

# **Отчёт о расследовании инцидента информационной безопасности**

**Лабораторная работа: Защита научно-технической информации  
предприятия**

Мугари Абдеррахим

Королёв Иван

Кудряшов Артём

Ощепков Дмитрий

Оганнисян Давит

Шуплецов Александр

# Содержание

<b>1</b>	<b>Введение</b>	<b>6</b>
1.1	Цель работы . . . . .	6
1.2	Описание инфраструктуры . . . . .	6
<b>2</b>	<b>Ход расследования</b>	<b>8</b>
2.1	Этап 1: Начальная компрометация . . . . .	8
2.1.1	Обнаружение подозрительной активности . . . . .	8
2.1.2	Анализ логов аутентификации . . . . .	8
2.2	Этап 2: Lateral Movement и установка backdoor . . . . .	9
2.2.1	Загрузка вредоносных файлов . . . . .	9
2.2.2	Создание персистентности . . . . .	9
2.2.3	Кража учетных данных . . . . .	10
2.3	Этап 3: Атака XSS на Redmine (CVE-2019-17427) . . . . .	11
2.3.1	Внедрение вредоносного кода . . . . .	11
2.3.2	Результат XSS атаки . . . . .	12
2.4	Этап 4: SQL Injection (CVE-2019-18890) . . . . .	13
2.4.1	Эксплуатация Blind SQL Injection . . . . .	13
<b>3</b>	<b>Анализ с помощью средств мониторинга</b>	<b>14</b>
3.1	ViPNet IDS NS . . . . .	14
3.1.1	Обнаруженные события . . . . .	14
<b>4</b>	<b>Устранение уязвимостей</b>	<b>15</b>
4.1	Уязвимость 1: Слабый пароль . . . . .	15
4.1.1	Изменение пароля в Active Directory . . . . .	15
4.2	Уязвимость 2: XSS (CVE-2019-17427) . . . . .	15
4.2.1	Исправление в коде Redmine . . . . .	15
4.2.2	Перезапуск сервера . . . . .	17
4.3	Уязвимость 3: SQL Injection (CVE-2019-18890) . . . . .	17
4.3.1	Исправление в query.rb . . . . .	17
4.4	Удаление последствий . . . . .	18
4.4.1	Удаление backdoor . . . . .	18
4.4.2	Удаление пользователя hacker . . . . .	19
4.4.3	Отключение REST API . . . . .	19
<b>5</b>	<b>Классификация инцидентов</b>	<b>20</b>
5.1	Общая информация о выявленных инцидентах . . . . .	20

5.2	Уязвимость 1: Слабый пароль пользователя dev1 (рис. 5.1) . . . . .	20
5.3	Последствие 1: Установка backdoor и кража credentials через LaZagne (рис. 5.2) . . . . .	21
5.4	Уязвимость 2: XSS (CVE-2019-17427) . . . . .	21
5.4.1	Описание . . . . .	21
5.5	Последствие 2: Создание admin (hacker) аккаунта для доступа к конфиденциальным проектам . . . . .	22
5.5.1	Описание . . . . .	22
5.6	Уязвимость 3: Blind SQL Injection (CVE-2019-18890) . . . . .	23
5.6.1	Описание . . . . .	23
5.7	Долгосрочные меры . . . . .	24
5.7.1	Организационные меры . . . . .	24
<b>6</b>	<b>Заключение</b>	<b>26</b>
6.1	Выводы . . . . .	27
<b>7</b>	<b>Список использованных инструментов</b>	<b>28</b>

# Список иллюстраций

1.1	Схема сети AMPIRE . . . . .	7
2.1	События в ViPNet IDS - попытки подключения . . . . .	8
2.2	ViPNet IDS NS . . . . .	9
2.3	Загрузка файлов на File Server через SMB . . . . .	9
2.4	Планировщик задач - Evil task . . . . .	10
2.5	Вывод LaZagne с паролями . . . . .	10
2.6	Wiki страница с XSS payload . . . . .	11
2.7	Исходный код страницы с вредоносным JavaScript . . . . .	11
2.8	Включенный REST API в настройках Redmine . . . . .	12
2.9	Созданный пользователь hacker с правами администратора . . . . .	12
2.10	HTTP запрос с SQL injection в параметре subproject_id . . . . .	13
3.1	Общий список событий в ViPNet IDS . . . . .	14
4.1	Active Directory - сброс пароля пользователя . . . . .	15
4.2	Файл redcloth3.rb до исправления . . . . .	16
4.3	Внесение изменений в redcloth3.rb . . . . .	16
4.4	Перезапуск сервера . . . . .	17
4.5	Файл query.rb с уязвимым кодом . . . . .	17
4.6	Исправленный код . . . . .	18
4.7	Удаление задачи из планировщика . . . . .	18
4.8	Удаление пользователя hacker из Redmine . . . . .	19
4.9	Отключение REST API в настройках . . . . .	19
5.1	Уязвимость 1: Слабый пароль пользователя dev1 . . . . .	20
5.2	Последствие 1: Установка backdoor и кража credentials через LaZagne . . . . .	21
5.3	Уязвимость 2: XSS (CVE-2019-17427) . . . . .	22
5.4	Последствие 2: Создание admin (hacker) аккаунта для доступа к конфиденциальным проектам . . . . .	23
5.5	Уязвимость 3: Blind SQL Injection (CVE-2019-18890) . . . . .	24
6.1	успешно расследован инцидент информационной безопасности в инфраструктуре AMPIRE . . . . .	26

## **Список таблиц**

# 1 Введение

## 1.1 Цель работы

Исследовать и задокументировать инцидент информационной безопасности в корпоративной инфраструктуре компании AMPIRE, выявить уязвимости и предложить меры по их устранению.

## 1.2 Описание инфраструктуры

Инфраструктура компании AMPIRE включает:

- Developer Workstation (10.10.4.13) - рабочее место разработчика dev1
- Manager Workstation (10.10.4.11) - рабочее место менеджера
- File Server (10.10.2.12) - файловый сервер
- Redmine Server (10.10.2.15) - сервер управления проектами
- Internal Router (10.10.2.254) - внутренний маршрутизатор

На (рис. 1.1) представлена схема сети компании.

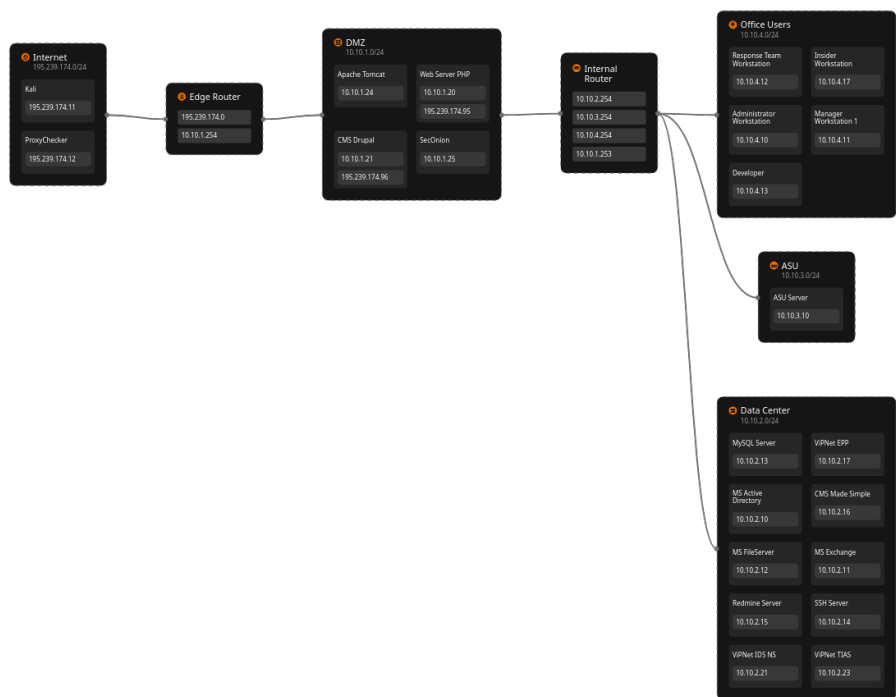


Рис. 1.1: Схема сети AMPIRE

## 2 Ход расследования

### 2.1 Этап 1: Начальная компрометация

#### 2.1.1 Обнаружение подозрительной активности

При анализе событий ViPNet IDS были обнаружены подозрительные попытки подключения с узла 10.10.4.13 (Developer Workstation) к узлу 10.10.4.11 (Manager Workstation) (рис. 2.1).

21:31:09.039 30.09.2025	ET ATTACK_RESPONSE Microsoft Powershell Banner Outbound	successful-admin	TCP	10.10.4.13	10.10.4.11	🔒→🔒
21:31:09.039 30.09.2025	ET ATTACK_RESPONSE Nishang Invoke-PowerShellTcp Shell Prompt Out...	bad-unknown	TCP	10.10.4.13	10.10.4.11	🔒→🔒
21:31:09.086 30.09.2025	ET INFO PowerShell Command Prompt Outbound On High Port	misc-activity	TCP	10.10.4.13	10.10.4.11	🔒→🔒
21:31:09.197 30.09.2025	ET POLICY SMB2 NT Create AndX Request For a .bat File	bad-unknown	TCP	10.10.4.13	10.10.2.12	🔒→🔒
21:31:09.197 30.09.2025	ET POLICY SMB2 NT Create AndX Request For a .bat File	bad-unknown	TCP	10.10.2.254	10.10.2.12	🔒→🔒
21:31:09.380 30.09.2025	ET POLICY SMB2 NT Create AndX Request For a .bat File	bad-unknown	TCP	10.10.4.13	10.10.2.12	🔒→🔒
21:31:09.380 30.09.2025	ET POLICY SMB2 NT Create AndX Request For a .bat File	bad-unknown	TCP	10.10.2.254	10.10.2.12	🔒→🔒
21:31:09.465 30.09.2025	ET POLICY SMB2 NT Create AndX Request For a .bat File	bad-unknown	TCP	10.10.4.13	10.10.2.12	🔒→🔒
21:31:09.465 30.09.2025	ET POLICY SMB2 NT Create AndX Request For a .bat File	bad-unknown	TCP	10.10.2.254	10.10.2.12	🔒→🔒
21:31:09.473 30.09.2025	ET POLICY SMB2 NT Create AndX Request For an Executable File	bad-unknown	TCP	10.10.4.13	10.10.2.12	🔒→🔒
21:31:09.473 30.09.2025	ET POLICY SMB2 NT Create AndX Request For an Executable File	bad-unknown	TCP	10.10.2.254	10.10.2.12	🔒→🔒
21:31:09.698 30.09.2025	ET POLICY SMB2 NT Create AndX Request For an Executable File	bad-unknown	TCP	10.10.4.13	10.10.2.12	🔒→🔒
21:31:09.698 30.09.2025	ET POLICY SMB2 NT Create AndX Request For an Executable File	bad-unknown	TCP	10.10.2.254	10.10.2.12	🔒→🔒

Рис. 2.1: События в ViPNet IDS - попытки подключения

#### 2.1.2 Анализ логов аутентификации

Проверка журналов ViPNet IDS NS показала множественные попытки входа (рис. 2.2):



21:31:09.039 30.09.2025	ET ATTACK_RESPONSE Microsoft Powershell Banner Outbound	successful-admin	TCP	10.10.4.13	10.10.4.11	🚩
21:31:09.039 30.09.2025	ET ATTACK_RESPONSE Nishang Invoke-PowerShellTcp Shell Prompt Out...	bad-unknown	TCP	10.10.4.13	10.10.4.11	🚩
21:31:09.086 30.09.2025	ET INFO PowerShell Command Prompt Outbound On High Port	misc-activity	TCP	10.10.4.13	10.10.4.11	🚩
21:31:09.197 30.09.2025	ET POLICY SMB2 NT Create AndX Request For a .bat File	bad-unknown	TCP	10.10.4.13	10.10.2.12	🚩
21:31:09.197 30.09.2025	ET POLICY SMB2 NT Create AndX Request For a .bat File	bad-unknown	TCP	10.10.2.254	10.10.2.12	🚩
21:31:09.380 30.09.2025	ET POLICY SMB2 NT Create AndX Request For a .bat File	bad-unknown	TCP	10.10.4.13	10.10.2.12	🚩
21:31:09.380 30.09.2025	ET POLICY SMB2 NT Create AndX Request For a .bat File	bad-unknown	TCP	10.10.2.254	10.10.2.12	🚩
21:31:09.465 30.09.2025	ET POLICY SMB2 NT Create AndX Request For a .bat File	bad-unknown	TCP	10.10.4.13	10.10.2.12	🚩
21:31:09.465 30.09.2025	ET POLICY SMB2 NT Create AndX Request For a .bat File	bad-unknown	TCP	10.10.2.254	10.10.2.12	🚩
21:31:09.473 30.09.2025	ET POLICY SMB2 NT Create AndX Request For an Executable File	bad-unknown	TCP	10.10.4.13	10.10.2.12	🚩
21:31:09.473 30.09.2025	ET POLICY SMB2 NT Create AndX Request For an Executable File	bad-unknown	TCP	10.10.2.254	10.10.2.12	🚩
21:31:09.698 30.09.2025	ET POLICY SMB2 NT Create AndX Request For an Executable File	bad-unknown	TCP	10.10.4.13	10.10.2.12	🚩
21:31:09.698 30.09.2025	ET POLICY SMB2 NT Create AndX Request For an Executable File	bad-unknown	TCP	10.10.2.254	10.10.2.12	🚩

Рис. 2.2: ViPNet IDS NS

**Обнаружено:** - Множественные неудачные попытки входа - Успешный вход после серии неудачных попыток - Источник: 10.10.4.13 (Developer Workstation) - Цель: 10.10.4.11 (Manager Workstation)

## 2.2 Этап 2: Lateral Movement и установка backdoor

### 2.2.1 Загрузка вредоносных файлов

После успешной компрометации Manager Workstation, с неё были загружены файлы на File Server (рис. 2.3):

21:31:13.446 30.09.2025	ET ATTACK_RESPONSE LaZagne Artifact Outbound in FTP	troj...	TCP	10.10.4.13
21:31:09.039 30.09.2025	ET ATTACK_RESPONSE Microsoft Powershell Banner Outbound	suc...	TCP	10.10.4.13
21:30:45.338 30.09.2025	ET ATTACK_RESPONSE Microsoft Powershell Banner Outbound	suc...	TCP	10.10.4.13

Рис. 2.3: Загрузка файлов на File Server через SMB

**Загруженные файлы:** - bcdoor.exe (backdoor) - legacy.exe (LaZagne - инструмент для кражи паролей) - Вредоносный .bat файл

### 2.2.2 Создание персистентности

На Developer Workstation была обнаружена задача в планировщике (рис. 2.4):

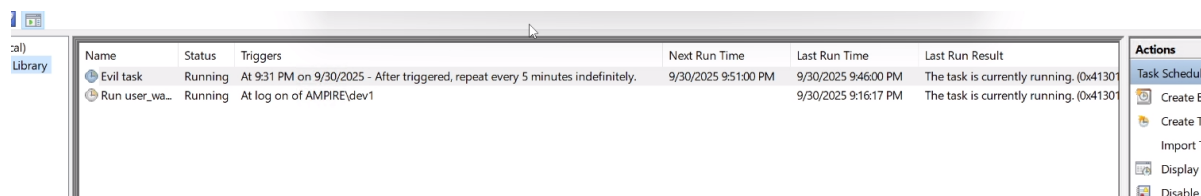


Рис. 2.4: Планировщик задач - Evil task

**Параметры задачи:** - Название: "Evil task" - Запуск: каждые 5 минут

### 2.2.3 Кража учетных данных

Запуск LaZagne для извлечения сохраненных паролей (рис. 2.5):

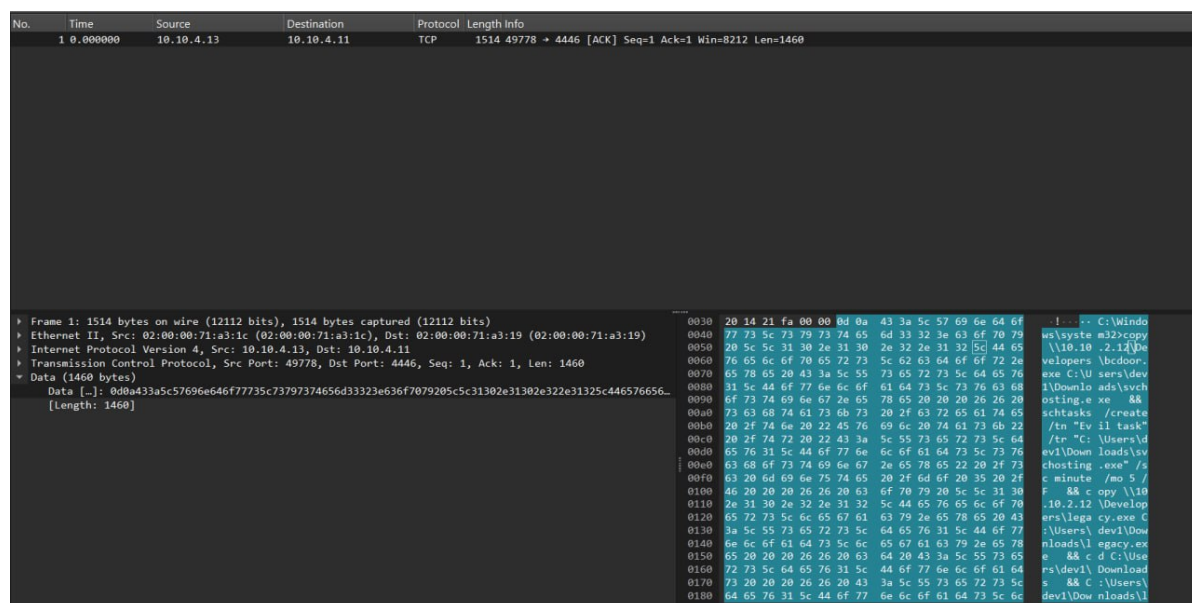


Рис. 2.5: Вывод LaZagne с паролями

### Извлеченные данные:

URL: <http://redmine.ampire.corp/>

Username: dev1

Password: qwe123!@#

## 2.3 Этап 3: Атака XSS на Redmine (CVE-2019-17427)

### 2.3.1 Внедрение вредоносного кода

С Manager Workstation была проведена XSS атака на Redmine. На (рис. 2.6) показана wiki страница с внедренным payload:

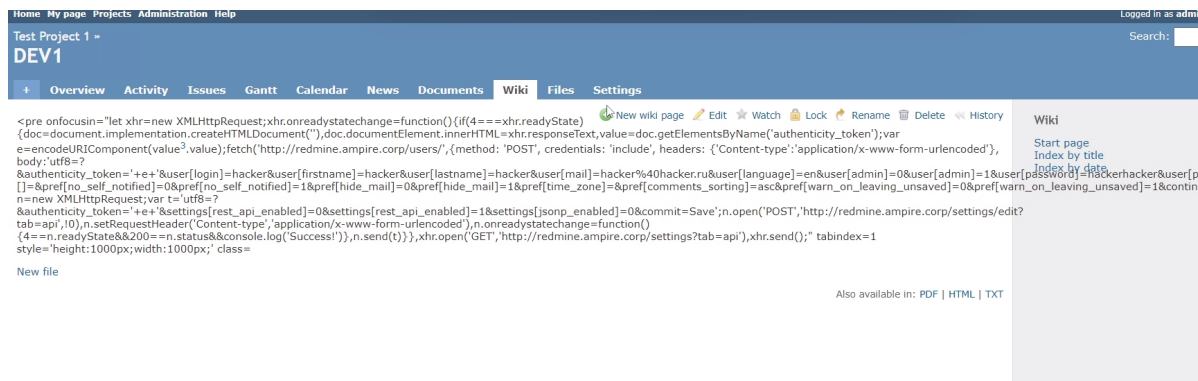


Рис. 2.6: Wiki страница с XSS payload

Исходный код страницы с вредоносным JavaScript представлен на (рис. 2.7):

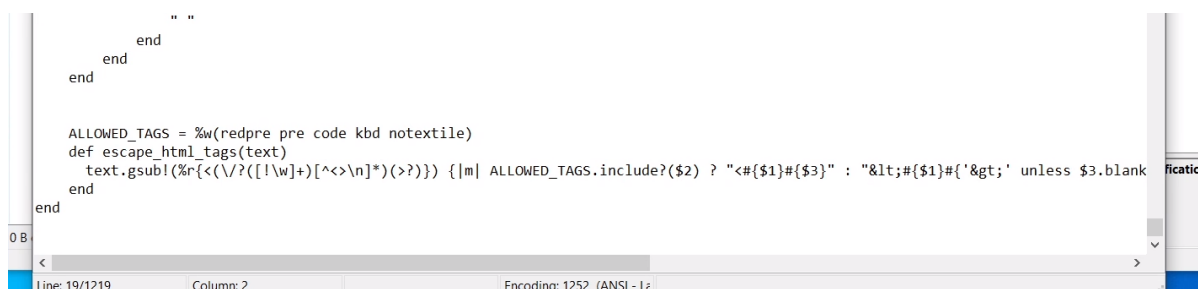


Рис. 2.7: Исходный код страницы с вредоносным JavaScript

#### XSS Payload:

```
<pre onfocusin="let xhr=new XMLHttpRequest;
xhr.onreadystatechange=function(){
  if(4===xhr.readyState){
    // Извлечение CSRF токена
    // Создание admin пользователя "hacker"
```

```

// Включение REST API
}
},
xhr.open('GET','http://redmine.ampire.corp/settings?tab=api'),
xhr.send();" tabindex=1>

```

## 2.3.2 Результат XSS атаки

После срабатывания XSS при посещении страницы администратором были получены следующие результаты (рис. 2.8, 2.9):

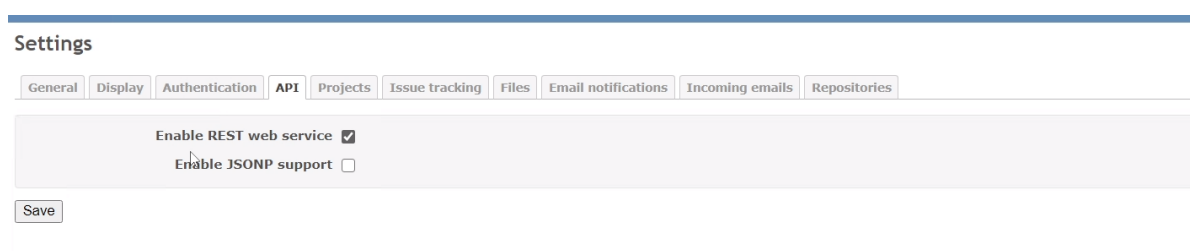


Рис. 2.8: Включенный REST API в настройках Redmine

Login	First name	Last name	Email	Administrator	Created	Last connection	
admin	Redmine	Admin	admin@example.net	✓	02/13/2020 02:10 PM	09/30/2025 09:50 PM	
DEV1	John	Doe	dev1@ampire.corp		02/17/2020 08:18 AM	09/30/2025 09:50 PM	Lock Delete
DEV2	Jane	Dow	janedow@ampire.corp	✓	02/19/2020 12:31 PM	09/30/2025 09:50 PM	Lock Delete
hacker	hacker	hacker	hacker@hacker.ru	✓	09/30/2025 09:31 PM		Lock Delete

(1-4/4)

Рис. 2.9: Созданный пользователь hacker с правами администратора

**Созданный пользователь:** - Login: hacker - Email: hacker@hacker.ru - Права: Administrator - REST API: Enabled

## 2.4 Этап 4: SQL Injection (CVE-2019-18890)

### 2.4.1 Эксплуатация Blind SQL Injection

Используя REST API, была проведена Blind SQL инъекция. HTTP запрос с инъекцией показан на (рис. 2.10):



21:31:43.128 30.09.2025	ET WEB_SERVER SQL Injection Select Sleep Time Delay	we...	TCP	10.10.4.11	10.10.2.15	🔍 → 📄
21:31:43.128 30.09.2025	AM SQL Generic SQLi in HTTP URI: 'SELECT FROM' query	clie...	TCP	10.10.4.11	10.10.2.15	🔍 → 📄
21:31:43.128 30.09.2025	AM SQL Generic SQLi in HTTP URI: 'SELECT SLEEP' query	we...	TCP	10.10.4.11	10.10.2.15	🔍 → 📄
21:31:43.128 30.09.2025	ET WEB_SERVER SQL Injection Select Sleep Time Delay	we...	TCP	10.10.2.254	10.10.2.15	🔍 → 📄
21:31:43.128 30.09.2025	AM SQL Generic SQLi in HTTP URI: 'SELECT FROM' query	clie...	TCP	10.10.2.254	10.10.2.15	🔍 → 📄

Рис. 2.10: HTTP запрос с SQL injection в параметре subproject\_id

#### Техника атаки:

GET /issues.xml?project\_id=1&subproject\_id=1;SELECT+SLEEP(2)

Посимвольное извлечение данных:

- Если символ верный → задержка 2 секунды
- Если символ неверный → быстрый ответ

## 3 Анализ с помощью средств мониторинга

### 3.1 ViPNet IDS NS

#### 3.1.1 Обнаруженные события

Общий список событий в ViPNet IDS представлен на (рис. 3.1):

21:31:32.703 30.09.2025	AM EXPLOIT Possible Redmine < v4.0.4 XSS (CVE-2019-17427)	web-application-a...	TCP	10.10.4.11	10.10.2.15	🔍→🔍
21:31:32.703 30.09.2025	AM EXPLOIT Generic Possible XSS in HTTP Body: 'onfocus()' in request	web-application-a...	TCP	10.10.4.11	10.10.2.15	🔍→🔍
21:31:32.703 30.09.2025	AM EXPLOIT Generic Possible XSS in HTTP Body: 'onreadystatechange' L...	web-application-a...	TCP	10.10.4.11	10.10.2.15	🔍→🔍
21:31:32.704 30.09.2025	AM EXPLOIT Possible Redmine < v4.0.4 XSS (CVE-2019-17427)	web-application-a...	TCP	10.10.2.254	10.10.2.15	🔍→🔍
21:31:32.704 30.09.2025	AM EXPLOIT Generic Possible XSS in HTTP Body: 'onfocus()' in request	web-application-a...	TCP	10.10.2.254	10.10.2.15	🔍→🔍
21:31:32.704 30.09.2025	AM EXPLOIT Generic Possible XSS in HTTP Body: 'onreadystatechange' L...	web-application-a...	TCP	10.10.2.254	10.10.2.15	🔍→🔍
21:31:43.128 30.09.2025	ET WEB_SERVER SQL Injection Select Sleep Time Delay	web-application-a...	TCP	10.10.4.11	10.10.2.15	🔍→🔍
21:31:43.128 30.09.2025	AM SQL Generic SQLi in HTTP URI: 'SELECT FROM' query	client-side-exploit	TCP	10.10.4.11	10.10.2.15	🔍→🔍
21:31:43.128 30.09.2025	AM SQL Generic SQLi in HTTP URI: 'SELECT SLEEP' query	web-application-a...	TCP	10.10.4.11	10.10.2.15	🔍→🔍
21:31:43.128 30.09.2025	ET WEB_SERVER SQL Injection Select Sleep Time Delay	web-application-a...	TCP	10.10.2.254	10.10.2.15	🔍→🔍
21:31:43.128 30.09.2025	AM SQL Generic SQLi in HTTP URI: 'SELECT FROM' query	client-side-exploit	TCP	10.10.2.254	10.10.2.15	🔍→🔍
21:31:43.128 30.09.2025	AM SQL Generic SQLi in HTTP URI: 'SELECT SLEEP' query	web-application-a...	TCP	10.10.2.254	10.10.2.15	🔍→🔍
21:31:43.253 30.09.2025	ET WEB_SERVER SQL Injection Select Sleep Time Delay	web-application-a...	TCP	10.10.4.11	10.10.2.15	🔍→🔍

Рис. 3.1: Общий список событий в ViPNet IDS

**Критические события:** - ET ATTACK\_RESPONSE LaZagne Artifact Outbound - AM EXPLOIT Possible Redmine < v4.0.4 XSS (CVE-2019-17427) - ET WEB\_SERVER SQL Injection Select Sleep Time Delay

## 4 Устранение уязвимостей

### 4.1 Уязвимость 1: Слабый пароль

#### 4.1.1 Изменение пароля в Active Directory

Процесс сброса пароля пользователя в Active Directory показан на (рис. 4.1):

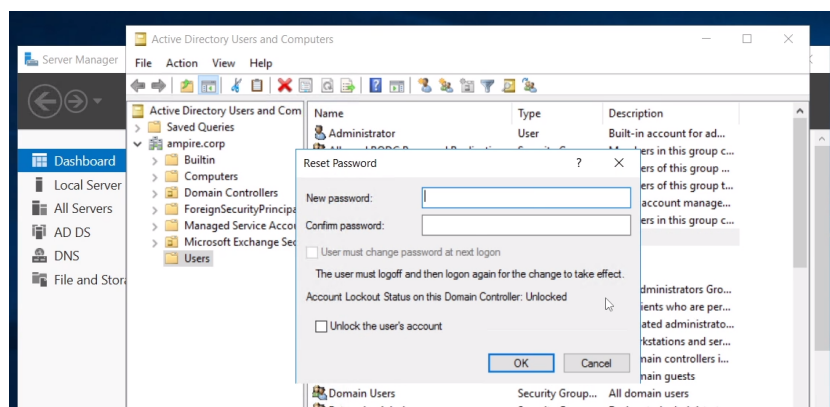


Рис. 4.1: Active Directory - сброс пароля пользователя

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

#### 4.2.1 Исправление в коде Redmine

Файл redcloth3.rb до исправления показан на (рис. 4.2):

```

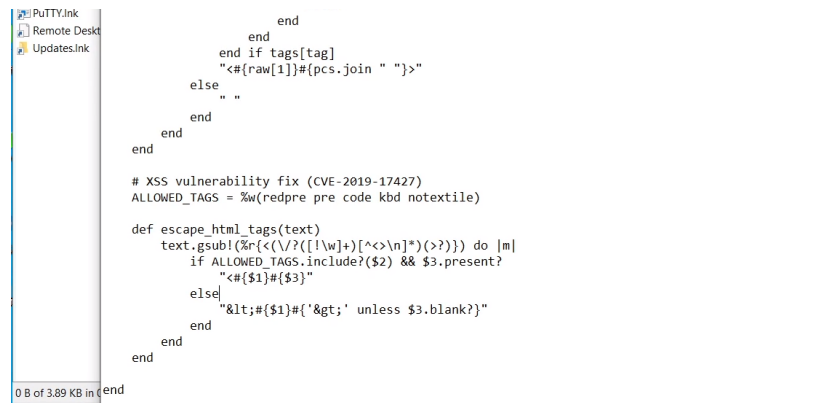
end
end
end

ALLOWED_TAGS = %w(redpre pre code kbd notextile)
def escape_html_tags(text)
  text.gsub!(/%r{<(\/?([!\\w]+)[^<>\n]*)(>?)})/ do |m|
    if ALLOWED_TAGS.include?(m[2])
      "<#{m[1]}#{m[3]}"
    else
      "&lt;#{m[1]}#{m[3]}" unless m[3].blank?
    end
  end
end
end

```

Рис. 4.2: Файл redcloth3.rb до исправления

Процесс внесения изменений в redcloth3.rb представлен на (рис. 4.3):



```

end
end
end if tags[tag]
"<#{raw[1]}#{pcs.join " ">"
else
  ""
end
end
end
end

# XSS vulnerability fix (CVE-2019-17427)
ALLOWED_TAGS = %w(redpre pre code kbd notextile)

def escape_html_tags(text)
  text.gsub!(/%r{<(\/?([!\\w]+)[^<>\n]*)(>?)})/ do |m|
    if ALLOWED_TAGS.include?(m[2]) && m[3].present?
      "<#{m[1]}#{m[3]}"
    else
      "&lt;#{m[1]}#{m[3]}" unless m[3].blank?
    end
  end
end
end
end

```

Рис. 4.3: Внесение изменений в redcloth3.rb

### Код исправления:

```

ALLOWED_TAGS = %w(redpre pre code kbd notextile)
def escape_html_tags(text)
  text.gsub!(/%r{<(\/?([!\\w]+)[^<>\n]*)(>?)})/ do |m|
    if ALLOWED_TAGS.include?(m[2]) && m[3].present?
      "<#{m[1]}#{m[3]}"
    else
      "&lt;#{m[1]}#{m[3]}" unless m[3].blank?
    end
  end
end
end
end

```



## 4.2.2 Перезапуск сервера

- После внесения изменений необходимо было перезапустить службу веб сервера (рис. 4.4):

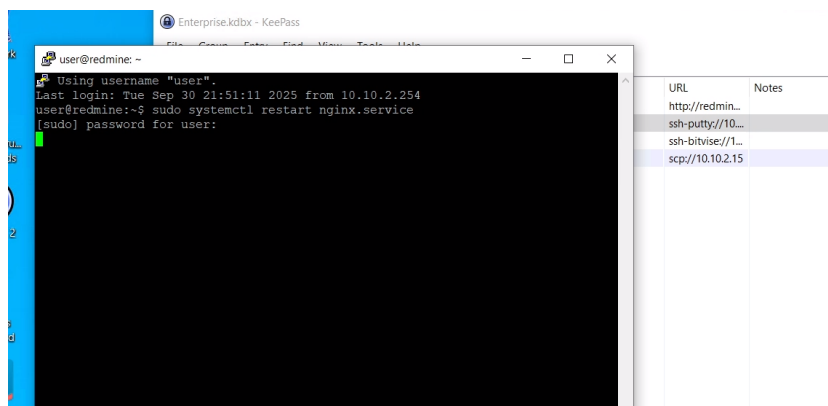


Рис. 4.4: Перезапуск сервера

## 4.3 Уязвимость 3: SQL Injection (CVE-2019-18890)

### 4.3.1 Исправление в query.rb

Файл query.rb с уязвимым кодом представлен на (рис. 4.5):

```
end

def project_statement
  project_clauses = []
  if project && !project.descendants.active.empty?
    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)
        project_clauses << "#{Project.table_name}.id IN (%s)" % ids.join(',')
      when '!=*'
        # main project only
```

Рис. 4.5: Файл query.rb с уязвимым кодом

Исправленный код показан на (рис. 4.6):

```

end

def project_statement
  project_clauses = []
  if project && !project.descendants.active.empty?
    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)
        project_clauses << "#{Project.table_name}.id IN (%s)" % ids.join(',')
      when '!=*'
        # main project only

```

Рис. 4.6: Исправленный код

```
sudo nano /var/www/redmine/app/models/query.rb
```

- Нашли строку:

```
ids = [project.id] + values_for(column.name).map(&:to_i)
```

- Закомментировали ее:

```
# ids = [project.id] + values_for(column.name).map(&:to_i)
```

## 4.4 Удаление последствий

### 4.4.1 Удаление backdoor

Процесс удаления задачи из планировщика показан на (рис. 4.7):

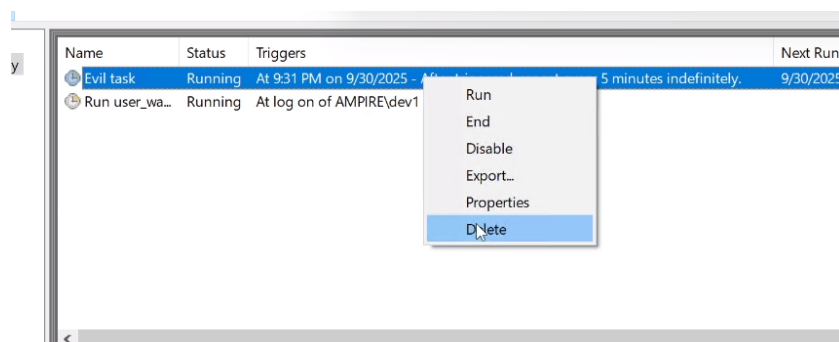


Рис. 4.7: Удаление задачи из планировщика

```
schtasks /delete /tn "Evil task" /F
del C:\Users\dev1\Downloads\svchosting.exe /F
del C:\Users\dev1\Downloads\legacy.exe /F
```

#### 4.4.2 Удаление пользователя hacker

Удаление пользователя hacker из Redmine показано на (рис. 4.8):

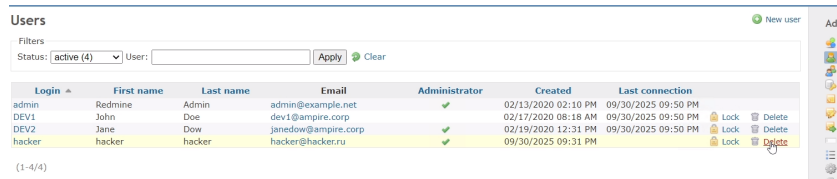


Рис. 4.8: Удаление пользователя hacker из Redmine

#### 4.4.3 Отключение REST API

Процесс отключения REST API в настройках представлен на (рис. 4.9):

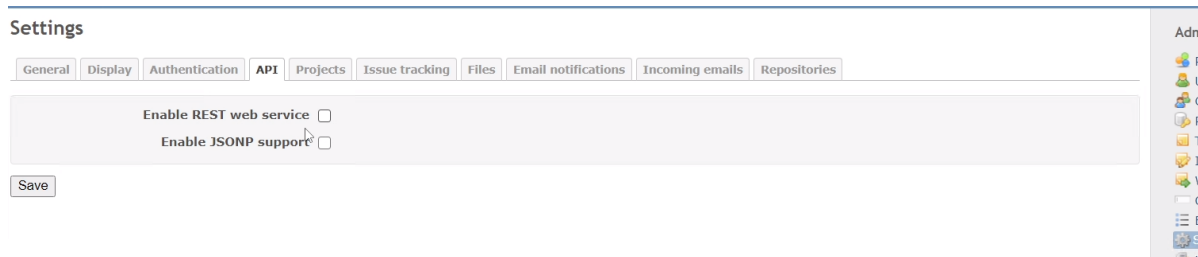


Рис. 4.9: Отключение REST API в настройках

## 5 Классификация инцидентов

### 5.1 Общая информация о выявленных инцидентах

В результате расследования были выявлены и задокументированы три уязвимости и два последствия их эксплуатации.

### 5.2 Уязвимость 1: Слабый пароль пользователя dev1 (рис. 5.1)

Слабый пароль пользователя dev1

Основная информацияЧат

Новый

Дата и время события ⓘ

30.09.2025 21:30

Описание ⓘ

Злоумышленник использовал словарную атаку для подбора слабого пароля пользователя AMPIRE\dev1 через SMB протокол. После серии неудачных попыток аутентификации был подобран корректный пароль, что предоставило злоумышленнику доступ к общим папкам файлового сервера.

Индикаторы компрометации ⓘ

WINDOWS EVENT LOG (File Server 10.10.2.12), Множественные SMB соединения

Рекомендации ⓘ

1. Сбросить пароль dev1 на сложный (мин. 12 символов, буквы, цифры, спецсимволы) 2. Проверить файловый сервер на вредоносные файлы 3. Заблокировать доступ при подозрении на активную компрометацию

Прикреплённые файлы ⓘ

IDS\_packet\_time-2025-09-30T18\_30\_45.338655Z\_ruleid-2020084 (3).pcap

Оценка

☆☆☆☆

Автор

Мугари Абдеррахим  
@1032215692@pfur.ru

Ответственный

Не заполнено

Источник

10.10.4.13

Поражённые активы

10.10.4.1110.10.2.12

Рис. 5.1: Уязвимость 1: Слабый пароль пользователя dev1

## 5.3 Последствие 1: Установка backdoor и кража credentials через LaZagne (рис. 5.2)

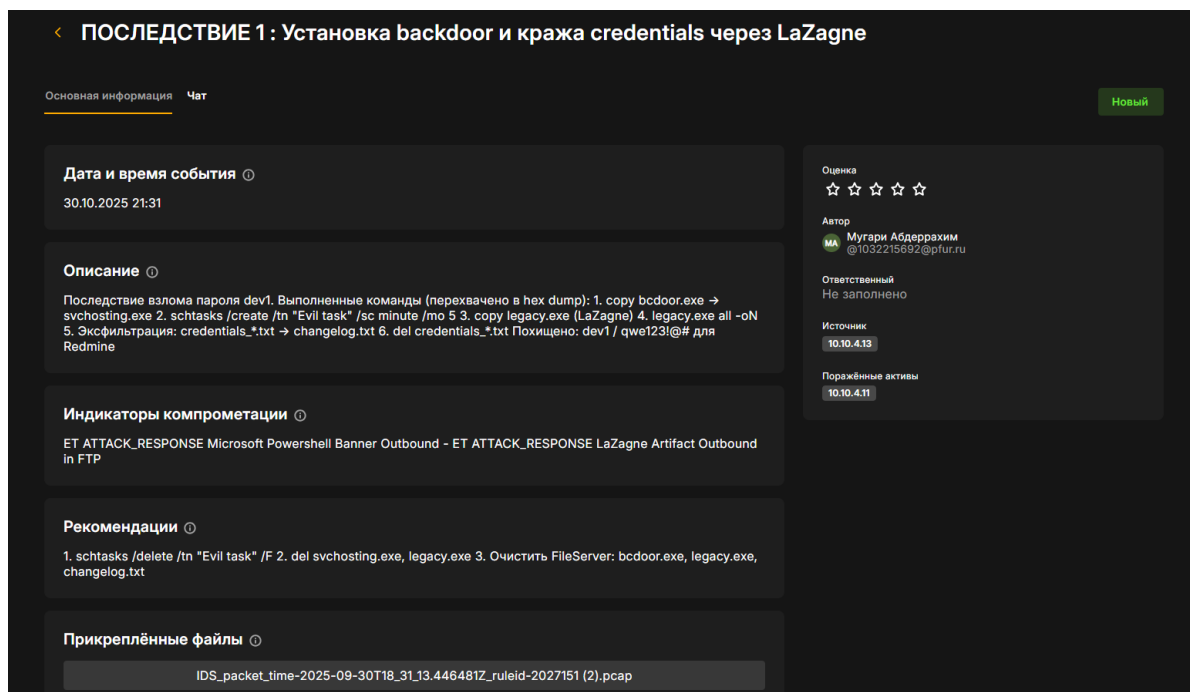


Рис. 5.2: Последствие 1: Установка backdoor и кража credentials через LaZagne

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

### 5.4.1 Описание

Используя украденные credentials `ampire\dev1`, инсайдер провел XSS атаку для получения административных прав в Redmine. Уязвимость в обработке wiki-разметки Redmine позволяет внедрить вредоносный JavaScript код, который выполняется при посещении страницы администратором. (рис. 5.3)

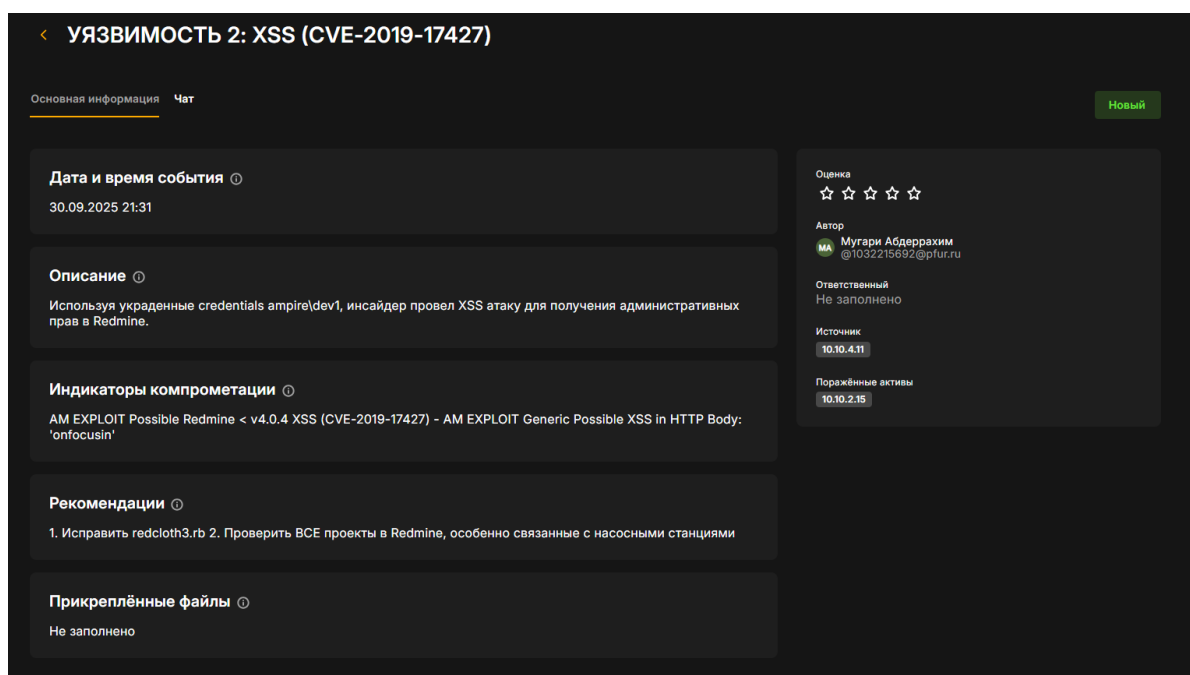


Рис. 5.3: Уязвимость 2: XSS (CVE-2019-17427)

## 5.5 Последствие 2: Создание admin (hacker) аккаунта для доступа к конфиденциальным проектам

### 5.5.1 Описание

Инсайдер создал admin аккаунт для полного доступа к базе проектов: - **Login:** hacker - **Admin:** YES - **REST API:** Enabled

Этот аккаунт предоставляет полный доступ ко всем проектам Redmine, включая конфиденциальные проекты разработки насосных станций.(рис. 5.4)

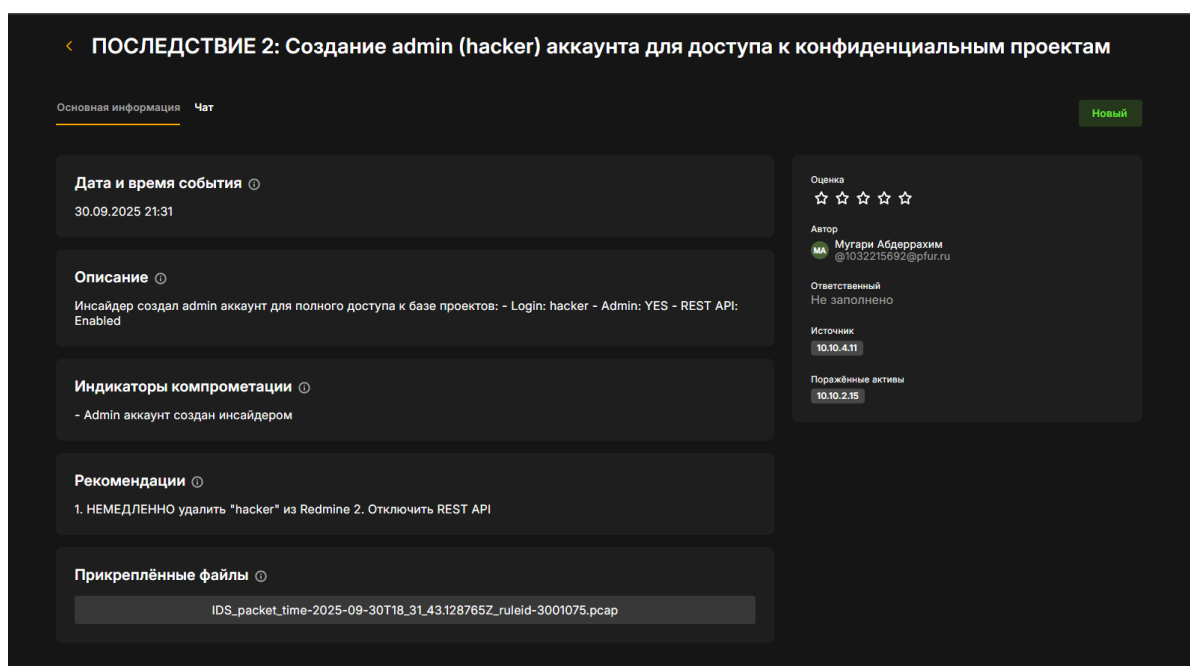


Рис. 5.4: Последствие 2: Создание admin (hacker) аккаунта для доступа к конфиденциальным проектам

## 5.6 Уязвимость 3: Blind SQL Injection (CVE-2019-18890)

### 5.6.1 Описание

CVE-2019-18890: SQL injection в параметре subproject\_id в Redmine < 3.3.10 позволяет выполнять произвольные SQL запросы, обходя систему прав доступа. (рис. 4.7)

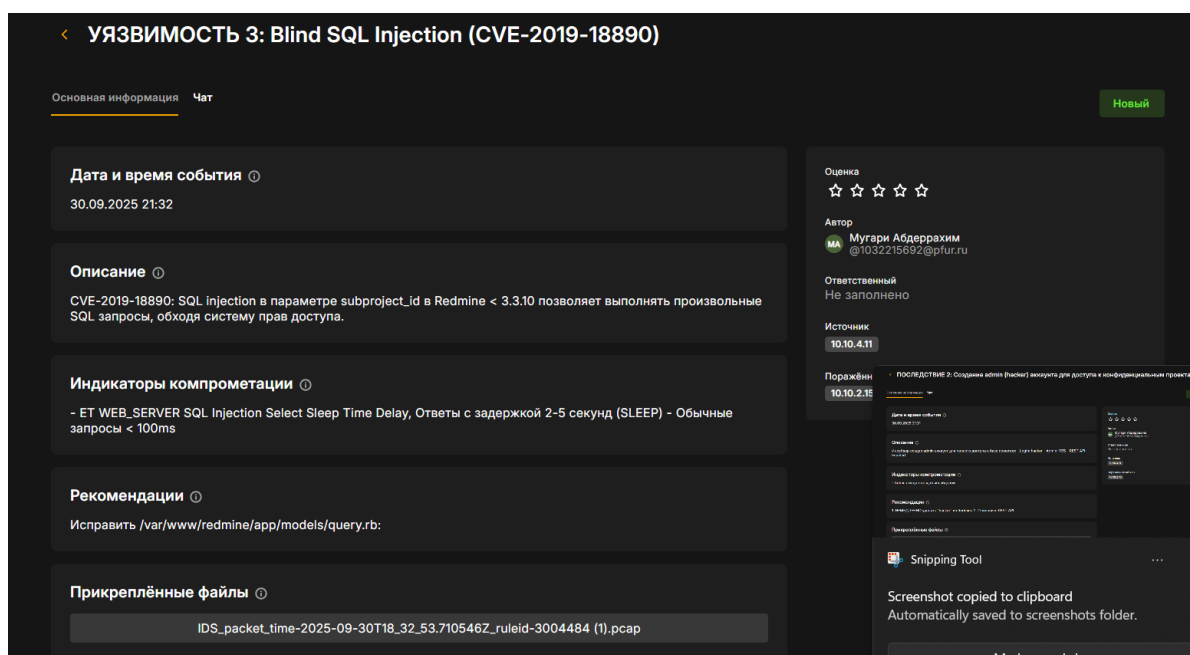


Рис. 5.5: Уязвимость 3: Blind SQL Injection (CVE-2019-18890)

## 5.7 Долгосрочные меры

### 5.7.1 Организационные меры

#### 1. Усиление процедур найма:

- Тщательная проверка кандидатов
- Background check
- Проверка рекомендаций

#### 2. Security Awareness Training:

- Обучение персонала
- Регулярные тренинги
- Симуляции атак

#### 3. Incident Response Plan:

- Документированные процедуры



- Назначенные роли
- Регулярные учения

## 6 Заключение

В ходе лабораторной работы был успешно расследован инцидент информационной безопасности в инфраструктуре AMPIRE (рис. 6.1).

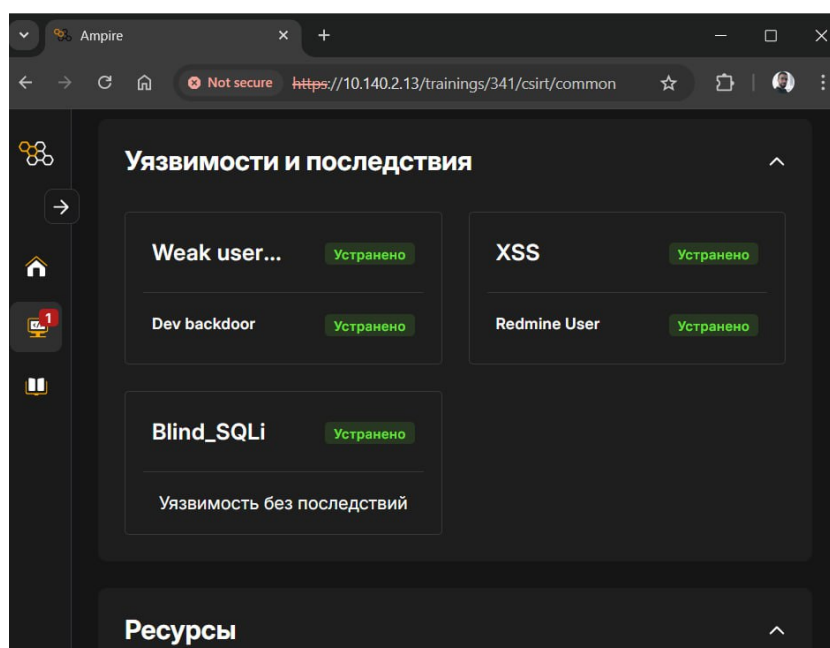


Рис. 6.1: успешно расследован инцидент информационной безопасности в инфраструктуре AMPIRE

Атака представляла собой сложную многоэтапную операцию, включающую:

1. **Insider threat** - инсайдер dev1 с рабочей станции 10.10.4.13
2. **Lateral movement** - компрометация Manager Workstation для использования как pivot point
3. **Dead drop механизм** - использование File Server для обмена данными

Все выявленные уязвимости были успешно устранены, вредоносное ПО удалено, несанкционированные учетные записи заблокированы. Предложенные рекомендации позволят предотвратить подобные инциденты в будущем.

## **6.1 Выводы**

1. Критически важно внедрение многоуровневой защиты.
2. Необходим постоянный мониторинг insider threats
3. Своевременное обновление ПО предотвращает эксплуатацию известных уязвимостей
4. Корреляция событий из разных источников позволяет выявлять сложные атаки
5. Human factor остается слабым звеном в системе безопасности

## **7 Список использованных инструментов**

- ViPNet IDS NS - обнаружение вторжений
- ViPNet TIAS - корреляция событий
- Security Onion (Kibana, Squert) - анализ сетевого трафика
- Wireshark - анализ пакетов
- Active Directory - управление учетными записями
- Планировщик задач Windows - поиск персистентности