Отчет по лабораторной работе №2

Дисциплина: Кибербезопасность предприятия

Боровиков Даниил

Хрусталев Влад

Гисматуллин Артём

Чесноков Артёмий

Коннова Татьяна

Нефедова Наталья

Уткина Алина

Бансимба Клодели

Содержание

# 1 Задание. Сценарий №5.

ЗАЩИТА НАУЧНО-ТЕХНИЧЕСКОЙ ИНФОРМАЦИИ ПРЕДПРИЯТИЯ

Внешний нарушитель умеет использовать инструментарий для проведения компьютерных атак, знает техники постэксплуатации.

Средство обнаружения вторжений – программно-аппаратный комплекс для обнаружения вторжений в информационные системы ViPNet IDS NS.

Автоматическое выявление инцидентов на основе интеллектуального анализа событий информационной безопасности – программно-аппаратный комплекс ViPNet TIAS.

ViPNet EPP применяется для защиты отдельных компонентов информационной инфраструктуры организаций – персональных компьютеров пользователей и корпоративных серверов.

Специализированный контроль сетевой безопасности и предотвращение проникновения, упрощающие централизованное управление сетью – Security Onion. Security Onion связывает воедино три основные функции: - полный захват пакетов; - обнаружение сетей и конечных точек; - мощные инструменты анализа.

# 2 Последовательность действий нарушителя

1. Внутренний нарушитель подбирает пароль на файловый сервер и меняет существующий на сервере файл другим файлом с backdoor (дефектом алгоритма).
2. Пользователь Dev-1 загружает и запускает файл с backdoor.
3. Внутренний нарушитель получает контроль над компьютером пользователя Dev-1 и загружает скрипт для похищения учетных данных из браузера. Запускает данный скрипт и получает логин и пароль к Redmine.
4. Внутренний нарушитель проводит атаку stored XSS для включения на Redmine сервере REST API. Вредоносный код записывается на Wikiстраницу проекта Dev1. Получив доступ к консоли администратора, внутренний нарушитель создает нового пользователя Redmine с правами администратора.
5. Внутренний нарушитель ожидает, когда администратор просмотрит страницу с внедренным вредоносным кодом.
6. Внутренний нарушитель проводит Blind SQL-инъекцию, получает доступ к данным конфиденциального проекта.

# 3 Выполнение лабораторной работы

## 3.1 Перечень уязвимостей и последствий

### 3.1.1 Слабый пароль пользователя

**Обнаружение:** На файловом сервере использовался слабый пароль учетной записи dev1.

**Устранение:** Пароль изменен на сложный через Active Directory Users and Computers.

### 3.1.2 Последствие Dev backdoor

**Обнаружение:**

* В папке Downloads пользователя dev1 обнаружен файл svchosting.exe
* В планировщике задач создано задание Evil task с автозапуском при входе пользователя
* Задание настроено на выполнение каждые 5 минут

**Устранение:**

* Удалено задание Evil task из планировщика задач
* Удален файл svchosting.exe из папки Downloads (рис. 1 - рис. 3)

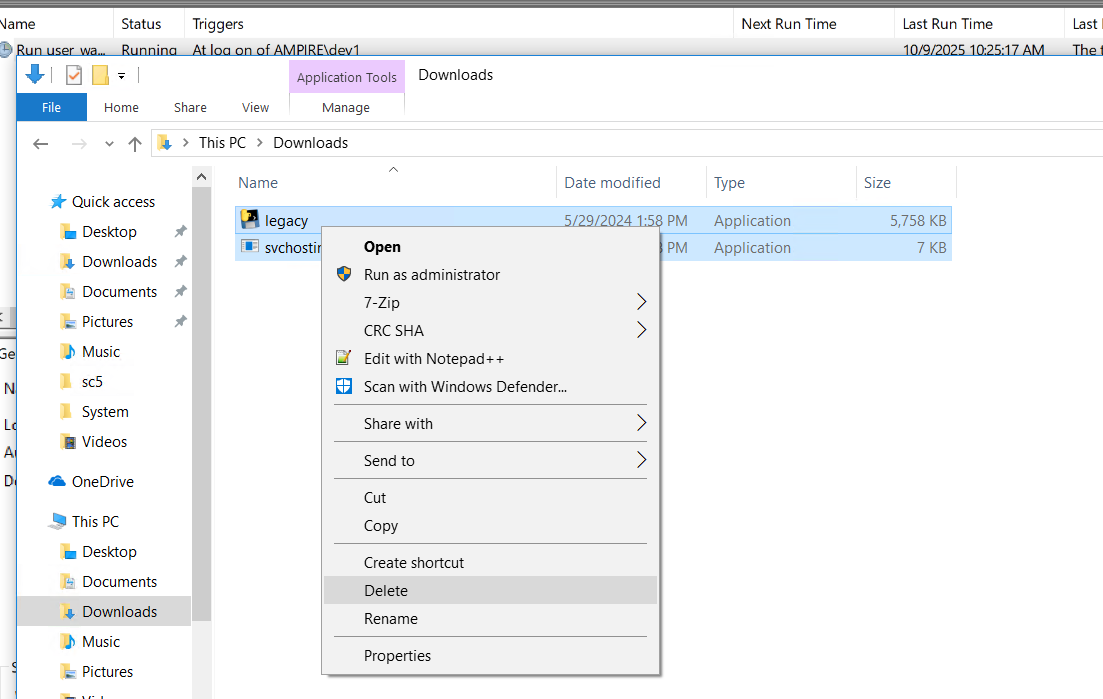


Рис. 1: Файл svchosting.exe в папке Downloads

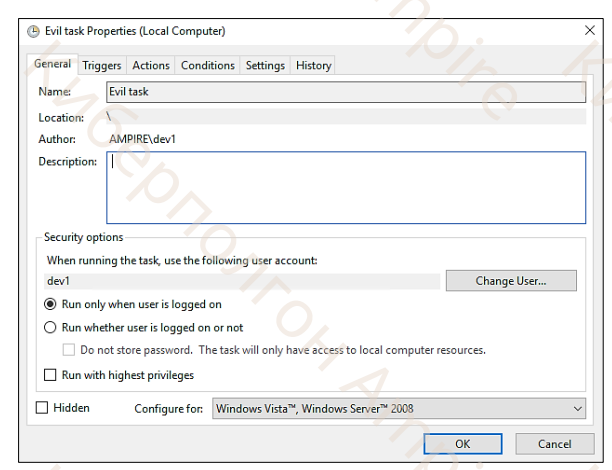


Рис. 2: Задание “Evil task” в планировщике задач

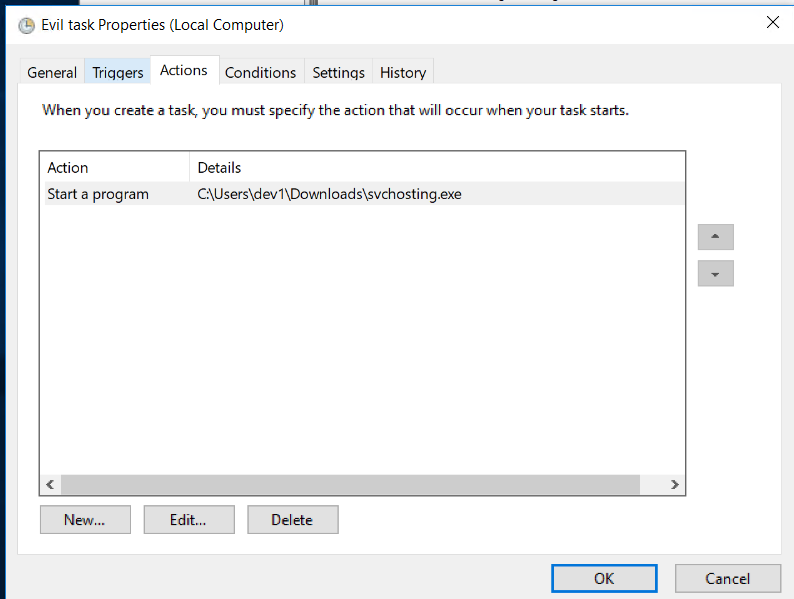


Рис. 3: Настройки задания с путем к вредоносному файлу

### 3.1.3 Уязвимость 2: XSS (CVE-2019-17427)

**Обнаружение:** На Wiki-странице проекта DEV1 обнаружен сложный XSS-код, который:

* Создает пользователя “hacker” с правами администратора
* Включает REST API в настройках Redmine
* Использует событие onfocusin для автоматического выполнения

**Устранение:**

* В файле redcloth3.rb исправлена обработка HTML-тегов
* Удален тег pre из списка разрешенных тегов (ALLOWED\_TAGS)
* Перезапущена служба nginx: sudo systemctl restart nginx.service (рис. 4 - рис. 7)

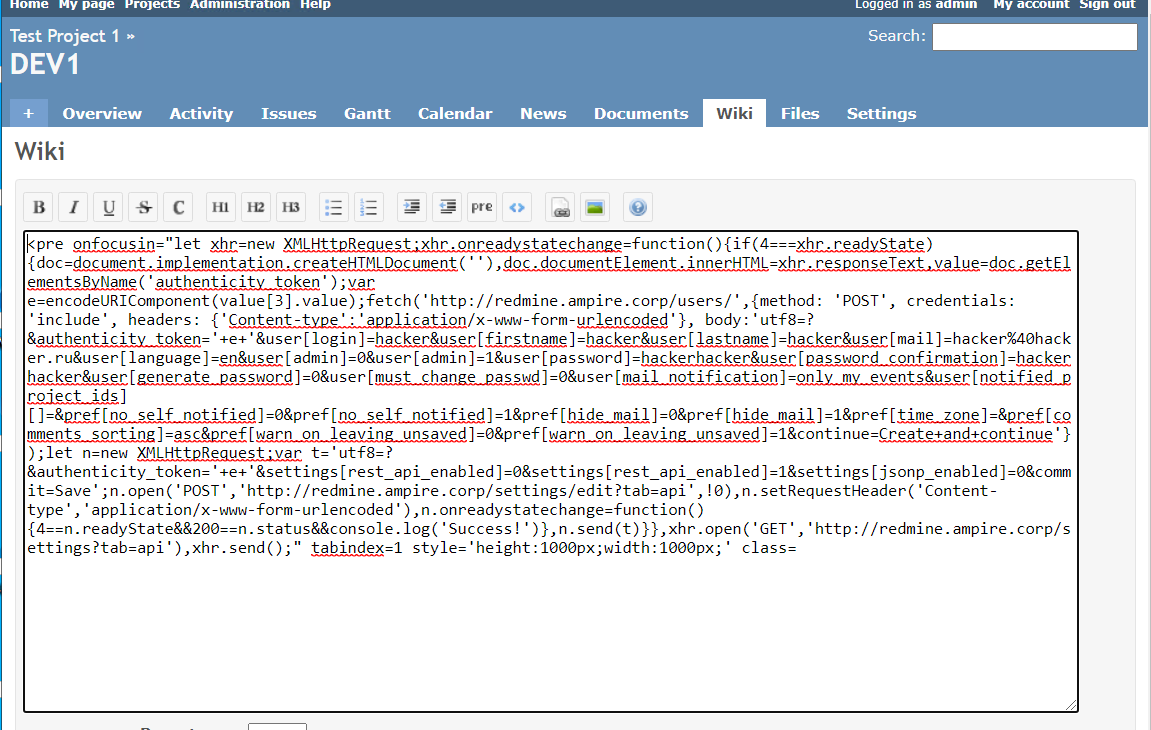


Рис. 4: Вредоносный XSS-код на Wiki-странице



Рис. 5: Исходный код файла redcloth3.rb

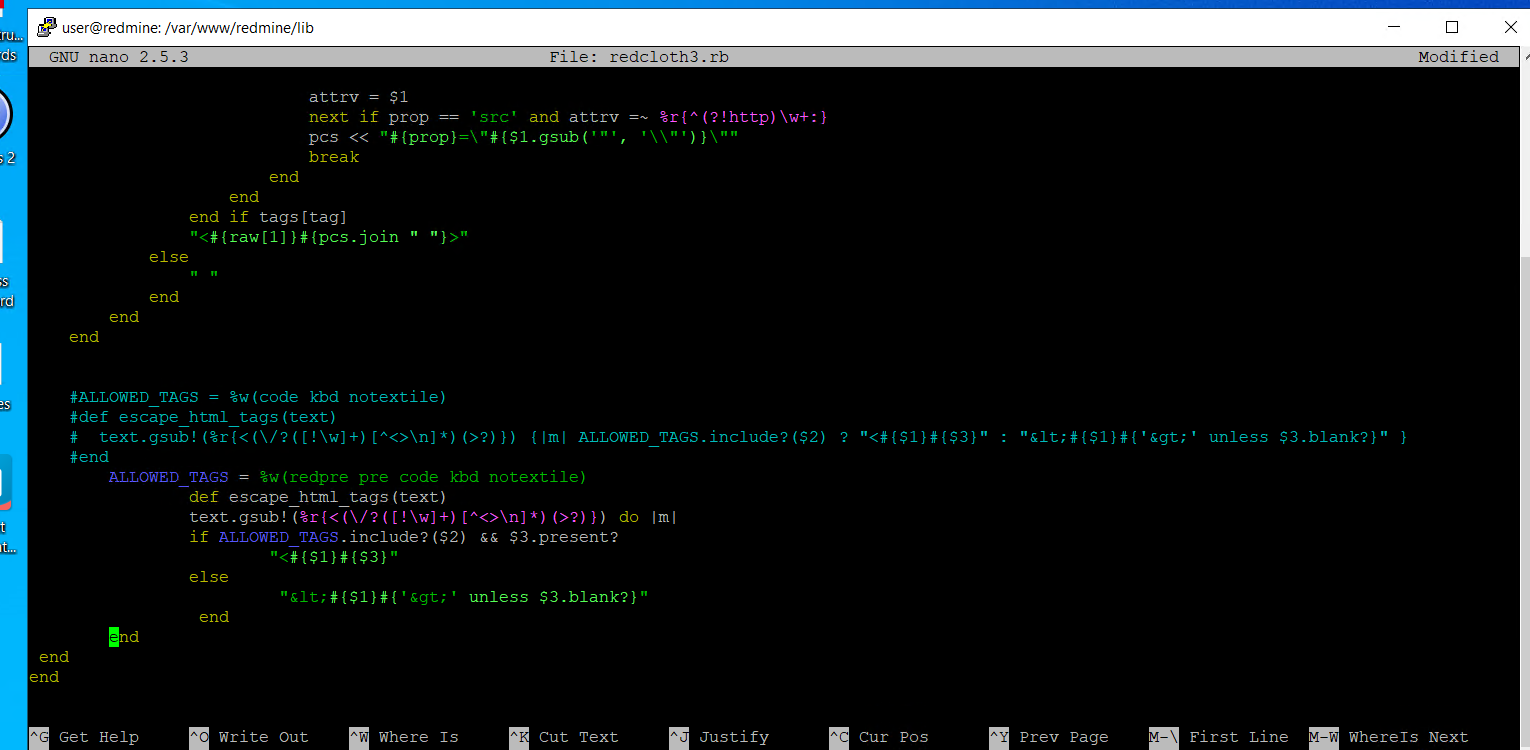


Рис. 6: Исправленная версия файла redcloth3.rb

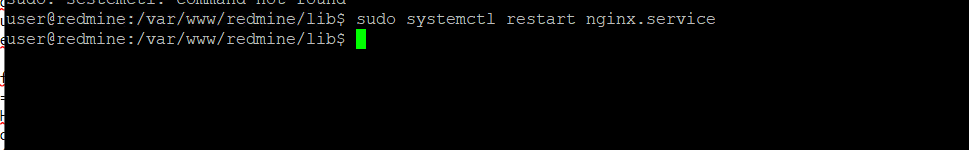


Рис. 7: Перезапуск службы nginx

### 3.1.4 Последствие: Redmine User

**Обнаружение:** В Redmine создан пользователь “hacker” с email hacker@hacker.ru (рис. 8)

**Устранение:** Пользователь “hacker” удален через веб-интерфейс Redmine (рис. 9)

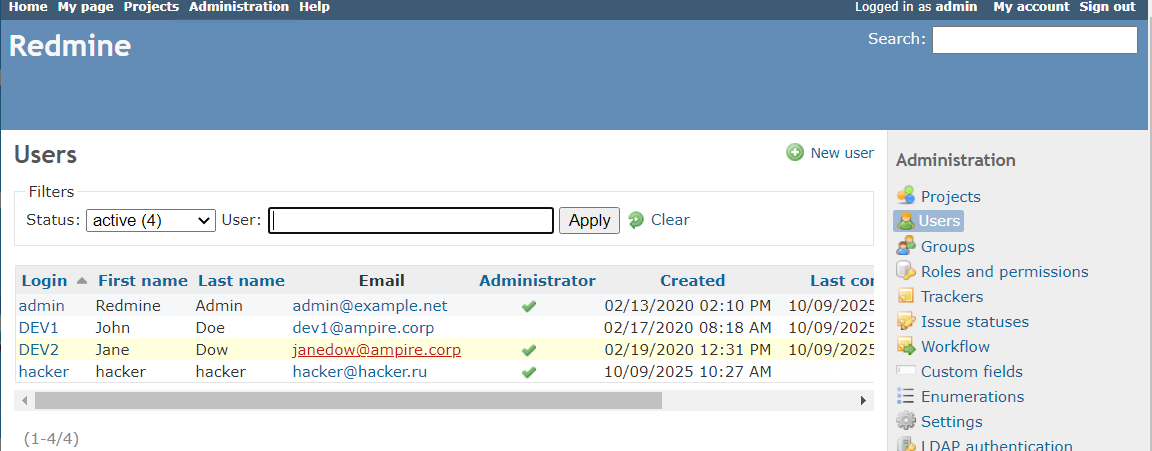


Рис. 8: Список пользователей Redmine с пользователем “hacker”

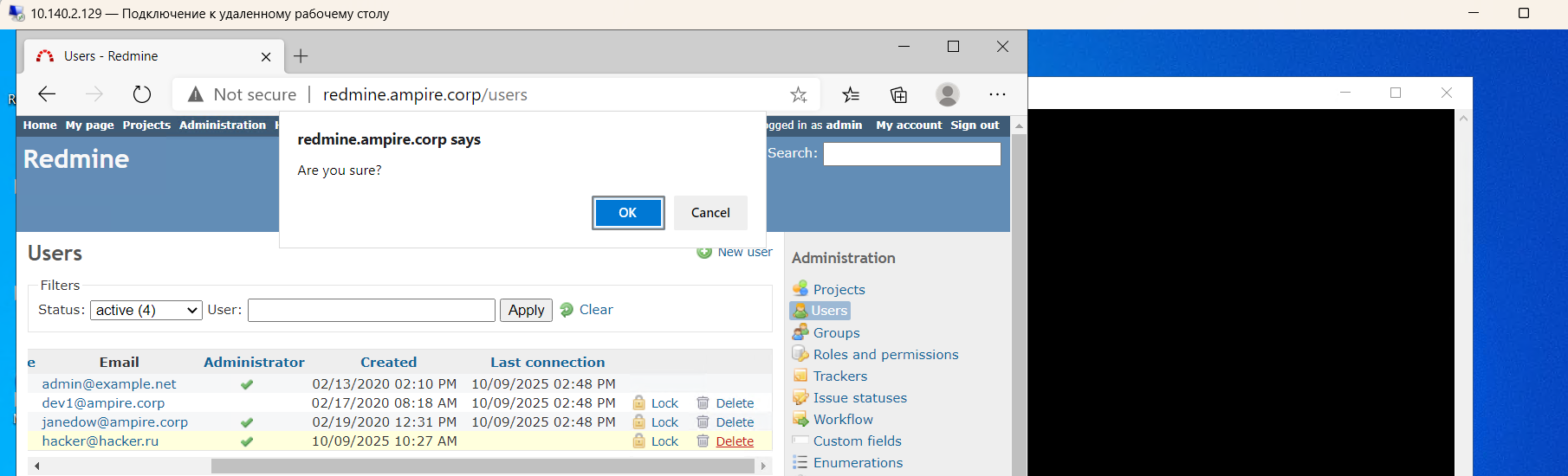


Рис. 9: Подтверждение удаления пользователя

### 3.1.5 Уязвимость 3: Blind SQL-инъекция (CVE-2019018890)

**Обнаружение:**

* В логах Redmine зафиксированы запросы с SLEEP(3) в параметре subproject\_id
* Время выполнения запросов увеличилось до 6074 мс (вместо обычных ~30 мс) (рис. 10)

**Устранение:**

* В файле query.rb закомментирован уязвимый код обработки subproject\_id
* Добавлена фильтрация входных параметров (рис. 11)

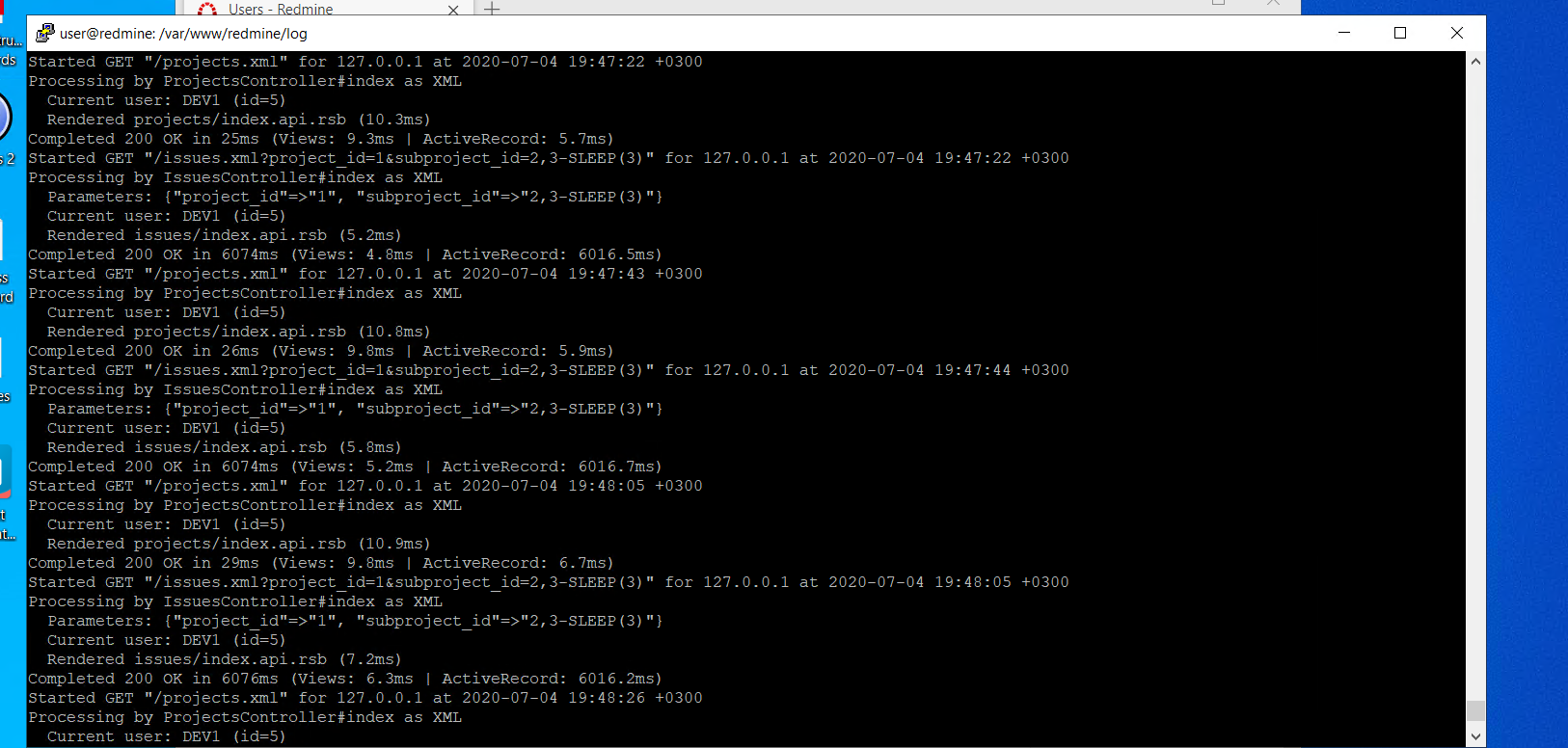


Рис. 10: Логи Redmine с SQL-инъекцией

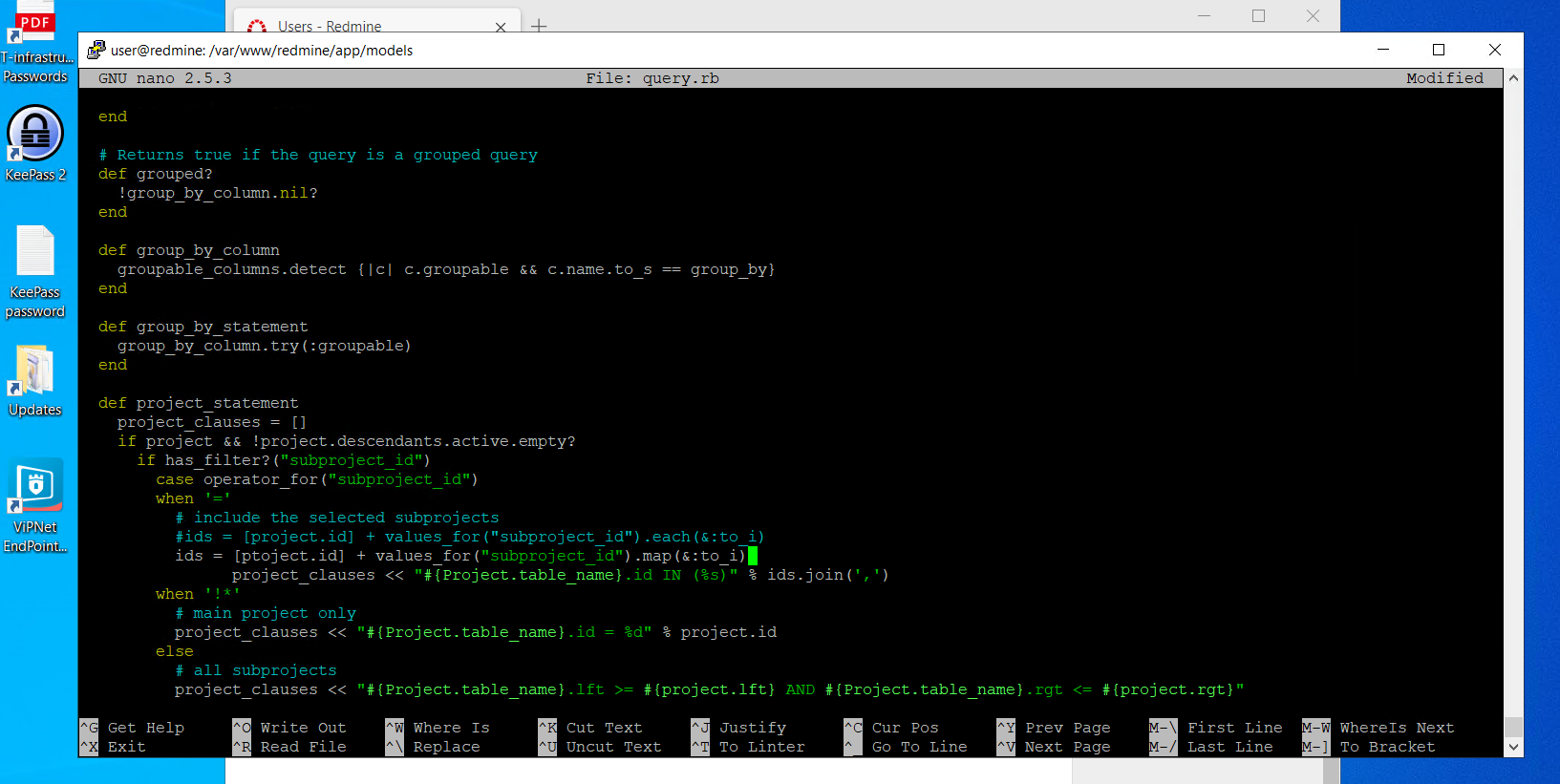


Рис. 11: Исправление в файле query.rb

Общий результат выполненной работы: (рис. 12 - рис. 13)

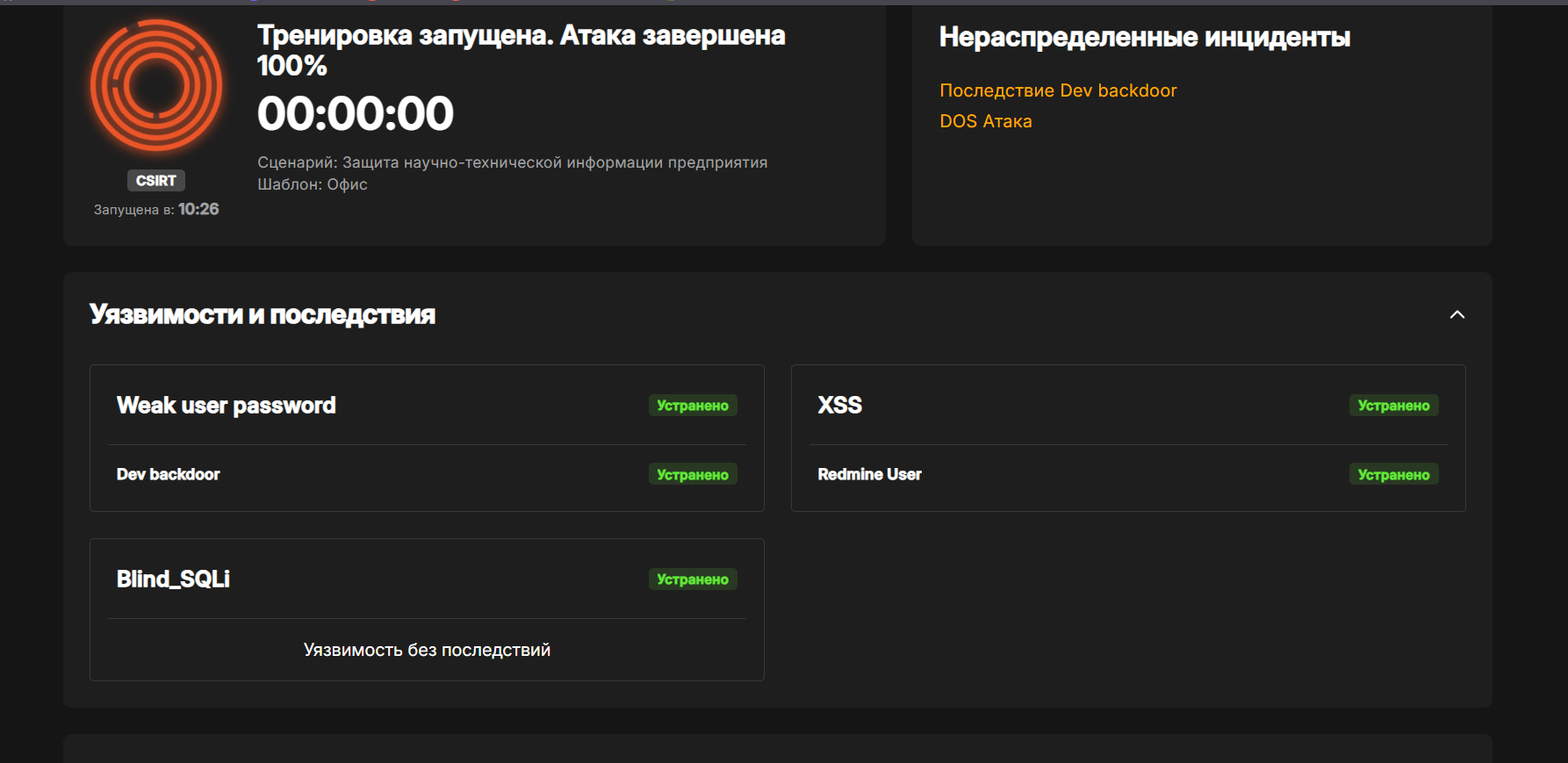


Рис. 12: Главная страница

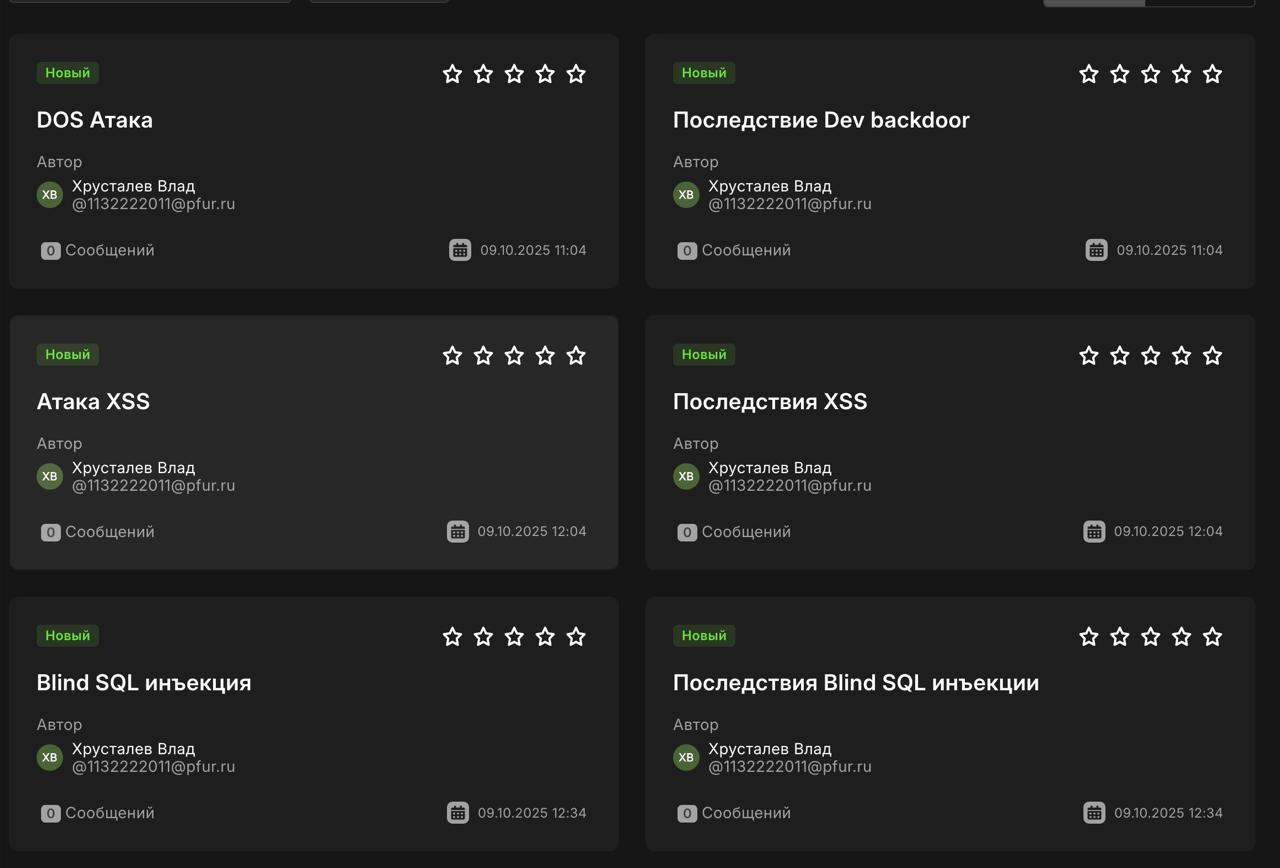


Рис. 13: Карточки инцидентов и последствий

# 4 Общие выводы

В рамках учебно-практического занятия на базе программного комплекса обучения методам обнаружения, анализа и устранения последствий компьютерных атак «Ampire» мы выполнили сценарий №5 «Защита научно-технической информации предприятия». Внутренний нарушитель, используя слабые пароли и уязвимости в веб-приложении Redmine, осуществил комплексную атаку с целью получения доступа к конфиденциальной информации. Нарушитель применил техники внедрения backdoor, эксплуатации XSS-уязвимости и слепой SQL-инъекции для создания привилегированного пользователя и несанкционированного доступа к данным. Уровень сложности сценария — 8 (из 10). Мы успешно выявили уязвимости, проанализировали последствия атаки, устранили их и отработали методы детектирования с использованием инструментов ViPNet IDS NS, ViPNet TIAS и Security Onion, а также освоили методики исправления исходного кода приложений для устранения уязвимостей.