

Лабораторная работа №1-С «ЗАЩИТА НАУЧНО-ТЕХНИЧЕСКОЙ ИНФОРМАЦИИ ПРЕДПРИЯТИЯ»

Кибербезопасность предприятия

Александрова У.В., Волгин И.А., Голощапов Я.В., Дворкина Е.В.,
Серегина И.А.

2025-10-02

Содержание I

1. Выполнение лабораторной работы

0.1 Состав команды

Александрова Ульяна Вадимовна
Волгин Иван Алексеевич
Голощапов Ярослав Вячеславович
Дворкина Ева Владимировна
Серёгина Ирина Андреевна
Чемоданова Ангелина Александровна

0.2 Цели и задачи

Освоить практических навыков выявления, анализа и устранения уязвимостей информационных систем в рамках сценария «Защита научно-технической информации предприятия».

Обнаружить, проанализировать и закрыть уязвимости:

Слабый пароль пользователя;

- ▶ XSS (CVE-2019-17427);

Определить и устраниТЬ последствия эксплуатации уязвимостей:

Разработать и применить меры по устранению выявленных уязвимостей.

0.2 Цели и задачи

Освоить практических навыков выявления, анализа и устранения уязвимостей информационных систем в рамках сценария «Защита научно-технической информации предприятия».

Обнаружить, проанализировать и закрыть уязвимости:

Слабый пароль пользователя;

- ▶ XSS (CVE-2019-17427);
- ▶ Blind SQL (CVE-2019-18890).

Определить и устраниТЬ последствия эксплуатации уязвимостей:

Разработать и применить меры по устранению выявленных уязвимостей.

0.2 Цели и задачи

Освоить практических навыков выявления, анализа и устранения уязвимостей информационных систем в рамках сценария «Защита научно-технической информации предприятия».

Обнаружить, проанализировать и закрыть уязвимости:

Слабый пароль пользователя;

- ▶ XSS (CVE-2019-17427);
- ▶ Blind SQL (CVE-2019-18890).

Определить и устраниТЬ последствия эксплуатации уязвимостей:

- ▶ Developer backdoor (последствие уязвимости 1);

Разработать и применить меры по устранению выявленных уязвимостей.

0.2 Цели и задачи

Освоить практических навыков выявления, анализа и устранения уязвимостей информационных систем в рамках сценария «Защита научно-технической информации предприятия».

Обнаружить, проанализировать и закрыть уязвимости:

Слабый пароль пользователя;

- ▶ XSS (CVE-2019-17427);
- ▶ Blind SQL (CVE-2019-18890).

Определить и устраниТЬ последствия эксплуатации уязвимостей:

- ▶ Developer backdoor (последствие уязвимости 1);
- ▶ Redmine User (последствие уязвимости 2).

Разработать и применить меры по устранению выявленных уязвимостей.

└ 1. Выполнение лабораторной работы

Раздел 1

1. Выполнение лабораторной работы

1.1 Обнаружение уязвимостей

Уязвимости и последствия будут детектироваться с помощью ViPNet IDS NS.

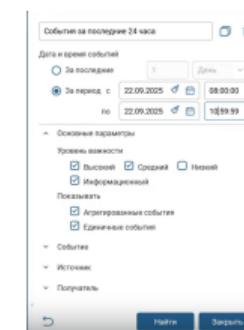


Рисунок 1: Установка фильтров

└ 1. Выполнение лабораторной работы

1.2 Обнаружение уязвимости «Слабый пароль пользователя»

Сканирование системы и множество одинаковых событий со стороны 10.10.4.11 на 10.10.2.12.

Событие класса «successful-admin»: пользователь успешно вошел в систему, подбрав пароль.

Действия между узлами 10.10.4.11, 10.10.2.12, 10.10.4.13: был скомпрометирован пароль от компьютера Developer Workstation.

События

События за последние 24 часа

Дата и время	Код события	Класс	Название правила	Ключ
00:11:10.015 15.09...	2025707	bad-unison	ET POLICY SMB2 NT Create An...	1
00:11:10.015 15.09...	2025707	bad-unison	ET POLICY SMB2 NT Create An...	1
00:11:10.009 15.09...	2044771	maso-activity	ET INFO PowerShell Command L...	1
00:11:09.801 15.09...	2038605	bad-unison	ET ATTACK_RESPONSE Nishan...	1
00:11:09.801 15.09...	2020084	successful-admin	ET ATTACK_RESPONSE Mimica...	1
00:11:02.103 15.09...	2025701	bad-unison	ET POLICY SMB2 NT Create An...	5
00:10:52.808 15.09...	2025699	bad-unison	ET POLICY SMB Executable File...	1
00:10:52.808 15.09...	2025699	bad-unison	ET POLICY SMB2 Executable File...	1
00:10:52.799 15.09...	2025701	bad-unison	ET POLICY SMB2 NT Create An...	1
00:10:52.692 15.09...	2025701	bad-unison	ET POLICY SMB2 NT Create An...	1
00:10:52.468 15.09...	2025701	bad-unison	ET POLICY SMB2 NT Create An...	1
00:10:52.103 15.09...	2025701	bad-unison	ET POLICY SMB2 NT Create An...	1
00:10:51.144 15.09...	2025699	bad-unison	ET POLICY SMB Executable File...	1

Событие 00:11:09.801 15.09.2025

Событие Источник Получатель Пакет

Общая информация

Дата и время: 00:11:09.801 15.09.2025
История атаки: etm2
Уровень важности: Высокий
Тип события: Сигнатурное событие
Протокол: TCP
Код события: 2020084

Правило анализа

Класс: successful-admin
Группа: attack_response
Название: ET ATTACK_RESPONSE Microsoft PowerShell Banner Outbound
Описание: Правило обнаруживает ответную (аторченую) часть атаки (например, попытку запустить произвольный код на ранее взломанный ресурс или отправку команды управления на такой ресурс)

1.3 Карточка инцидента

Уязвимость - слабый пароль пользователя. Рекомендации по устраниению - изменить пароль на более сложный

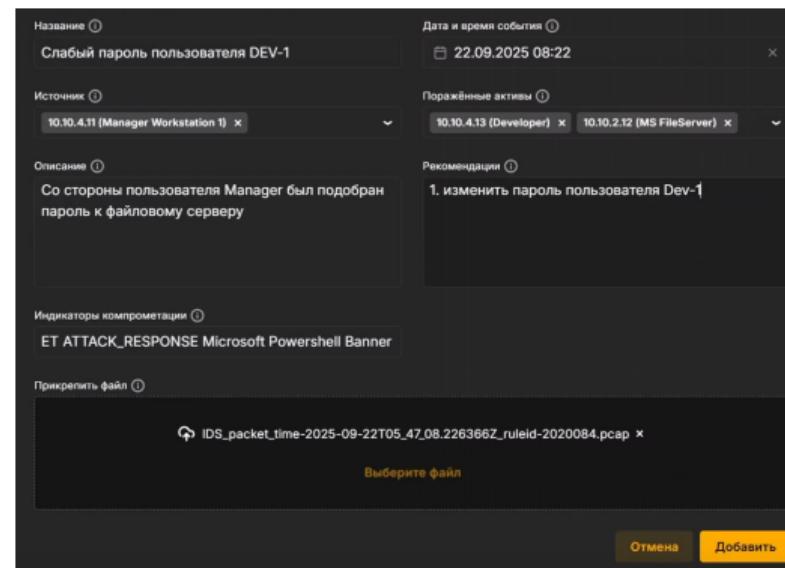


Рисунок 3: Карточка инцидента

└ 1. Выполнение лабораторной работы

1.4 Обнаружение последствия «Developer backdoor»

Создание исполняемого файла на файловом сервере 10.10.2.12 и обращения к нему

События

События за последние 24 часа

Событие 08:22:00.494 22.09.2025

Событие	Источник	Получатель	Пакет
Общая информация			
Дата и время	08:22:00.494 22.09.2025		
Интерфейс захвата	et2		
Уровень важности	Средний		
Тип события	Сигнатурное событие		
Протокол	TCP		
Код события	2025707		
Правило анализа			
Класс	bad-unknown		
Группа	policy		
Название	ET POLICY SMB2 NT Create AndX Request For a .bat File		
Описание:	Сигнатуры возможного нарушения политики информационной безопасности		
Текст:	click to see raw → BHOME_NET 445 (req: "ET POLICY SMB2 NT Create AndX Request For a .bat File") [nw-establishedto_servercontent: "\$MB"!depth: &content: "1"]		

Рисунок 4: Детектирование создания неизвестного файла

└ 1. Выполнение лабораторной работы

1.5 Обнаружение последствия «Developer backdoor»

Событие класса trojan-activity (LaZagne), указывающее на часть атаки, запускающую программу для извлечения информации из браузера.

The screenshot shows a security log viewer interface. On the left is a list of events from the last 24 hours, with the top event highlighted. On the right is a detailed view of the selected event.

События

Событие	Источник	Пользователь	Пакет
2027151	Itrojan-activity	attack_reponse	ET ATTACK_RESPONSE LaZagne Artifact Outbound in FTP

Правило анализа

Класс: trojan-activity
Группа: attack_reponse
Название: ET ATTACK_RESPONSE LaZagne Artifact Outbound in FTP

Описание:
Правило обнаруживает отдаленную («горячую») часть атаки (например, попытку запустить произвольный код на ранее взломанный ресурс или отправку команды управления на такой ресурс).¹²

Текст:

```
alert top $HOME_NET.ary + $EXTERNAL_NET.1024:(msg: 'ET ATTACK_RESPONSE
SE LaZagne Artifact Outbound in FTP'; flow: established; server: content: 'The La
Zagne Project'; fast; patternreference: url:github.com/AlessandroZ/LaZagne/class
type: trojan-activity;id: 2027151;rev: 2;metadata: affectedAsset;src_ip: affected;pro
duct: microsoft/windows; affected_vendor: microsoft; attack_target: Client; EndUser
t; confidence: Medium; created_at: 2019-04-04; deployment: Perimeter; malware: fa
mily: LaZagne; malware_family: Stealer; signature_severity: Major; tag: category:Expl
oration; updated_at: 2019-04-04)
```

Описание уязвимости: url:github.com/AlessandroZ/LaZagne

Рисунок 5: Обнаружение файла с backdoor

1.6 Карточка инцидента

Первичные рекомендации по устранению последствия - удаление исполняемого файла с backdoor и остановка его работы.

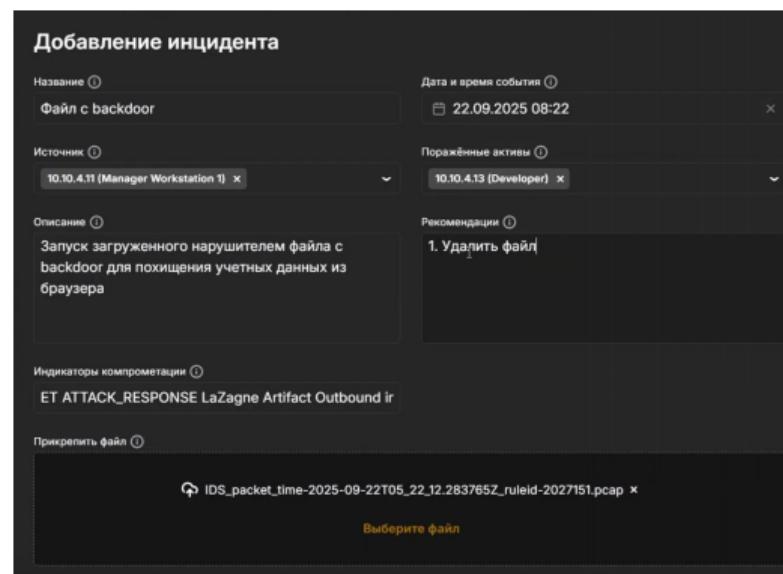


Рисунок 6: Карточка инцидента

└ 1. Выполнение лабораторной работы

1.7 Обнаружение уязвимости «XSS (CVE-2019-17427)»

События с источником - 10.10.4.11, получателем - 10.10.2.15 (сервер Redmine).

События AM EXPLOIN Possible Redmine XSS и событие AM EXPLOIT Generic Possible XSS in HTTP Body: они говорят о том, что эксплуатируется уязвимость Redmine, существующая в версиях до 4.0.4, позволяющая внедрять вредоносный JavaScript-код в веб-страницы, просматриваемые другими пользователями .

The screenshot shows a network event monitoring interface. On the left, a list of events is displayed under the heading 'События' (Events). The list includes several entries, with the last one highlighted in blue. The right side shows a detailed view of the selected event, titled 'Событие 08:47:32.437 22.09.2025' (Event 08:47:32.437 22.09.2025). This view is divided into sections: 'Общая информация' (General information), 'Правила анализа' (Analysis rules), and 'Описание' (Description). The 'General information' section contains details such as the date and time (08:47:32.437 22.09.2025), interface (eth2), severity (High), type (Signature-based event), protocol (TCP), and application (python-requests/2.31.0). The 'Analysis rules' section lists the rule class (web-application-attack), group (exploit), name (AM EXPLOIT Generic Possible XSS in HTTP Body 'onfocusin' in re...'), and description (AM EXPLOIT Generic Possible XSS in HTTP Body 'onfocusin' in re...'). The 'Description' section provides a detailed explanation of the exploit.

Рисунок 7: Обнаружение эксплуатации уязвимости

└ 1. Выполнение лабораторной работы

1.8 Обнаружение уязвимости «XSS (CVE-2019-17427)»

На сервере Redmine в файле production.log увидим сильно отличающиеся от остальных этапы, говорящие о внедрении JS кода.

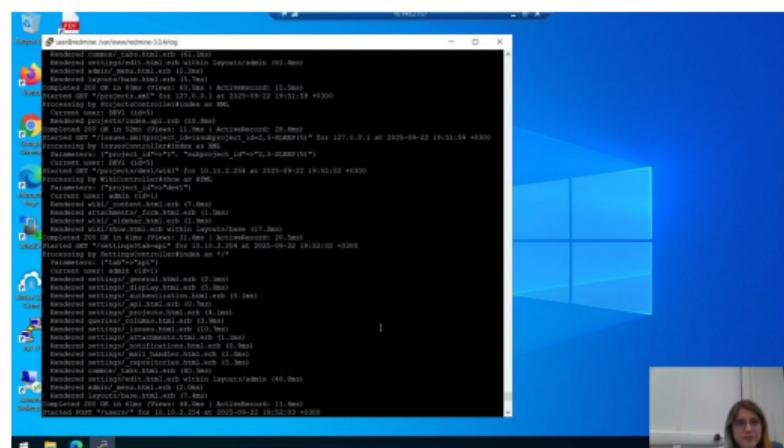


Рисунок 8: Обнаружение эксплуатации уязвимости через логи

└ 1. Выполнение лабораторной работы

1.9 Карточка инцидента

Составляем карточку уязвимости, общее описание и рекомендации можно найти на сайте АМТИР.

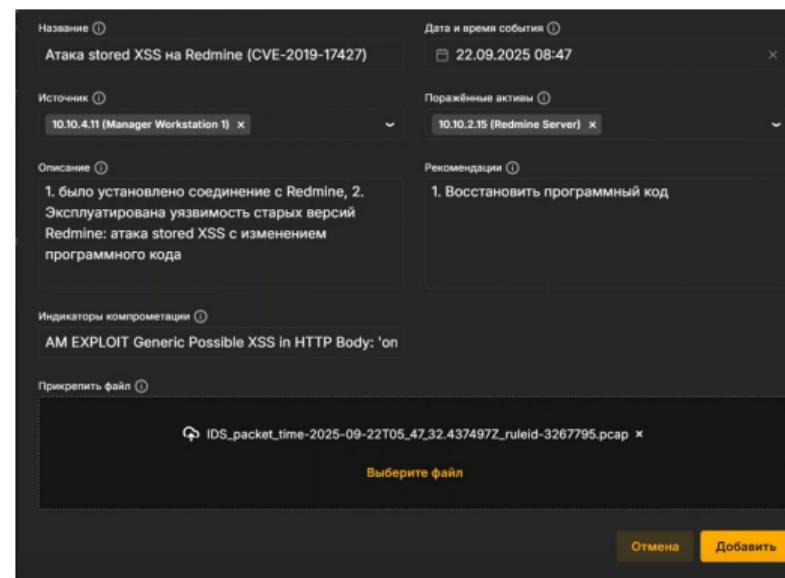


Рисунок 9: Карточка уязвимости

└ 1. Выполнение лабораторной работы

1.10 Обнаружение последствия «Redmine User»

В проекте DEV1 во вкладке wiki включен REST API

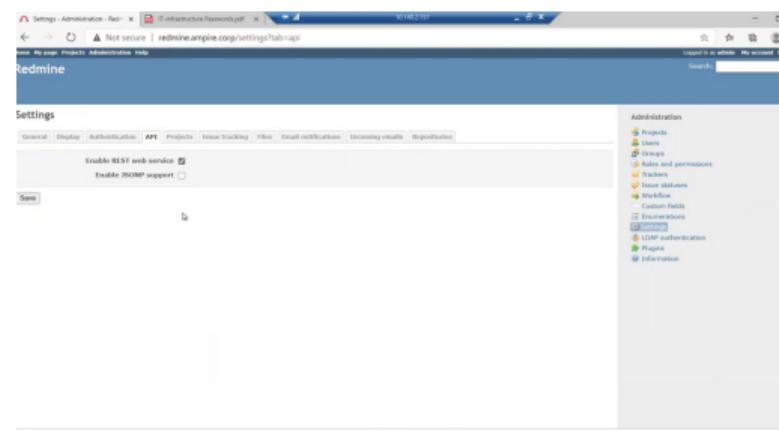


Рисунок 10: Обнаружение REST API

1.11 Обнаружение последствия «Redmine User»

В коде упоминается пользователь с именем `hacker`, его мы обнаружим и в списках пользователей.

Код мы видели в пакете события

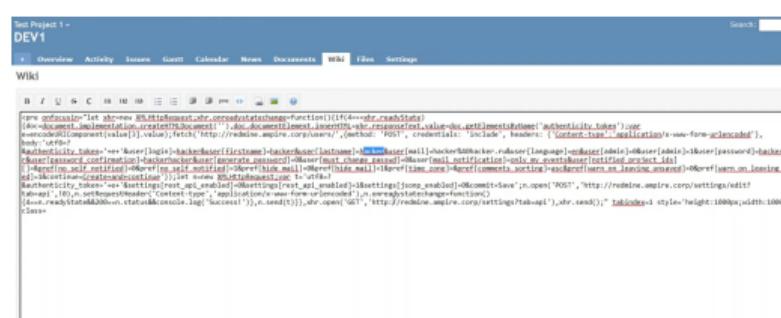
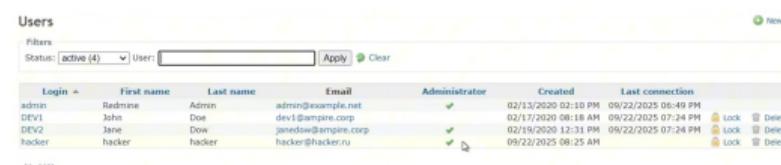


Рисунок 11: Упоминание пользователя в коле

1.12 Обнаружение последствия «Redmine User»



Users						
Filters						
Status:	active (4)	User:	Apply	Clear		
Login	First name	Last name	Email	Administrator	Created	Last connection
admin	Redmine	Admin	admin@example.net	<input checked="" type="checkbox"/>	02/13/2020 02:10 PM	09/22/2025 08:49 PM
DEV1	John	Doe	dev1@redmine.org	<input type="checkbox"/>	02/17/2020 08:18 AM	09/22/2025 07:24 PM
DEV2	Jane	Doe	janedoe@redmine.org	<input checked="" type="checkbox"/>	02/19/2020 12:31 PM	09/22/2025 07:24 PM
hacker	hacker	hacker	hacker@hacker.ru	<input checked="" type="checkbox"/>	09/22/2025 08:25 AM	09/22/2025 08:25 AM

Рисунок 12: Подозрительный пользователь с правами администратора

└ 1. Выполнение лабораторной работы

1.13 Карточка инцидента

Заполняем карточку инцидента, в рекомендациях удаление нового пользователя.

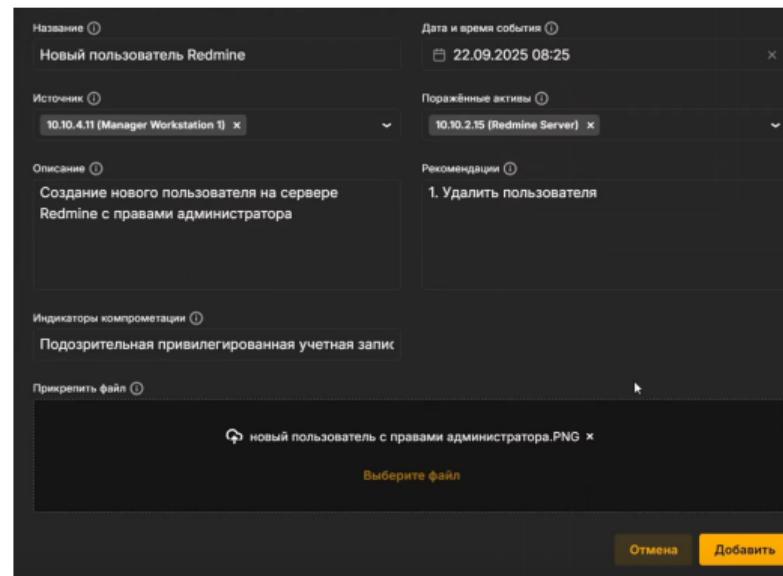


Рисунок 13: Карточка инцидента

└ 1. Выполнение лабораторной работы

1.14 Обнаружение уязвимости «Blind SQL (CVE-2019-18890)»

Большое количество SQL запросов SELECT SLEEP и SELECT FROM от сервера 10.10.4.11 на сервер 10.10.2.15

События						
События за последние 24 часа		Кол.	Название правила	Класс	IP-адрес источника	IP-адрес получателя
08:47:33.142	22.09.2025	1	ET WEB_SERVER SQL Injection Select Sleep Time Delay	web-application...	10.10.2.254	10.10.2.15
08:47:33.142	22.09.2025	1	AM SQL Generic:SQL in HTTP URI: 'SELECT SLEEP' query	web-application...	10.10.4.11	10.10.2.15
08:47:33.142	22.09.2025	1	AM SQL Generic:SQL in HTTP URI: 'SELECT FROM' query	client-side-exploit...	10.10.4.11	10.10.2.15
08:47:33.009	22.09.2025	1	ET WEB_SERVER SQL Injection Select Sleep Time Delay	web-application...	10.10.4.11	10.10.2.15
08:47:33.009	22.09.2025	1	AM SQL Generic:SQL in HTTP URI: 'SELECT SLEEP' query	web-application...	10.10.2.254	10.10.2.15
08:47:33.009	22.09.2025	1	AM SQL Generic:SQL in HTTP URI: 'SELECT FROM' query	client-side-exploit...	10.10.2.254	10.10.2.15
08:47:33.009	22.09.2025	1	ET WEB_SERVER SQL Injection Select Sleep Time Delay	web-application...	10.10.2.254	10.10.2.15
08:47:33.009	22.09.2025	1	AM SQL Generic:SQL in HTTP URI: 'SELECT SLEEP' query	web-application...	10.10.4.11	10.10.2.15
08:47:33.009	22.09.2025	1	AM SQL Generic:SQL in HTTP URI: 'SELECT FROM' query	client-side-exploit...	10.10.4.11	10.10.2.15
08:47:33.009	22.09.2025	1	ET WEB_SERVER SQL Injection Select Sleep Time Delay	web-application...	10.10.4.11	10.10.2.15

Рисунок 14: SQL-запросы

└ 1. Выполнение лабораторной работы

1.15 Карточка инцидента

При заполнении карточки уязвимости ссылаемся на гитхаб.

Добавление инцидента

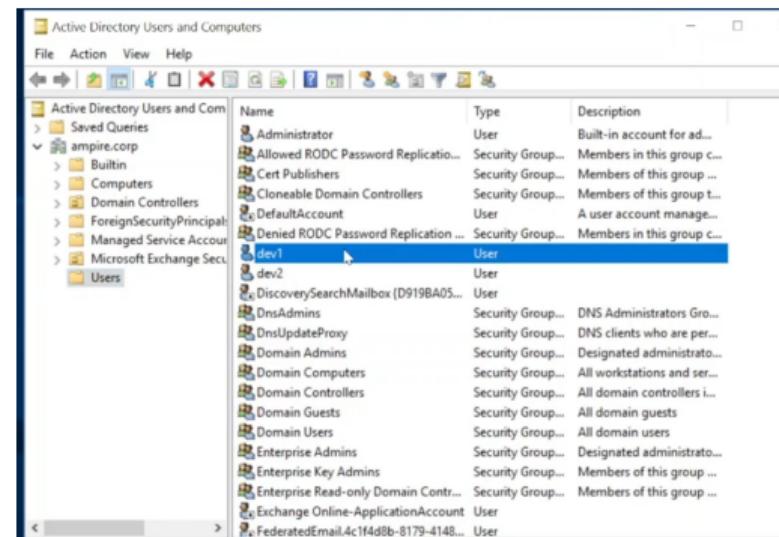
Название	Дата и время события
BLIND SQL-инъекция (CVE-2019-18890)	22.09.2025 08:47
Источник	Поражённые активы
10.10.4.11 (Manager Workstation 1) ×	10.10.2.15 (Redmine Server) ×
Описание	Рекомендации
3.2.9 и 3.3.x до 3.3.10 позволяет пользователям Redmine получать доступ к защищенной информации с помощью запроса к созданному объекту. Множественные запросы к созданному объекту.	Обновить Redmine до новой версии или изменить код Redmine
Индикаторы компрометации	
AM SQL Generic SQLi in HTTP URI: 'SELECT FROM' c	
Прикрепить файл	
IDS_packet_time-2025-09-22T05_47_44.253953Z_ruleid-3001075.pcap ×	
Выберите файл	

Рисунок 15: Карточка инцидента

└ 1. Выполнение лабораторной работы

1.16 Устранение уязвимостей и их последствий: Уязвимость Слабый пароль пользователя DEV-1

Для закрытия уязвимости меняем пароль на более сложный, не содержащийся в словаре. На сервер MS Active Directory подключаемся через удаленный рабочий стол. Открываем «Active Directory Users and Computers», переходим в users, находим dev1.



1.17 Устранение уязвимостей и их последствий: Уязвимость Слабый пароль пользователя DEV-1

Меняем пароль пользователя

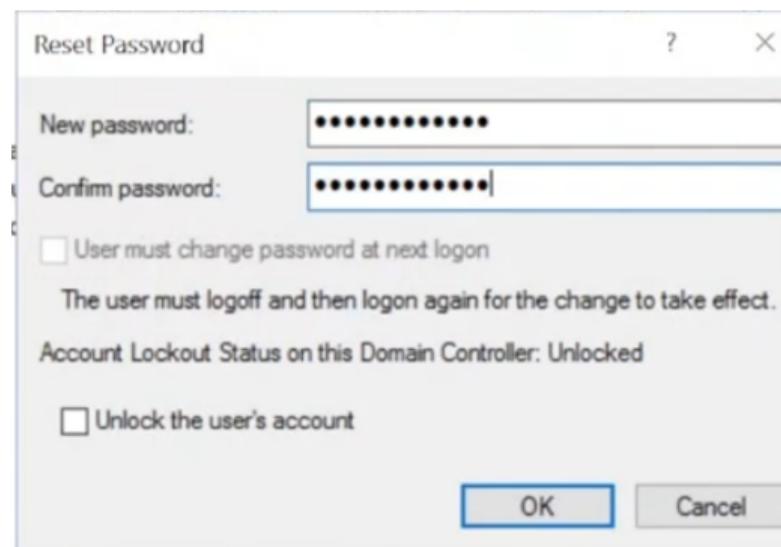


Рисунок 17: Смена пароля

└ 1. Выполнение лабораторной работы

1.18 Последствие «Developer backdoor»

Через удаленный рабочий стол переходим на сервер Developer (10.10.4.13). Новая задача, записанная нарушителем, находится на узле Developer 1 в планировщике задач.

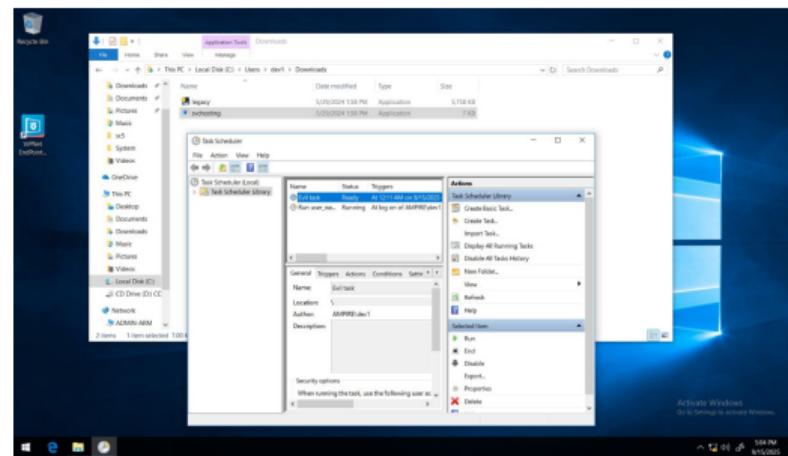


Рисунок 18: Запуск исполняемого файла в планировщике

└ 1. Выполнение лабораторной работы

1.19 Последствие «Developer backdoor»

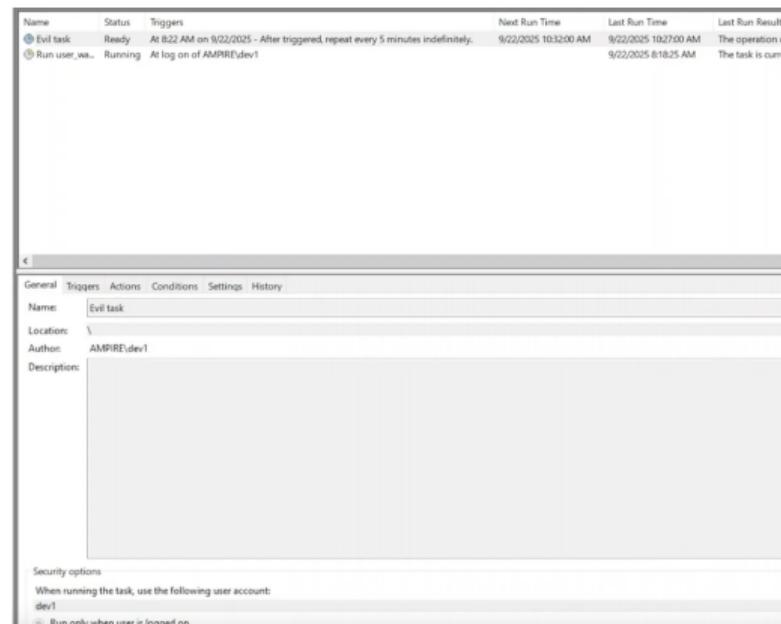
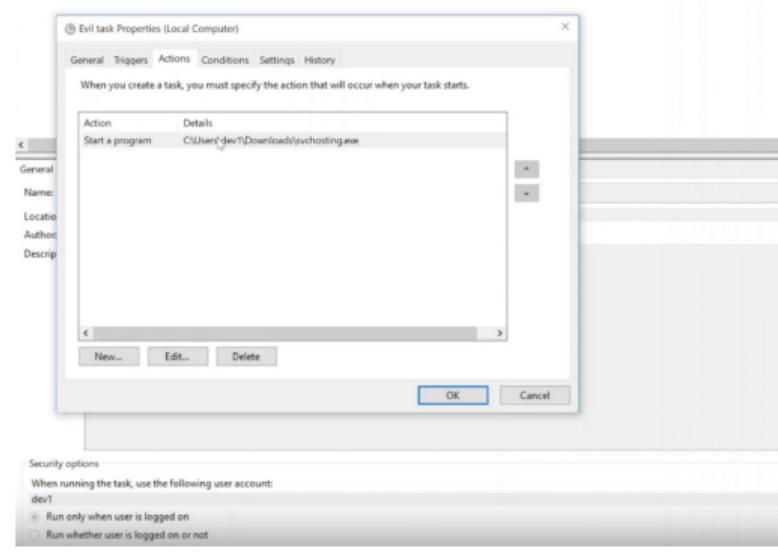


Рисунок 19: Запуск исполняемого файла в планировщике

1.20 Последствие «Developer backdoor»

Удаляем задачу в планировщике, и теперь надо удалить файл. Во вкладке action мы обнаружили путь к файлу C:\Users\dev1\Downloads\svchosting.exe, благодаря этому нашли его и удалили.



└ 1. Выполнение лабораторной работы

1.21 Уязвимость атака XSS

В Redmine до версии 4.0.4 постоянный XSS существует из-за ошибок форматирования при работе с textile текстом. В данном сценарии используется для включения REST API для эксплуатации следующей уязвимости.

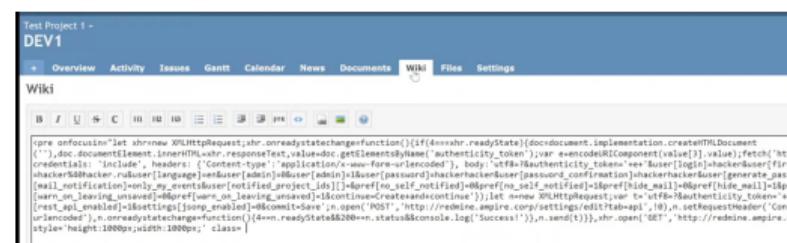


Рисунок 21: Пример добавления кода, выводящего на экран надпись XSS в wiki-страницу

1.22 Уязвимость атака XSS

Из описания уязвимости понятно, что необходимо найти библиотеку для преобразования textile разметки в html. В Redmine за данное преобразование отвечает файл redcloth3.rb. Для устранения изменим в нем следующие строки

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

Рисунок 22: Содержимое файла redcloth3.rb

1.23 Уязвимость атака XSS

Строки после изменения:

```
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
end
```

Рисунок 23: Исправления в файле redcloth3.rb

└ 1. Выполнение лабораторной работы

1.24 Уязвимость атака XSS

Перезапускаем службу веб-сервера `sudo systemctl restart nginx.service`. Уязвимость успешно устранена, так как изменилось отображение страницы на Redmine Wiki.



Рисунок 24: Успешное устранение уязвимости

1.25 Последствие «Redmine User»

Нарушитель создал пользователя на портале Redmine. Для обнаружения добавления нового привилегированного пользователя заходим в консоль администратора Redmine, переходим в раздел «Administration» – «Users» и смотрим список существующих пользователей. Удаляем его.

Login	First name	Last name	Email	Administrator	Created	Last connection
admin	Redmine	Admin	admin@example.net	✓	02/13/2020 02:10 PM	09/22/2025 08:22 PM
DEV1	John	Doe	dev1@example.corp	✓	02/17/2020 08:18 AM	09/22/2025 08:32 PM
DEV2	Jane	Doe	janedew@example.corp	✓	02/19/2020 12:31 PM	09/22/2025 08:32 PM
hacker	hacker	hacker	hacker@hacker.ru	✓	09/22/2025 08:25 AM	09/22/2025 08:25 AM

Рисунок 25: Список пользователей Redmine

1.26 Уязвимость Blind SQL-инъекция

Эксплуатируемая уязвимость – CVE-2019-18890.

В Redmine до версии 3.2.9 и 3.3.x до версии 3.3.10 уязвимость позволяет пользователям Redmine получать доступ к защищенной информации с помощью сгенерированного объектного запроса. Уязвимость реализуется посимвольным перебором с замером времени ответа. Время прихода пакета является индикатором: при запоздании пакета – символ подобран верно, иначе – перебор продолжается

```

<?xml version="1.0" encoding="UTF-8"?>
<issues type="array" limit="25" offset="0" total_count="4">
  <issue>
    <id>1</id>
    <project id="1" name="DEV1"/>
    <tracker id="1" name="Bug"/>
    <status id="1" name="New"/>
    <priority id="2" name="Normal"/>
    <author id="1" name="Redmine Admin"/>
    <subject>Task1</subject>
    <description>qq</description>
    <start_date>2020-02-19</start_date>
    <due_date/>
    <done_ratio>0</done_ratio>
    <estimated_hours>0</estimated_hours>
    <created_on>2020-02-19T10:10:39Z</created_on>
    <updated_on>2020-02-19T10:10:39Z</updated_on>
    <closed_on/>
  </issue>
  <issue>
    <id>14</id>
    <project id="3" name="DEV2"/>
    <tracker id="1" name="Bug"/>
    <status id="1" name="New"/>
    <priority id="2" name="Normal"/>
  </issue>
</issues>

```

Name	Protocol	Method	Result	Content type	Received	Time	Initiator	dns
issues.xml?project_id=1&subproject_id=2-3-SLEEP(2)	HTTP	GET	304	application/xml	(from cache)	8.55 s	document	

1.27 Уязвимость Blind SQL-инъекция

Вносим изменения в код, добавляя фильтрацию значений, и после перезапуска веб-сервера через команду sudo systemctl restart nginx.service уязвимость устраняется.

```
# include the selected subprojects
ids = [project.id] + values_for("subproject_id").each(&to_i)
project_clauses << "#{Project.table_name}.id IN (?)" % ids.join(',')
when true
```

Рисунок 27: Содержимое файла query.rb до исправления уязвимости

1.28 Уязвимость Blind SQL-инъекция

Исправленный файл:

```
# include the selected subprojects
ids = [project.id] + values_for("subproject_id").map{|&to_i|
  project_clauses << "#{Project.table_name}.id IN (%s)" % ids.join(',')
when true
```

Рисунок 28: Содержимое файла query.rb с исправлением уязвимости

1.29 Результат

Закрыли все обнаруженные инциденты,
Устранили уязвимости и последствия

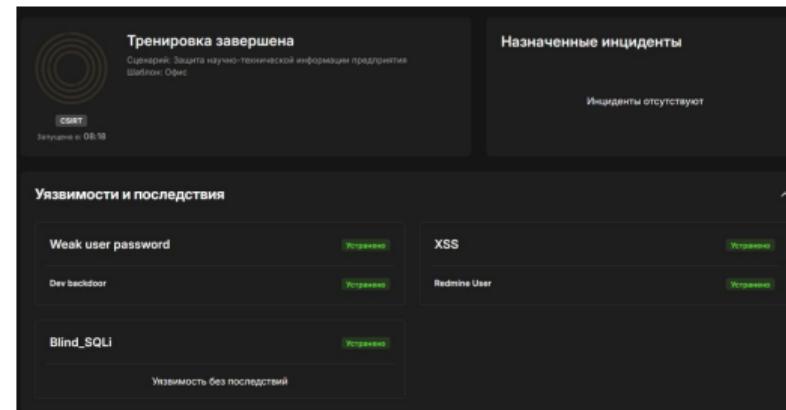


Рисунок 29: Устраниенные уязвимости и последствия

1.30 Выводы

В ходе выполнения лабораторной работы были успешно достигнуты поставленные цели: освоены практические навыки выявления, анализа и устранения типовых уязвимостей информационной системы. В рамках сценария «Защита научно-технической информации предприятия» были обнаружены и закрыты критические уязвимости и их последствия эксплуатации.