

Лабораторная работа № 2-Д

Защита интеграционной платформы

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

Российский университет дружбы народов, Москва, Россия

Информация

Докладчик

- Доберштейн А., Оразгелдиев Я., Лобанова П., Лушин А.,
Барабанова К.
- НФИбд-02-22
- Российский университет дружбы народов

Цель работы

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

Выполнение лабораторной работы

Для начала изучили вектор атаки, адреса злоумышленника и атакуемых серверов.



Рис. 1: Вектор атаки

Уязвимость Bitrix vote RCE

Залогинились в ViPNet для обнаружения уязвимости в журнале событий.



Уязвимость Bitrix vote RCE

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.

У...	Дата и время ё...	Код события	Ко...	Название правила	Класс	Протокол	IP-адрес источ...	Порт ист...	IP-адрес получ...	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...	2025808	1	ET EXPLOIT php script base6...	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. 3: Журнал событий

Уязвимость Bitrix vote RCE

Изучили информацию по CVE-коду об обнаруженной уязвимости, изучили рекомендации по нейтрализации.

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

Уязвимость Bitrix vote RCE

Для устранения уязвимости подключились к удаленному рабочему столу.

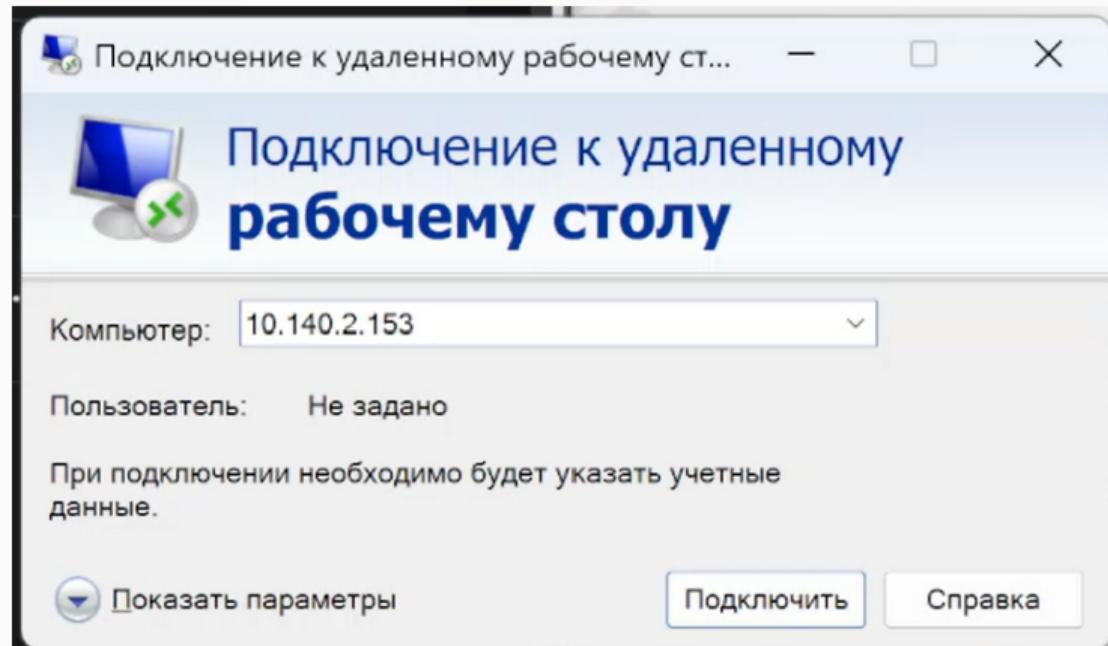
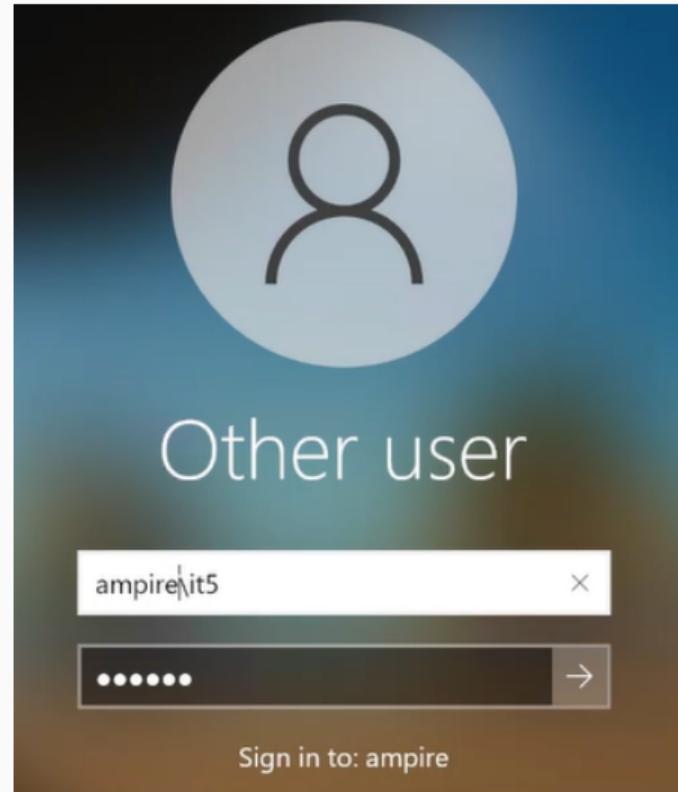


Рис. 5: Подключение к удаленному рабочему столу

Уязвимость Bitrix vote RCE

Вошли под указанной учетной записью.



Уязвимость Bitrix vote RCE

В соответствии с вектором атаки в KeePass нашли CMS Bitrix.

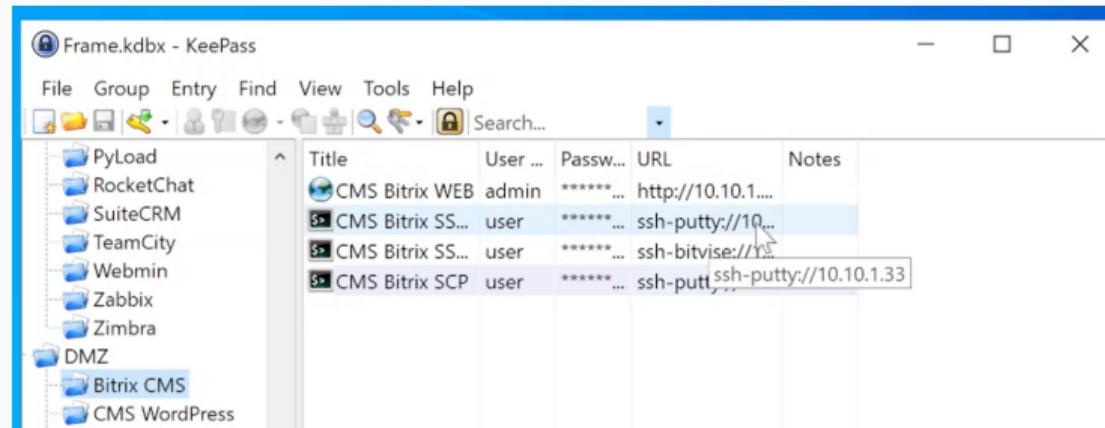


Рис. 7: KeePass

Уязвимость Bitrix vote RCE

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.

```
user@bitrix:/var/log/apache2$ cat access.log
195.239.174.11 - - [02/Oct/2025:16:31:05 +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%5BMODULE_ID%5D=iblock&attachId%5BENTITY_TYPE%5D=CFileUploader&action=vo
te&sessid=defe73a4cledfdc0406d9076561bd3cb&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%5BMODULE_ID%5D=iblock&attachId%5BENTITY_TYPE%5D=Phar&attachId%5BENTITY_
ID%5D=%2Fvar%2Fwww%2Fhtml%2Fupload%2Ftmp%2FBXTEMP-2025-10-03%2F04%2Fbxu%2Fmain%2
F427c3fcf040a09292ba412d66fe315bf%2Fc4238a0b923820dcc509a6f75849b%2Fpayload2.
phar&action=vote&sessid=defe73a4cledfdc0406d9076561bd3cb 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
```

Уязвимость Bitrix vote RCE

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

```
user@bitrix:/var/log/apache2$ find /var/www/html/ -iname "payload2.phar"
./var/www/html/upload/tmp/BXTEMP-2025-10-03/04/bxu/main/427c3fcf040a09292ba412d66fe315bf/c4ca4238a0b
923820dcc509a6f75849b/payload2.phar
```

Рис. 9: Поиск файла

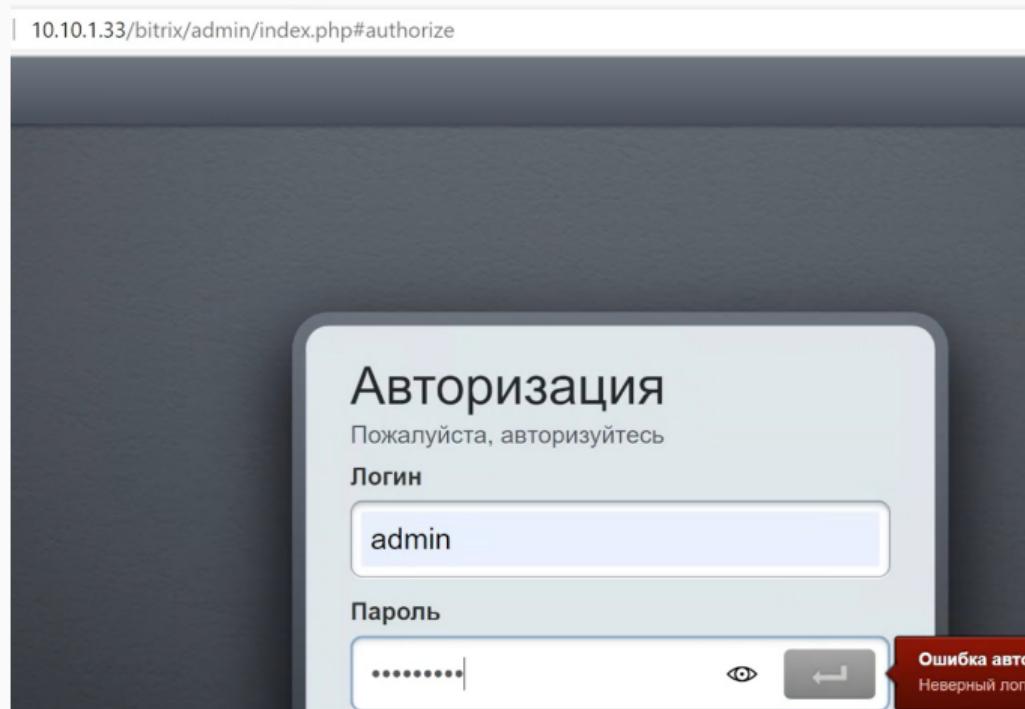
Уязвимость Bitrix vote RCE

Просмотрели содержимое с помощью текстового редактора, отобразилась информация о скачивании веб-backdoor по пути /var/www/html/caidao.php.

Рис. 10: Информация о полезной нагрузке

Уязвимость Bitrix vote RCE

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



Уязвимость Bitrix vote RCE

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.

```
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
```

Уязвимость Bitrix vote RCE

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:



```
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. 13: Редактирование uf.php

Уязвимость Bitrix vote RCE

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.



The screenshot shows a terminal window with the following content:

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

The terminal prompt is "user@bitrix: /var". Below it, the command "[1/1]" is shown, followed by the path "/var/www/html/bitrix/tools/vote/.htaccess *". The final line of the command is "deny from all". The "deny from all" line is highlighted with a green rectangular selection.

Рис. 14: Создание .htaccess

Уязвимость Bitrix vote RCE

С помощью утилиты ss и команды kill закрыли meterpreter сессии.

```
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
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
```

Ошибка авторизации!

Рис. 15: Закрытие meterpreter сессий

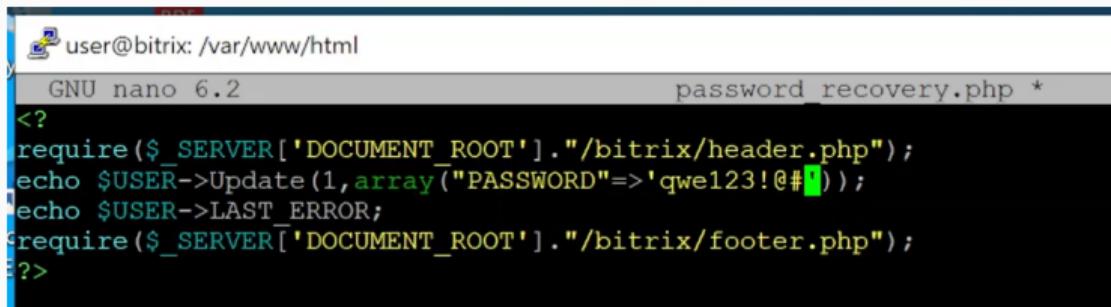
Уязвимость Bitrix vote RCE

В директории веб-сервера обнаружили скрипт password_recovery.php.

```
: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
-rw-rwxr-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
drwxr-xr-x  2 www-data www-data 4096 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$
```

Уязвимость Bitrix vote RCE

Прописали новый пароль.



```
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. 17: password_recovery.php

Уязвимость Bitrix vote RCE

Подключились к веб-серверу, в ссылке указали название данного файла.

Авторизация - 10.10.1.33 Взломанная компания

Not secure | 10.10.1.33/password_recovery.php

Слоган компании
шная информация по лучшей
цене

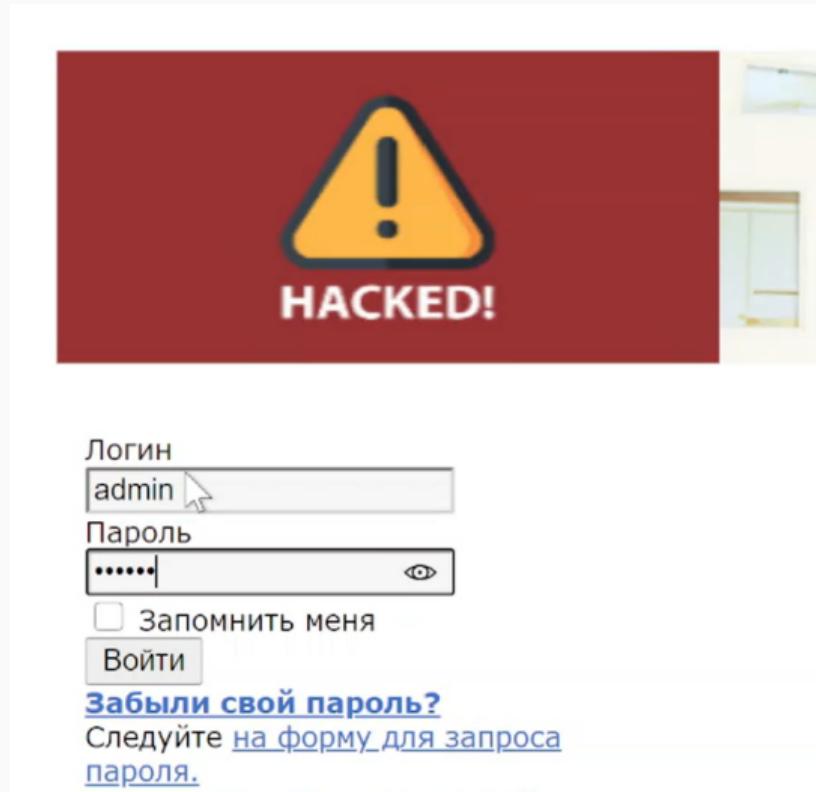
HACKED!

Наша компания взламывается на
Российском рынке с 1992 года. За
это время «Взломанная
компания» прошла большой
путь от маленькой фирмы до
одного из крупнейших
сборщиков личной информации в
России.

«Взломанная компания»
осуществляет сбор личной
информации на высококлассном
оборудовании с применением
минимальной доли ручного

Уязвимость Bitrix vote RCE

Авторизовались с правами администратора



Уязвимость Bitrix vote RCE

Открылась панель администрирования.

The screenshot shows a web browser window with the URL `10.10.1.33/login/`. The title bar indicates "Not secure". The top navigation bar has tabs for "Меню", "Сайт", and "Администрирование". A user profile for "Maksim Ivanov" is visible. The main content area displays a green banner with a checkmark and the text "Обнаружены ошибки в работе сайта. Проверить и исправить." Below this, there's a slogan "Слоган компании" followed by the text "Лучшая информация по лучшей цене". On the left, a red box contains a yellow warning sign with an exclamation mark and the word "HACKED!". To its right is a small image of a computer monitor. On the right side of the page, there's a large text block in Russian: "Наша компания взламывается Российской рынке с 1992 года. это время «Взломанная компания» прошла большой путь от маленькой фирмы до одного из крупнейших сборщиков личной информации России." At the bottom left, there's a message: "Вы зарегистрированы и успешно авторизовались." and a link "Вернуться на главную страницу".

Уязвимость Bitrix vote RCE

Удалили файл password_recovery.php.

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

Рис. 21: Удаление файла

Уязвимость Bitrix vote RCE

Доступ к панели администрирования восстановлен. Удалили все файлы в директории взломанного веб-сервера.

```
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. 22: Удаление файлов

Уязвимость Bitrix vote RCE

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.

```
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. 23: Резервная копия

Уязвимость Bitrix vote RCE

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.

```
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 statistic.php
```

Уязвимость Bitrix vote RCE

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:



```
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. 25: Редактирование uf.php

Уязвимость Bitrix vote RCE

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



The screenshot shows a terminal window with the following content:

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

The terminal window has a light gray background. The command prompt is "user@bitrix: /var". Below it, the file path is shown as "[1/1] /var/www/html/bitrix/tools/vote/.htaccess *". The command "deny from all" is typed at the bottom of the screen.

Рис. 26: Создание .htaccess

Уязвимость Bitrix vote RCE

Удалили файл /var/www/html/apache_restart.



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

Рис. 27: Удаление файла

Уязвимость Bitrix vote RCE

Уязвимость с ее последствием успешно устранены

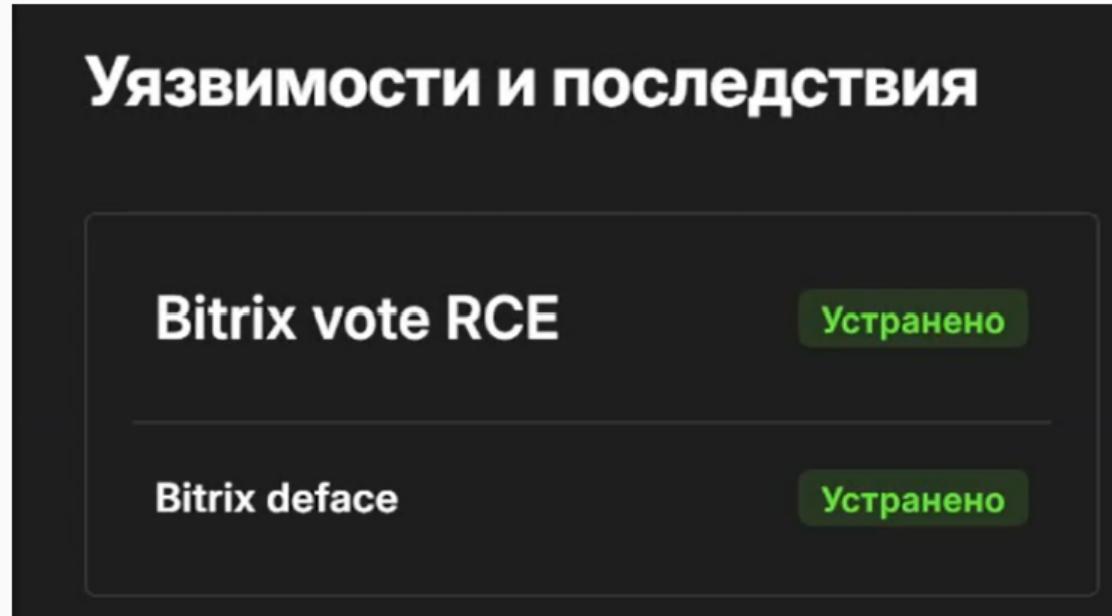


Рис. 28: Успех

Уязвимость GitLab RCE

Вернулись в ViPNet для обнаружения подозрительной активности в журнале событий.
Изучили информацию об обнаруженной уязвимости.

The screenshot shows the AMTIP interface with the following details:

- Search Bar:** /AMTIP
- Search Results Title:** Результаты поиска по IOC
- Search Results Subtitle:** CVE-2021-22205
- Navigation Tabs:** Основное (highlighted), Правила обнаружения вторжений 4, Взаимосвязи 0, Граф
- Main Content Area - Основное:**
 - Metrics:** CVSS версии 3.1
 - CVSS Score:** 10 Высокая
 - Vector:** CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H
 - NVD Publication Date:** 23.04.2021 21:15
 - NVD Last Update:** 23.04.2021 21:15

Уязвимость GitLab RCE

В соответствии с вектором атаки в KeePass нашли GitLab.

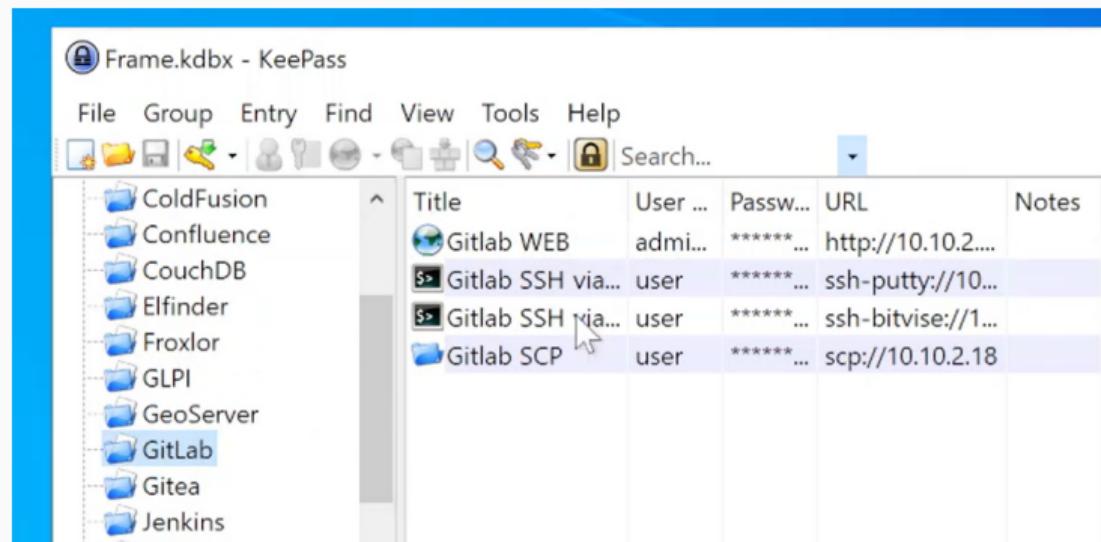


Рис. 30: KeePass

Уязвимость GitLab RCE

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

Not secure | 10.10.2.18/gitlab/users/sign_in

Invalid Login or password.

GitLab

A complete DevOps platform

GitLab is a single application for the entire software development lifecycle. From project planning and source code management to CI/CD, monitoring, and security.

This is a self-managed instance of GitLab.

Username or email
administrator

Password
.....

Remember me [Forgot your password?](#)

Sign in

Уязвимость GitLab RCE

Перешли на страницу Admin Area.

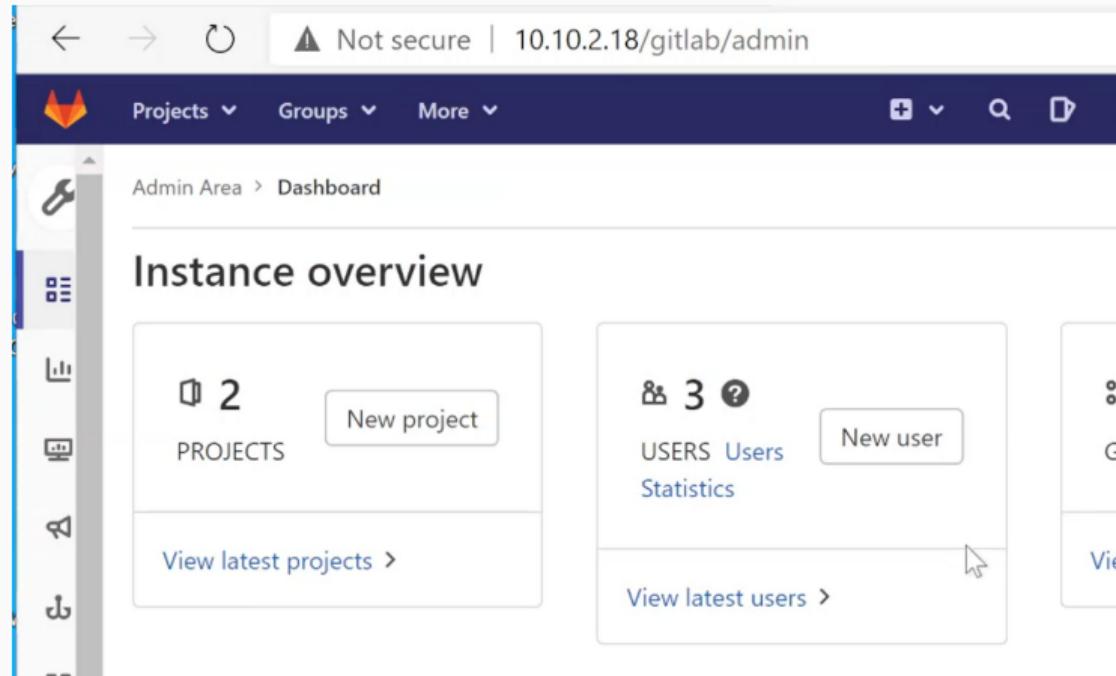
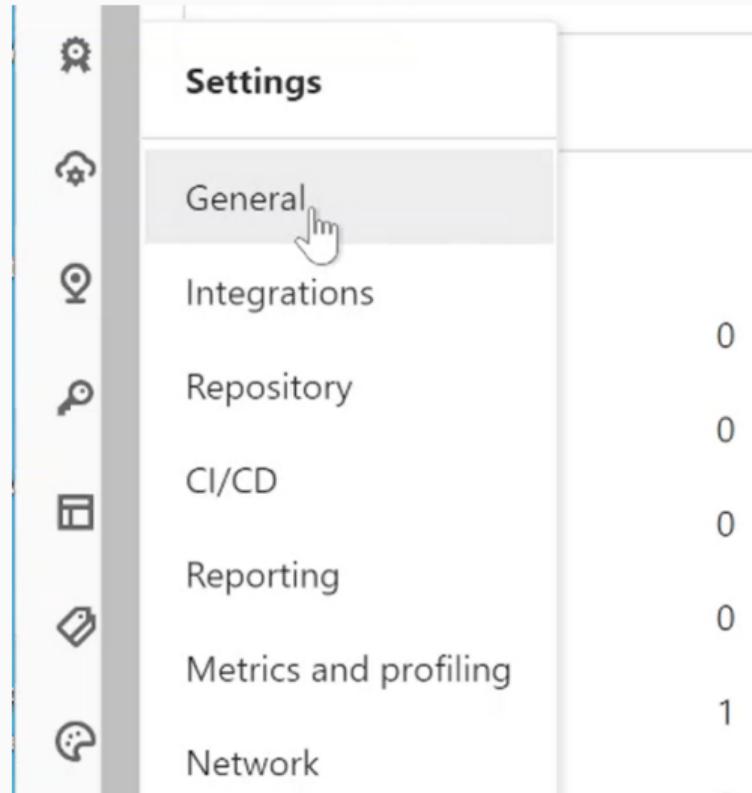


Рис. 32: Admin Area

Уязвимость GitLab RCE

В левой панели инструментов перешли во вкладку Settings – General.



Уязвимость GitLab RCE

в настройках нашли пункт Sign-up restrictions и нажали кнопку Expand.

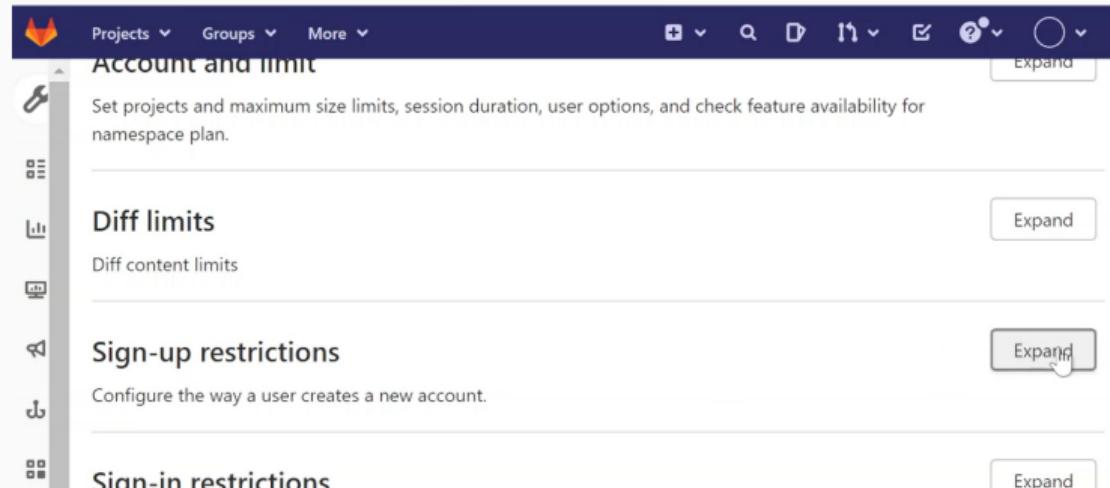


Рис. 34: Sign-up restrictions

Уязвимость GitLab RCE

Настроили конфигурацию, разрешающую регистрацию новых аккаунтов только с одобрения администратора.

Sign-up restrictions Collapse

Configure the way a user creates a new account.

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. 35: Настройка

Уязвимость GitLab RCE

Сохранили конфигурацию.



Рис. 36: Сохранение конфигурации

Уязвимость GitLab RCE

В панели администратора перешли во вкладку Users

The screenshot shows the 'Users' section of the GitLab Admin interface. At the top, there are tabs for 'Users' and 'Cohorts'. Below the tabs is a blue button labeled 'New user'. Underneath the button, there are several status filters: 'Active' (2), 'Admins' (1), '2FA Enabled' (0), '2FA Disabled' (3), 'External' (0), 'Blocked' (0), 'Pending approval' (0), and 'Deactivate'. A search bar with placeholder text 'Search by name, email or username' and a sorting dropdown set to 'Name' are also present. The main table lists two users:

Name	Projects	Created on	Last activity	
Script Kiddie 4889193623250975886@evil.com	0	2 Oct, 2025	2 Oct, 2025	Edit ⚙️
Administrator It's you! admin@example.com	2	1 Jul, 2021	2 Oct, 2025	Edit

Рис. 37: Users

Уязвимость GitLab RCE

В строке с пользователем Script Kiddie нажали Delete user and contributions.

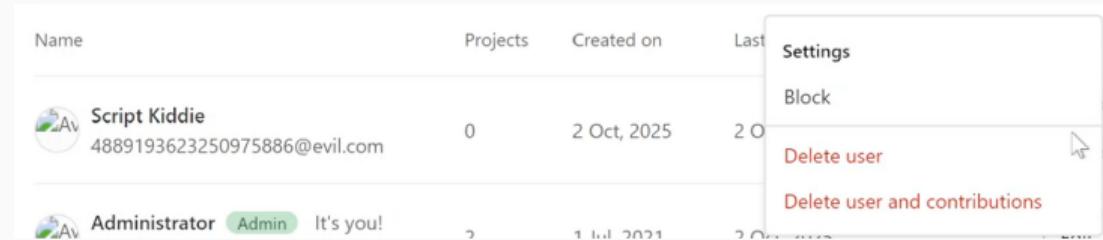


Рис. 38: Удаление пользователя

Уязвимость GitLab RCE

Подтвердили удаление.

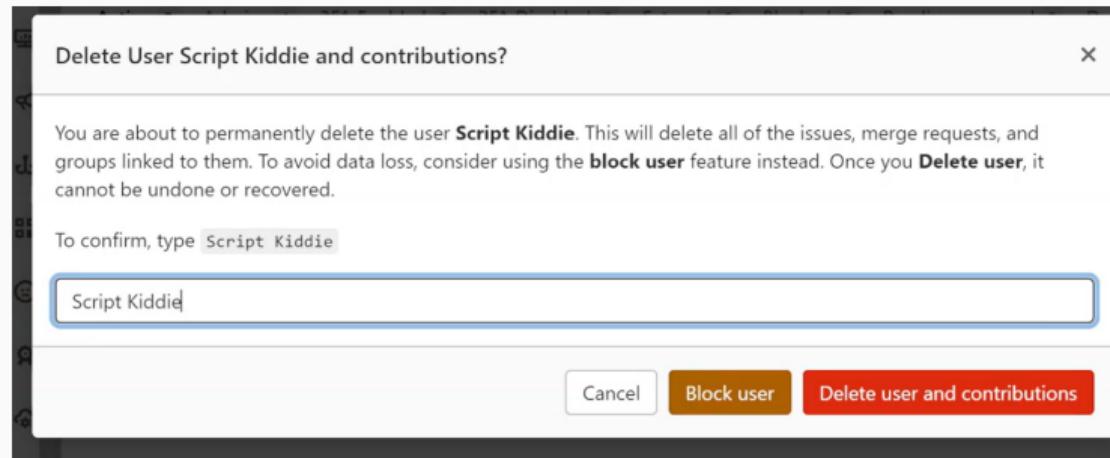
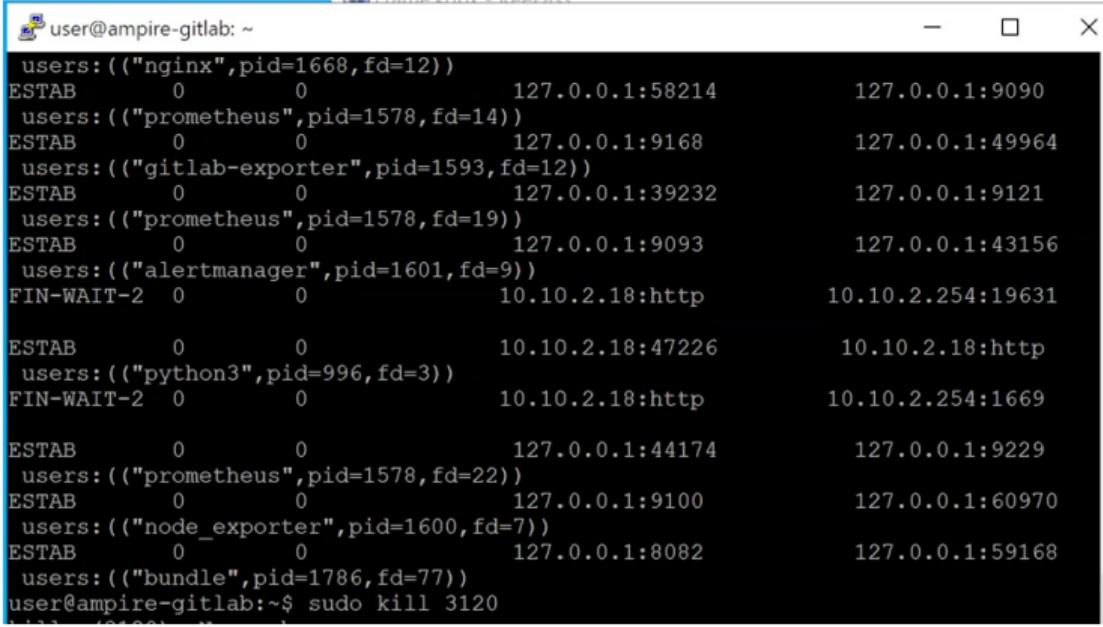


Рис. 39: Подтверждение удаления

Уязвимость GitLab RCE

С помощью утилиты ss и команды kill закрыли meterpreter сессии.



```
user@ampire-gitlab: ~
users:(("nginx",pid=1668,fd=12))
ESTAB      0      0          127.0.0.1:58214          127.0.0.1:9090
users:(("prometheus",pid=1578,fd=14))
ESTAB      0      0          127.0.0.1:9168          127.0.0.1:49964
users:(("gitlab-exporter",pid=1593,fd=12))
ESTAB      0      0          127.0.0.1:39232          127.0.0.1:9121
users:(("prometheus",pid=1578,fd=19))
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. 40: Закрытие meterpreter сессий

Уязвимость GitLab RCE

Уязвимость с ее последствием успешно устранены

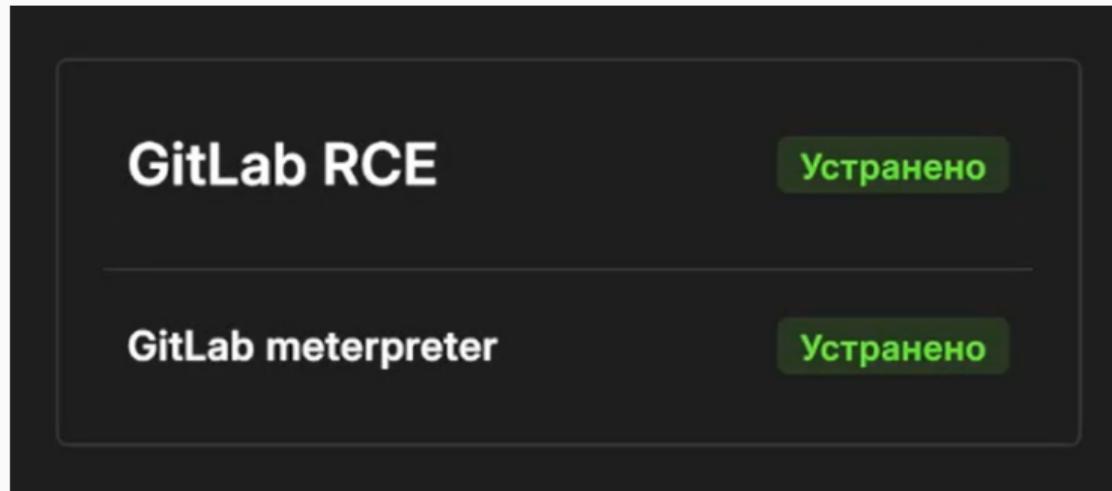


Рис. 41: Успех

Уязвимость WSO2 API-Manager RCE

Вернулись в ViPNet для обнаружения подозрительной активности в журнале событий.

События				Событие 16:58:42.519 10.10.2025															
				Событие	Источник	Получатель	Пакет												
События за последние 2 часа															Данные в виде текста				
У...	Дата и время	К...	Смещение	Шестнадцатеричные данные															
●	16:58:39.483 10...	3	0000	02 00 00 0E 63 10 02 00 00 0E 63 00 08 00 45c....c....E...														
●	16:58:39.483 10...	3	0010	05 DC DD DE 40 00 3E 06 DB 26 C3 EF AE 0B 0AÜÝP@>. Ü&ÄI%...														
●	16:58:39.483 10...	3	0020	02 12 15 B7 ED 5C 96 2E 35 4F D6 53 B3 45 80i\B. 500S³E9...														
●	16:58:42.519 10...	3	0030	01 FE 5A C4 00 00 01 01 08 0A 9F 06 90 BD A8þZÄ.... .B.Æ%"ä...														
●	16:58:42.519 10...	3	0040	9C BE 7F 45 4C 46 02 01 01 00 00 00 00 00 00 ...	þXREFL...														
●	16:58:42.519 10...	3	0050	00 00 03 00 3E 00 01 00 00 00 75 8E 00 00 00>.... .uB....														
●	16:58:44.572 10...	3	0060	00 00 40 00 00 00 00 00 00 00 60 46 10 00 00@..... F....														
●	16:58:45.175 10...	3	0070	00 00 00 00 00 00 40 00 38 00 06 00 40 00 20@. 8...@. .														
●	17:00:21.170 10...	3	0080	1D 00 01 00 00 00 05 00 00 00 00 00 00 00 00														
●	17:00:21.263 10...	3	0090	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00														
●	17:00:51.429 10...	3	00A0	00 00 04 40 0D 00 00 00 00 00 04 40 0D 00 00@.... .@....														
●	17:00:51.480 10...	3	00B0	00 00 00 00 20 00 00 00 00 00 01 00 00 00 06														
●	17:00:51.480 10...	3	00C0	00 00 20 4A 0D 00 00 00 00 00 20 4A 2D 00 00J.... .J....														

Уязвимость WSO2 API-Manager RCE

Изучили информацию об обнаруженной уязвимости.

AMTIP

Результаты поиска по IOC
CVE-2022-29464

Основное Правила обнаружения вторжений 1 Взаимосвязи 0 Граф

Основное

Метрики

Оценка cvss ① CVSS версии 3.1

9.8 Высокая

Вектор ①

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

Дата публикации NVD ① Последнее изменение NVD ①

19.04.2022 01:15 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

Уязвимость WSO2 API-Manager RCE

В соответствии с вектором атаки в KeePass нашли API-Manager.

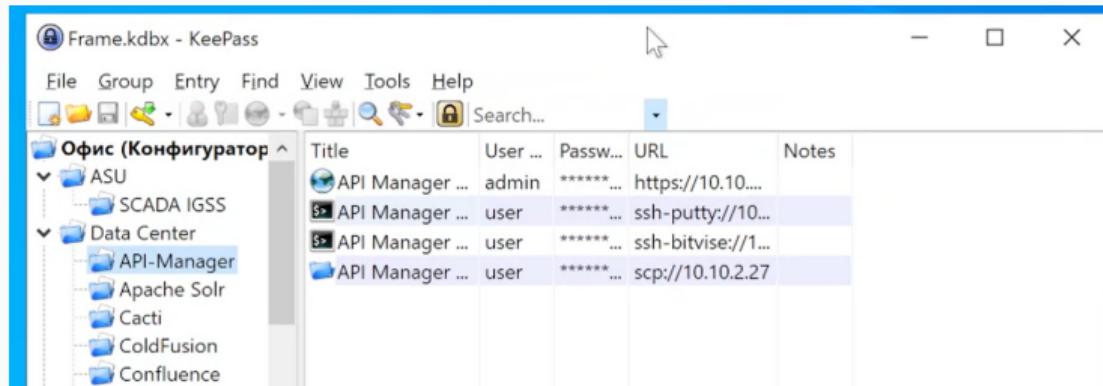


Рис. 44: KeePass

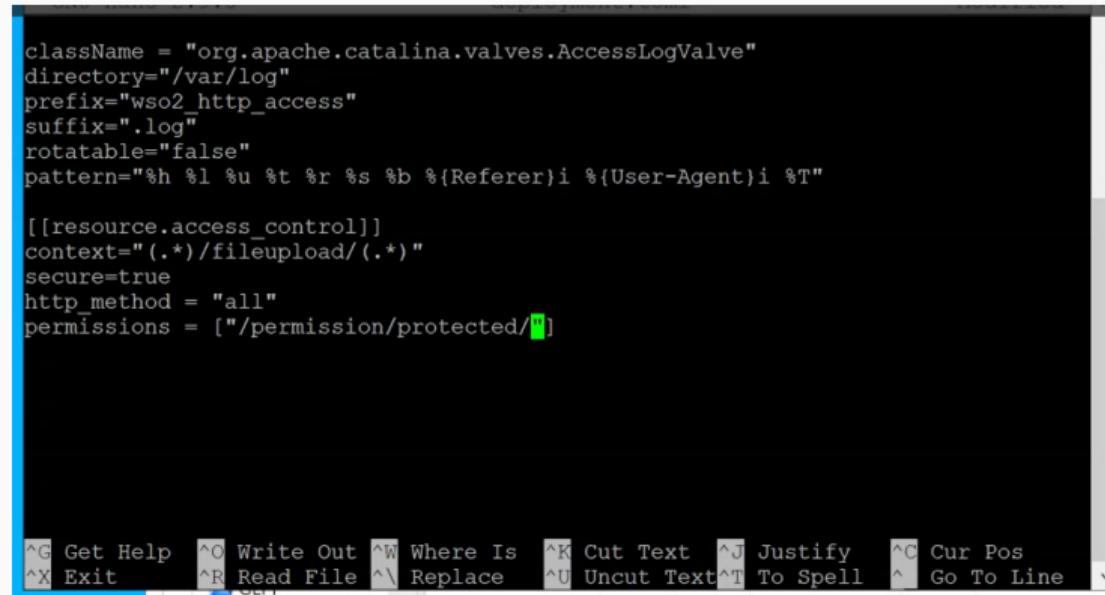
Уязвимость WSO2 API-Manager RCE

Открыли файл конфигурации WSO2 API-Manager и добавили в конец запись resource.access_control.

```
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. 45: Файл конфигурации

Уязвимость WSO2 API-Manager RCE



```
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. 46: Редактирование

Уязвимость WSO2 API-Manager RCE

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

```
user@wso2-virtual-machine:/opt/wso2am-4.0.0/repository/deployment/server$ cd web  
apps/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. 47: Удаление файла

Уязвимость WSO2 API-Manager RCE

Удалили сгенерированный файл /tmpp/payload.elf.

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

Рис. 48: Удаление файла

Уязвимость WSO2 API-Manager RCE

С помощью утилиты ss и команды kill закрыли meterpreter сессии.

```
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. 49: Закрытие meterpreter сессий

Уязвимость WSO2 API-Manager RCE

Зашли в веб-интерфейс WSO2 API-Manager по ссылке <https://10.10.2.27:9443/carbon> и авторизовались под учетной записью администратора.

The screenshot shows a web browser window for the WSO2 API-Manager Management Console at the URL <https://10.10.2.27:9443/carbon>. The browser status bar indicates "Not secure". The main page title is "Management Console". Below it are links for "Sign-in", "Docs", and "About". A "Help" link is also present. On the right side of the page is a "Sign-in" form. The "Username" field contains "admin" and the "Password" field contains "*****". There is a "Remember Me" checkbox and a "Sign-in" button. Below the sign-in form is a link "Sign-in Help". The left side of the page has some footer text about JIRA issues and suggestions.

Management Console

Sign-in | Docs | About

Help

Sign-in

Username: admin

Password: *****

Remember Me

Sign-in

Sign-in Help

ring information, questions and comments about WSO2 products.

& suggest improvements using the JIRA issue tracker. In addition,
orted issues in progress.

Уязвимость WSO2 API-Manager RCE

Просмотрели список пользователей.

Home > Users

Users

Search Users

Select Domain: ALL-USER-STORE-DOMAINS

Enter Username Pattern (* for all)

Select Claim URI: Select

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. 51: Пользователи

Уязвимость WSO2 API-Manager RCE

Удалили пользователя hacker.

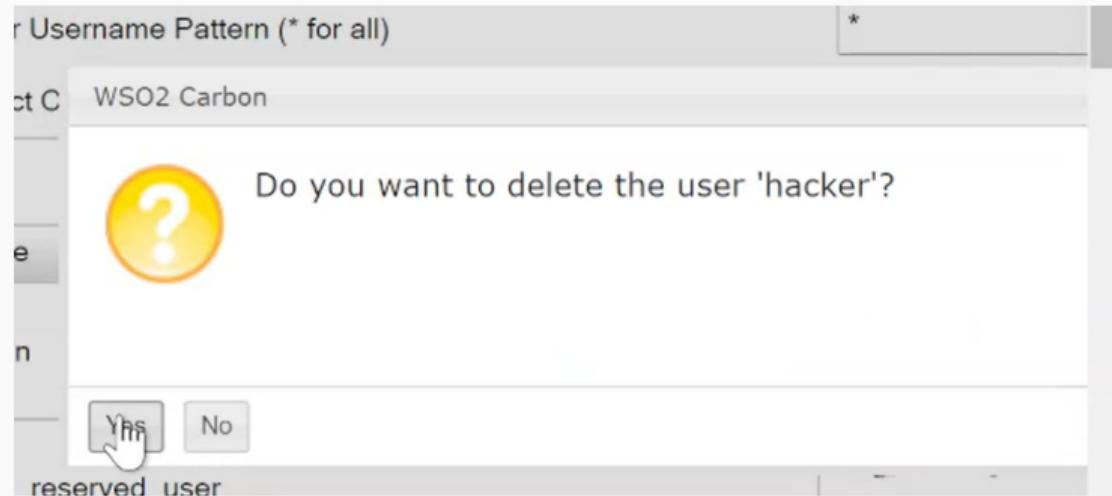


Рис. 52: Удаление пользователя

Уязвимость WSO2 API-Manager RCE

Уязвимость с ее последствием успешно устранены.

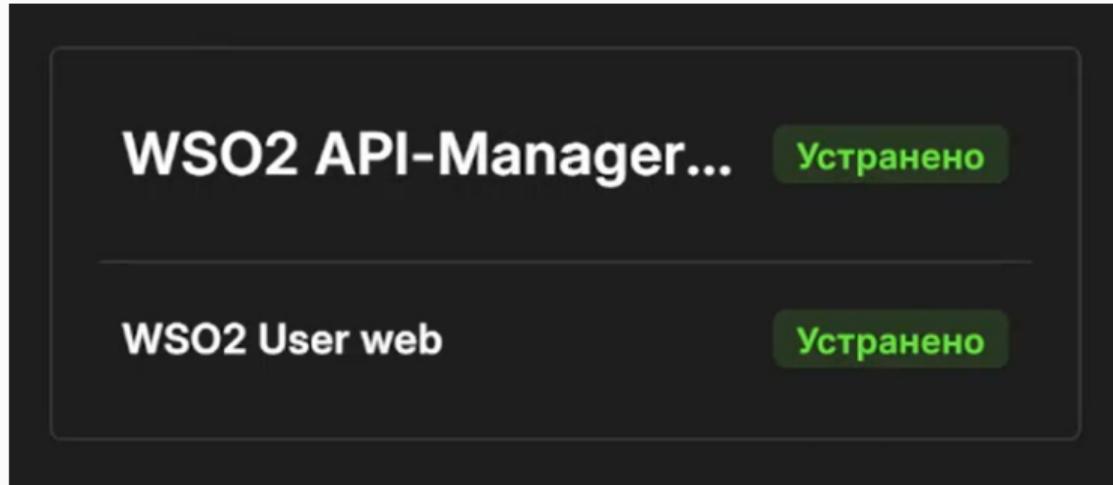


Рис. 53: Успех

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.