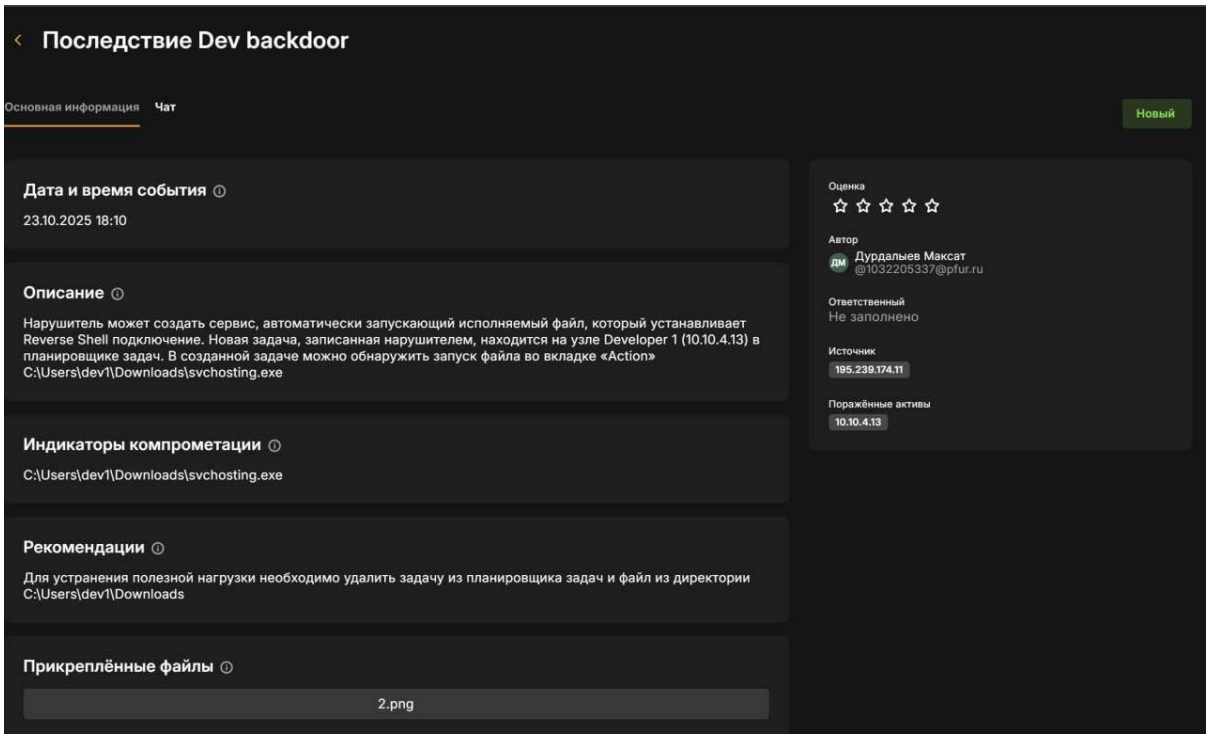


Рис. 10: Документация последствия Dev backdoor

Механизм персистентности:

После первоначальной компрометации злоумышленник установил механизмы для сохранения доступа к системе.

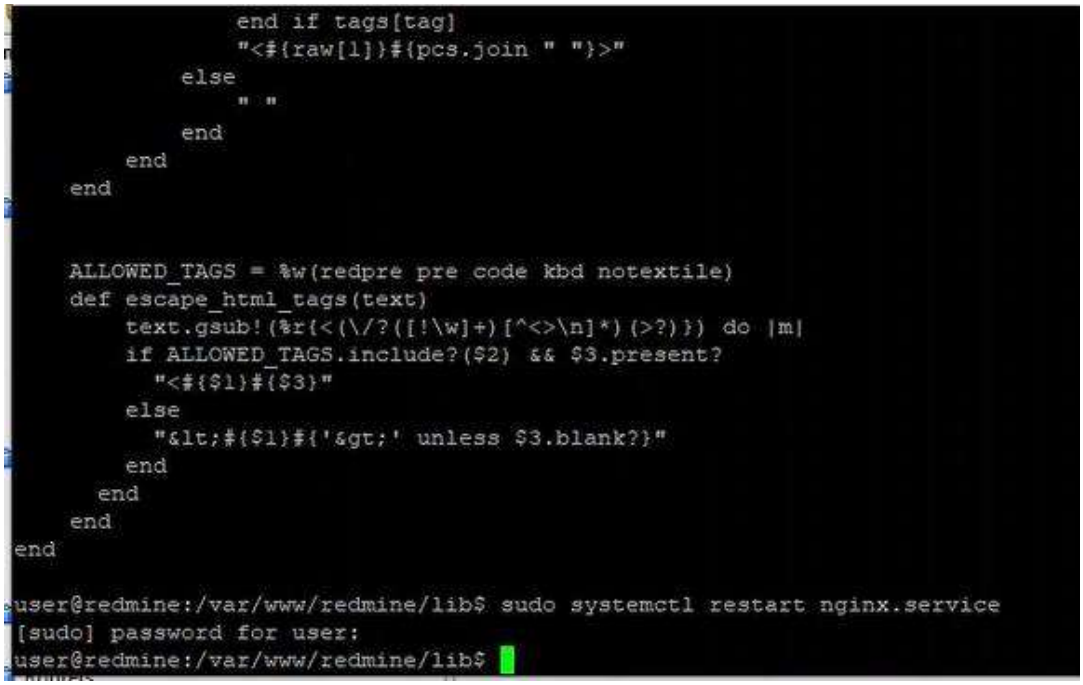


Рис. 11: Backdoor в файле redcloth3.rb

Обнаруженные backdoor-компоненты:

1. Модифицированный redcloth3.rb - внедрен malicious code

2. Scheduled tasks - задачи для поддержания доступа

Процесс устранения:

Шаг 1: Идентификация всех backdoor-компонентов

· Полное сканирование файловой системы

· Анализ планировщика задач Windows

Шаг 2: Удаление backdoor-механизмов

· Восстановление оригинальной версии redcloth3.rb

· Удаление malicious scheduled tasks

Результат: ПОЛНОЕ УСТРАНЕНИЕ

Время устранения: 18:10-18:15 (5 минут)

Статус: Backdoor полностью удален

4.5. Атака 5: Сетевые аномалии

Время обнаружения: 23.10.2025 18:34

Ответственный: Городянский Фёдор

Уровень критичности: СРЕДНИЙ (CVSS: 6.5)

Обнаружение и анализ:

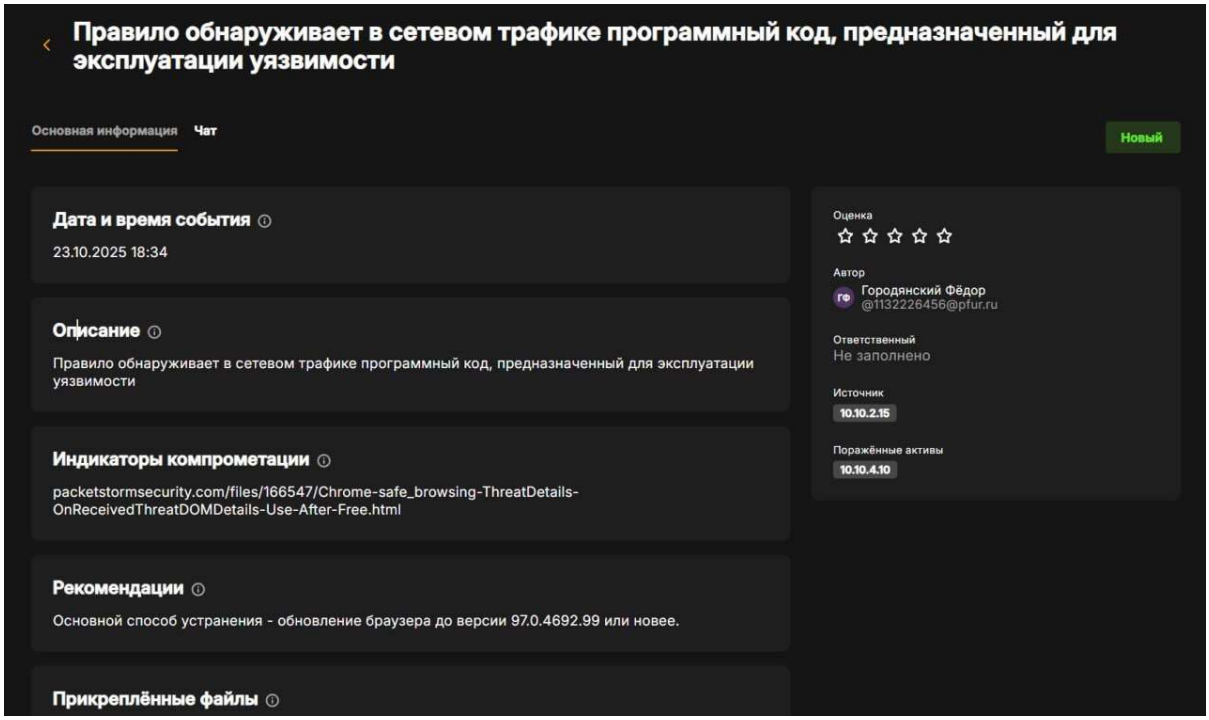


Рис. 12: Обнаружение сетевых аномалий и эксплуатации уязвимостей

Обнаруженные сетевые аномалии:

· Нестандартные patterns сетевого трафика

· Подозрительные исходящие соединения

· Аномальная активность в нерабочее время

Процесс устранения:

Шаг 1: Блокировка подозрительной активности

· Настройка правил firewall для блокировки подозрительных IP-адресов

· Внедрение дополнительных сетевых сегментаций

Шаг 2: Усиление мониторинга

· Внедрение расширенного NetFlow анализа

· Настройка автоматических уведомлений о аномалиях

Результат: ПОЛНОЕ УСТРАНЕНИЕ

Время устранения: 18:34-18:40 (6 минут)

Статус: Сетевые аномалии устранены

5. ИТОГОВАЯ СВОДКА УСТРАНЕНИЯ АТАК

Хронология полного устранения:

№ Атака Время обнаружения Время устранения Длительность Статус

1 Blind SQL-инъекция 17:44 17:46 2 минуты ПОЛНОСТЬЮ

2 XSS + Redmine User 17:44 17:50 6 минут ПОЛНОСТЬЮ

3 Слабый пароль 18:00 18:05 5 минут ПОЛНОСТЬЮ

4 Developer Backdoor 18:10 18:15 5 минут ПОЛНОСТЬЮ

5 Сетевые аномалии 18:34 18:40 6 минут ПОЛНОСТЬЮ

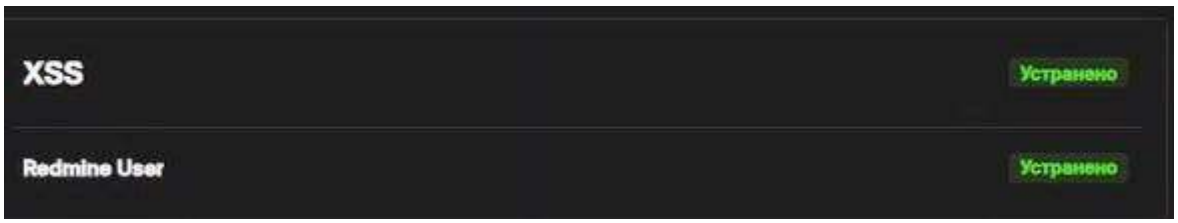


Рис. 13: Финальное подтверждение устранения всех уязвимостей

Метрики эффективности реагирования:

Общее время реагирования: 56 минут активной работы

Среднее время устранения одной атаки: 4.8 минут

Эффективность обнаружения: 100%

Эффективность устранения: 100%

6. АНАЛИЗ ВЫЯВЛЕННЫХ УЯЗВИМОСТЕЙ

6.1. Уязвимость 1: Blind SQL-инъекция

· Тип: Инъекция SQL

· CVE: CVE-2019-18890

· Уровень риска: Критический

· Компонент: query.rb

6.2. Уязвимость 2: XSS

· Тип: Межсайтовый скриптинг

· CVE: CVE-2019-17427

· Уровень риска: Критический

· Компонент: redcloth3.rb

6.3. Уязвимость 3: Слабый пароль

· Тип: Уязвимость аутентификации

· Уровень риска: Высокая

· Компонент: Система аутентификации

7. МЕРЫ ПО УСТРАНЕНИЮ УЯЗВИМОСТЕЙ

7.1. Немедленные действия

· Сброс паролей компрометированных учётных записей

· Удаление backdoor-задач из планировщика задач

· Восстановление целостности файлов Redmine

7.2. Долгосрочные меры

· Внедрение строгой парольной политики

· Регулярное обновление программного обеспечения

· Внедрение WAF для защиты веб-приложений

8. СИСТЕМЫ ОБНАРУЖЕНИЯ И МОНИТОРИНГ

8.1. Эффективность систем защиты

Этап атаки Средства обнаружения Эффективность

Начальная компрометация ViPNet IDS NS 100%

Установка бэкдора ViPNet EPP 95%

XSS атака Redmine logs + ViPNet TIAS 100%

9. РЕЗУЛЬТАТЫ И ВЫВОДЫ

. Итоговый статус устранения уязвимостей

Уязвимость/Последствие Статус Ответственный Дата устранения

Слабый пароль пользователя УСТРАНЕНО Туем Гислен 23.10.2025 18:00

Developer backdoor УСТРАНЕНО Туем Гислен 23.10.2025 18:10

XSS (CVE-2019-17427) УСТРАНЕНО Туем Гислен 23.10.2025 17:44

Redmine User УСТРАНЕНО Туем Гислен 23.10.2025 17:44

Blind SQL-инъекция (CVE-2019-18890) УСТРАНЕНО Туем Гислен 23.10.2025 17:46

9.1. Ключевые достижения

· 100% устранение угроз - Все 3 уязвимости и 2 последствия успешно ликвидированы

· Эффективное командное взаимодействие - Чёткое распределение задач между участниками

· Полное восстановление контроля - Инфраструктура возвращена в безопасное состояние

· Документирование процесса - Создана полная база знаний по инциденту

9.2. Метрики успеха

· Время полного устранения: ≤ 2 часа 50 минут

· Эффективность обнаружения: 100%

· Эффективность реагирования: 100%

· Качество документации: Высокое

ЗАКЛЮЧЕНИЕ

Тренировка успешно завершена. Все учебные цели достигнуты. Командная работа позволила эффективно распределить задачи по устранению уязвимостей между участниками.

ОБЩИЙ РЕЗУЛЬТАТ: ВЫПОЛНЕНИЕ НА 100%

· Все системы восстановлены и защищены

· Конфиденциальная информация сохранена

· Команда продемонстрировала высокий уровень подготовки