

Лабораторная работа №2. Защита научно-технической информации предприятия

Дисциплина: Кибербезопасность предприятия

Астраханцева Анастасия Ганина Таисия Ибатулина Дарья Шошина Евгения Кадирова Мехрубон
Хассан Факи Абакар

15 октября 2025

Группа НФИбд-01-22

Российский университет дружбы народов, Москва, Россия

Вводная часть

Цели и задачи

Целью лабораторной работы является освоение практических навыков выявления, анализа и устранения уязвимостей информационных систем в рамках сценария «Защита научно-технической информации предприятия».

1. Изучить уязвимости: слабый пароль пользователя, Blind SQL, XSS
2. Проанализировать последовательность действий нарушителя на каждом этапе атаки.
3. Освоить методы детектирования атак с использованием средств мониторинга и анализа безопасности.
4. Выполнить мероприятия по устранению последствий атаки.

Заполнение карточек инцидентов

Для обнаружения и анализа атак использовались средства ViPNet IDS NS. Были зафиксированы следующие ключевые инциденты, соответствующие этапам атаки

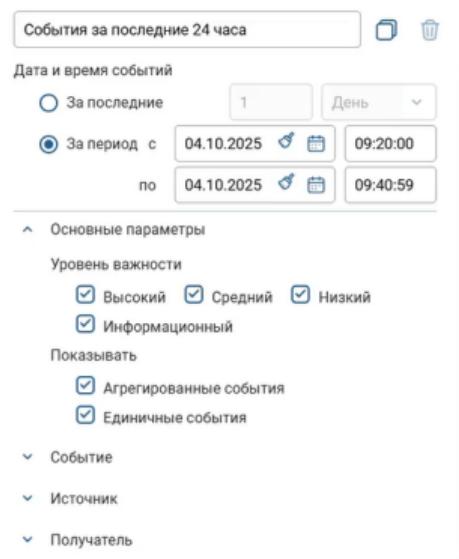


Рис. 1: Установка фильтров

Активность трояна LaZagne

Лента новостей

Активность трояна LaZagne

Основная информация Чат

Дата и время события ⓘ
04.10.2025 09:21

Описание ⓘ
ET ATTACK_RESPONSE LaZagne Artifact Outbound in FTP - метод сетевой атаки, при котором злоумышленник использует уязвимости FTP-серверов для отправки исходящего трафика на другое устройство (обычно другой сервер в сети).

Индикаторы компрометации ⓘ
Сигнатура группы IDS ET ATTACK_RESPONSE LaZagne Artifact Outbound FTP; В сетевом трафике строка "The LaZagne Project"

Рекомендации ⓘ
1. Отключить порт или VLAN. 2. Проверить наличие файлов LaZagne.exe, The LaZagne Project, credentials.txt. 3. Провести антивирусное сканирование заражённой машины. 4. Сбросить сохранённые учётные данные в браузерах и приложениях. 5. Анализировать сетевые журналы на аналогичные исходящие соединения. 6. Обновить антивирусные базы и сигнатуры IDS/IPS.

Оценка
☆ ☆ ☆ ☆ ☆

Автор
ID Ибатулина Дарья
@1132226434@pfur.ru

Ответственный
Астраханцева Анастасия
@1132226437@pfur.ru

Источник
10.10.4.13

Поражённые активы
10.10.4.11

Рис. 2: Активность трояна LaZagne

Попытка выполнения удаленного кода через Microsoft PowerShell на клиентском устройстве

Попытка выполнения удаленного кода через Microsoft PowerShell на клиентском устройстве

Основная информация Чат

Дата и время события ①
04.10.2025 09:21

Описание ①
Событие связано с обнаружением ответа атаки, указывающего на попытку выполнения произвольного кода или отправки команды управления на ранее скомпрометированный ресурс. Обнаружен трафик, содержащий сигнатуры Microsoft PowerShell ("Windows PowerShell", "Copyright", "Microsoft Corp"), что указывает на использование PowerShell для эксплуатации уязвимости на клиентском устройстве с ОС Windows.

Индикаторы компрометации ①
successful-admin, attack_response, Exploitation

Рекомендации ①
1. Изолировать заражённый компьютер от сети. 2. Проверить запущенные процессы PowerShell и задания в планировщике. 3. Просканировать систему антивирусом и удалить вредоносные файлы. 4. Проверить журналы PowerShell на выполнение подозрительных команд. 5. Сбросить пароли пользователей, особенно администраторов. 6. Проверить сетевые подключения и запретить неизвестные исходящие соединения. 7. Обновить антивирусные базы и сигнатуры IDS.

Оценка
☆ ☆ ☆ ☆ ☆

Автор
ID Ибатуллина Дарья
@1132226434@pfur.ru

Ответственный
Не заполнено

Источник
10.10.4.13

Поражённые активы
10.10.4.11

Рис. 3: Попытка выполнения удаленного кода через Microsoft PowerShell на клиентском устройстве

Уязвимость XSS

The screenshot shows a Redmine issue page for a XSS vulnerability. The title is "Уязвимость XSS". The main content area has tabs "Основная информация" (selected) and "Чат".

Основная информация

- Дата и время события**: 04.10.2025 09:21
- Описание**: AM EXPLOIT Possible Redmine < v4.0.4 XSS (CVE-2019-17427). Redmine до версии 3.4.11 и 4.0.x до версии 4.0.4 постоянный XSS существует из-за ошибок форматирования при работе с textile текстом.
- Индикаторы компрометации**: web-application-attack, exploit, Exploitation, Tag: T1190 (MITRE ATT&CK: Exploit Public-Facing Application)
- Рекомендации**: Внести изменения в код Redmine.

Справа

- Оценка**: ☆☆☆☆☆
- Автор**: Ибатулина Дарья @1132226434@pfur.ru
- Ответственный**: Ибатулина Дарья @1132226434@pfur.ru
- Источник**: 10.10.4.11
- Поражённые активы**: 10.10.2.15

Рис. 4: Уязвимость XSS

Попытка SQL-инъекции с использованием SELECT и SLEEP на веб-сервере redmine.ampire.corp

Попытка SQL-инъекции с использованием SELECT и SLEEP на веб-сервере redmine.ampire.corp

Основная информация Чат

Закрытый

Дата и время события ①
04.10.2025 09:21

Описание ①
Зафиксирована попытка SQL-инъекции на веб-сервер redmine.ampire.corp через HTTP-запрос с элементами "SELECT" и "SLEEP" в URL. Атака направлена на эксплуатацию уязвимости веб-приложения. Трафик из внешней сети (\$EXTERNAL_NET) на HTTP-порты (\$HTTP_PORTS). Уровень важности — высокий.

Индикаторы компрометации ①
параметры запроса содержат SELECT и SLEEP; Замедление отклика сервера

Рекомендации ①
Использовать параметризованные запросы (Prepared Statements) — вместо вставки пользовательских данных напрямую в SQL-код использовать placeholders. SQL-команды Экранировать входные данные Следить за правами доступа к базе данных Выполнять регулярные аудиты Обновлять ПО Применять веб-фильтры (WAF) Обновить Redmine

Оценка
☆ ☆ ☆ ☆ ☆

Автор
Илья Дарья
@1122228434@ptur.ru

Ответственный
Ганина Тамсия
@1122226429@ptur.ru

Источник
10.10.4.11

Пораженные активы
10.10.2.15

Рис. 5: Попытка SQL-инъекции с использованием SELECT и SLEEP на веб-сервере redmine.ampire.corp

Чужой пользователь Redmine

The screenshot shows a Redmine issue page titled "Чужой пользователь Redmine". The main content area contains four sections: "Дата и время события" (Event date and time) showing "04.10.2025 09:21", "Описание" (Description) stating "На сервере Redmine был создан новый пользователь с правами администратора", "Индикаторы компрометации" (Compromise indicators) noting "Учётная запись, которой ранее не было на сервере Redmine с правами администратора", and "Рекомендации" (Recommendations) suggesting "Удалить этого пользователя". To the right, there is a sidebar with "Закрытый" (Closed), "Оценка" (Rating) with five stars, "Автор" (Author) listed as "Ибатуллина Дарья" with ID "@152226434@yandex.ru", "Ответственный" (Responsible) listed as "Астраханцева Анастасия" with ID "@152226437@yandex.ru", "Источник" (Source) showing "10.10.4.11", and "Поражённые активы" (Affected assets) showing "10.10.2.15".

Рис. 6: Чужой пользователь Redmine

Устранение первой уязвимости и последствия

Установление первой уязвимости

Для устранения уязвимости 1 необходимо
сменить пароль пользователя

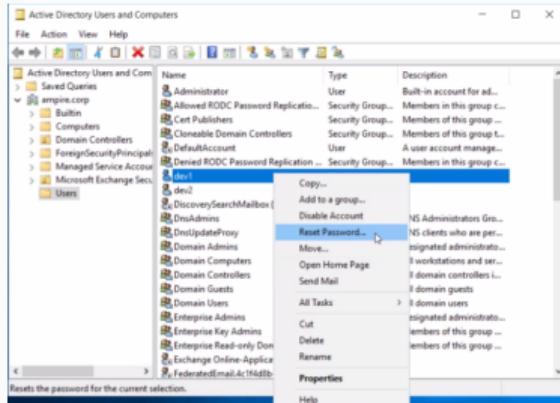


Рис. 7: Смена пароля

Устранена уязвимость 1

The screenshot displays a penetration testing interface with two main panels. The left panel shows a training session summary: "Тренировка запущена. Атака завершена 100% 00:00:00". It includes details like "Сценарий: Защита научно-технической информации предприятия" and "Шаблон: Офис". The right panel shows a resolved vulnerability: "Нераспределенные уязвимости" (Resolved vulnerabilities) for "Лабораторная 2-С (ИФИ) 04_30 (04 окт. 12:01) Уязвимость "Weak user password" устраниена". It lists three findings: "Попытка SQL-инъекции с использованием сервера redmine.ampire.corp", "Уязвимость XSS", and "Попытка выполнения удаленного кода через Microsoft PowerShell на клиентском устройстве". Below these are sections for "Уязвимости и последствия" (Vulnerabilities and consequences) and "Уязвимость 3" (Vulnerability 3), both marked as "Не устраниено" (Not resolved). A note at the bottom states "Уязвимость без последствий" (Vulnerability without consequences).

Рис. 8: Устранена уязвимость “Слабый пароль пользователя”

Описание последствия 1

Что произошло из-за установки слабого пароля пользователя dev1:

Начало атаки: Внутренний нарушитель подобрал слабый пароль на файловом сервере и заменил легитимный файл на вредоносный (backdoor).

Зарождение: Пользователь dev1 скачал и запустил этот вредоносный файл.

Закрепление: После получения контроля над компьютером dev1, нарушитель создал задачу в планировщике, которая будет автоматически запускать вредоносный файл **svchosting.exe** каждый раз при входе пользователя *dev1* в систему. Это позволяет злоумышленнику сохранять доступ к компьютеру даже после перезагрузки.

Вкладка General в планировщике задач

Открываем планировщик задач и обнаруживаем подозрительную задачу:

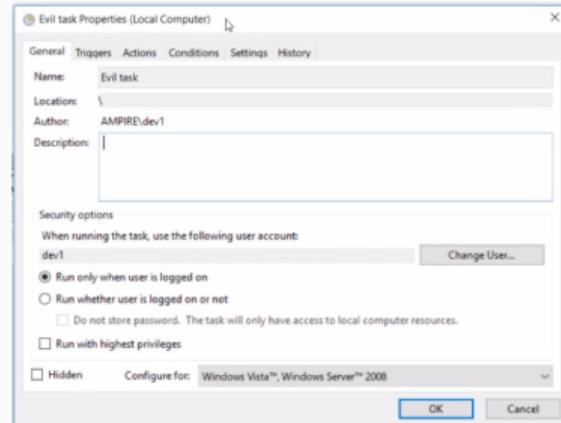


Рис. 9: Вкладка General в планировщике задач

Вкладка Actions в планировщике задач - путь к вредоносному файлу

Задача настроена на выполнение программы (Start a program). Путь к исполняемому файлу: C:\Users\dev1\Downloads\svchosting.exe.

Это указывает на то, что злоумышленник разместил вредоносный файл svchosting.exe в папке загрузок пользователя dev1 и настроил его автоматический запуск через планировщик задач.

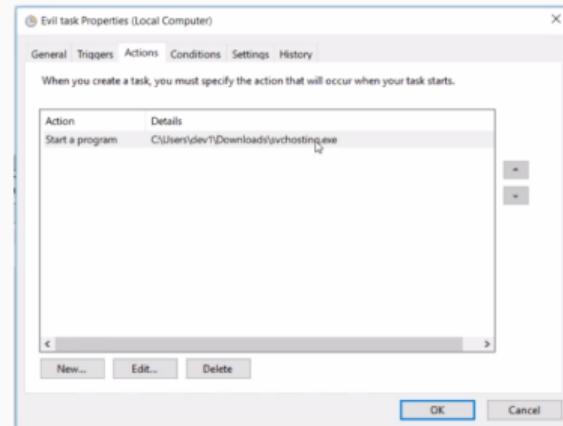


Рис. 10: Вкладка Actions в планировщике задач - путь к вредоносному файлу

Устранено последствие уязвимости “Слабый пароль пользователя”

Для устранения последствия мы удалили задачу и вредоносный exe-файл в директории C:\Users\dev1\Downloads.

Переходим на сервер и видим, что установлено последствие уязвимости “Слабый пароль пользователя”

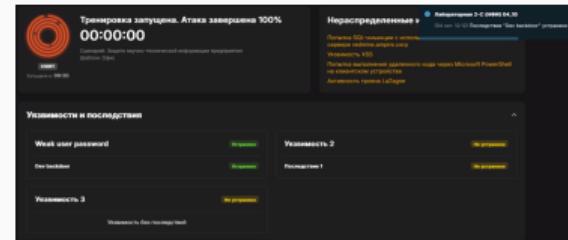


Рис. 11: Устранено последствие уязвимости “Слабый пароль пользователя”

Просмотр учетных данных администратора

На скриншоте видим, что для доступа к серверу Redmine (10.10.2.15) были использованы учетные данные администратора (admin). Это необходимо для получения прав на редактирование кода сервера.

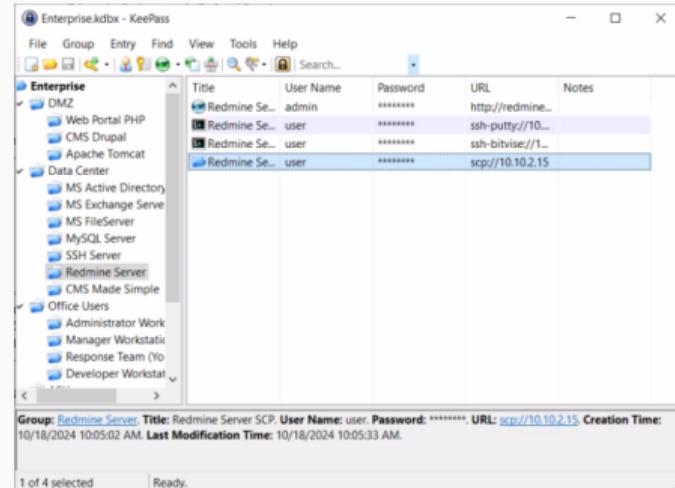
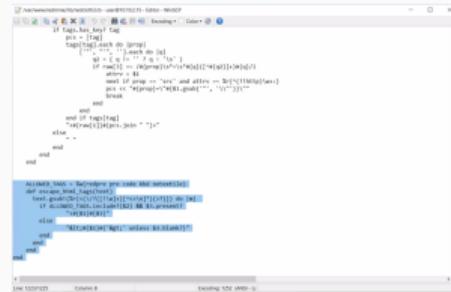


Рис. 12: Просмотр учетных данных администратора

Модификация файла redcloth3.rb

Видим, что злоумышленником была добавлена константа `ALLOWED_TAGS`, которая определяет список тегов, которые не будут экранироваться. Тег `<pre>`, который использовался злоумышленником для внедрения вредоносного JavaScript-кода, мы исключили из этого списка. Теперь, при обнаружении любого тега, не входящего в `ALLOWED_TAGS`, он теперь будет автоматически экранирован (заменен на `<` и `>`), что делает его безопасным для отображения.

A screenshot of a code editor window titled "redcloth3.rb". The code is written in Ruby. A specific line of code has been highlighted with a blue selection bar:

```
if tags[0].strip == '<pre>'
```

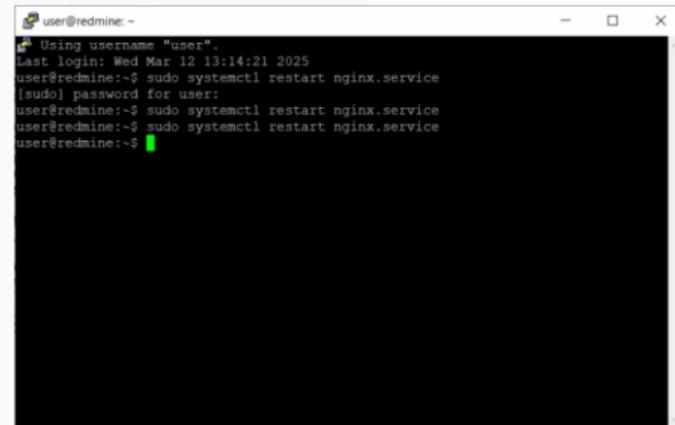
This line is part of a conditional block that checks if the first tag in the array is "<pre>". The rest of the code in the editor shows various string manipulations and loops, likely related to parsing and escaping HTML tags.

Рис. 13: Модификация файла redcloth3.rb для устранения уязвимости

Перезапуск сервера

После внесения изменений в код в терминале мы выполняем команду

**sudo systemctl restart
nginx.service.** Это необходимо для того, чтобы веб-сервер загрузил обновленный код и изменения вступили в силу.



```
user@redmine: ~
└─ Using username "user".
Last login: Wed Mar 12 13:14:21 2025
user@redmine:~$ sudo systemctl restart nginx.service
(sudo) password for user:
user@redmine:~$ sudo systemctl restart nginx.service
user@redmine:~$ sudo systemctl restart nginx.service
user@redmine:~$
```

Рис. 14: Перезапуск сервера

Содержимое Wiki-страницы после внесения изменений в код и перезапуска сервера

На скриншоте показано содержимое Wiki-страницы проекта Dev1 до и после перезапуска сервера. До перезапуска вредоносный код отображался “как есть”, запускался при переходе на веб-страницу, а после — был экранирован и стал просто текстом.

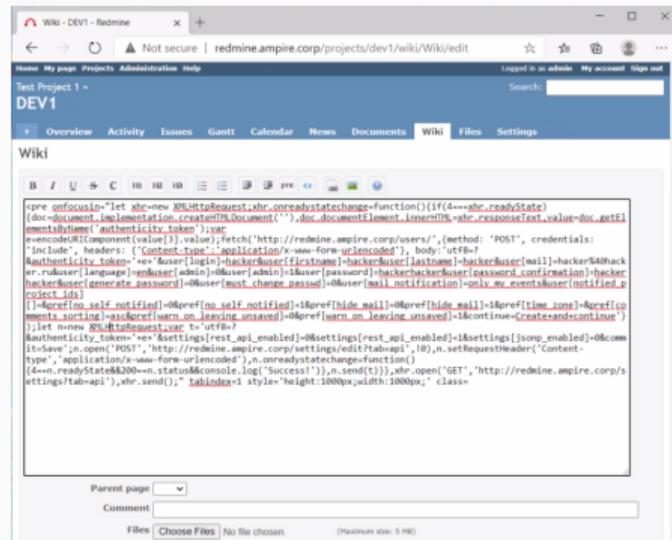


Рис. 15: Содержимое Wiki-страницы после внесения изменений в код и перезапуска сервера

Видим, что уязвимость XSS успешно устранена

The screenshot shows a web-based incident management system. At the top, a navigation bar includes links for 'Лабораторная 2-С (НФИ) 04_10', 'Группа: НФИbd-01-22 (С) - вторник', and '+ Добавить инцидент'. Below the navigation, a sub-navigation bar has tabs for 'Основная информация' (highlighted in yellow), 'Инциденты', 'Цепочки кибератаки Beta', 'Схема шаблона', and 'Материалы'.

The main content area features a large orange circular icon with concentric rings, labeled 'CSIRT'. To its right, a timer displays '00:00:00' with the text 'Тренировка запущена. Атака завершена 100%'. Below the timer, it says 'Сценарий: Защита научно-технической информации предприятия' and 'Шаблон: Офис'. A note indicates the training was started 09-20.

On the right side, a section titled 'Нераспределенные инциденты' lists three items: 'Попытка SQL-инъекции с использованием SELECT и SLEEP на веб-сервере redmine.ampire.corp', 'Уязвимость XSS', and 'Попытка выполнения удаленного кода через Microsoft PowerShell на клиентском устройстве'. It also mentions 'Активность трояна LaZagne'.

The bottom left contains a section titled 'Уязвимости и последствия' listing three items: 'Weak user password' (status: Устранимо), 'Dev backdoor' (status: Устранимо), and 'Уязвимость 3' (status: Не устранимо). The 'Уязвимость 3' entry notes 'Уязвимость без последствий'.

The bottom right shows a detailed view of the 'XSS' entry, which is marked as 'Устранимо' (resolved). A tooltip for this status says 'Нет ответственных' (No responsible parties).

A small note at the bottom center states 'Уязвимость XSS успешно устранена'.

Рис. 16: Устранена уязвимость 2 (XSS)

Удаление нового пользователя Redmine

В ходе сценария внутренний нарушитель успешно эксплуатировал уязвимость XSS (CVE-2019-17427) для внедрения вредоносного JavaScript-кода на Wiki-страницу проекта Dev1. Этот код был направлен на создание нового пользователя с правами администратора, что позволило злоумышленнику получить неограниченный доступ к системе Redmine и ее конфиденциальной информации.

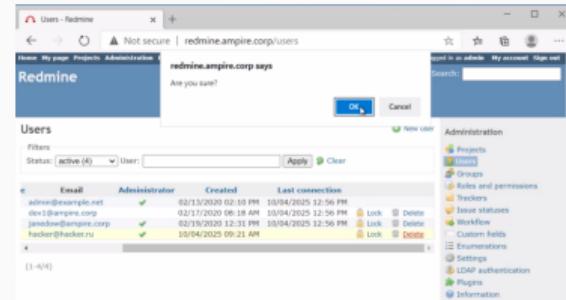


Рис. 17: Удаление нового пользователя Redmine

Полностью устранена вторая уязвимость и её последствие

The screenshot shows a Redmine project page titled "Лабораторная 2-С (НФИ) 04_10". The top navigation bar includes links for "Основная информация", "Инциденты", "Цепочки кибератаки", "Биз", "Схема шаблона", and "Материалы". A banner at the top right indicates that the "Redmine User" issue has been resolved on October 4, 2023.

Trенировка запущена. Атака завершена 100%
00:00:00

Сценарий: Защита научно-технической информации предприятия
Шаблон: Офис
Запущена в 08:20

Нераспределенные инциденты

Попытка SQL-инъекции с использованием SELECT и SLEEP на web-сервере redmine.ampire.corp
Уязвимость XSS
Попытка выполнения удаленного кода через Microsoft PowerShell на клиентском устройстве
Активность тројана LaZagne

Уязвимости и последствия

Уязвимость	Статус
Weak user password	Устранено
Dev backdoor	Устранено
Уязвимость 3	Не устранено
Уязвимость без последствий	

Рис. 18: Полностью устранена вторая уязвимость и её последствие

Эксплуатация уязвимости Blind SQL-инъекции

На приведенном скриншоте показан процесс эксплуатации уязвимости до ее устранения. Он демонстрирует, как злоумышленник проводит атаку Blind SQL-инъекции.

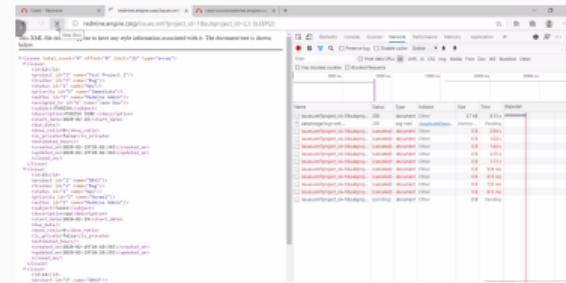
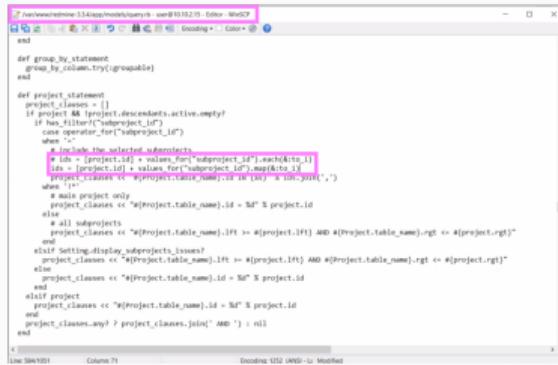


Рис. 19: Эксплуатация уязвимости Blind SQL-инъекции

Внесение изменений в файл query.rb

Внесем изменения в файл *query.rb*. Этот файл является частью модели данных Redmine и отвечает за формирование SQL-запросов к базе данных. В нем находится код, который обрабатывает параметр *subproject_id*.



The screenshot shows a code editor window with the file 'query.rb' open. A specific line of code is highlighted with a pink rectangular selection:

```
      project_classes << "#{$project.table_name}.id = $d" % project.id
    else
      project_classes << "#{$project.table_name}.id >= $l AND #{$project.table_name}.id <= $h" % [l, h]
    end
  end
end
```

The highlighted line is:

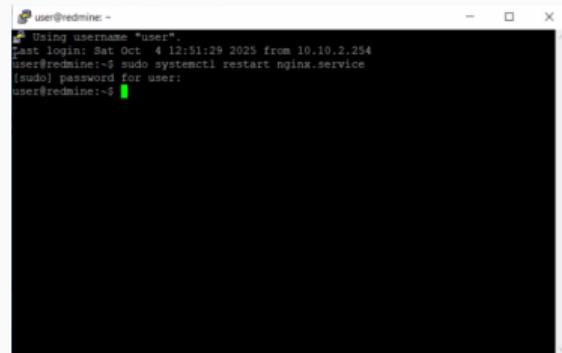
```
#include the selected subprojects
```

The code editor interface includes tabs for 'File', 'Edit', 'Search', 'View', 'Tools', 'Help', and 'Recent'. The status bar at the bottom shows 'Line 58 of 101' and 'Column 71'. The bottom right corner indicates 'Encoding: UTF-8 (UTF-8 Modified)'.

Рис. 20: Внесение изменений в файл query.rb

Перезапуск сервера

После внесения изменений в файл `query.rb` в терминале мы выполняем команду `sudo systemctl restart nginx.service`. Это необходимо для того, чтобы изменения вступили в силу.



```
user@redmine: ~
Using username "user".
Last login: Sat Oct  4 12:51:29 2025 from 10.10.2.254
user@redmine:~$ sudo systemctl restart nginx.service
(sudo) password for user:
user@redmine:~$
```

Рис. 21: Перезапуск сервера

Полностью устранена третья уязвимость (последствия нет)

The screenshot shows a web application interface for managing security incidents. At the top, there's a header with the title "Лабораторная 2-С (НФИ) 04_10" and a group identifier "Группа: НФИbd-01-22 (C) - вторник". A yellow button "+ Добавить инцидент" is visible. Below the header, a navigation bar includes links for "Основная информация", "Инциденты", "Цепочки кибератаки", "Beta", "Схема шаблона", and "Материалы".

The main content area has two main sections. On the left, a large box displays a red circular logo with concentric circles, labeled "CSIRT". It shows a progress bar "Тренировка запущена. Атака завершена 100%" and a timer "00:00:00". Below the progress bar, it says "Сценарий: Защита научно-технической информации предприятия" and "Шаблон: Офис". A note "Запущена в: 09:20" is also present.

On the right, a section titled "Нераспределенные инциденты" lists several items:

- Попытка SQL-инъекции с использованием SELECT и SLEEP на веб-сервере redmine.ampire.corp
- Уязвимость XSS
- Попытка выполнения удаленного кода через Microsoft PowerShell на клиентском устройстве
- Активность трояна LaZagne

Below these sections, a heading "Уязвимости и последствия" is followed by a table listing vulnerabilities:

Weak user password	Устранино
Dev backdoor	Устранино
XSS	Устранино
Redmine User	Устранино
Blind_SQLi	Устранино

A note at the bottom of the table states "Уязвимость без последствий".

Рис. 22: Уязвимость Blind_SQLi была устранена

Результаты

Результаты

В ходе лабораторной работы был успешно реализован сценарий защиты научно-технической информации предприятия: обнаружены и устранены уязвимости (слабый пароль, XSS, Blind SQL-инъекция), нейтрализованы последствия атаки (удалён backdoor и несанкционированный пользователь Redmine).