

Лабораторная работа № 2-Д

Защита интеграционной платформы

Доберштейн А., Оразгелдиев Я., Лобанова П., Лушин А., Барабанова К.

Содержание

1 Цель работы	5
2 Выполнение лабораторной работы	6
2.1 Подготовка к выполнению лабораторной работы	6
2.2 Уязвимость Bitrix vote RCE	6
2.3 Уязвимость GitLab RCE	18
2.4 Уязвимость WSO2 API-Manager RCE	24
3 Выводы	29

Список иллюстраций

2.1	Вектор атаки	6
2.2	Вход в ViPNet	7
2.3	Журнал событий	7
2.4	Обзор уязвимости	8
2.5	Подключение к удаленному рабочему столу	8
2.6	Вход	9
2.7	KeePass	9
2.8	Лог-файл	10
2.9	Поиск файла	10
2.10	Информация о полезной нагрузке	10
2.11	Попытка входа в Bitrix	11
2.12	Устранение LPE	12
2.13	Редактирование uf.php	12
2.14	Создание .htaccess	12
2.15	Закрытие meterpreter сессий	13
2.16	Директория веб-сервера	13
2.17	password_recovery.php	14
2.18	Deface веб-сервера	14
2.19	Авторизация	15
2.20	Администрирование	16
2.21	Удаление файла	16
2.22	Удаление файлов	16
2.23	Резервная копия	16
2.24	Устранение LPE	17
2.25	Редактирование uf.php	17
2.26	Создание .htaccess	18
2.27	Удаление файла	18
2.28	Успех	18
2.29	Обзор уязвимости	19
2.30	KeePass	19
2.31	GitLab	20
2.32	Admin Area	20
2.33	Settings -> General	21
2.34	Sign-up restrictions	21
2.35	Настройка	22
2.36	Сохранение конфигурации	22
2.37	Users	22

2.38 Удаление пользователя	23
2.39 Подтверждение удаления	23
2.40 Закрытие meterpreter сессий	23
2.41 Успех	24
2.42 Журнал событий	24
2.43 Обзор уязвимости	25
2.44 KeePass	25
2.45 Файл конфигурации	25
2.46 Редактирование	26
2.47 Удаление файла	26
2.48 Удаление файла	26
2.49 Закрытие meterpreter сессий	26
2.50 Вход в веб-интерфейс	27
2.51 Пользователи	27
2.52 Удаление пользователя	28
2.53 Успех	28

1 Цель работы

Основной целью работы является получение навыков обнаружения и устранение уязвимостей Bitrix vote RCE, GitLab RCE, WSO2 API-Manager RCE и их последствий.

2 Выполнение лабораторной работы

2.1 Подготовка к выполнению лабораторной работы

Для начала изучили вектор атаки, адреса злоумышленника и атакуемых серверов.(рис. 2.1).



Рис. 2.1: Вектор атаки

2.2 Уязвимость Bitrix vote RCE

Залогинились в ViPNet для обнаружения уязвимости в журнале событий.(рис. 2.2).



Рис. 2.2: Вход в ViPNet

В “Событиях” обнаружили события: внедрение полезной нагрузки в HTTP-запрос, PHP-скрипт с кодом для удаленного выполнения команд, информирование о скачивании исполняемого файла с машины нарушителя. (рис. 2.3).

...	Дата и время ю...	Код события	Ко...	Название правила	Класс	Протокол	IP-адрес источ...	Порт ист...	IP-адрес полу...	Порт по...	Направл...
●	16:56:12.282 10.1...	3171405	1	AM EXPLOIT Generic Comma...	web-application-attack	TCP	195.239.174.11	46863	10.10.1.33	80	⊗→龠
●	16:56:12.282 10.1...	2025809	1	ET EXPLOIT php script base...	attempted-user	TCP	195.239.174.11	46863	10.10.1.33	80	⊗→龠
●	16:56:12.282 10.1...	3171403	1	AM EXPLOIT Generic Comma...	web-application-attack	TCP	195.239.174.11	46863	10.10.1.33	80	⊗→龠
●	16:56:12.282 10.1...	3105389	1	AM EXPLOIT Generic Comma...	web-application-attack	TCP	195.239.174.11	46863	10.10.1.33	80	⊗→龠
●	16:56:12.282 10.1...	3203254	1	AM EXPLOIT Generic Comma...	web-application-attack	TCP	195.239.174.11	46863	10.10.1.33	80	⊗→龠
○	16:56:46.137 10.1...	2034567	1	ET INFO curl User-Agent to Do...	bad-unknown	TCP	10.10.1.33	59896	195.239.174.11	8010	龠→⊗
●	16:56:46.139 10.1...	3129327	1	ET POLICY Executable and lin...	policy-violation	TCP	195.239.174.11	8010	10.10.1.33	59896	⊗→龠
●	16:56:52.432 10.1...	3105345	1	AM CURRENT_EVENTS HTTP ...	trojan-activity	TCP	10.10.1.33	37916	195.239.174.11	8010	龠→⊗
○	16:56:52.432 10.1...	2034567	1	ET INFO curl User-Agent to Do...	bad-unknown	TCP	10.10.1.33	37916	195.239.174.11	8010	龠→⊗
●	16:57:02.638 10.1...	3121915	1	ET POLICY Executable and lin...	policy-violation	TCP	195.239.174.11	5558	10.10.1.33	47080	⊗→龠

Рис. 2.3: Журнал событий

Изучили информацию по CVE-коду об обнаруженной уязвимости, изучили рекомендации понейтрализации. (рис. 2.4).

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 - добавление кода в исходный файл модуля, ограничивающего POST запросы;

Рекомендации по нейтрализации:

- 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. 2.4: Обзор уязвимости

Для устранения уязвимости подключились к удаленному рабочему столу. (рис. 2.5).

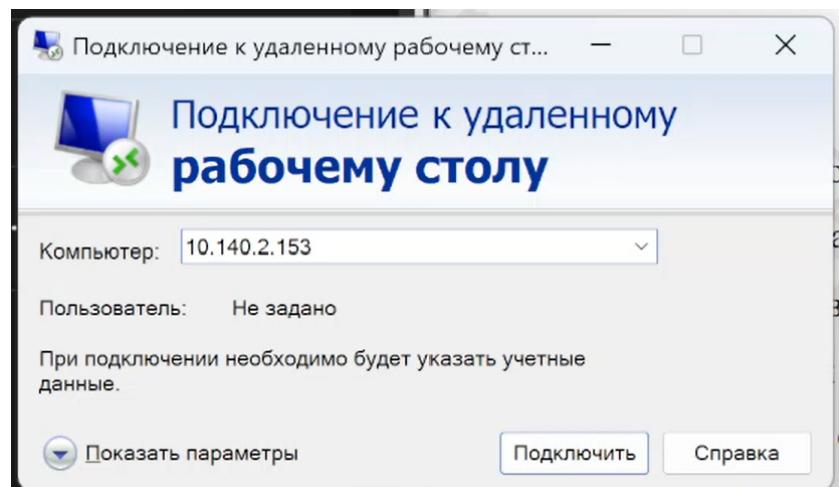


Рис. 2.5: Подключение к удаленному рабочему столу

Вошли под указанной учетной записью. (рис. 2.6).

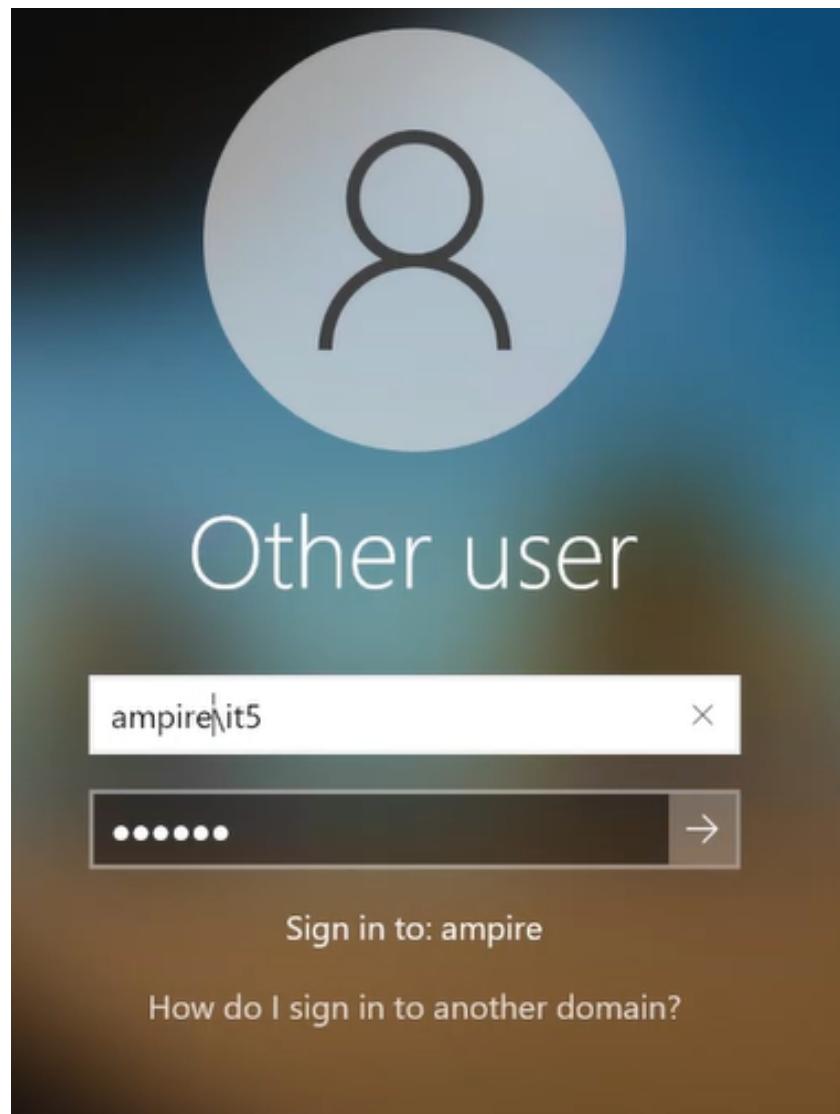


Рис. 2.6: Вход

В соответствии с вектором атаки в KeePass нашли CMS Bitrix.(рис. 2.7).

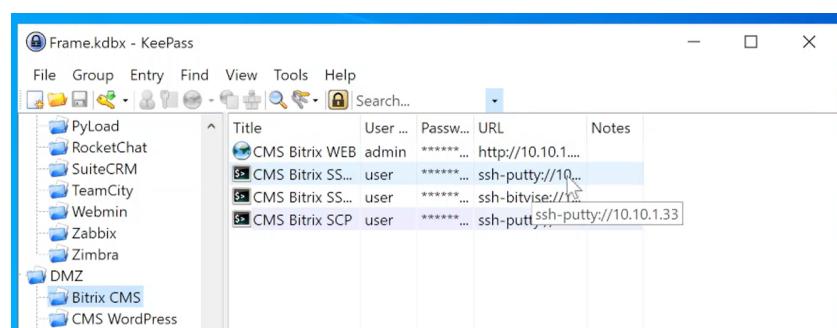


Рис. 2.7: KeePass

В лог-файле apache2 по пути /var/log/apache2/access.log обнаружили следующую информацию:
два запроса к файлу /bitrix/tools/vote/uf.php с внедрением полезной нагрузки для последующей загрузки веб-backdoor и запрос к файлу веб-backdoor для создания WebShell сессии с машиной нарушителя.(рис. 2.8).

```
user@bitrix:/var/log/apache2$ cat access.log
195.239.174.11 - - [02/Oct/2025:16:31:08 +0300] "GET /caidao.php HTTP/1.1" 404 3
502 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0"
195.239.174.11 - - [02/Oct/2025:16:31:18 +0300] "GET /bitrix/tools/composite.dat
a.php HTTP/1.1" 200 720 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/2010
0101 Firefox/78.0"
195.239.174.11 - - [02/Oct/2025:16:31:18 +0300] "POST /bitrix/tools/vote/uf.php?
attachId=d5#MODULE_ID=d5#block=attachId#BENITYTYPE%5D=CfileUploader&action=vo
te&sessid=def73a4cledfd0c406d907651bd3cb#attachId%5BENTITY_ID%5D%5Bcopies%5D%5
Bpayload2#phar%5D=1 HTTP/1.1" 200 1147 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:7
8.0) Gecko/20100101 Firefox/78.0"
195.239.174.11 - - [02/Oct/2025:16:31:18 +0300] "POST /bitrix/tools/vote/uf.php?
attachId=d5#MODULE_ID=d5#block=attachId#BENITYTYPE%5D=Phar#attachId%5BENTITY
ID%5D%5B%2Fvar%2Fwww%2Fhtml%2Fupload%2Ftmp%2FBFXTEMP-2025-10-03%2F04%2F2bxuu%2Fmain%2
F427c3fc0aa9292ba112d6fe315b%2Fcd4a238a0b923820dc59a6f75849b%2Fpayload2.
phar&action=vote&sessid=def73a4cledfd0c406d907651bd3cb HTTP/1.1" 200 1155 "-"
"Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0"
195.239.174.11 - - [02/Oct/2025:16:31:28 +0300] "GET /caidao.php HTTP/1.1" 200 2
03 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0"
195.239.174.11 - - [02/Oct/2025:16:32:59 +0300] "GET /password_recovery.php HTTP
/1.1" 200 2415 "-" "python-requests/2.28.1"
10.10.1.253 - - [02/Oct/2025:16:42:05 +0300] "GET /bitrix HTTP/1.1" 301 571 "-"
"Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko
) Chrome/87.0.4280.67 Safari/537.36 Edg/87.0.664.47"
10.10.1.253 - - [02/Oct/2025:16:42:05 +0300] "GET /bitrix/ HTTP/1.1" 200 348 "-"
"Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Geck
o) Chrome/87.0.4280.67 Safari/537.36 Edg/87.0.664.47"
10.10.1.253 - - [02/Oct/2025:16:42:05 +0300] "GET /favicon.ico HTTP/1.1" 404 279
```

Рис. 2.8: Лог-файл

Произвели поиск по названию полезной нагрузки с помощью команды `find /var/www/html/-iname «payload2.phar»`, нашли данный файл.(рис. 2.9).

```
user@bitrix:/var/log/apache2$ find /var/www/html/ -name "payload2.phar"
/var/www/html/upload/tmp/BXTEMP-2015-10-03/04/bxu/main/427c3fcf040a09292ba1d2d6fe315bf/c4ca4238a0b
932820dc509af757849bf/payload2.phar
```

Рис. 2.9: Поиск файла

Просмотрели содержимое с помощью текстового редактора, отобразилась информация о сканировании веб-backdoor по пути /var/www/html/caidao.php.(рис. 2.10).

Рис. 2.10: Информация о полезной нагрузке

Открыли сайт Bitrix. Не удалось получить доступ к интерфейсу администрирования из-за действующей полузной нагрузки. (рис. 2.11).

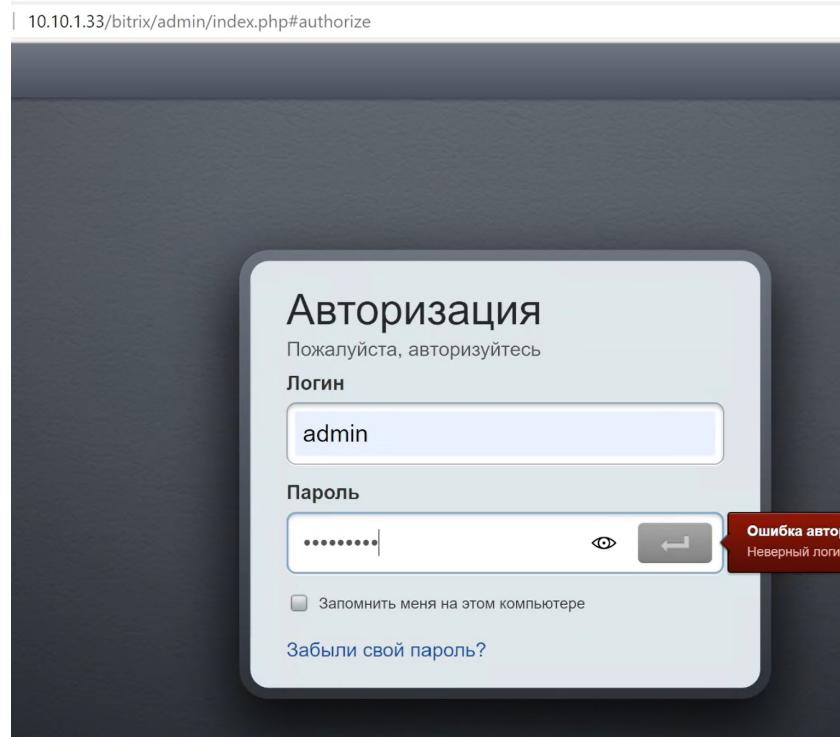


Рис. 2.11: Попытка входа в Bitrix

Для устранения вектора для локального повышения привилегий (LPE) удалили SUID-бит у файла /var/www/html/apache_restart с помощью команды chmod –s /var/www/html/apache_restart. (рис. 2.12).

```

user@bitrix:/var$ cd /var/www/html/
user@bitrix:/var/www/html$ ls -la
итого 5640
drwxrwxr-x 12 www-data www-data 4096 окт 2 16:32 .
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 22 2023 bitrix
-rw-r--r-- 1 www-data www-data 265 июл 7 2023 .bottom.menu.php
-rw-r--r-- 1 www-data www-data 34 окт 2 16:31 caidao.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 1168 окт 2 16:32 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
-rw-r--r-- 1 root root 201 окт 2 16:32 password_recovery.php
drwxr-xr-x 2 www-data www-data 4096 июл 7 2023 products
-rw-r--r-- 1 root root 5661008 окт 2 16:32 RickRolled.mp4
-rw-r--r-- 1 www-data www-data 76 окт 2 16:32 script.sh
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 окт 2 16:32 upload
-rw-r--r-- 1 www-data www-data 509 июл 7 2023 urlrewrite.php
user@bitrix:/var/www/html$ su -
su: неверный ключ - «i»
Try 'su --help' for more information.
user@bitrix:/var/www/html$ sudo chmod -s /var/www/html/apache_restart

```

Рис. 2.12: Устранение LPE

Для закрытия уязвимости добавив в изменения в файл /var/www/html/bitrix/tools/vote/uf.php, перед require_once и между знаков вопроса вставили код:(рис. 2.13).

```

user@bitrix:/var
GNU nano 6.2          /var/www/html/bitrix/tools/vote/uf.php *
<?
if ($_SERVER['REQUEST_METHOD'] === 'POST')
{
header('Status: 404 Not Found');
die();
}
require($_SERVER["DOCUMENT_ROOT"]. "/bitrix/modules/vote/tools/uf.php");?>

```

Рис. 2.13: Редактирование uf.php

Создали файл .htaccess в директории /var/www/html/bitrix/tools/vote, задающий правила работы веб-сервера для конкретного каталога и подкаталогов. Для закрытия уязвимости в данном файле можно прописали команду deny from all(рис. 2.14).

```

user@bitrix:/var
[1/1]          /var/www/html/bitrix/tools/vote/.htaccess *
deny from all

```

Рис. 2.14: Создание .htaccess

С помощью утилиты ss и команды kill закрыли meterpreter сессии. (рис. 2.15).

```

user@bitrix:/var/www/html$ sudo ss -tp
State      Recv-Q  Send-Q      Local Address:Port          Peer Address:Port
Process
ESTAB     0        0           10.10.1.33:57024          195.239.174.11:5557
users:(({"systemctl",pid=1752,fd=12}, {"sh",pid=1751,fd=12}, {"apache_restart",pid=1750,fd=12}, {"sh",pid=1746,fd=12}), {"sh",pid=1745,fd=12}, {"apache2",pid=804,fd=12})
ESTAB     0        0           10.10.1.33:ssh            195.239.174.11:42713
users:({"sshd",pid=1808,fd=4})
FIN-WAIT-2 0        0           10.10.1.33:44314          10.10.2.27:9763
users:({"sshd",pid=1808,fd=9})
ESTAB     0        0           10.10.1.33:41370          195.239.174.11:5558
users:({"systemctl",pid=1752,fd=3})
ESTAB     0        0           10.10.1.33:ssh            10.10.1.253:19666
users:( {"sshd",pid=2619,fd=4}, {"sshd",pid=2554,fd=4})
CLOSE-WAIT 1        0           [:ffff:10.10.1.33]:http       [:ffff:195.239.174.11]:41085
users:( {"apache2",pid=804,fd=11})
user@bitrix:/var/www/html$ kill -9 1752
-bash: kill: (1752) - Операция не позволена
user@bitrix:/var/www/html$ sudo kill -9 1752
user@bitrix:/var/www/html$ sudo kill -9 1808
user@bitrix:/var/www/html$ sudo kill -9 1745
user@bitrix:/var/www/html$ sudo ss -tp
State      Recv-Q  Send-Q      Local Address:Port          Peer Address:Port
Process
ESTAB     0        0           10.10.1.33:57024          195.239.174.11:5557
users:(({"systemctl",pid=3644,fd=12}, {"sh",pid=3643,fd=12}, {"apache_restart",pid=1750,fd=12}, {"sh",pid=1746,fd=12}), {"apache2",pid=804,fd=12})
FIN-WAIT-2 0        0           10.10.1.33:44314          10.10.2.27:9763
ESTAB     0        0           10.10.1.33:ssh            10.10.1.253:19666
users:( {"sshd",pid=2619,fd=4}, {"sshd",pid=2554,fd=4})
CLOSE-WAIT 1        0           [:ffff:10.10.1.33]:http       [:ffff:195.239.174.11]:41085
users:( {"apache2",pid=804,fd=11})
user@bitrix:/var/www/html$ sudo kill -9 1745

```

Рис. 2.15: Закрытие meterpreter сессий

В директории веб-сервера обнаружили скрипт password_recovery.php. (рис. 2.16).

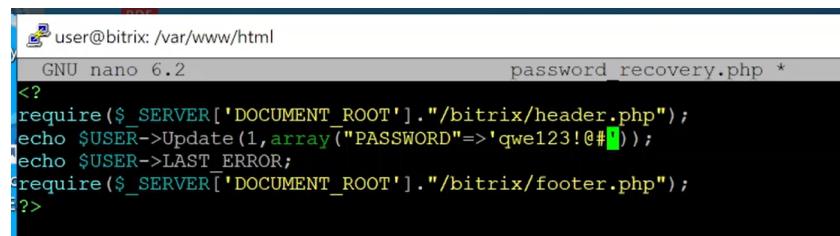
```

user@bitrix:/var/www/html$ ls -la
итого 5640
drwxrwxr-x 12 www-data www-data   4096 окт  2 16:32 .
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
drwxr-xr-x  1 root    root    16048 июл 31 2023 apache_restart
drwxrwxr-x 25 www-data www-data  4096 сен 22 2023 bitrix
-rw-r--r--  1 www-data www-data  265 июл  7 2023 .bottom.menu.php
-rw-r--r--  1 www-data www-data   34 окт  2 16:31 caidao.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 1168 окт  2 16:32 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--r--  1 root    root    201 окт  2 16:32 password_recovery.php
drwxr-xr-x  2 www-data www-data  4096 июл  7 2023 products
-rw-r--r--  1 root    root    5661008 окт  2 16:32 RickRolled.mp4
-rw-r--r--  1 www-data www-data   76 окт  2 16:32 script.sh
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 окт  2 16:32 upload
-rw-r--r--  1 www-data www-data  509 июл  7 2023 urlrewrite.php

```

Рис. 2.16: Директория веб-сервера

Прописали новый пароль. (рис. 2.17).



```
user@bitrix: /var/www/html
GNU nano 6.2                                     password_recovery.php *
<?
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");
?>
```

Рис. 2.17: password_recovery.php

Подключились к веб-серверу, в ссылке указали название данного файла. (рис. 2.18).

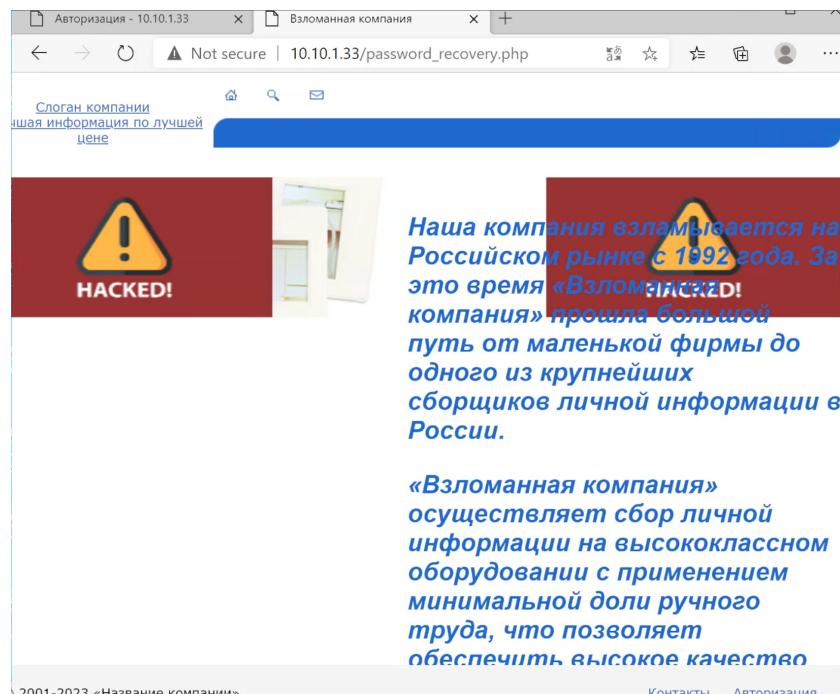


Рис. 2.18: Deface веб-сервера

Авторизовались с правами администратора (рис. 2.19).



Логин
 

Пароль
 

Запомнить меня

[Забыли свой пароль?](#)

Следуйте [на форму для запроса пароля.](#)

После получения контрольной строки следуйте на [форму для смены пароля.](#)

Рис. 2.19: Авторизация

Открылась панель администрирования. (рис. 2.20).

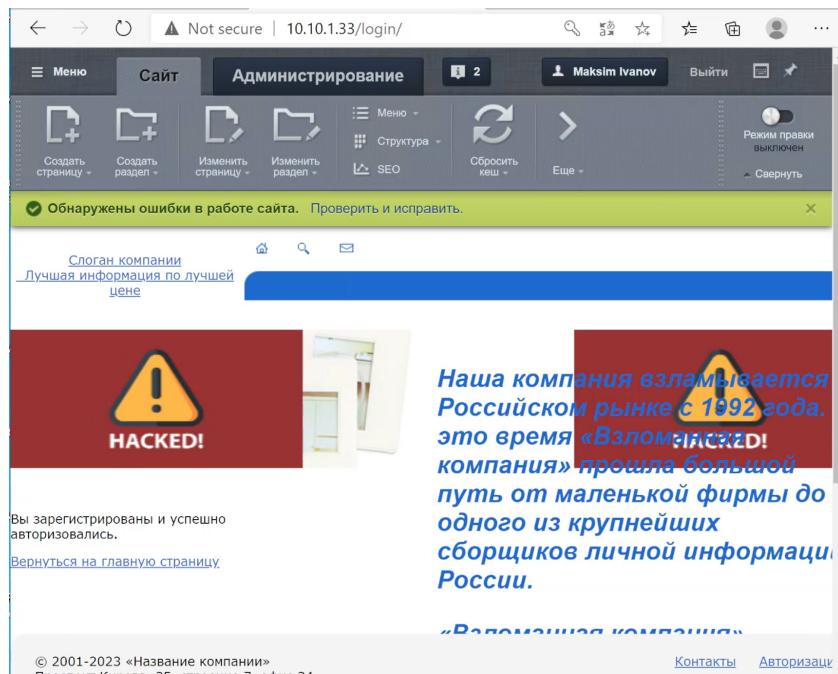


Рис. 2.20: Администрирование

Удалили файл password_recovery.php. (рис. 2.21).

```
user@bitrix:/var/www/html$ sudo nano password_recovery.php
user@bitrix:/var/www/html$ sudo rm /var/www/html/password_recovery.php
```

Рис. 2.21: Удаление файла

Доступ к панели администрирования восстановлен. Удалили все файлы в директории взломанного веб-сервера. (рис. 2.22).

```
user@bitrix:/var/bitrix_backups$ ls -la
итого 412112
drwxr-xr-x  2 root root    4096 дек 11  2023 .
drwxr-xr-x 16 root root    4096 окт  2 17:01 ..
-rw-r--r--  1 root root 420715270 сен 15  2023 Bitrix_full_backup.tar.gz
-rw-r--r--  1 root root 1270146 дек 11  2023 Bitrix_sitemanager_DB.tar.gz
user@bitrix:/var/bitrix_backups$ rm -r /var/www/html/*
```

Рис. 2.22: Удаление файлов

Файл резервной копии разархивировали в директорию /var/www/html с помощью команды tar xvzf /var/bitrix_backups/Bitrix_full_backup.tar.gz -C /var/www/html. (рис. 2.23).

```
user@bitrix:/var/bitrix_backups$ cd ..
user@bitrix:/var$ cd ..
user@bitrix:/$ tar xvzf /var/bitrix_backups/Bitrix_full_backup.tar.gz -C /var/www/html
```

Рис. 2.23: Резервная копия

Далее повторили действия по устранению полезной нагрузки: Для устранения вектора для локального повышения привилегий (LPE) удалили SUID-бит у файла /var/www/html/apache_restart с помощью команды chmod –s /var/www/html/apache_restart. (рис. 2.24).

```
user@bitrix:/var$ cd /var/www/html/
user@bitrix:/var/www/html$ ls -la
итого 5640
drwxrwxr-x 12 www-data www-data 4096 окт 2 16:32 .
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 22 2023 bitrix
-rw-r--r-- 1 www-data www-data 265 июл 7 2023 .bottom.menu.php
-rw-r--r-- 1 www-data www-data 34 окт 2 16:31 caidao.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 1168 окт 2 16:32 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
-rw-r--r-- 1 root root 201 окт 2 16:32 password_recovery.php
drwxr-xr-x 2 www-data www-data 4096 июл 7 2023 products
-rw-r--r-- 1 root root 5661008 окт 2 16:32 RickRoiled.mp4
-rw-r--r-- 1 www-data www-data 76 окт 2 16:32 script.sh
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 окт 2 16:32 upload
-rw-r--r-- 1 www-data www-data 509 июл 7 2023 urlrewrite.php
user@bitrix:/var/www/html$ su -i
su: неверный ключ - «i»
Try 'su --help' for more information.
user@bitrix:/var/www/html$ sudo chmod -s /var/www/html/apache_restart
```

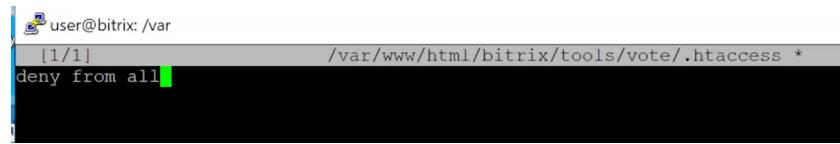
Рис. 2.24: Устранение LPE

Для закрытия уязвимости добавили изменения в файл /var/www/html/bitrix/tools/vote/uf.php, перед require_once и между знаков вопроса вставили код:(рис. 2.25).

```
user@bitrix:/var
GNU nano 6.2          /var/www/html/bitrix/tools/vote/uf.php *
<?
if ($_SERVER['REQUEST_METHOD'] === 'POST')
{
header('Status: 404 Not Found');
die();
}
require($_SERVER["DOCUMENT_ROOT"]."/bitrix/modules/vote/tools/uf.php");?>
```

Рис. 2.25: Редактирование uf.php

Создали файл .htaccess в директории /var/www/html/bitrix/tools/vote, задающий правила работы веб-сервера для конкретного каталога и подкаталогов. Для закрытия уязвимости в данном файле можно прописали команду deny from all(рис. 2.26).



```
user@bitrix: /var  
[1/1]          /var/www/html/bitrix/tools/vote/.htaccess *
```

The terminal window shows the command being run to create an .htaccess file in the /var/www/html/bitrix/tools/vote directory. The command is "deny from all".

Рис. 2.26: Создание .htaccess

Удалили файл /var/www/html/apache_restart.(рис. 2.27).



```
user@bitrix:/$ sudo rm /var/www/html/apache_restart
```

Рис. 2.27: Удаление файла

Уязвимость с ее последствием успешно устранены (рис. 2.28).

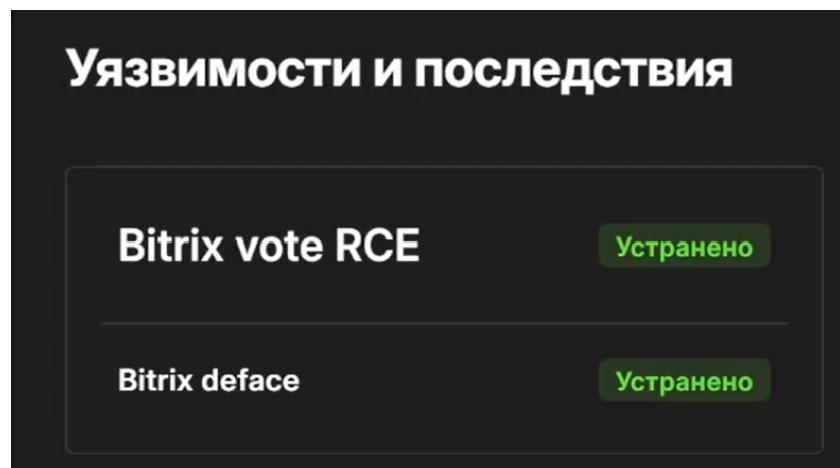


Рис. 2.28: Успех

2.3 Уязвимость GitLab RCE

Вернулись в ViPNet для обнаружения подозрительной активности в журнале событий. Изучили информацию об обнаруженной уязвимости.(рис. 2.29).

The screenshot shows the AMTIP tool interface with the following details:

- Search Bar:** /AMTIP
- Title:** Результаты поиска по IOC
- Search Query:** CVE-2021-22205
- Navigation:** Основное (selected), Правила обнаружения вторжений 4, Взаимосвязи 0, Граф
- Section: Основное**
 - Метрики:** CVSS версии 3.1
 - Оценка CVSS: 10 Высокая
 - Вектор: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H
 - Дата публикации NVD: 23.04.2021 21:15
 - Последнее изменение NVD: 23.04.2021 21:15
- Section: Описание**

An issue has been discovered in GitLab CE/EE affecting all versions starting from 11.9. GitLab was not properly validating image files that were passed to a file parser which resulted in a remote command execution.

Рис. 2.29: Обзор уязвимости

В соответствии с вектором атаки в KeePass нашли GitLab.(рис. 2.30).

The screenshot shows the KeePass application interface with the following details:

- Title Bar:** Frame.kdbx - KeePass
- Menu:** File, Group, Entry, Find, View, Tools, Help
- Toolbar:** Includes icons for file operations, group management, entry creation, search, and lock.
- Search Bar:** Search...
- Left Panel:** Shows a tree view of stored entries, including ColdFusion, Confluence, CouchDB, Elfinder, Froxlor, GLPI, GeoServer, GitLab, Gitea, and Jenkins.
- Right Panel:** A table view of stored entries for GitLab:

Title	User ...	Passw...	URL	Notes
Gitlab WEB	admin...	*****...	http://10.10.2...	
Gitlab SSH via...	user	*****...	ssh-putty://10...	
Gitlab SSH via...	user	*****...	ssh-bitvise://1...	
Gitlab SCP	user	*****...	scp://10.10.2.18	

Рис. 2.30: KeePass

Подключились к удаленному рабочему столу по адресу в соответствии с вектором атаки. Открыли веб-интерфейс GitLab и авторизовались под учетной записью администратора. (рис. 2.31).

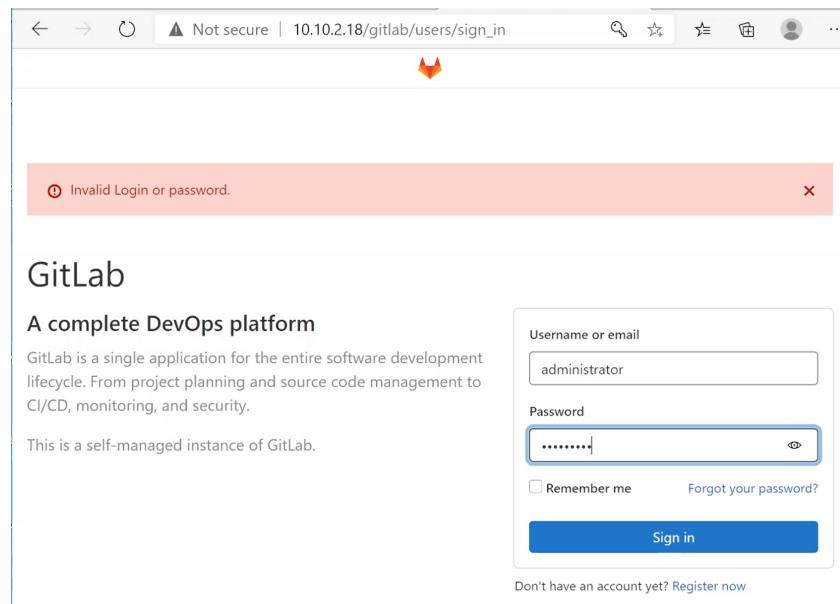


Рис. 2.31: GitLab

Перешли на страницу Admin Area. (рис. 2.32).

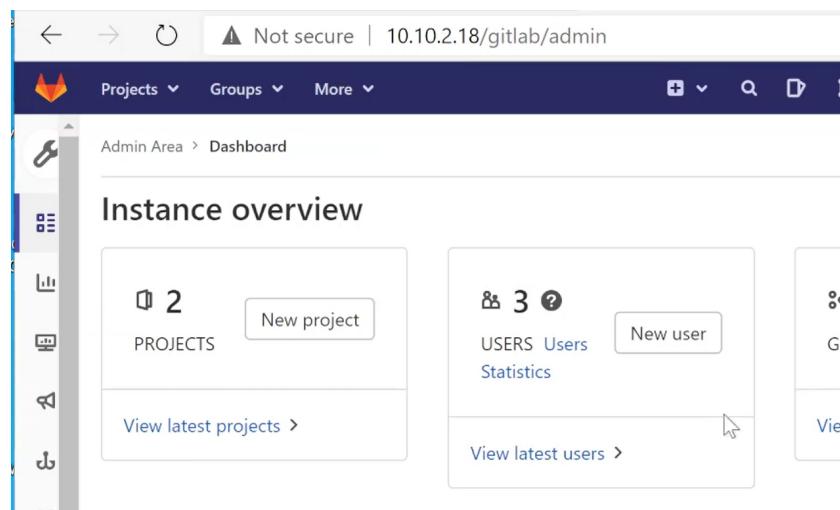


Рис. 2.32: Admin Area

В левой панели инструментов перешли во вкладку Settings – General.(рис. 2.33).

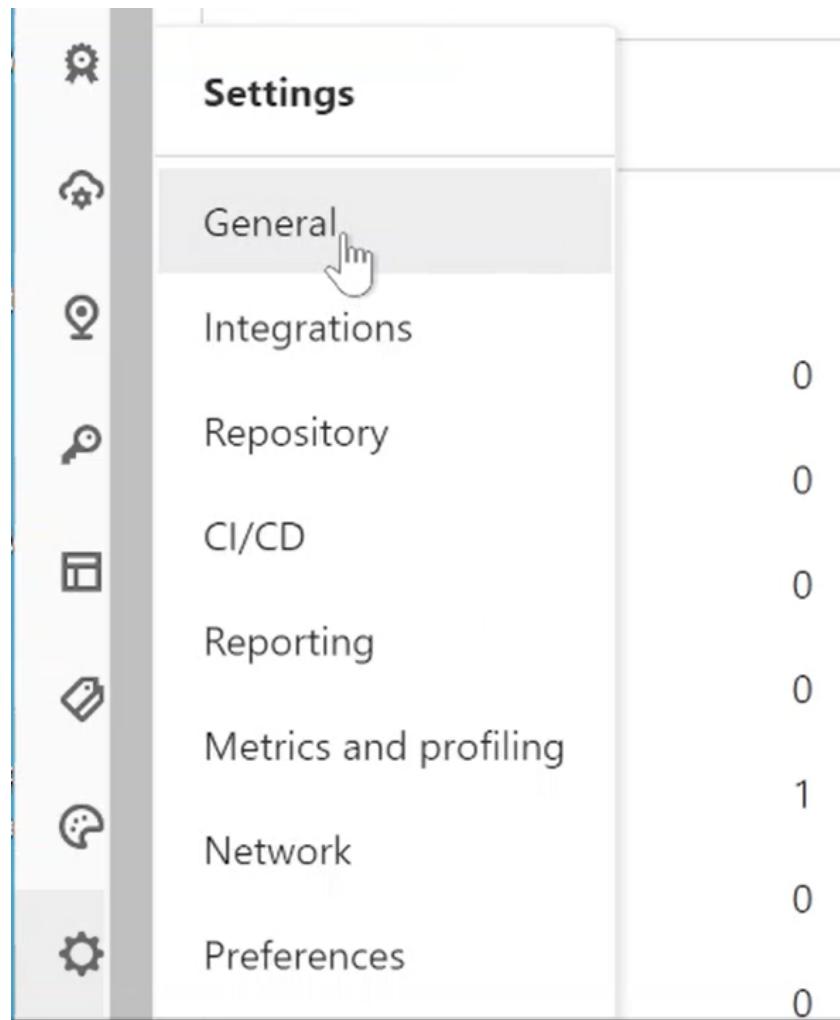


Рис. 2.33: Settings -> General

в настройках нашли пункт Sign-up restrictions и нажали кнопку Expand. (рис. 2.34).

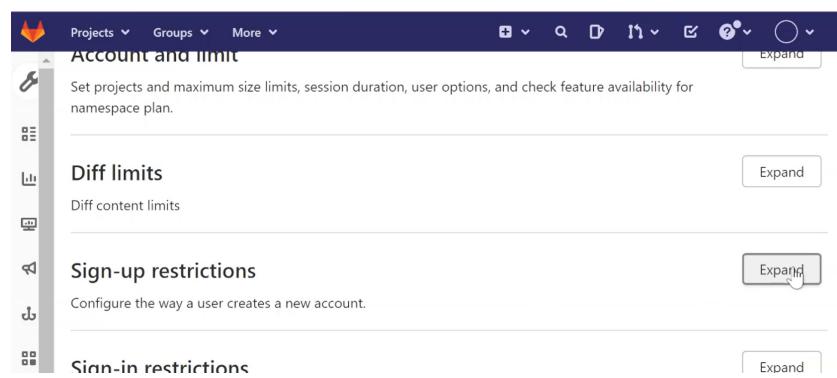


Рис. 2.34: Sign-up restrictions

Настроили конфигурацию, разрешающую регистрацию новых аккаунтов только с одобрения администратора.(рис. 2.35).

The screenshot shows the 'Sign-up restrictions' configuration page. It includes a 'Configure the way a user creates a new account.' section with three options: 'Sign-up enabled' (checked), 'Require admin approval for new sign-ups' (checked), and 'Send confirmation email on sign-up' (unchecked). A 'Collapse' button is in the top right corner.

- Sign-up enabled
When enabled, any user visiting http://10.10.2.18/gitlab/users/sign_in will be able to create an account.
- Require admin approval for new sign-ups
When enabled, any user visiting http://10.10.2.18/gitlab/users/sign_in and creating an account will have to be explicitly approved by an admin before they can sign in. This setting is effective only if sign-ups are enabled.
- Send confirmation email on sign-up

Рис. 2.35: Настройка

Сохранили конфигурацию. (рис. 2.36).



Рис. 2.36: Сохранение конфигурации

В панели администратора перешли во вкладку Users(рис. 2.37).

The screenshot shows the 'Users' page in the GitLab administrator panel. It features a search bar and filters for 'Active' (2), 'Admins' (1), '2FA Enabled' (0), '2FA Disabled' (3), 'External' (0), 'Blocked' (0), 'Pending approval' (0), and 'Deactivate'. Two users are listed: 'Script Kiddie' (Active, Admin, 0 projects, 2 Oct, 2025 last activity) and 'Administrator' (Active, Admin, 2 projects, 1 Jul, 2021 last activity). Each user has an 'Edit' and a gear icon for more options.

Name	Projects	Created on	Last activity	Action
Script Kiddie 4889193623250975886@example.com	0	2 Oct, 2025	2 Oct, 2025	Edit
Administrator admin@example.com	2	1 Jul, 2021	2 Oct, 2025	Edit

Рис. 2.37: Users

В строке с пользователем Script Kiddie нажали Delete user and contributions. (рис. 2.38).

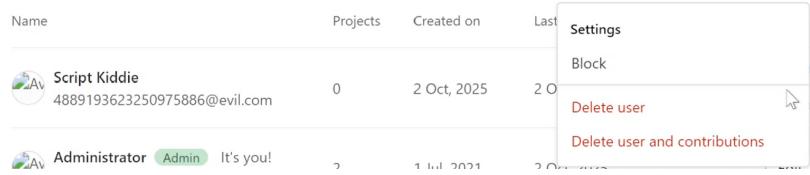


Рис. 2.38: Удаление пользователя

Подтвердили удаление. (рис. 2.39).

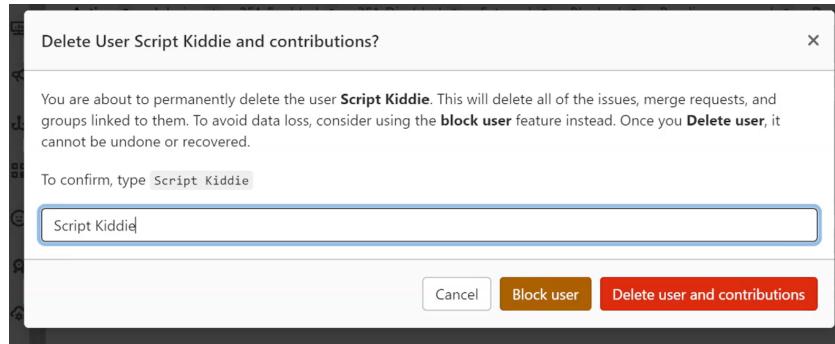


Рис. 2.39: Подтверждение удаления

С помощью утилиты ss и команды kill закрыли meterpreter сессии. (рис. 2.40).

```
user@ampire-gitlab: ~
users:(("nginx",pid=1668,fd=12))          127.0.0.1:58214      127.0.0.1:9090
ESTAB      0      0                         127.0.0.1:9168      127.0.0.1:49964
users:(("prometheus",pid=1578,fd=14))        127.0.0.1:9168      127.0.0.1:49964
ESTAB      0      0                         127.0.0.1:39232      127.0.0.1:9121
users:(("gitlab-exporter",pid=1593,fd=12))    127.0.0.1:39232      127.0.0.1:43156
ESTAB      0      0                         127.0.0.1:9093      127.0.0.1:43156
users:(("alertmanager",pid=1601,fd=9))
FIN-WAIT-2  0      0                         10.10.2.18:http      10.10.2.254:19631
ESTAB      0      0                         10.10.2.18:47226     10.10.2.18:http
users:(("python3",pid=996,fd=3))           FIN-WAIT-2  0      0                         10.10.2.18:http      10.10.2.254:1669
ESTAB      0      0                         127.0.0.1:44174      127.0.0.1:9229
users:(("prometheus",pid=1578,fd=22))
ESTAB      0      0                         127.0.0.1:9100      127.0.0.1:60970
users:(("node_exporter",pid=1600,fd=7))
ESTAB      0      0                         127.0.0.1:8082      127.0.0.1:59168
users:(("bundle",pid=1786,fd=77))
user@ampire-gitlab:~$ sudo kill 3120
```

Рис. 2.40: Закрытие meterpreter сессий

Уязвимость с ее последствием успешно устраниены (рис. 2.41).

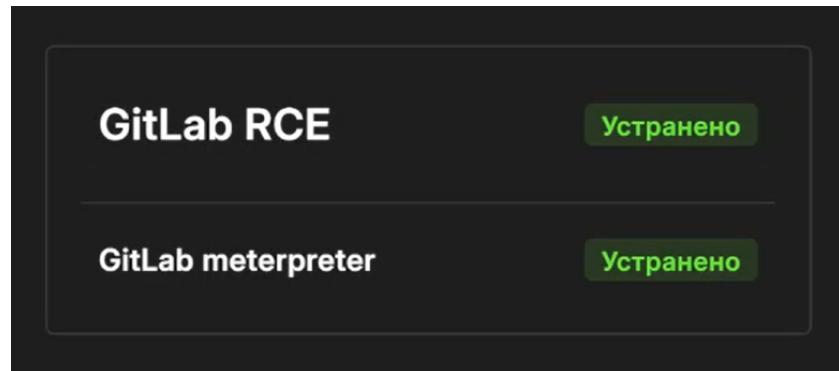


Рис. 2.41: Успех

2.4 Уязвимость WSO2 API-Manager RCE

Вернулись в ViPNet для обнаружения подозрительной активности в журнале событий. (рис. 2.42).

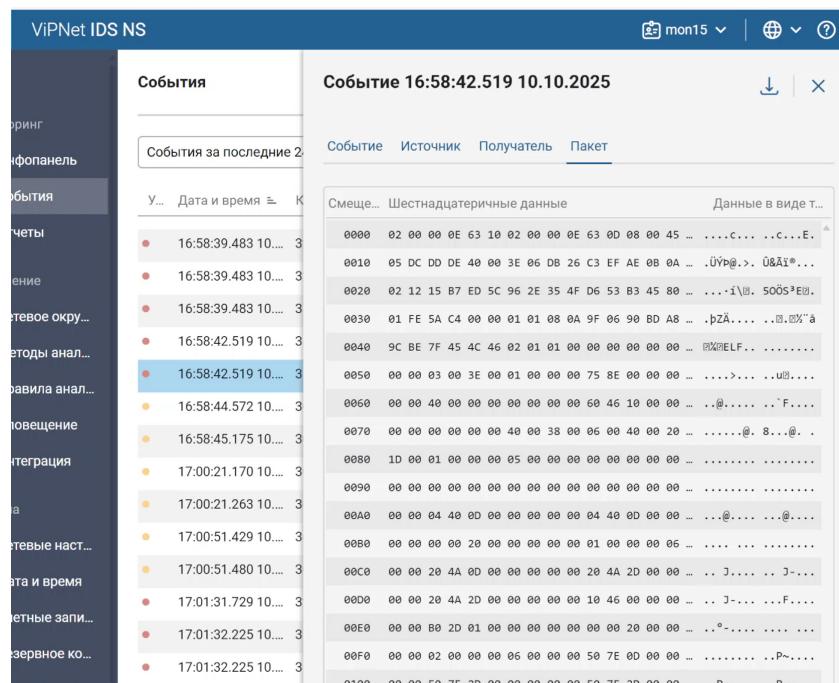


Рис. 2.42: Журнал событий

Изучили информацию об обнаруженной уязвимости.(рис. 2.43).

Основное

Метрики

Оценка cvss **9.8 Высокая**

Вектор **CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H**

Дата публикации NVD **19.04.2022 01:15** Последнее изменение NVD **19.04.2022 01:15**

Описание

Certain WSO2 products allow unrestricted file upload with resultant remote code execution. The attacker must use a /fileupload endpoint with a Content-Disposition directory traversal sequence to reach a directory under the web root, such as a/..../repository/deployment/server/webapps directory. This affects WSO2 API Manager 2.2.0 up to 4.0.0, WSO2 Identity Server 5.2.0 up to 5.11.0, WSO2 Identity Server Analytics 5.4.0, 5.4.1, 5.5.0 and 5.6.0, WSO2 Identity Server as Key Manager 5.3.0 up to 5.11.0, WSO2 Enterprise Integrator 6.2.0 up to 6.6.0, WSO2 Open Banking AM 1.4.0 up to 2.0.0 and WSO2 Open Banking KM 1.4.0, up to 2.0.0.

Рис. 2.43: Обзор уязвимости

В соответствии с вектором атаки в KeePass нашли API-Manager.(рис. 2.44).

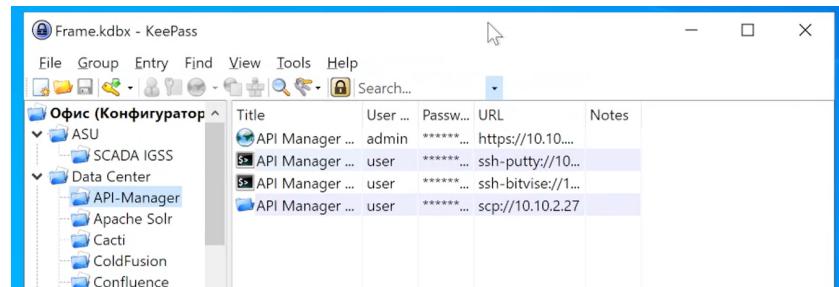


Рис. 2.44: KeePass

Открыли файл конфигурации WSO2 API-Manager и добавили в конец запись resource.access_control.(рис. 2.45 - 2.46).

```
user@wso2-virtual-machine:~$ cd /opt/wso2am-4.0.0/repository/conf
user@wso2-virtual-machine:/opt/wso2am-4.0.0/repository/conf$ sudo nano deployment.toml
```

Рис. 2.45: Файл конфигурации

```
className = "org.apache.catalina.valves.AccessLogValve"
directory="/var/log"
prefix="wso2_http_access"
suffix=".log"
rotatable="false"
pattern="%h %l %u %t %r %s %b %{Referer}i %{User-Agent}i %T

[[resource.access_control]]
context="(.*)/fileupload/(.*)"
secure=true
http_method = "all"
permissions = ["/permission/protected/"]
```

^G Get Help ^O Write Out ^W Where Is ^K Cut Text ^J Justify ^C Cur Pos
^X Exit ^R Read File ^\ Replace ^U Uncut Text ^T To Spell ^ ^ Go To Line

Рис. 2.46: Редактирование

Удалили загруженный exploit.jsp файл по пути /opt/wso2am-4.0.0/repository/deployment/server/webapps/authenticationendpoint. (рис. 2.47).

```
user@wso2-virtual-machine:/opt/wso2am-4.0.0/repository/deployment/server$ cd 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
```

Рис. 2.47: Удаление файла

Удалили сгенерированный файл /tmp/payload.elf. (рис. 2.48).

```
user@wso2-virtual-machine:/tmp$ cd tmp
user@wso2-virtual-machine:/tmp$ sudo rm payload.elf
user@wso2-virtual-machine:/tmp$
```

Рис. 2.48: Удаление файла

С помощью утилиты ss и команды kill закрыли meterpreter сессии. (рис. 2.49).

```
user@wso2-virtual-machine:/tmp$ sudo ss -tp
State      Recv-Q      Send-Q      Local Address:Port          Peer Address:Port
ESTAB      0            0           10.10.2.27:ssh          10.10.2.254:52524
users:(("sshd",pid=24415,fd=3), ("sshd",pid=24413,fd=3))
SYN-SENT   0            1           10.10.2.27:55970        195.239.174.125:puppet
users:(("puppet",pid=25273,fd=6))
user@wso2-virtual-machine:/tmp$ sudo kill 25273
user@wso2-virtual-machine:/tmp$
```

Рис. 2.49: Закрытие meterpreter сессий

Зашли в веб-интерфейс WSO2 API-Manager по ссылке https://10.10.2.27:9443/carbon и авторизовались под учетной записью администратора. (рис. 2.50).

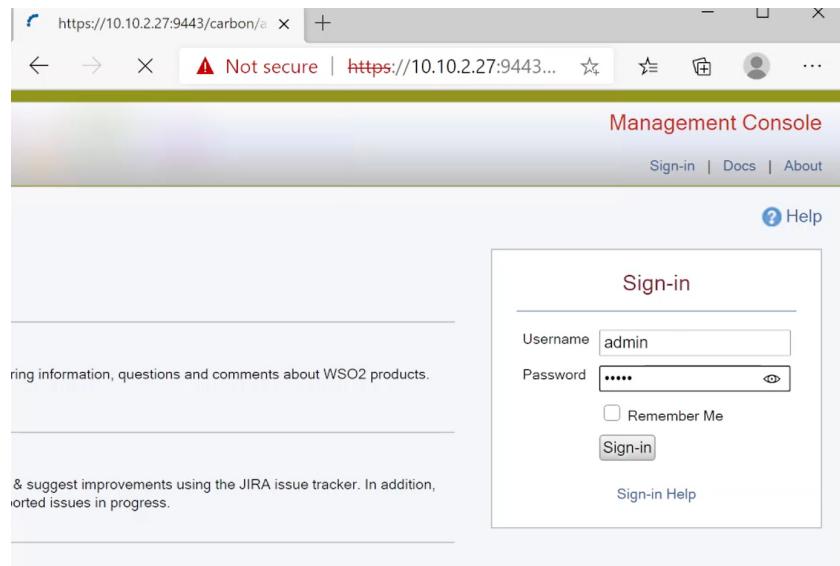


Рис. 2.50: Вход в веб-интерфейс

Просмотрели список пользователей. (рис. 2.51).

A screenshot of the 'Users' page in the WSO2 Management Console. The URL is https://10.10.2.27:9443/carbon/users. The title bar says 'Home > Users'. The main content area has a 'Search Users' section with fields for 'Select Domain' (ALL-USER-STORE-DOMAINS), 'Enter Username Pattern (* for all)' (empty), and 'Select Claim URI' (Select). Below is a table of users:

Name	Actions
admin	Change Password Assign Roles V Delete User Profile
apim_reserved_user	Change Password Assign Roles V Delete User Profile
hacker	Change Password Assign Roles V Delete User Profile

Рис. 2.51: Пользователи

Удалили пользователя hacker.(рис. 2.52).

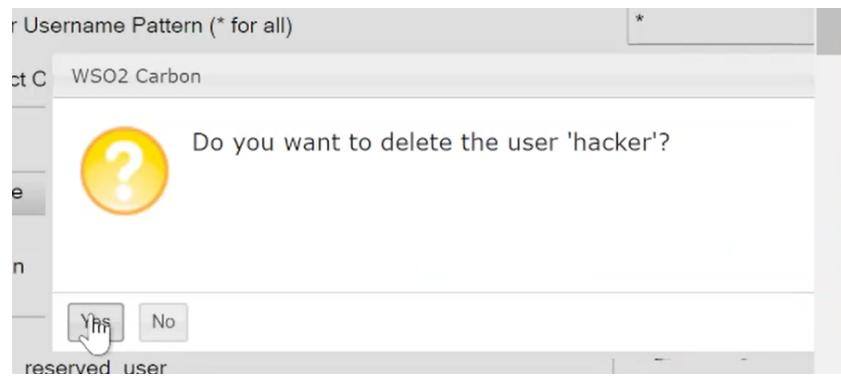


Рис. 2.52: Удаление пользователя

Уязвимость с ее последствием успешно устранены. (рис. 2.53).

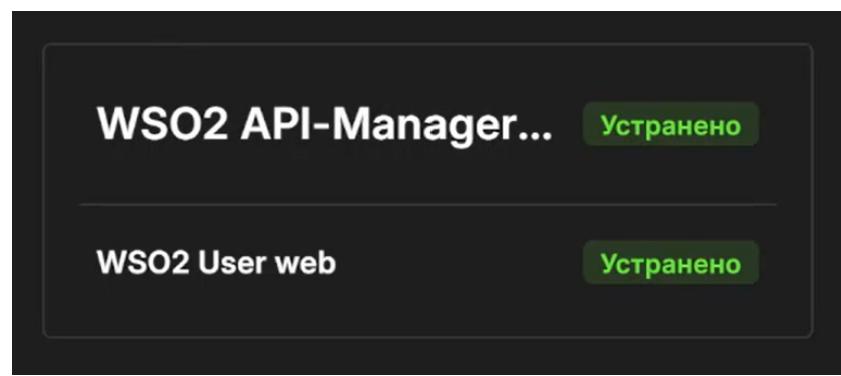


Рис. 2.53: Успех

3 Выводы

В результате выполнения лабораторной работы мы получили навыки обнаружения и устранение уязвимостей Bitrix vote RCE, GitLab RCE, WSO2 API-Manager RCE и их последствий.