

Лабораторная работа №3

Кибербезопасность предприятия

Тимофеева Екатерина Николаевна

Содержание

1	Цель работы	5
2	Выполнение лабораторной работы	6
2.1	1. Слабый пароль пользователя	6
2.1.1	Последствие Dev backdoor	7
2.2	Атака XSS	9
2.2.1	Последствие Redmine User	11
2.3	Blind SQL-инъекция	13
3	Выводы	16

Список иллюстраций

2.1	Сброс пароля	6
2.2	Запуск исполняемого файла	7
2.3	Удаление evil tasc из планировщика задач и удаление файла . . .	8
2.4	Атаки устранены	8
2.5	Создание карточки инцидента	9
2.6	Создание карточки	9
2.7	Изменение кода функции	10
2.8	Перезапуск веб-сервера	11
2.9	Удаление пользователя hacker	12
2.10	Ampire	12
2.11	Карточка инцидента	13
2.12	Карточка инцидента	13
2.13	Изменение кода	14
2.14	Перезапуск	14
2.15	Карточка инцидента	15
2.16	Ampire	15

Список таблиц

1 Цель работы

Устранить действия нарушителя «Защита научно-технической информации предприятия» для использования при проведении учебно-практических занятий на базе программного комплекса обучения методам обнаружения, анализа и устранения последствий компьютерных атак «Ampire».

2 Выполнение лабораторной работы

2.1 1. Слабый пароль пользователя

Для закрытия уязвимости необходимо изменить пароль на более сложный, не содержащийся в словаре.

Для этого на сервере AD открываем “Active Directory Users and Computers”, находим пользователя dev1, нажимаем на “Reset Password” и вводим новый пароль. (рис. 1).

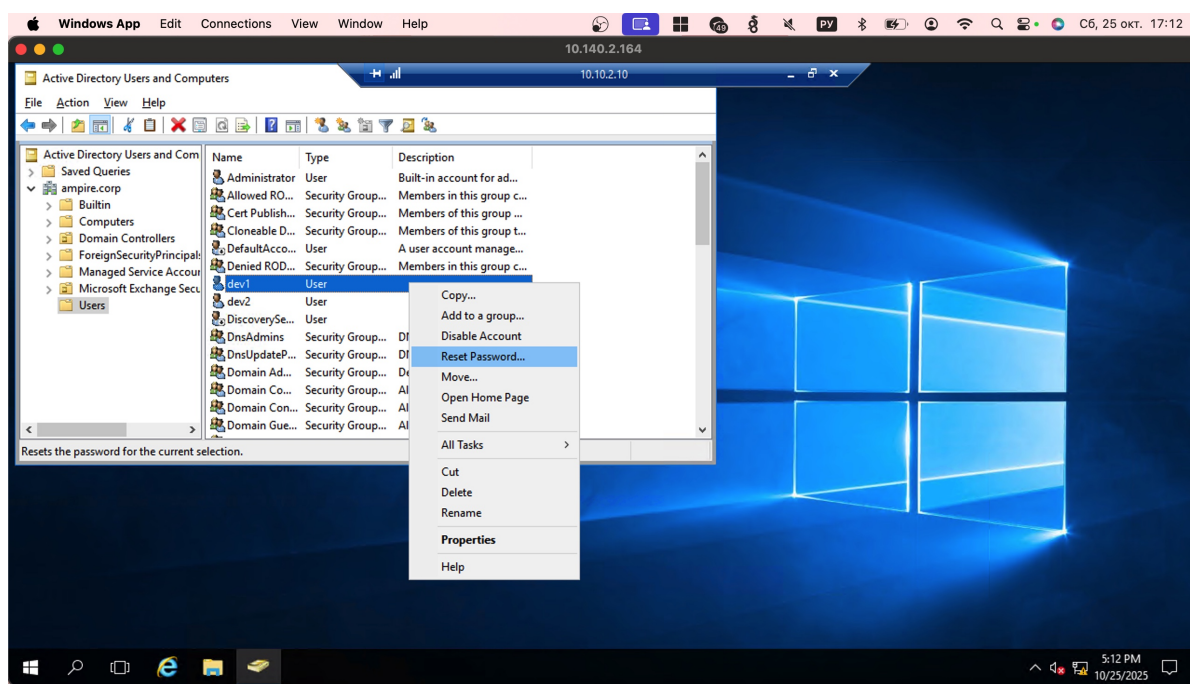


Рис. 2.1: Сброс пароля

2.1.1 Последствие Dev backdoor

Зпаускаем исполняемый файл в планировщике. (рис. 2).

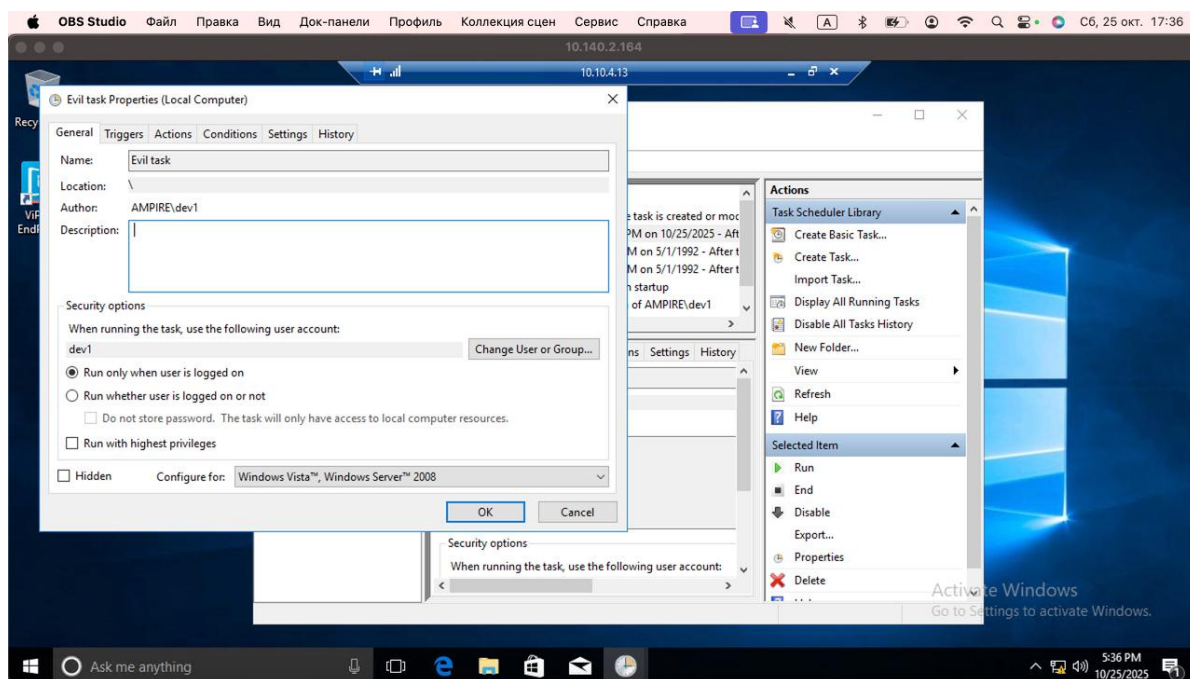


Рис. 2.2: Запуск исполняемого файла

Для того, чтобы устранить полезную нагрузку мы удаляем задачу из планировщика задач и файл из директории. (рис. 3).

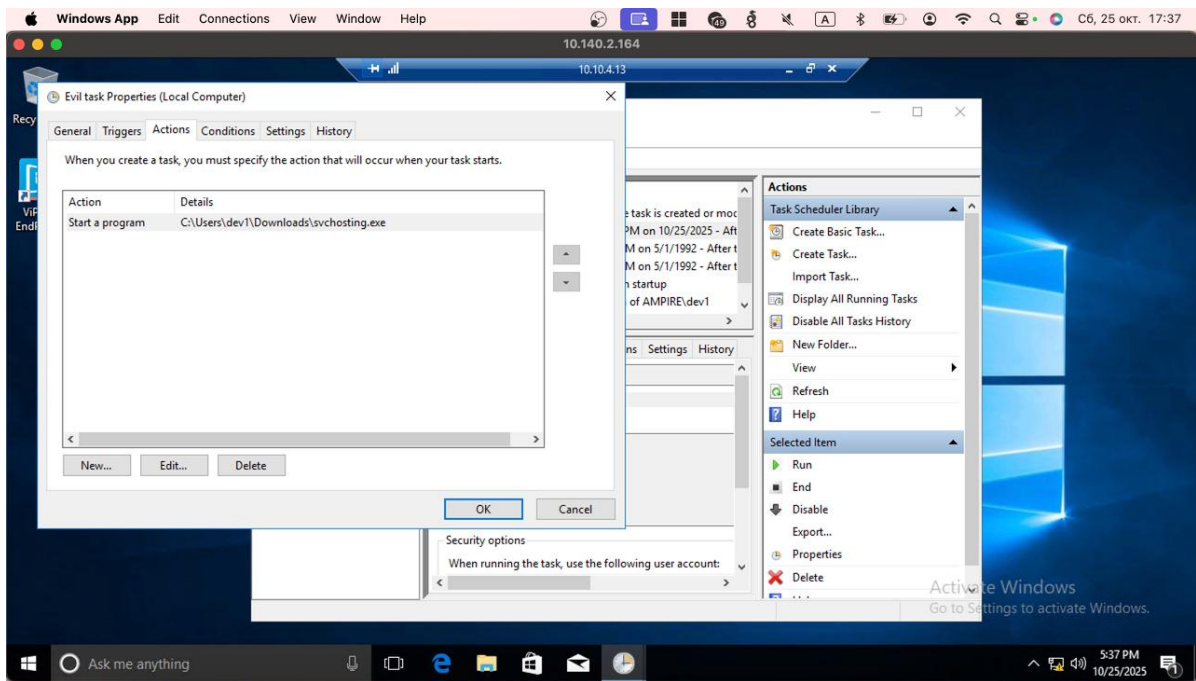


Рис. 2.3: Удаление evil tasc из планировщика задач и удаление файла

Устранили уязвимость 1 и последствие 1. (рис. 4).

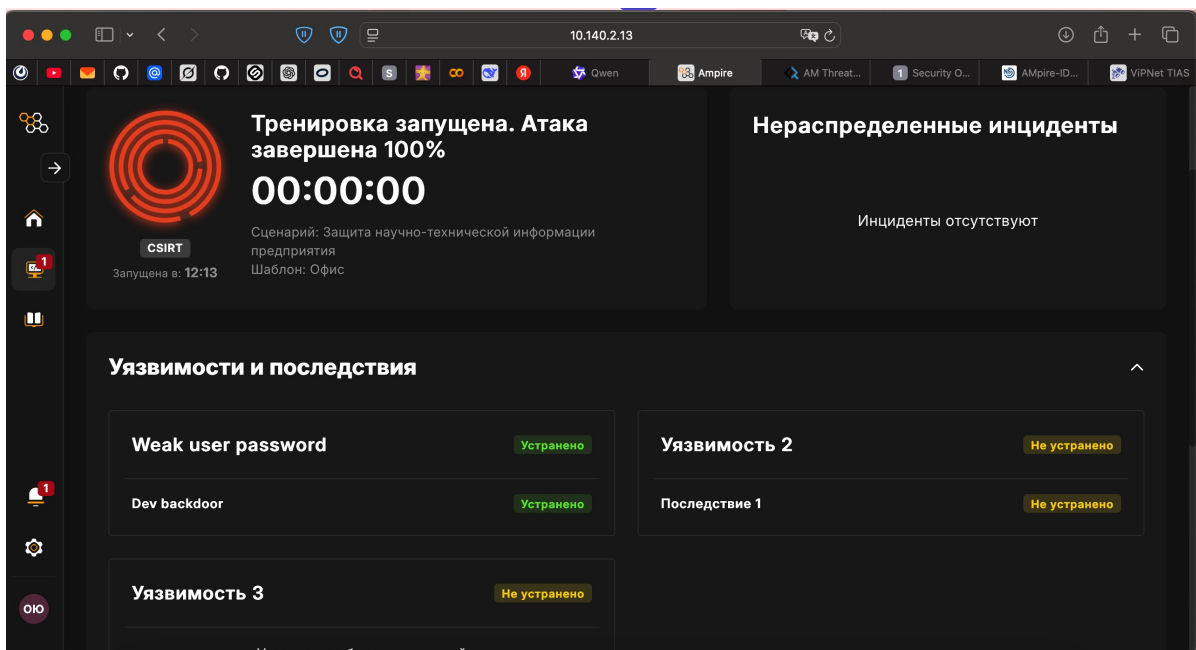


Рис. 2.4: Атаки устранены

Создаём карточку инцидента для уязвимости. (рис. 5).

Уязвимость 1 — Слабый пароль пользователя

Основная информация

Чат

В работе

Дата и время события

25.10.2025 17:12

Описание

Нарушитель с IP 195.239.174.11 (Kali) провёл брутфорс пароля учётной записи dev1 на файловом сервере (10.10.2.10). После успешной авторизации был загружен вредоносный .bat файл. Уязвимость устранена путём смены пароля на сложный.

Индикаторы компрометации

Weak credential policy

Рекомендации

1. Внедрить политику сложности паролей в домене. 2. Включить блокировку учётных записей после N неудачных попыток. 3. Провести обучение пользователей по созданию надёжных паролей.

Прикреплённые файлы

Снимок 25.10.2025 в 17:12.jpeg

Оценка

☆☆☆☆

Автор

Оширова Юлия @1132222843@pfur.ru

Ответственный

Оширова Юлия @1132222843@pfur.ru

Источник

195.239.174.11

Поражённые активы

10.10.2.10

Рис. 2.5: Создание карточки инцидента

Создаём карточку инцидента для последствия. (рис. 6).

Вредоносная задача в Планировщике заданий на машине Developer 1

Основная информация

Чат

В работе

Дата и время события

25.10.2025 17:36

Описание

На машине Developer 1 (10.10.4.13) обнаружена вредоносная задача Evil Task, запускающая файл svchosting.exe из папки Downloads. Задача удалена. Файл не обнаружен (возможно, был удален автоматически или скрыт). Backdoor нейтрализован.

Индикаторы компрометации

Создание задачи Evil Task в Task Scheduler, запуск исполняемого файла из Downloads

Рекомендации

1. Запретить выполнение исполняемых файлов из папок Downloads и Desktop через AppLocker или GPO. 2. Внедрить EDR-решение для мониторинга создания задач в Task Scheduler. 3. Регулярно аудировать автозагрузку и запланированные задачи.

Прикреплённые файлы

Снимок 25.10.2025 в 17:36.jpeg

Оценка

☆☆☆☆

Автор

Оширова Юлия @1132222843@pfur.ru

Ответственный

Оширова Юлия @1132222843@pfur.ru

Источник

10.10.2.10

Поражённые активы

10.10.4.13

Рис. 2.6: Создание карточки

2.2 Атака XSS

Необходимо внести изменения в код Redmine. Находим обработку текста wiki-страницы при наличии в тексте html-тегов. Удаляем тег pre из разрешенных тегов, которые не будут экранированы. (рис. 7).

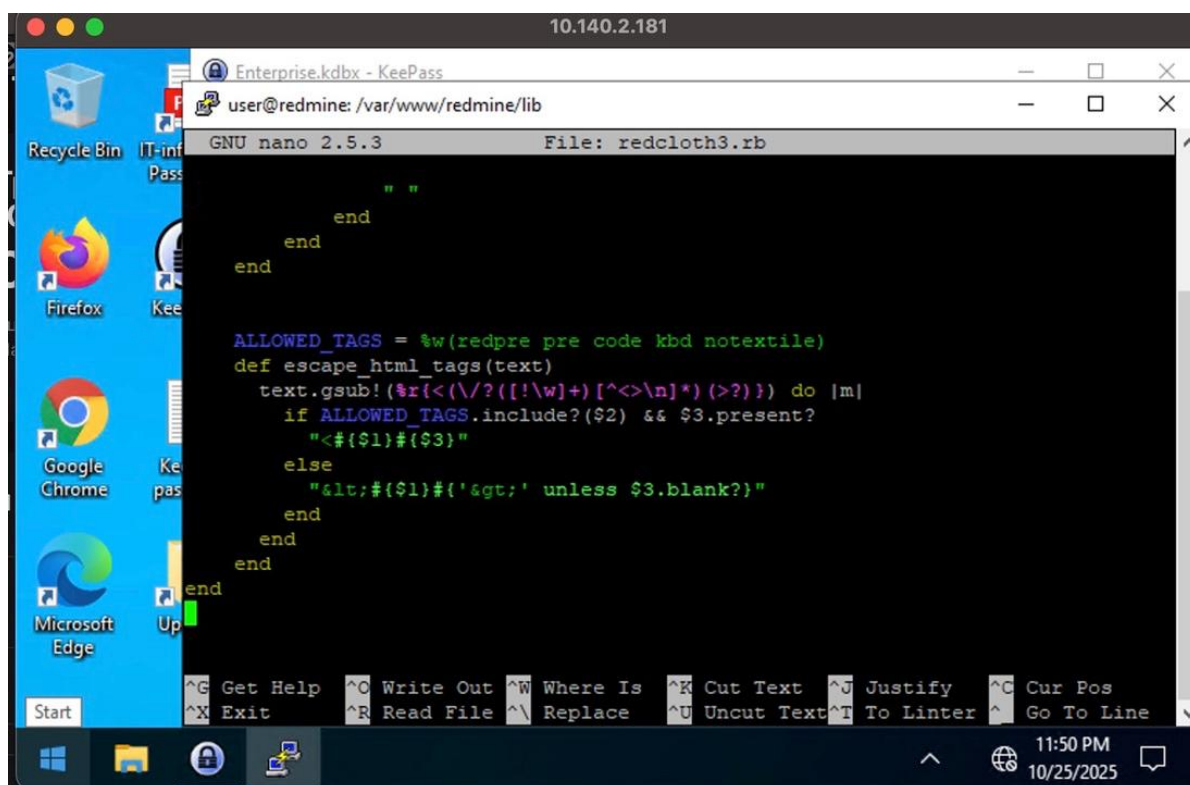
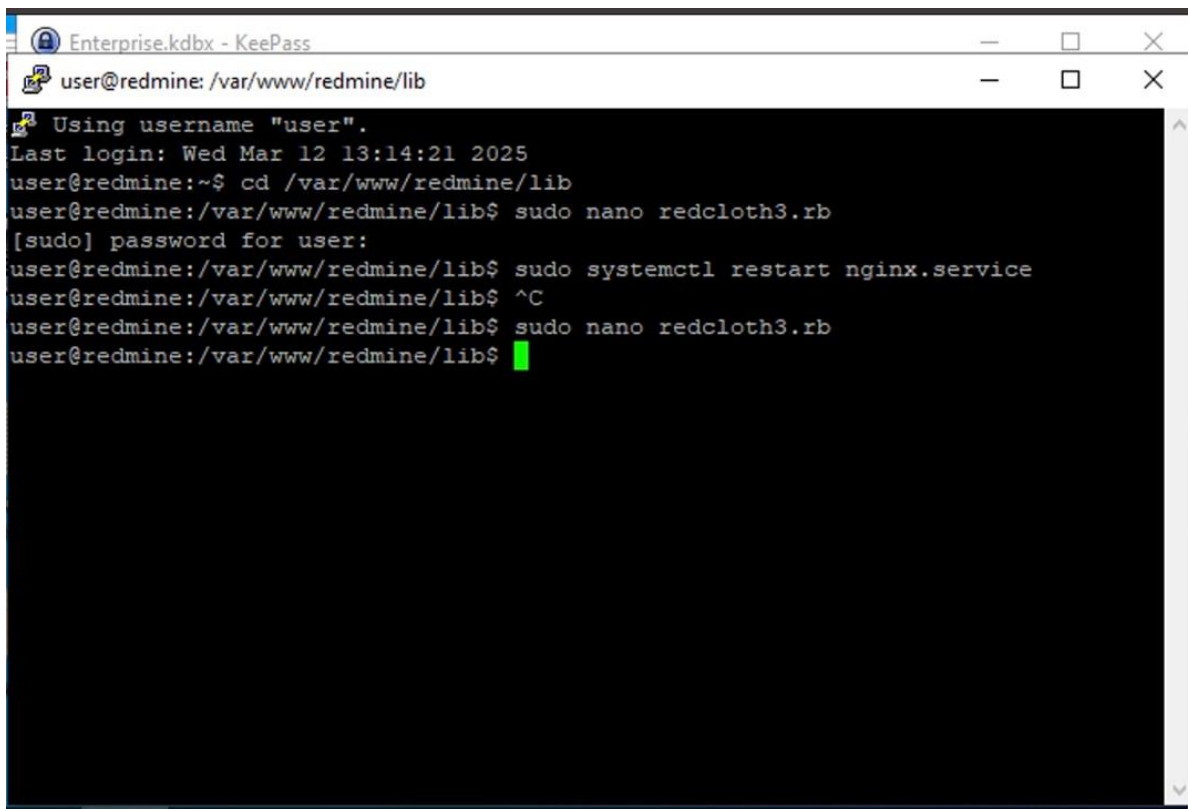


Рис. 2.7: Изменение кода функции

После внесения изменений перезапускаем службу веб-сервера. (рис. 8).



```
Enterprise.kdbx - KeePass
user@redmine: /var/www/redmine/lib

Using username "user".
Last login: Wed Mar 12 13:14:21 2025
user@redmine:~$ cd /var/www/redmine/lib
user@redmine:/var/www/redmine/lib$ sudo nano redcloth3.rb
[sudo] password for user:
user@redmine:/var/www/redmine/lib$ sudo systemctl restart nginx.service
user@redmine:/var/www/redmine/lib$ ^C
user@redmine:/var/www/redmine/lib$ sudo nano redcloth3.rb
user@redmine:/var/www/redmine/lib$
```

Рис. 2.8: Перезапуск веб-сервера

2.2.1 Последствие Redmine User

Для нейтрализации полезной нагрузки необходимо удалить созданного пользователя “hacker” через веб-интерфейс Redmine. (рис. 9).

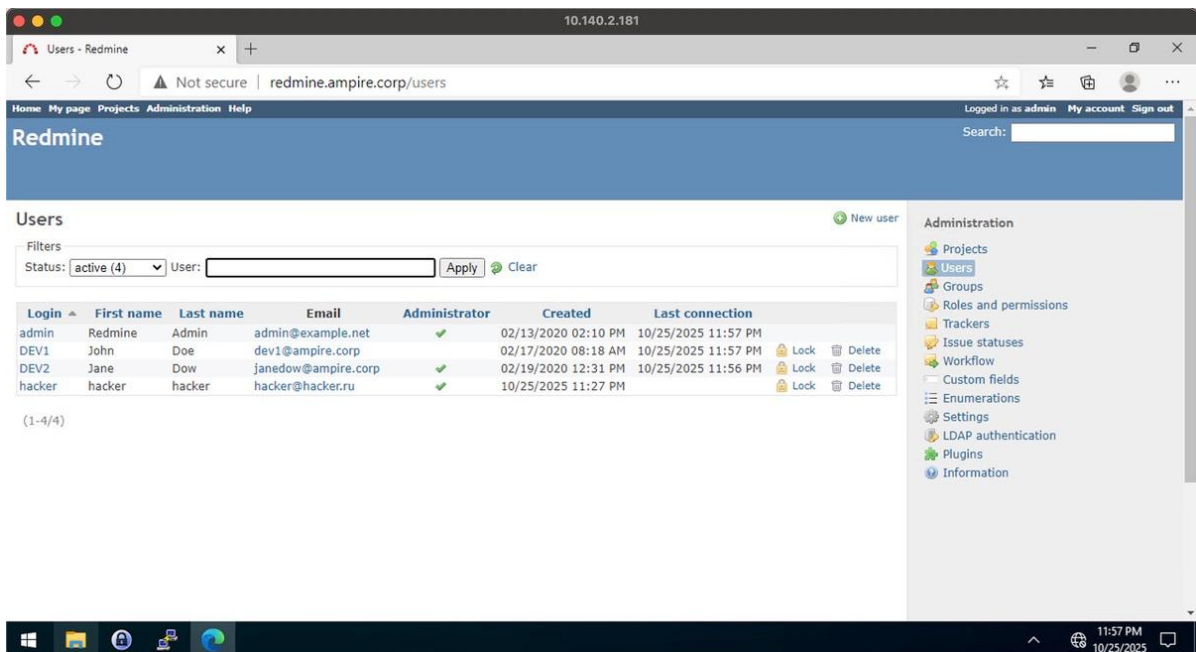


Рис. 2.9: Удаление пользователя hacker

Устранили 2 уязвимости и 2 последствия. (рис. 10).

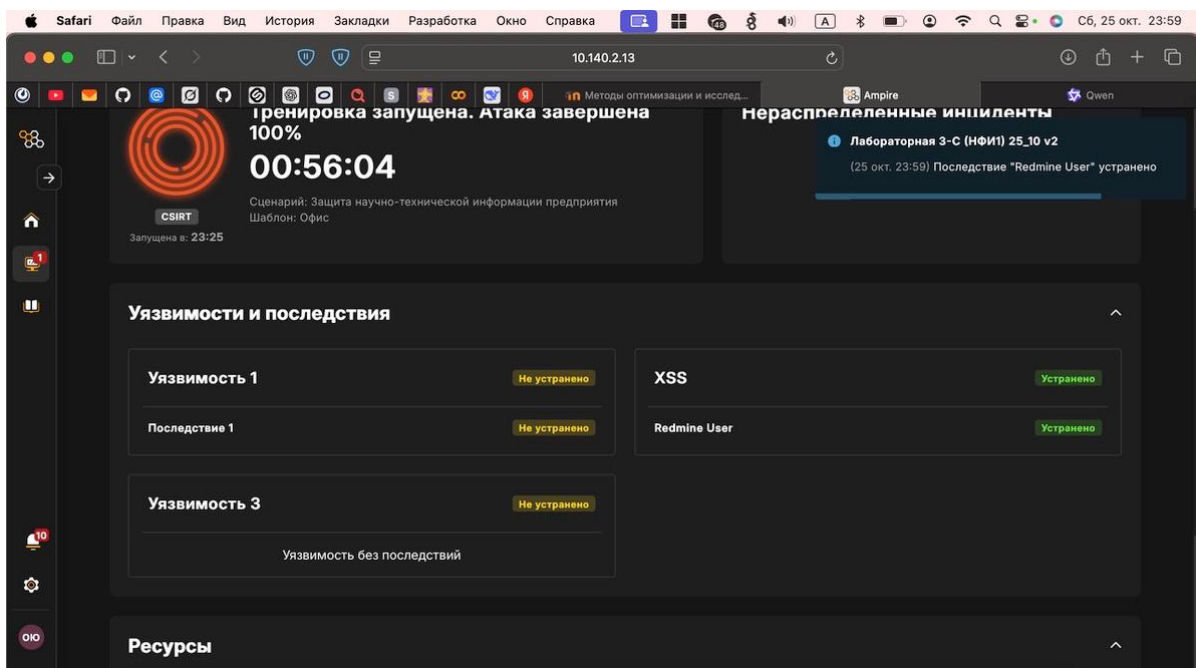


Рис. 2.10: Ampire

Заполняем карточку инцидента для 2 уязвимости. (рис. 11).

значений и часть закоментируем. (рис. 13).

```
if has_filter?("subproject_id")
  case operator_for("subproject_id")
  when '='
    # include the selected subprojects
    # ids = [project.id] + values_for("subproject_id").each(&:to_i)
    subproject_ids = values_for("subproject_id").
    project_clauses << "#{Project.table_name}.id IN (%s)" % ids.join(',')
  when '!=*'
    # main project only
    project_clauses << "#{Project.table_name}.id = %d" % project.id
  else
    # all subprojects
    project_clauses << "#{Project.table_name}.lft >= #{project.lft} AND #{$
  end
elsif Setting.display_subprojects_issues?
  project_clauses << "#{Project.table_name}.lft >= #{project.lft} AND #{P$
else
  project_clauses << "#{Project.table_name}.id = %d" % project.id
end
```

Рис. 2.13: Изменение кода

После внесения изменений перезапускаем службу веб-сервер. (рис. 14).

```
user@redmine: /var/www/redmine/app/models
ast login: Sat Oct 25 23:52:22 2025 from 10.10.2.254
ser@redmine:~$ cd /var/www/redmine/app/models
ser@redmine:/var/www/redmine/app/models$ nano query.rb
ser@redmine:/var/www/redmine/app/models$ sudo systemctl restart nginx.service
sudo] password for user:
ser@redmine:/var/www/redmine/app/models$
```

Рис. 2.14: Перезапуск

Заполняем карточку инцидента уязвимости. (рис. 15).

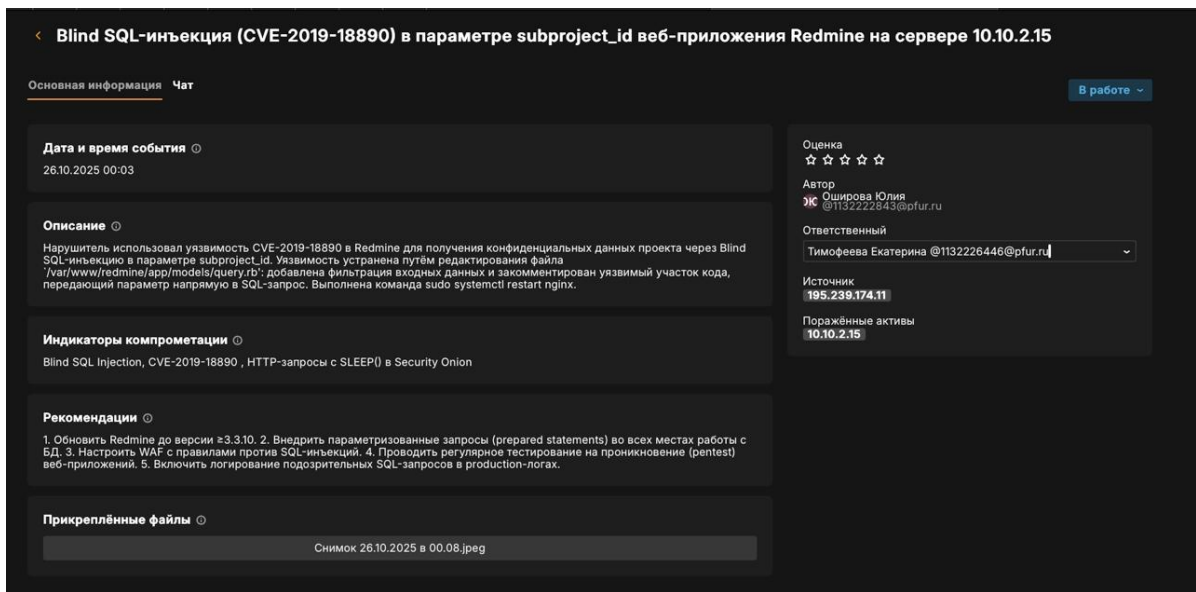


Рис. 2.15: Карточка инцидента

Успешно устранили 3 уязвимость. (рис. 16).

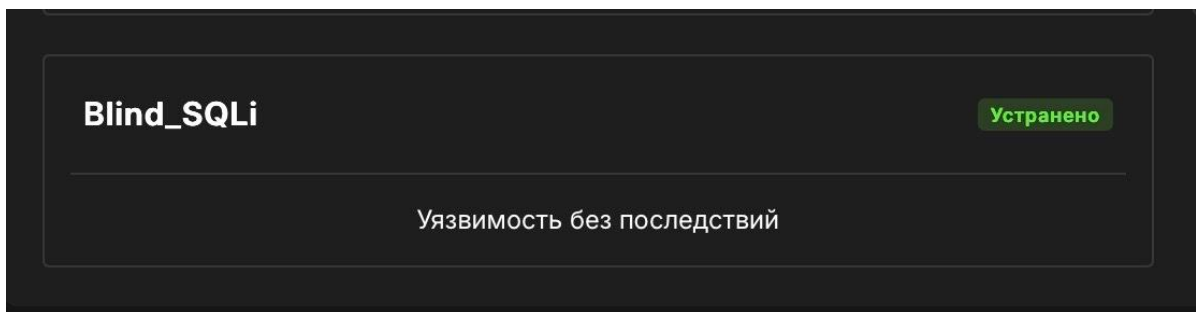


Рис. 2.16: Ampire

3 Выводы

В ходе данной лабораторной работы мы смогли устранить действия нарушителя «Защита научно-технической информации предприятия», а так же выполнить последствия к каждой уязвимости.