

Лабораторная работа №2

Создание презентации

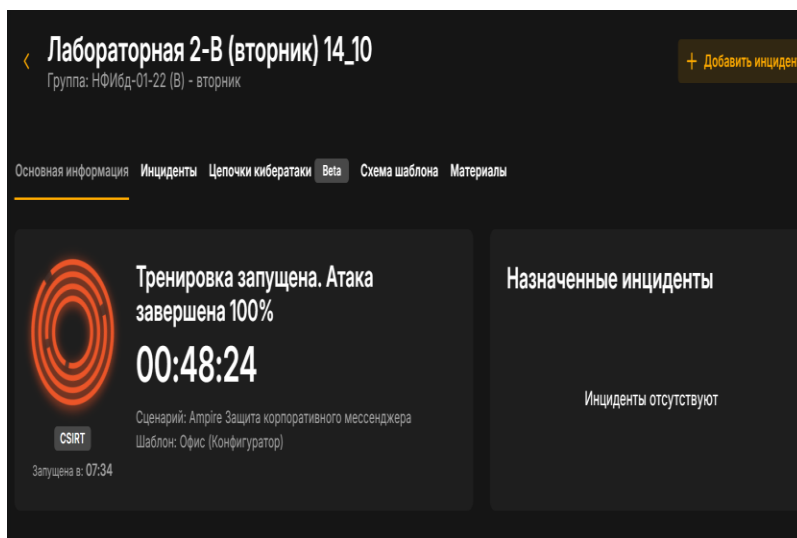
1 Цель работы

Пресекать действия нарушителя “Защита контроллера мессенджера” предназначена для использования в целях обучения и моделирования, тестирования безопасности, отработки реагирования на инциденты и демонстрации угроз в программном комплексе Ampire для обнаружения, анализа и устранения компьютерных атак.

2 Выполнение лабораторной работы

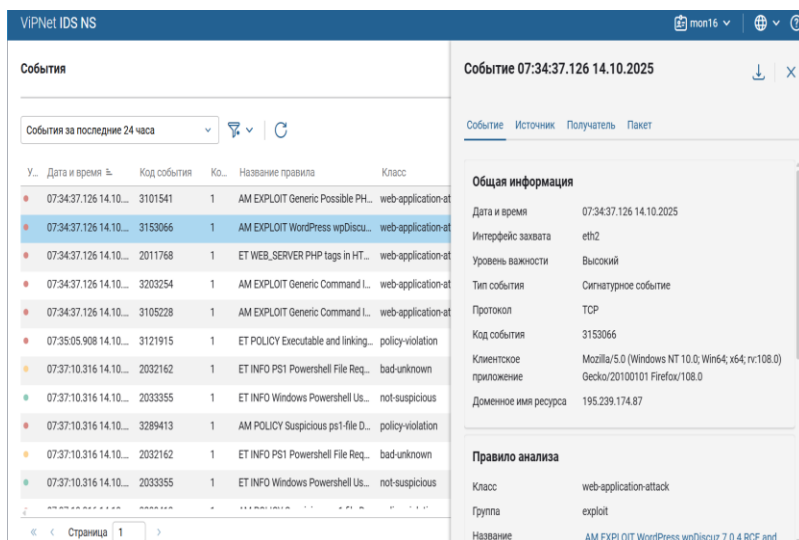
2.1 1. УЯЗВИМОГО УЗЛА WordPress «WPDISCUZ»

Уязвимость CVE-2020-24186 в плагине wpDiscuz для WordPress позволяет неавторизованным пользователям загружать файлы любого типа, включая PHP-файлы, через действие AJAX wmuUploadFiles. (рис. 1).



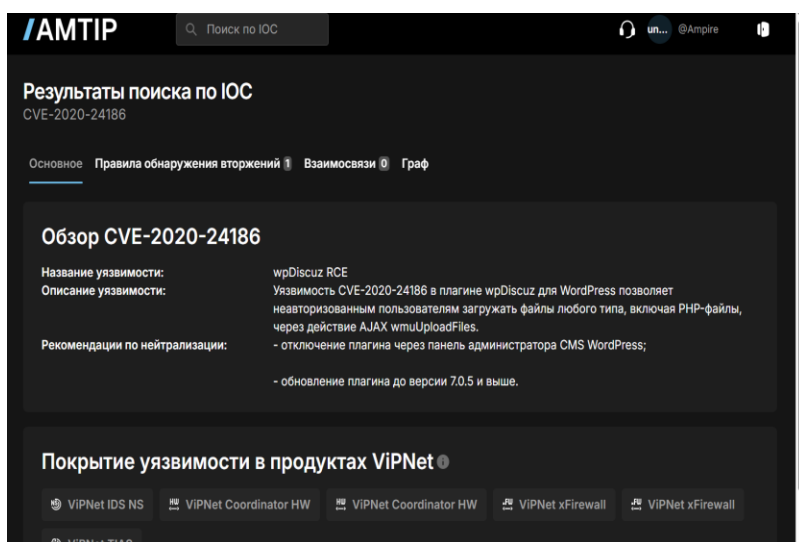
WordPress wpDiscuz

Мы нажали на “События” и установите “Для WordPress wpDiscuz” (как в инструкциях), начав просмотр времени немного раньше нашей атаки. (рис. 2).



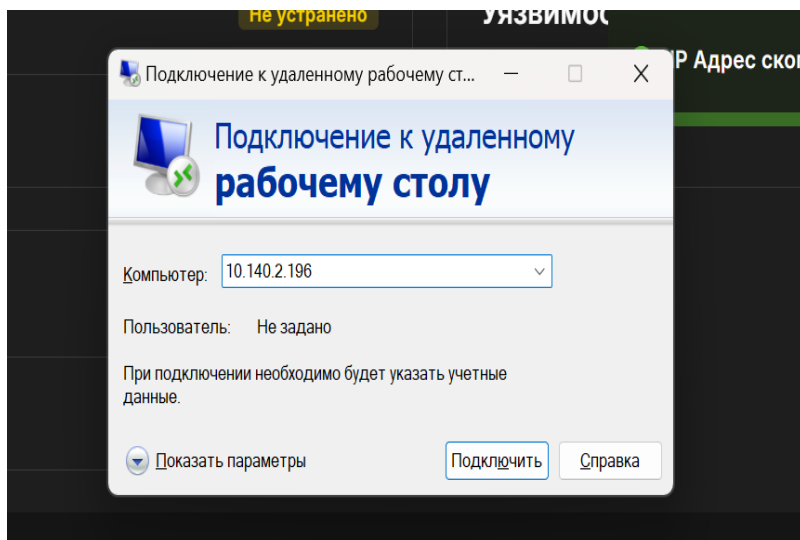
Применение фильтров и поиск WordPress wpDiscuz

Создаем карточку инцидента по WPDISCUZ (рис. 3).



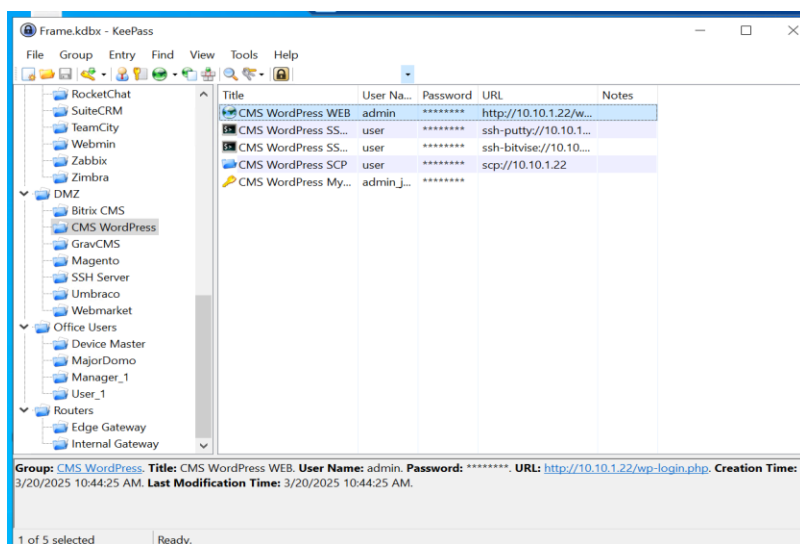
Создание карточки инцидента

Далее заходим на удаленный рабочий стол (рис. 4).



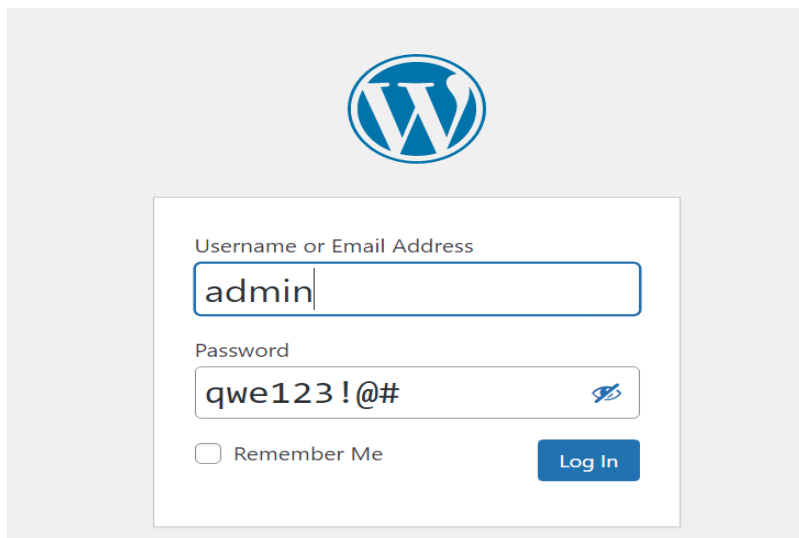
Вход на удаленный рабочий стол

Frame.kdbx - keepass, где находится логин в деталях для администратора CMS WordPress (рис. 5).



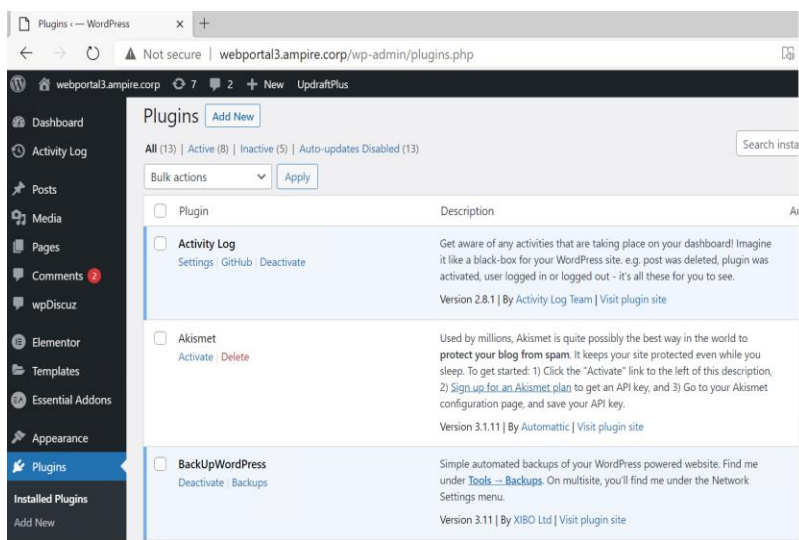
Frame.kdbx - keepass

Заходим не как user, а admin . Вводим следующие команды (рис. 6).



Поиск места уязвимого параметра

На веб-сервере работает ftp-сервер vsftpd, который дает возможность плагину Updraft сохранять и скачивать бэкап.(рис. 7).



Плагину

мы удалили wpDiscuz с веб-портала 3 ampire corp (рис. 9).



удалили wpDiscuz

Мы воспользовались уязвимостью с помощью панели управления. (рис. 10).

```
user@web-portal-3:~$ sudo ss -tnp
[sudo] password for user:
State      Recv-Q    Send-Q    Local Address:Port    Peer Address:Port
ESTAB      0          0          10.10.1.22:54000       195.239.174.11:1085
  users: ("chisel.sh",pid=1784,fd=11))
FIN-WAIT-2 0          0          10.10.1.22:41418       10.10.2.11:443
  users: ("chisel.sh",pid=1784,fd=16))
ESTAB      0          64          10.10.1.22:22          10.10.1.253:11067
  users: ("sshd",pid=11191,fd=3), ("sshd",pid=11121,fd=3))
ESTAB      0          0          10.10.1.22:22          10.10.1.253:22421
  users: ("sshd",pid=11120,fd=3), ("sshd",pid=11052,fd=3))
ESTAB      0          0          10.10.1.22:22          10.10.1.253:62477
  users: ("sshd",pid=11045,fd=3), ("sshd",pid=10972,fd=3))
CLOSE-WAIT 0          0          10.10.1.22:37744       195.239.174.11:5557
```

sudo ss -tnp

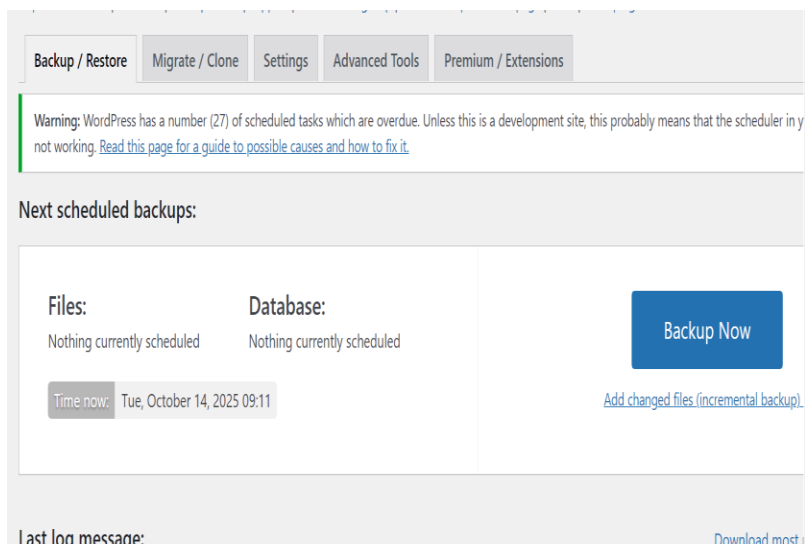
```

users: ("chisel.sh",pid=1784,fd=3), ("sh",pid=1785,fd=3), ("wifid",pid=1748,fd=3)
)
ESTAB      0      0      10.10.1.22:22      10.10.1.253:50321
users: ("sshd",pid=10962,fd=3), ("sshd",pid=10819,fd=3))
user@web-portal-3:~$ kill 1784
-bash: kill: (1784) - Operation not permitted
user@web-portal-3:~$ kill 1784
-bash: kill: (1784) - Operation not permitted
user@web-portal-3:~$ sudo kill 1784
user@web-portal-3:~$ sudo ss -tnp
State      Recv-Q  Send-Q      Local Address:Port      Peer Address:Port
FIN-WAIT-2  0        0      10.10.1.22:41418      10.10.2.11:443
ESTAB      0        64      10.10.1.22:22      10.10.1.253:11067 users: ("sshd",pid=11191,fd=3), ("sshd",pid=11120,fd=3), ("sshd",pid=11045,fd=3), ("sshd",pid=10972,fd=3))
ESTAB      0        0      10.10.1.22:22      10.10.1.253:22421 users: ("sshd",pid=11191,fd=3), ("sshd",pid=11120,fd=3), ("sshd",pid=11045,fd=3), ("sshd",pid=10972,fd=3))
ESTAB      0        0      10.10.1.22:22      10.10.1.253:62477 users: ("sshd",pid=11191,fd=3), ("sshd",pid=11120,fd=3), ("sshd",pid=11045,fd=3), ("sshd",pid=10972,fd=3))
CLOSE-WAIT 0        0      10.10.1.22:37744      195.239.174.11:5557 users: ("wifid",pid=1748,fd=12))
ESTAB      0        0      10.10.1.22:52524      195.239.174.11:5556 users: ("wifid",pid=1748,fd=3))
ESTAB      0        0      10.10.1.22:22      10.10.1.253:50321 users: ("sshd",pid=10962,fd=3), ("sshd",pid=10819,fd=3))
FIN-WAIT-2  0        0      [::ffff:10.10.1.22]:80 [::ffff:10.10.1.253]:12285
user@web-portal-3:~$ █

Last login: Tue Oct 14 08:57:25 2025 from 10.10.1.253
user@web-portal-3:~$ sudo ss -tnp
[sudo] password for user:
State      Recv-Q  Send-Q      Local Address:Port      Peer Address:Port
ESTAB      0        0      10.10.1.22:22      10.10.1.253:14742 users: ("sshd",pid=12189,fd=3), ("sshd",pid=12119,fd=3))
ESTAB      0        0      10.10.1.22:22      10.10.1.253:40767 users: ("sshd",pid=11764,fd=3), ("sshd",pid=11696,fd=3))
ESTAB      0        64      10.10.1.22:22      10.10.1.253:20857 users: ("sshd",pid=12260,fd=3), ("sshd",pid=12192,fd=3))
ESTAB      0        0      10.10.1.22:22      10.10.1.253:60367 users: ("sshd",pid=11615,fd=3), ("sshd",pid=11547,fd=3))
ESTAB      0        0      10.10.1.22:22      10.10.1.253:13680 users: ("sshd",pid=11523,fd=3), ("sshd",pid=11455,fd=3))
ESTAB      0        0      10.10.1.22:22      10.10.1.253:22421 users: ("sshd",pid=11120,fd=3), ("sshd",pid=11052,fd=3))
ESTAB      0        0      10.10.1.22:22      10.10.1.253:62477 users: ("sshd",pid=11045,fd=3), ("sshd",pid=10972,fd=3))
ESTAB      0        0      10.10.1.22:22      10.10.1.253:59512 users: ("sshd",pid=11692,fd=3), ("sshd",pid=11622,fd=3))
LAST-ACK   0        1      10.10.1.22:37744      195.239.174.11:5557
SYN-SENT   0        1      10.10.1.22:41330      195.239.174.125:8140 users: ("puppet",pid=11973,fd=24))
ESTAB      0        0      10.10.1.22:22      10.10.1.253:50321 users: ("sshd",pid=10962,fd=3), ("sshd",pid=10819,fd=3))
FIN-WAIT-20 0        0      [::ffff:10.10.1.22]:80 [::ffff:10.10.1.253]:6249
user@web-portal-3:~$ █

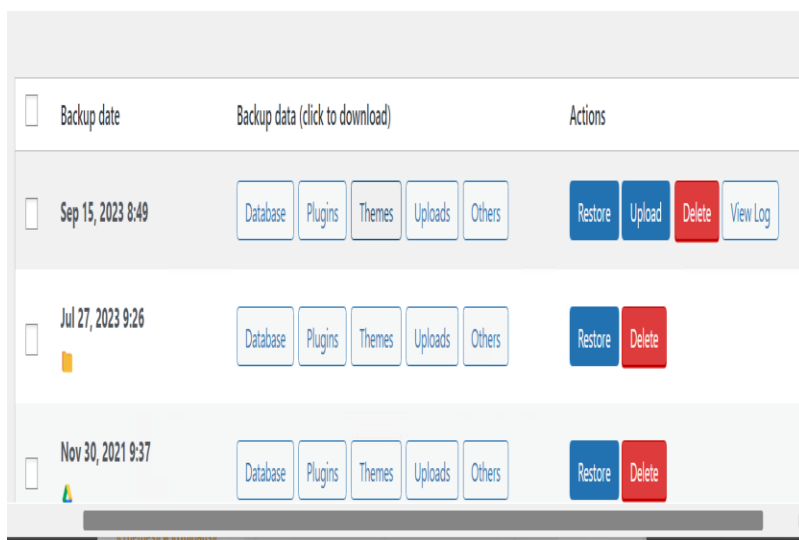
```

Мы выполнили восстановление из резервной копии последнего файла в Плагин UpdraftPlus в репозитории WordPress.(рис. 13).



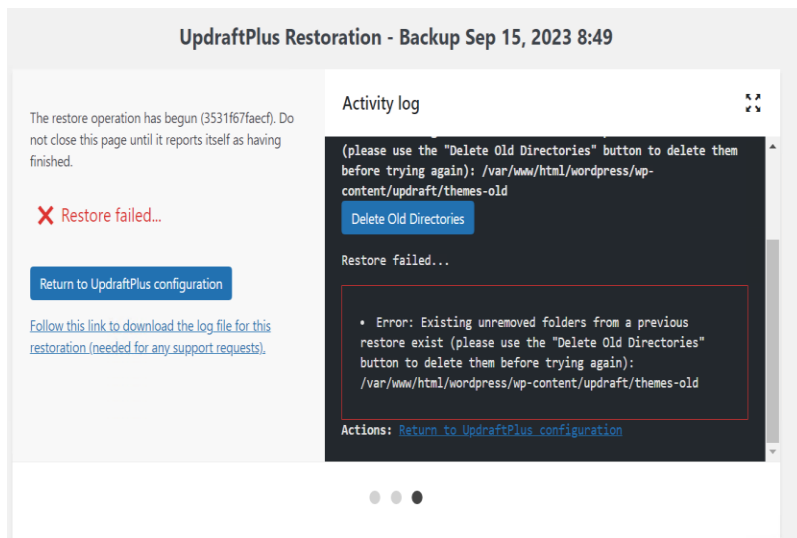
Backup

Мы нашли существующие резервные копии UpdraftPlus, затем выбрали только темы и загрузки в раскрывающемся списке выбора компонентов для восстановления.(рис. 14).



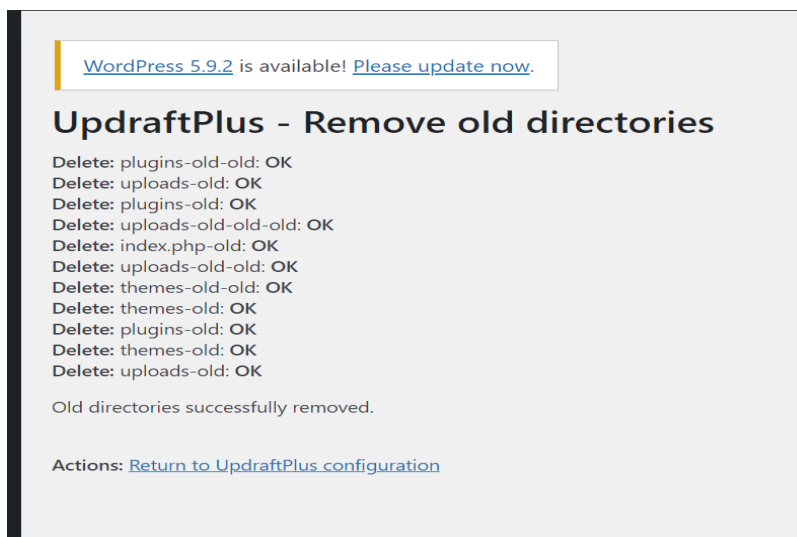
Существующие резервные копии UpdraftPlus

Затем мы нажали “Далее” и “Восстановить”, также столкнулись с ошибкой, нажали на опцию “Удалить старые каталоги” в журнале действий.(рис. 15).



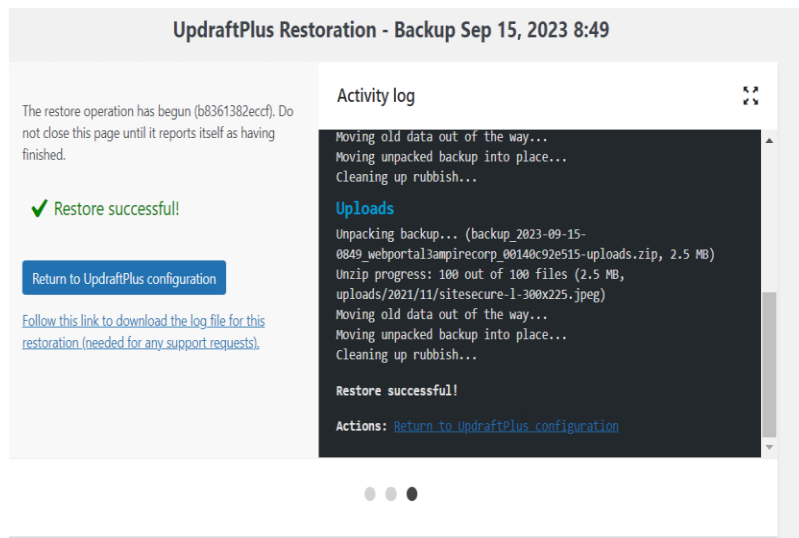
Ошибка восстановления

Из Updraftplus мы удалили старые каталоги.(рис. 16).



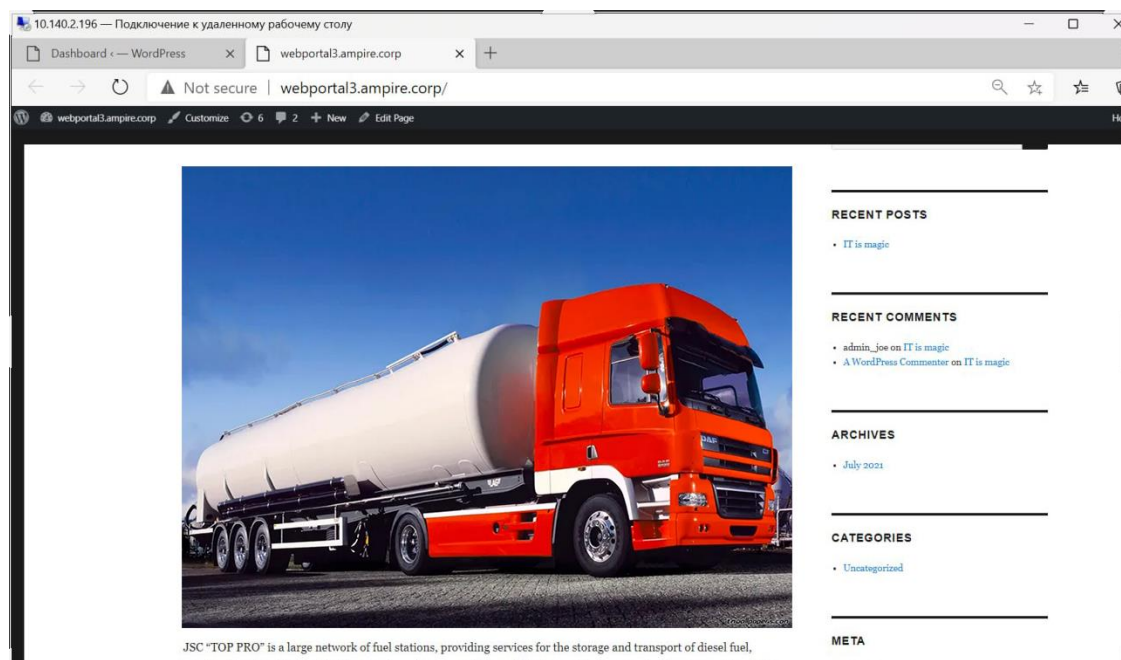
Remove old directories

Рестаурация была проведена успешно.(рис. 17).



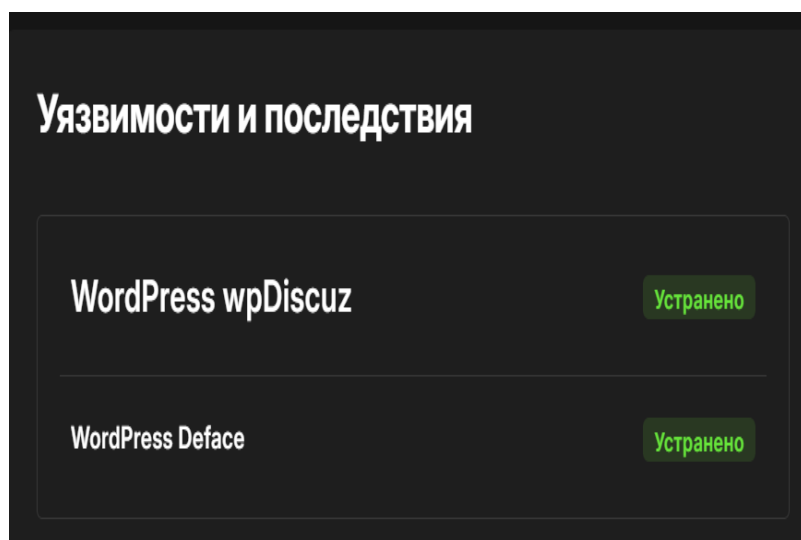
Успешное выполнение восстановления

После обновления страницы было открыто исходное изображение сайта.(рис. 18).



Обновленная страница сайта

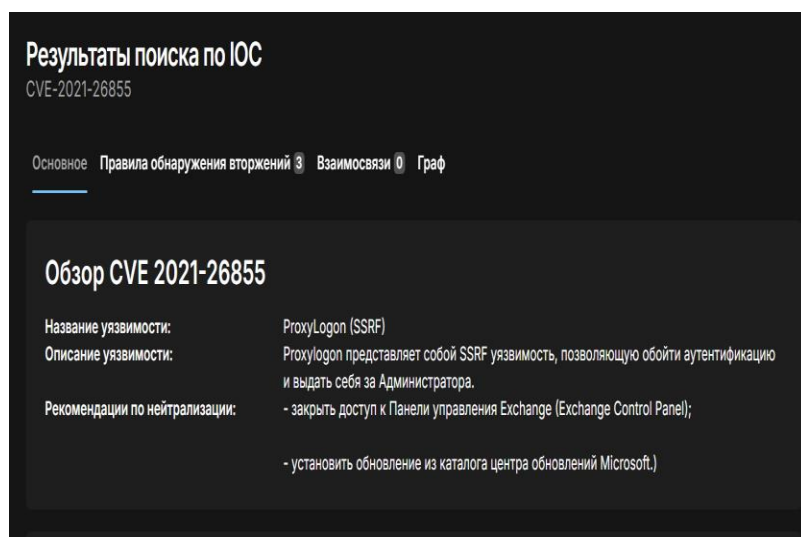
Уязвимости и последствия были исправлены, как показано на сайте ampire.(рис. 19).



устранено

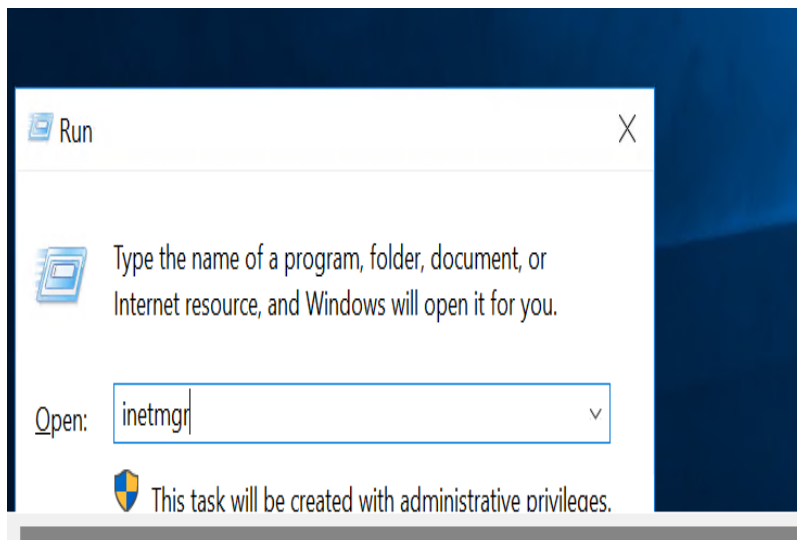
2.2 2. Proxylogon и (Exchange China Chopper)

Атака на почтовый сервер ProxyLogon(рис. 20).



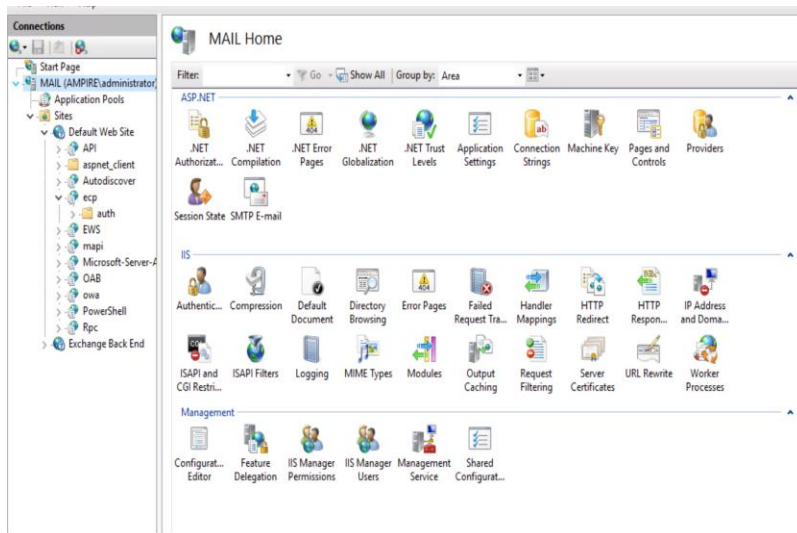
ProxyLogon

выбрав опцию WIN + “RUN”, мы ввели ярлык командной строки для IIS Manager, графического инструмента для настройки и управления информационными службами Интернета (IIS) на сервере Windows.(рис. 22).



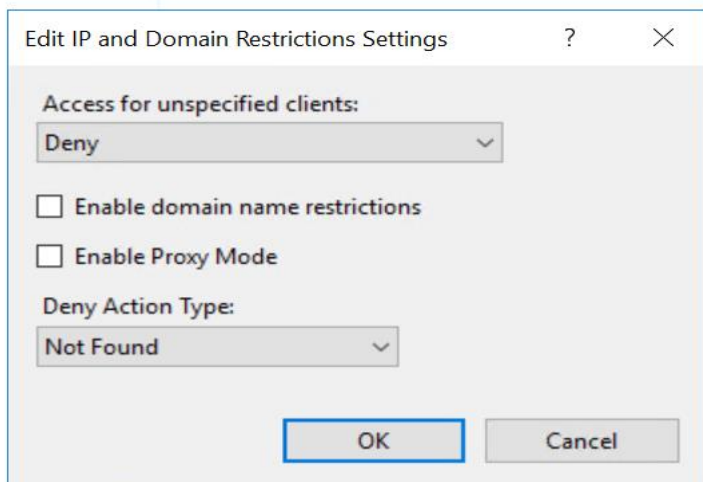
inetmgr

мы нашли почтовый ящик и страницу администрирования сайта.(рис. 23).



MAIL Home

Мы ограничили доступ для неуказанных клиентов в настройках ограничений домена.(рис. 24).



ограничений домена

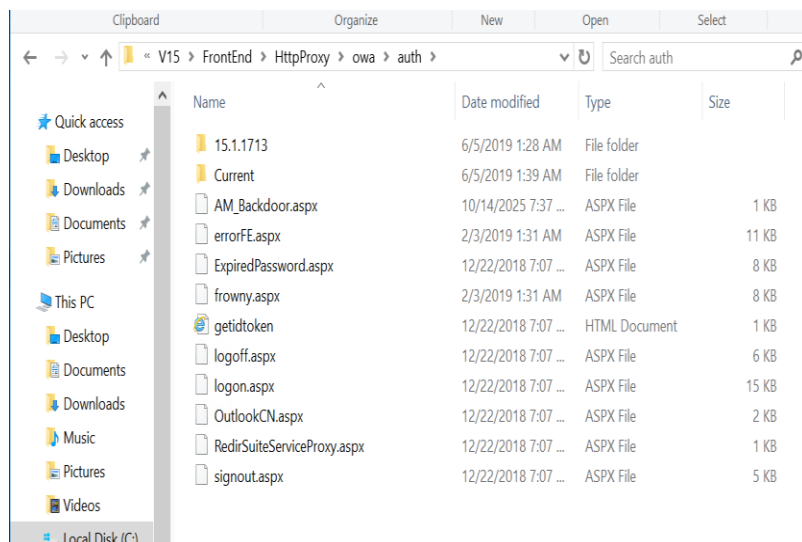
мы устранили последствия применения China Chopper.(рис. 25).

```
Administrator: Windows PowerShell
PS C:\Users\administrator.AMPIRE> netstat -b -o

Active Connections
Proto Local Address           Foreign Address         State       PID
TCP    10.10.2.11:443          10.10.1.22:41418       CLOSE_WAIT  4
Can not obtain ownership information
TCP    10.10.2.11:443          10.10.2.254:29963     ESTABLISHED  4
Can not obtain ownership information
TCP    10.10.2.11:3389         10.10.2.254:25866     ESTABLISHED  924
TermService
[svchost.exe]
TCP    10.10.2.11:6635         ad:msft-gc             ESTABLISHED  5248
[Microsoft.Exchange.ServiceHost.exe]
TCP    10.10.2.11:6659         ad:msft-gc             ESTABLISHED  5456
[MSEXchangeDelivery.exe]
TCP    10.10.2.11:6719         ad:msft-gc             ESTABLISHED  5132
[Microsoft.Exchange.RpcClientAccess.service.exe]
TCP    10.10.2.11:6742         ad:msft-gc             ESTABLISHED  6612
[Microsoft.Exchange.Imap4.exe]
TCP    10.10.2.11:6748         ad:msft-gc             ESTABLISHED  6676
[Microsoft.Exchange.Imap4.exe]
TCP    10.10.2.11:6824         ad:msft-gc             ESTABLISHED  9264
[Microsoft.Exchange.Store.Worker.exe]
TCP    10.10.2.11:6987         ad:msft-gc             ESTABLISHED  6812
[System]
TCP    10.10.2.11:7010         ad:msft-gc             ESTABLISHED  9912
[w3wp.exe]
TCP    10.10.2.11:7049         ad:ldap                ESTABLISHED  10332
[ForefrontActiveDirectoryConnector.exe]
TCP    10.10.2.11:7062         ad:msft-gc             ESTABLISHED  12080
[MSEXchangeHMWorker.exe]
TCP    10.10.2.11:7080         ad:msft-gc             ESTABLISHED  10976
[w3wp.exe]
TCP    10.10.2.11:7086         ad:ldap                ESTABLISHED  10976
[w3wp.exe]
TCP    10.10.2.11:7416         ad:ldap                ESTABLISHED  9912
[w3wp.exe]
```

Устранение последствияChina Chopper

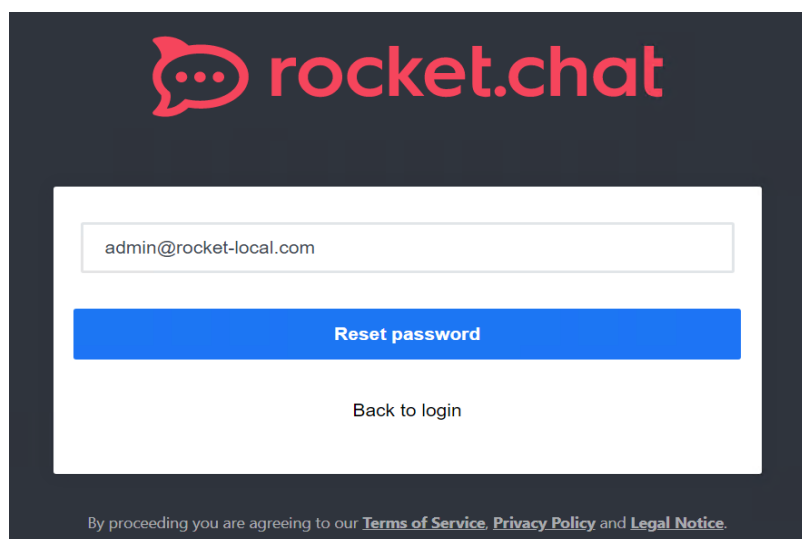
Файл am_backdoor был удален, и мы прекратили все сеансы связи с нарушителем..(рис. 26).



файл *AM_backdoor*

2.3 3. RocketChat RCE и (RocketChat meterpreter)

мы заходим в rockchat (рис. 27).



rocketchat

Пароль был сброшен, и в терминал была отправлена ссылка для сброса пароля.(рис. 28).

```
Failed to connect to https://changelogs.ubuntu.com/meta-release-lts. Check your
Internet connection or proxy settings
```

```
You have new mail.
```

```
admin@rocket-chat-server:~$ cd var/mail
```

```
-bash: cd: var/mail: No such file or directory
```

```
admin@rocket-chat-server:~$ cd /var/mail
```

```
admin@rocket-chat-server:/var/mail$ ls
```

```
admin user
```

Ссылка для сброса пароля

```
-----NmP-0131d624ad99580b-Part_1
```

```
Content-Type: text/plain
```

```
Content-Transfer-Encoding: quoted-printable
```

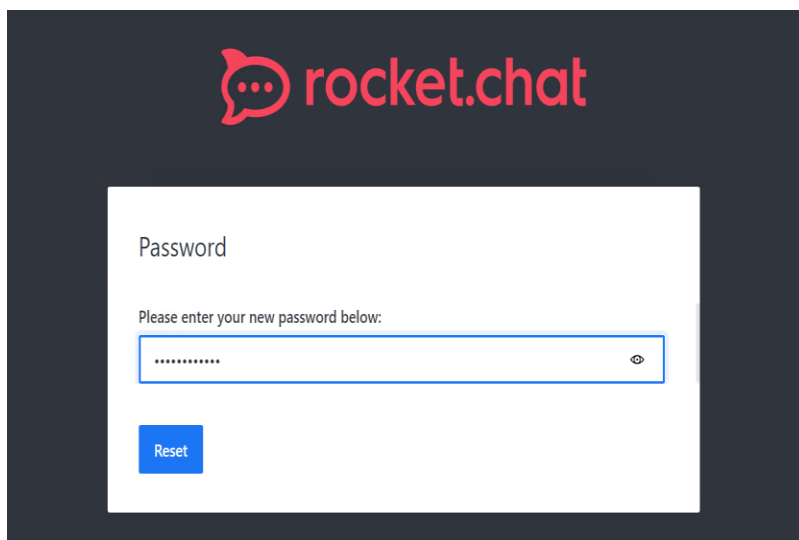
```
Hello,
```

```
To reset your password, simply click the link below.
```

```
http://10.10.2.22:3000/reset-password/0K_fHyNSqrbjSo06doLue_js9XgneI2bXEMrB=
uy9oJd
```

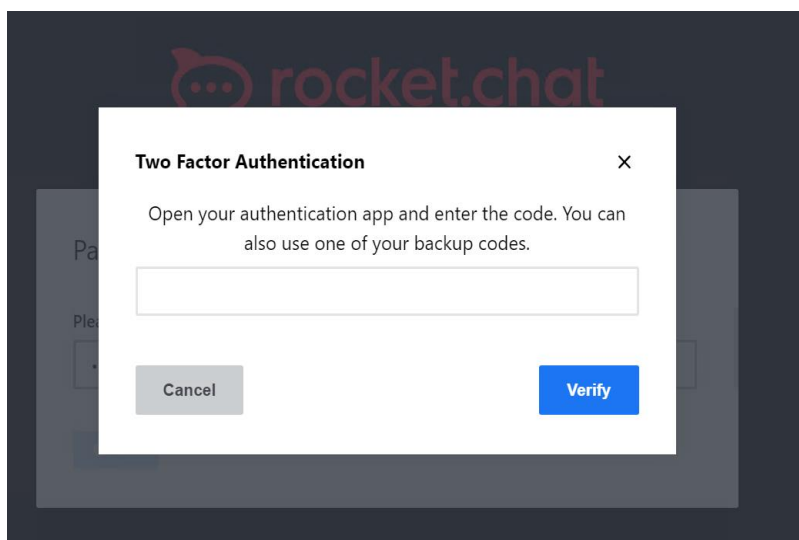
```
Thanks.
```

Ссылка для сброса пароля

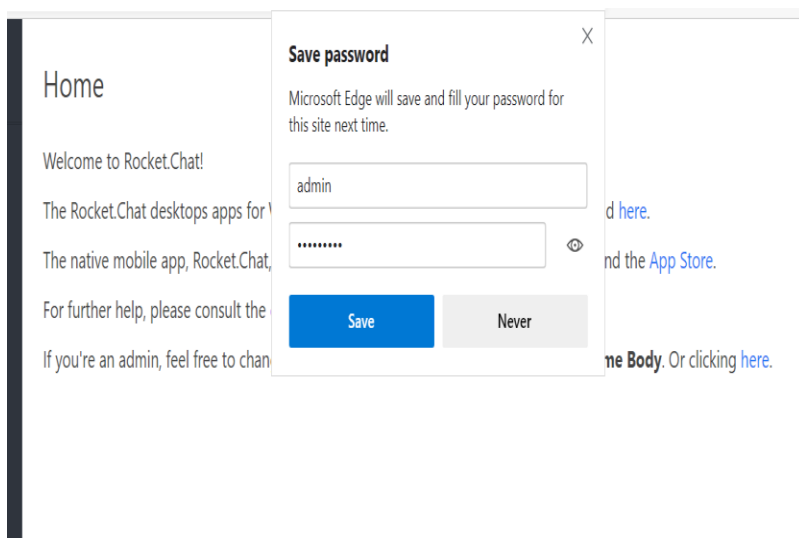


создание нового пароля

После этого TOTP был настроен для учетной записи администратора Rocket Chat для генерации одноразового пароля с помощью программы KeePass, которая была доступна на компьютере администратора.(рис. 32).

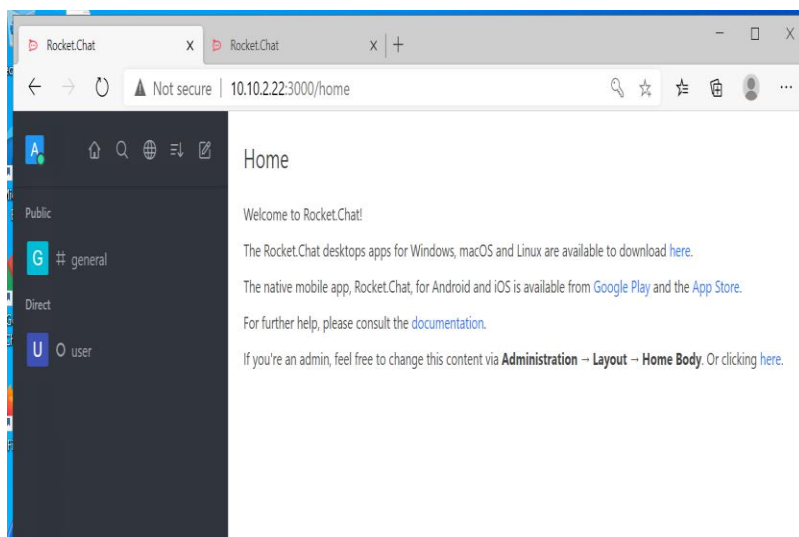


TOTP



TOTP

Мы успешно авторизовались на веб-сайте rocket chat. (рис. 34).



Rocketchat home

файла с одноразовыми кодами backup_codes. (рис. 35).

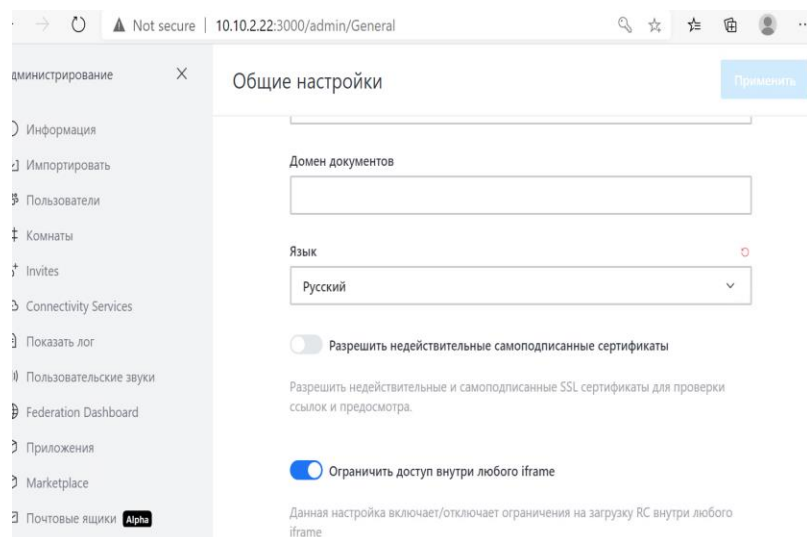

```

admin@rocket-chat-server:/home/user$ cat backup_codes
backup codes for admin Rocket Chat:
iF0DR6dy kpMfh9E 43ExiYom jhc4DGdw KiwwiGry LohP2b4A 9tiK2Sca THHC37gf mnPEZACy rdhc3y0B DvPHm0tz zZPyeKo2
admin@rocket-chat-server:/home/user$ ^C
admin@rocket-chat-server:/home/user$

```

backup_codes

Интерфейс RocketChat и настройка языка (рис. 36).



Интерфейс RocketChat

мы устранили уязвимость, изменив конфигурацию сервера, включив двухфакторную аутентификацию и право доступа, выбрав роль пользователя. (рис. 38).

Редактировать роль

Сохранено

Роль

user

Описание

Описание

Leave the description field blank if you dont want to show the role

Область

Общие

Пользователи должны использовать двухфакторную аутентификацию

Сохранить

Удалить

редактирующая роль

настройка автоматического подтверждения почты (рис. 49).

Учётные записи

Настройки обновлены

Префикс имени пользователя по умолчанию

user

Требуется имя для регистрации

Запрашивать подтверждение пароля

Подтверждение адреса электронной почты

Убедитесь, что у вас верные настройки SMTP для использования этой функции

Проверить электронную почту для внешних аккаунтов

Подтверждать новых пользователей вручную

Список разрешенных доменов

Список разрешенных доменов, разделенный запятыми

учётные записи

Настройка автоматической двухфакторной аутентификации по электронной почте для новых пользователей находится по пути «Администрирование» - «Учетные записи» - «Двухфакторная аутентификация. (рис. 51)

user

☒ Требуется имя для регистрации

☒ Запрашивать подтверждение пароля

☒ Подтверждение адреса электронной почты



Убедитесь, что у вас верные настройки SMTP для использования этой функции

учётные записи

Настройка автоматической двухфакторной аутентификации.(рис. 51)

для аутентификации пользователей действия, такие как вход в систему, изменение профиля и т.д.

☒ Автоматически настраивать двухфакторную аутентификацию по электронной почте для новых пользователей

У новых пользователей по умолчанию будет включена двухфакторная аутентификация по электронной почте. Они смогут отключить ее на странице своего профиля.

Время до истечения срока действия кода, отправленного по электронной почте, в секундах

учётные записи

мы отредактировали файл конфигурации базы данных /etc/mongod.conf, добавив строку javascriptEnabled: false. (рис. 53).

```

    enabled: true
    engine: wiredTiger
# mmapv1:
# wiredTiger:

# where to write logging data.
systemLog:
  destination: file
  logAppend: true
  path: /var/log/mongodb/mongod.log

# network interfaces
net:
  port: 27017
  bindIp: 127.0.0.1

# how the process runs
processManagement:
  timeZoneInfo: /usr/share/zoneinfo

#security: javascriptEnabled: false

#operationProfiling:

replication:
  replSetName: rs01

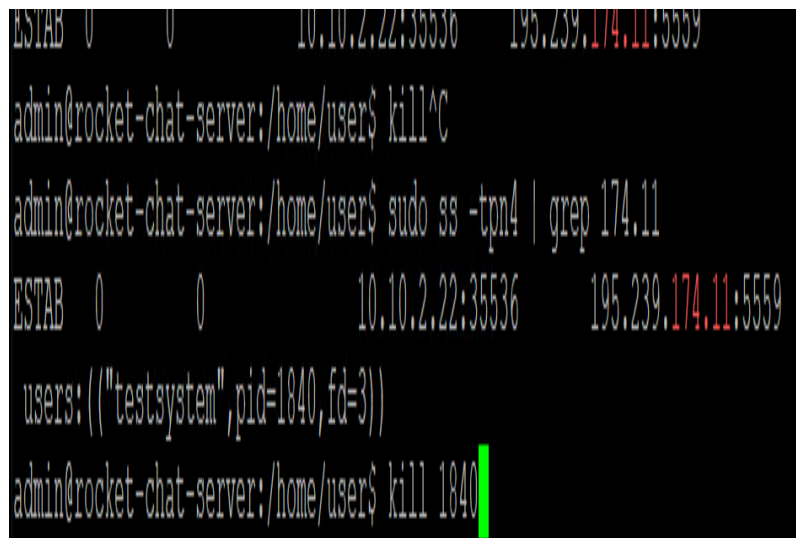
#sharding:

```

Line: 31/44 Column: 36 Encoding: 1252 (ANSI - L Modified)

Настройка конфигурации БД

Чтобы применить настройки, нам нужно было перезапустить службу: `sudo systemctl restart mongod.service` И закрыть сеанс с уничтожением нарушителя. (рис. 53).



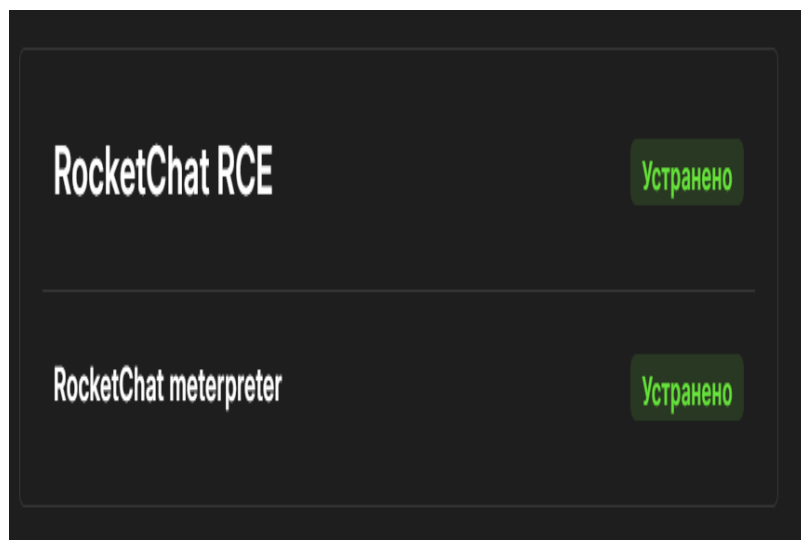
```

ESTAB 0 0 10.10.2.22:35536 195.239.174.11:5559
admin@rocket-chat-server:/home/user$ kill^C
admin@rocket-chat-server:/home/user$ sudo ss -tptn4 | grep 174.11
ESTAB 0 0 10.10.2.22:35536 195.239.174.11:5559
users: (("testsystem",pid=1840,fd=3))
admin@rocket-chat-server:/home/user$ kill 1840

```

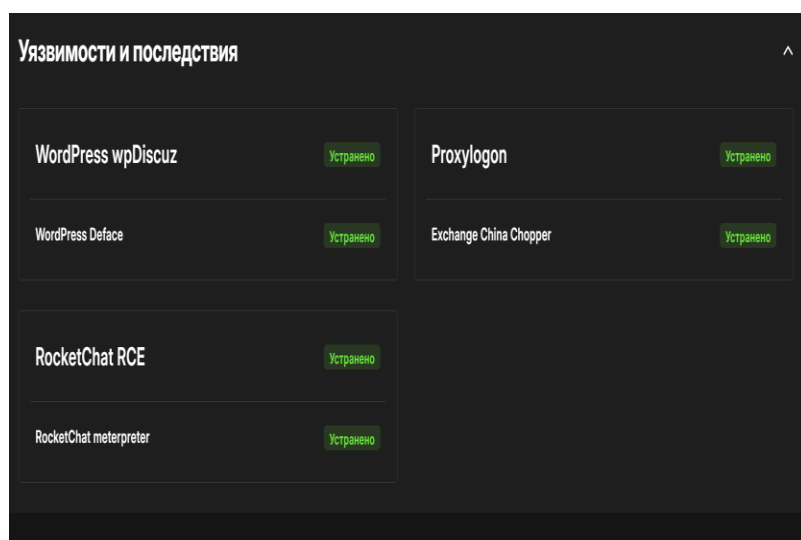
kill command

RocketChat RCE и RocketChat meterpreter были установлены. (рис. 59).



устранено

Все уязвимые места и последствия.(рис. 60).



устранено

Вся информация, касающаяся инцидентов. (рис. 61)

< wpDiscuz RCE

Основная информацияЧат

Дата и время события ⓘ
14.10.2025 07:34

Описание ⓘ
Уязвимость CVE-2020-24186 в плагине wpDiscuz для WordPress позволяет неавторизованным пользователям загружать файлы любого типа, включая PHP-файлы, через действие AJAX wmuUploadFiles.

Индикаторы компрометации ⓘ
Rule AM EXPLOIT WordPress wpDiscuz 7.0.4 RCE and Shell Upload (CVE-2020-24186)

Рекомендации ⓘ
- отключение плагина через панель администратора CMS WordPress; - обновление плагина до версии 7.0.5 и выше.

Прикреплённые файлы ⓘ
IDS_packet_time-2025-10-14T04_34_37126992Z_ruleid-3153066.pcap

Оценка
☆☆☆☆☆

Автор
АП Алади Принц Чисом
@1032225007@pfur.ru

Ответственный
ХА Хамдамова Айжана
@1032225989@pfur.ru

Источник
195.239.174.87

Поражённые активы
10.10.1.22

WordPress wpDiscuz

< WordPress Deface - последствие

Основная информацияЧат

Дата и время события ⓘ
14.10.2025 07:43

Описание ⓘ
Данная полезная нагрузка подразумевает изменение интерфейса главной страницы сайта.

Индикаторы компрометации ⓘ
AM EXPLOIT WordPress wpDiscuz 7.0.4 RCE and Shell Upload

Рекомендации ⓘ
1. сформировать резервную копию с помощью плагина, 2. осуществить возврат к конфигурации, активировать опцию

Прикреплённые файлы ⓘ
Не заполнено

Оценка
☆☆☆☆☆

Автор
ХА Хамдамова Айжана
@1032225989@pfur.ru

Ответственный
ОК Оширова Юлия
@1132222843@pfur.ru

Источник
195.239.174.11

Поражённые активы
10.10.1.22

WordPress Deface

< Proxylogon

Основная информацияЧат

Дата и время события ⓘ
14.10.2025 07:34

Описание ⓘ
Proxylogon представляет собой SSRF уязвимость, позволяющую обойти аутентификацию и выдать себя за Администратора.

Индикаторы компрометации ⓘ
AM EXPLOIT SSRF in Microsoft Exchange Server (CVE-2021-26855) var 4

Рекомендации ⓘ
- закрыть доступ к Панели управления Exchange (Exchange Control Panel); - установить обновление из каталога центра обновлений Microsoft.)

Прикреплённые файлы ⓘ
IDS_packet_time-2025-10-14T09_35_05.846671Z_ruleid-2012843.pcap

Оценка
☆☆☆☆☆

Автор
Алади Принц Чисом
@1032225007@pfur.ru

Ответственный
Тимофеева Екатерина
@1132226446@pfur.ru

Источник
195.239.174.11

Поражённые активы
10.10.2.11

Proxylogon

< Exchange China Chopper - последствие

Основная информацияЧат

Дата и время события ⓘ
14.10.2025 07:42

Описание ⓘ
Подделка запроса на стороне сервера. В директории скрытан атакующий файл

Индикаторы компрометации ⓘ
AM EXPLOIT Arbitrary File Write in Microsoft Exchange

Рекомендации ⓘ
1. удалить файл веб-оболочки 2. завершить все соединения между уязвимой машиной и нарушителем

Прикреплённые файлы ⓘ

Оценка
☆☆☆☆☆

Автор
Хамдамова Айжана
@1032225989@pfur.ru

Ответственный
Сидорова Наталья
@1132228432@pfur.ru

Источник
195.239.174.11

Поражённые активы
10.10.2.11

Exchange China Chopper

< RocketChat

Основная информация Чат

Дата и время события ⓘ
14.10.2025 07:34

Описание ⓘ
CVE-2021-22911 представляет собой две уязвимости NoSQL Injection, эксплуатация которых может позволить злоумышленникам повысить свои привилегии, выполнить произвольные системные команды на хост-сервере и украсть конфиденциальные пользовательские данные и сообщения чата. Обе уязвимости исправлены в версии 3.13.2 и перенесены в старые ветки в версиях 3.12.4 и 3.11.4

Индикаторы компрометации ⓘ
AM EXPLOIT Token BruteForce in RocketChat 3.12.1: via NoSQL injection in 'getPasswordPolicy' (CVE-2021-22911)

Рекомендации ⓘ
- обновление версии «RocketChat»; - запрет выполнения JavaScript на стороне сервера БД.

Прикреплённые файлы ⓘ
IDS_packet_time-2025-10-14T04_34_37126992Z_ruleid-3101541.pcap

Оценка
☆☆☆☆

Автор
Алади Принц Чисом
@1032225007@pfur.ru

Ответственный
Алади Принц Чисом
@1032225007@pfur.ru

Источник
195.239.174.11

Поражённые активы
10.10.2.22

RocketChat RCE

< RocketChat meterpreter - последствие

Основная информация Чат

Дата и время события ⓘ
14.10.2025 07:40

Описание ⓘ
Уязвимость представляет собой сочетание из двух SQL инъекций. Слепая NoSQL-инъекция (позволяет украсть токен сброса пароля пользователя). И повышение привилегий.

Индикаторы компрометации ⓘ
AM EXPLOIT Token BruteForce in RocketChat 3.12.1: via NoSQL injection in 'getPasswordPolicy'

Рекомендации ⓘ
1. отключить выполнение JavaScript кода на стороне сервера БД, 2. Перезапустить службу. 3. Закрыть сессию с нарушителем

Прикреплённые файлы ⓘ
Не заполнено

Оценка
☆☆☆☆

Автор
Хамдамова Айжана
@1032225969@pfur.ru

Ответственный
Пронякова Ольга
@1132226453@pfur.ru

Источник
195.239.174.11

Поражённые активы
10.10.2.22

RocketChat meterpreter

Выводы

В ходе данной лабораторной работы нам удалось устранить действия нарушителя “Сетевого датчика аппаратно-программного комплекса системы обнаружения атак ViPNet”, а также выполнить последствия для каждой уязвимости.