

Лабораторная работа №1

Дисциплина - Кибербезопасность предприятия

Тимофеева Е.Н.

28 сентября 2025

Российский университет дружбы народов, Москва, Россия

Создание презентации

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».

Этапы выполнения работы

1. Слабый пароль пользователя

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

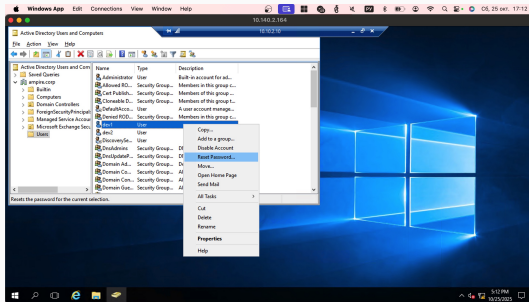


Рис. 1: Сброс пароля

Запускаем исполняемый файл в планировщике.

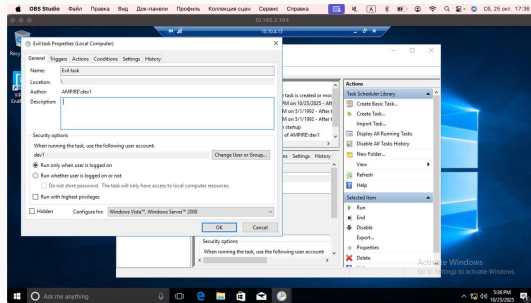


Рис. 2: Запуск исполняемого файла

Последствие Dev backdoor

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

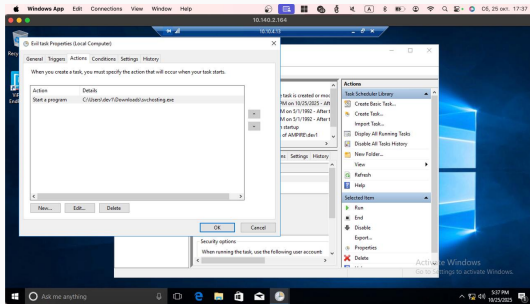


Рис. 3: Удаление evil tasc из планировщика задач и удаление файла

Устранили уязвимость 1 и последствие 1. (

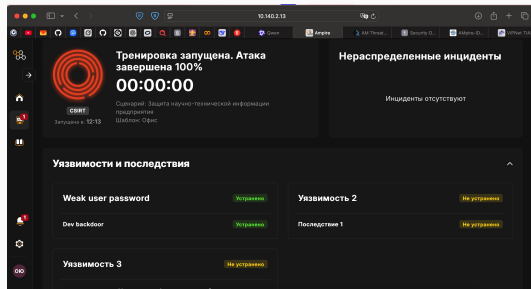


Рис. 4: Атаки устранены

Создаём карточку инцидента для уязвимости.

The screenshot shows a web interface for creating an incident ticket. The title is "Уязвимость 1 — Слабый пароль пользователя". The form is divided into several sections:

- Основная информация** (Main information): Includes a "Дата и время события" (Date and time of event) field with the value "25.10.2025 07:12".
- Описание** (Description): A text area containing the following text: "Надуться с IP 195.239.174.11 был проведён брутфорс пароля учётной записи dev1 на файловом сервере 170.10.2.51. После успешной авторизации был загружен вредоносный .bat файл. Уязвимость устранена путём смены пароля на сложный."
- Индикаторы компрометации** (Indicators of compromise): A field with the value "Weak credential pass".
- Рекомендации** (Recommendations): A list of steps: "1. Ввести политику сложности паролей в домене. 2. Включить блокировку учётных записей после N неудачных попыток. 3. Провести обучение пользователей по созданию надёжных паролей."
- Прикреплённые файлы** (Attached files): A field with the value "Снимок 25.10.2025 в 1712.png".
- Слева** (Left sidebar): Contains a "Создать" (Create) button, a "Автор" (Author) field with the value "Омарова Юлия", and an "Источники" (Sources) field with the value "195.239.174.11".

Рис. 5: Создание карточки инцидента

Создаём карточку инцидента для последствия.

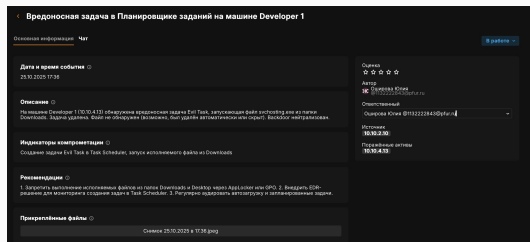


Рис. 6: Создание карточки

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.

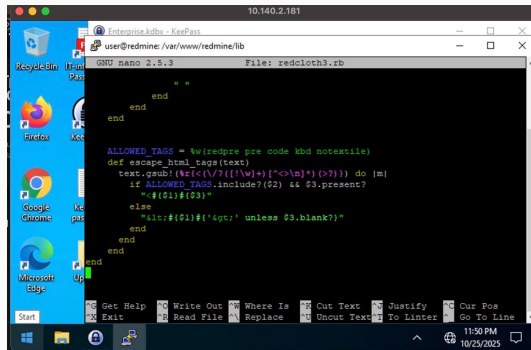
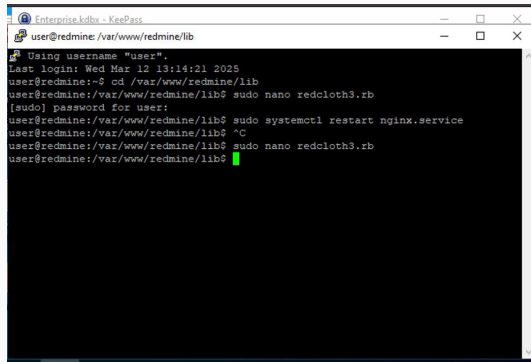


Рис. 7: Изменение кода функции

После внесения изменений перезапускаем службу веб-сервера.



```
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. 8: Перезапуск веб-сервера

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

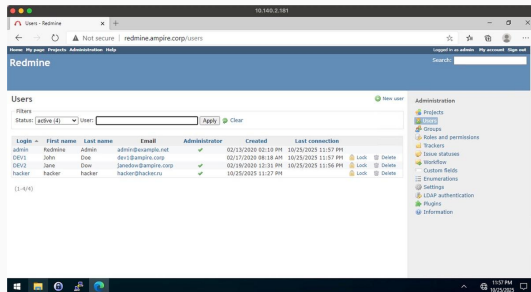


Рис. 9: Удаление пользователя hacker

Устранили 2 уязвимости и 2 последствия.

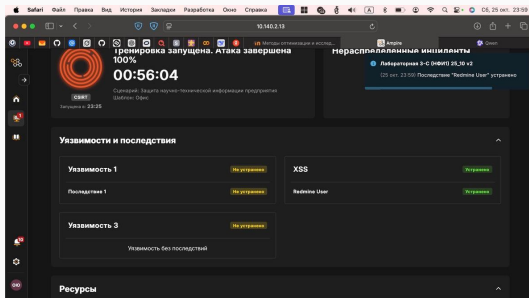


Рис. 10: Ampire

Заполняем карточку инцидента для 2 уязвимости.

< Stored XSS (CVE-2019-17427) в Wiki-разметке Redmine на сервере 10.10.2.15

Основная информация Чат [В работе](#)

Дата и время события

25.10.2025 23:55

Описание

Надуться на веб-браузерный JavaScript-код на Wiki-странице проекта Dev'n Redmine. Код автоматически включает REST API при просмотре страницы-карточки. Уязвимость исправлена путем рендеринга файла. Дополнительно CVE-2019-17427: была изменена функция в ALLOWED_TAGS, что предотвращает рендеринг HTML-тегов. Выполнено команда: node <url>test.html

Индикаторы компрометации

Stored Cross-Site Scripting, CVE-2019-17427, событие в Vulnerability -> Проведение атаки XSS на сервер Redmine

Рекомендации

1. Обновить Redmine до версии >4.0.4. 2. Регулярно обновлять зависимости и библиотеки (в т.ч. RedCloth). 3. Включить WAF с правилами против XSS. 4. Проводить аудит пользовательского контента в Wiki и комментариях.

Присоединенные файлы

Снимок 25.10.2025 в 23:50.png

Справка

Автор: [Сергей Югов](#)
ID: 01132222843@bph.ru

Ответственный

Сергей Югов @0132222843@bph.ru

Источник
(995,000,174,11)

Порядковые акты
(10,10,2,15)

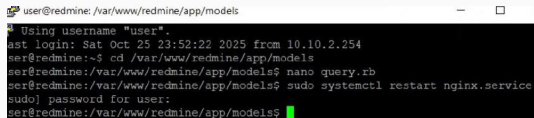
Рис. 11: Карточка инцидента

Для устранения этой уязвимости нам необходимо внести изменения в код Redmine. Находим файл `query.rb` и в нужный участок кода добавляем фильтрацию значений и часть закомментируем.

```
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 #{$}
  end
elsif Setting.display_subprojects_issues?
  project_clauses << "#{Project.table_name}.lft >= #{project.lft} AND #{$}
else
  project_clauses << "#{Project.table_name}.id = %d" % project.id
end
```

Рис. 13: Изменение кода

После внесения изменений перезапускаем службу веб-сервер.



```
user@redmine: /var/www/redmine/app/models
Using username "user".
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. 14: Перезапуск

Заполняем карточку инцидента уязвимости.

< Blind SQL-инъекция (CVE-2019-18890) в параметре subproject_id веб-приложения Redmine на сервере 10.10.2.15

Основная информация Чат В работе

Дата и время события ⌵
26.10.2025 00:03

Описание ⌵
Исследователь использовал уязвимость CVE-2019-18890 в Redmine для получения конфиденциальной информации проекта через Blind SQL-инъекцию в параметре subproject_id. Уязвимость устранена путем обновления файла /usr/share/redmine/redmine.rb и добавления фильтрации входных данных и закомментирован уязвимый участок кода, принимающий параметр subproject_id в SQL-запрос. Выполнена команда echo >/dev/null && exit 0.

Индикаторы компрометации ⌵
Blind SQL Injection, CVE-2019-18890, HTTP-запросы с SLEEP() в Security Onion

Рекомендации ⌵
1. Обновить Redmine до версии 4.3.3.3. 2. Выдавать параметризацию запросов (prepared statements) во всех местах работы с SQL. 3. Настроить WAF с правилами против SQL-инъекций. 4. Провести регулярное тестирование на проникновение (pentest) веб-приложения. 5. Включить логирование подозрительных SQL-запросов в веб-сервер.

Прикрепленные файлы ⌵
Ссылка: 26.10.2025 в 00:06.png

Оценки
☆☆☆☆

Автор
Олеся Юли
oleksia.yuliyeva@phd.ru

Отправитель
Тимофей Еленин @11222844@phd.ru

Источники
[BES-258.176.11]

Гравитные ссылки
10.10.2.15

Рис. 15: Карточка инцидента

Успешно устранили 3 уязвимость.

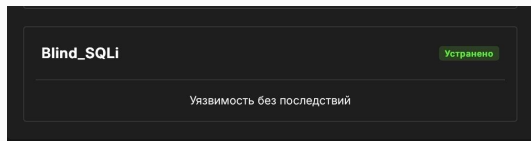


Рис. 16: Ampire

Выводы

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