

Лабораторная работа № 1-Д

Защита корпоративного мессенджера

Доберштейн А. С., Оразгелдиев Я. О., Барабанова К. А.

Российский университет дружбы народов, Москва, Россия

Информация

Докладчик

- Доберштейн А. С., Оразгелдиев Я. О., Барабанова К. А.
- НФИбд-02-22
- Российский университет дружбы народов

Цель работы

Основной целью работы является получение навыков обнаружения и устранение уязвимостей WordPress-wpDiscuz, Proxylogon, Rocket.Chat и их последствий.

Выполнение лабораторной работы

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



Рис. 1: Вектор атаки

Уязвимость WordPress-wpDiscuz

Залогинились в ViPNet для обнаружения уязвимости в журнале событий.



Уязвимость WordPress-wpDiscuz

В “Событиях” обнаружили событие AM Exploit Wordpress с программным кодом, предназначенным для эксплуатации уязвимости

Рис. 3: Журнал событий

Уязвимость WordPress-wpDiscuz

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

Результаты поиска по IOC
CVE-2020-24186

Основное Правила обнаружения вторжений 1 Взаимосвязи 0 Граф

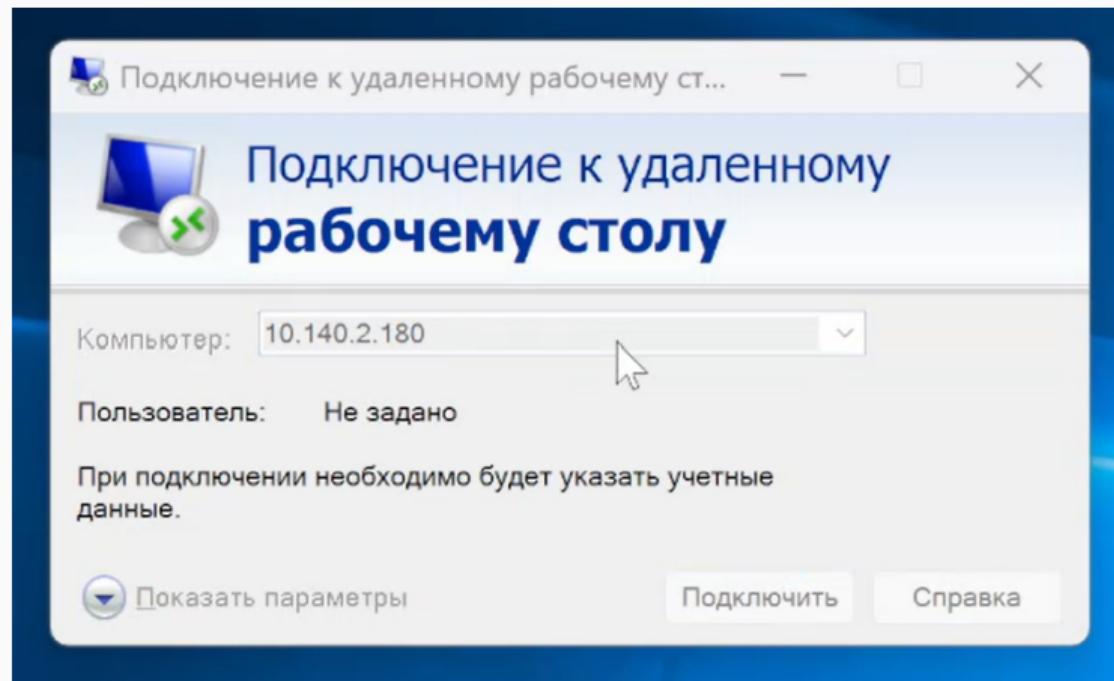
Обзор CVE-2020-24186

Название уязвимости: wpDiscuz RCE
Описание уязвимости: Уязвимость CVE-2020-24186 в плагине wpDiscuz для WordPress позволяет неавторизованным пользователям загружать файлы любого типа, включая PHP-файлы, через действие AJAX wmuUploadFiles.
Рекомендации по нейтрализации:
- отключение плагина через панель администратора CMS WordPress;
- обновление плагина до версии 7.0.5 и выше.

Рис. 4: Обзор уязвимости

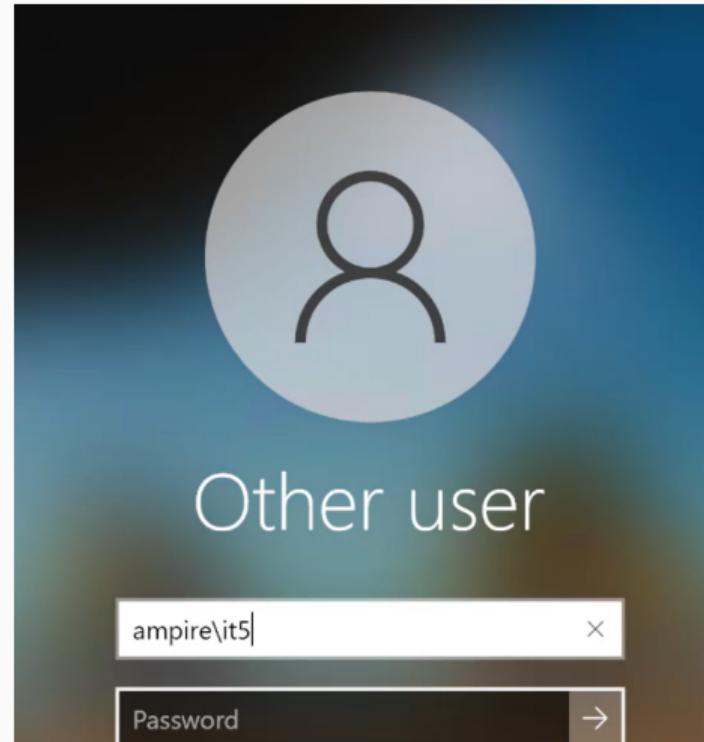
Уязвимость WordPress-wpDiscuz

Для устранения уязвимости подключились к удаленному рабочему столу по адресу 10.140.2.180



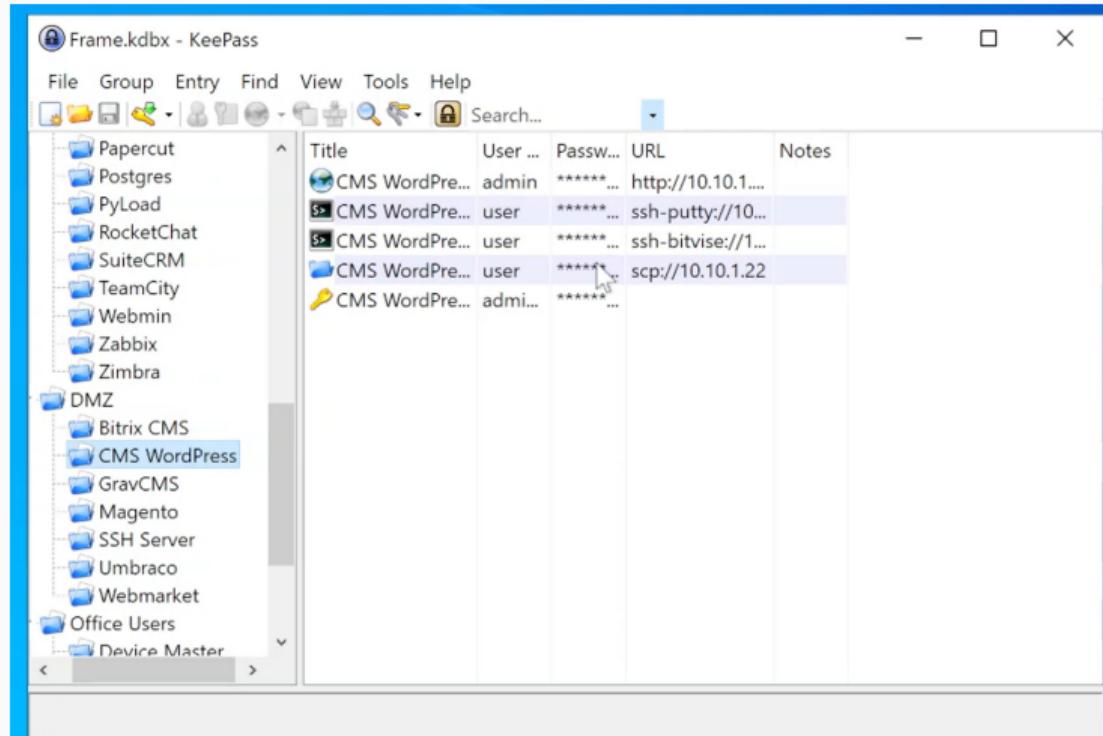
Уязвимость WordPress-wpDiscuz

Вошли под указанной учетной записью.



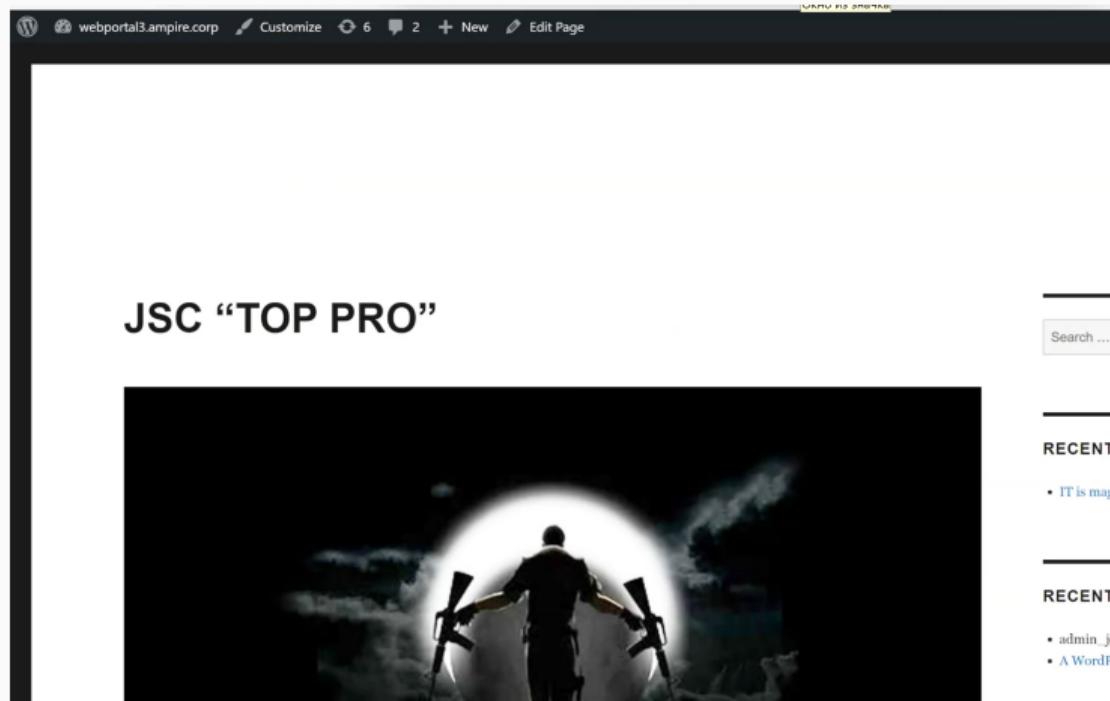
Уязвимость WordPress-wpDiscuz

В соответствии с вектором атаки в KeePass нашли CMS WordPress.



Уязвимость WordPress-wpDiscuz

Просмотрели сайт WordPress по указанному адресу. Здесь обнаружили последствие - Deface - изменение внешнего вида интерфейса.



Уязвимость WordPress-wpDiscuz

В панели администрирования перешли во вкладку с плагинами и деактивировали плагин wpDiscuz



Рис. 9: Плагин wpDiscuz

Уязвимость WordPress-wpDiscuz

Для того, чтобы устраниТЬ последствие Deface, необходимо откатить сайт до предыдущей резервной копии. Для этого перешли в панель администрации и во вкладке с плагинами нашли плагин UpdraftPlus - Backup/Restore, перешли в “Settings”.

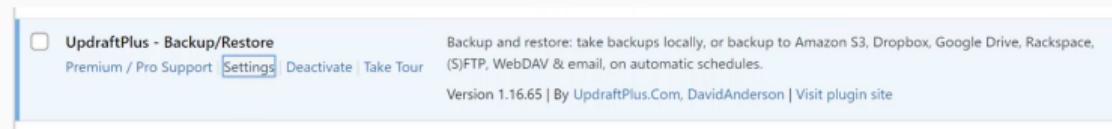


Рис. 10: Плагин UpdraftPlus - Backup/Restore

Уязвимость WordPress-wpDiscuz

Выбрали последнюю резервную копию и нажали “Restore”.

The screenshot shows the 'Existing backups' section of the UpdraftPlus plugin. It displays two backup entries:

<input type="checkbox"/>	Backup date	Backup data (click to download)	Actions
<input type="checkbox"/>	Sep 15, 2023 8:49	Database Plugins Themes Uploads Others	Restore
<input type="checkbox"/>	Jul 27, 2023 9:26	Database Plugins Themes Uploads Others	Restore

Рис. 11: Restore

Уязвимость WordPress-wpDiscuz

Поставили флагки у компонентов “Themes” и “Uploads”.

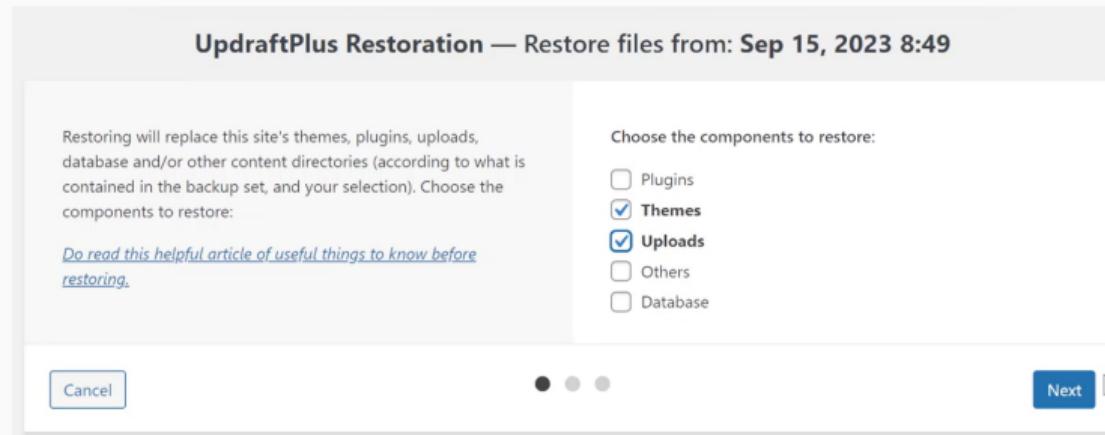


Рис. 12: Параметры восстановления

Уязвимость WordPress-wpDiscuz

Во всплывшем окне с ошибкой нажали “Удалить старые директории”

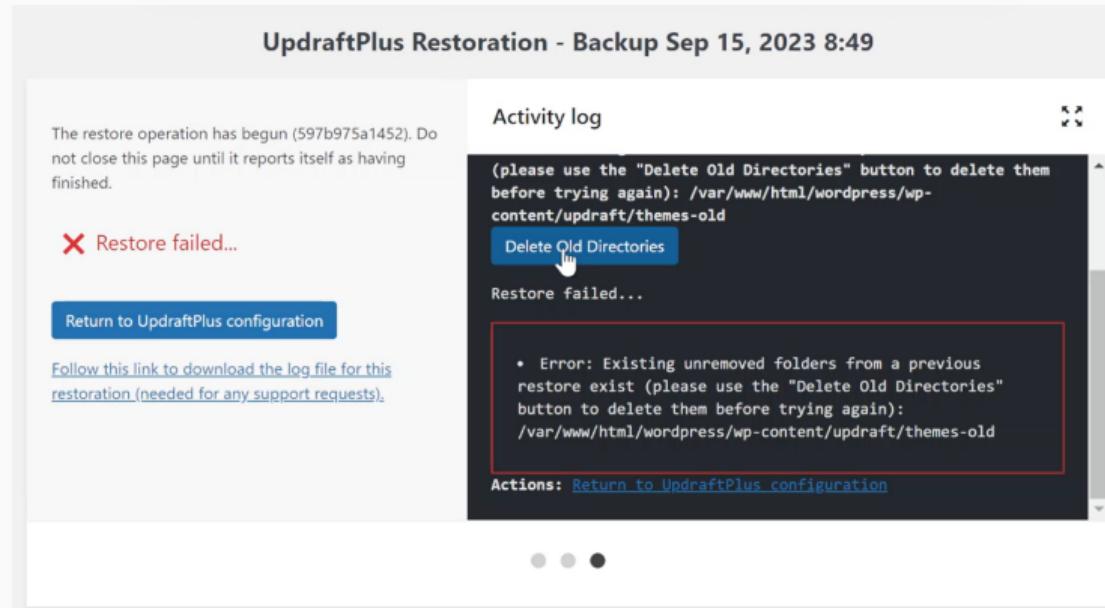


Рис. 13: Удаление старых директорий

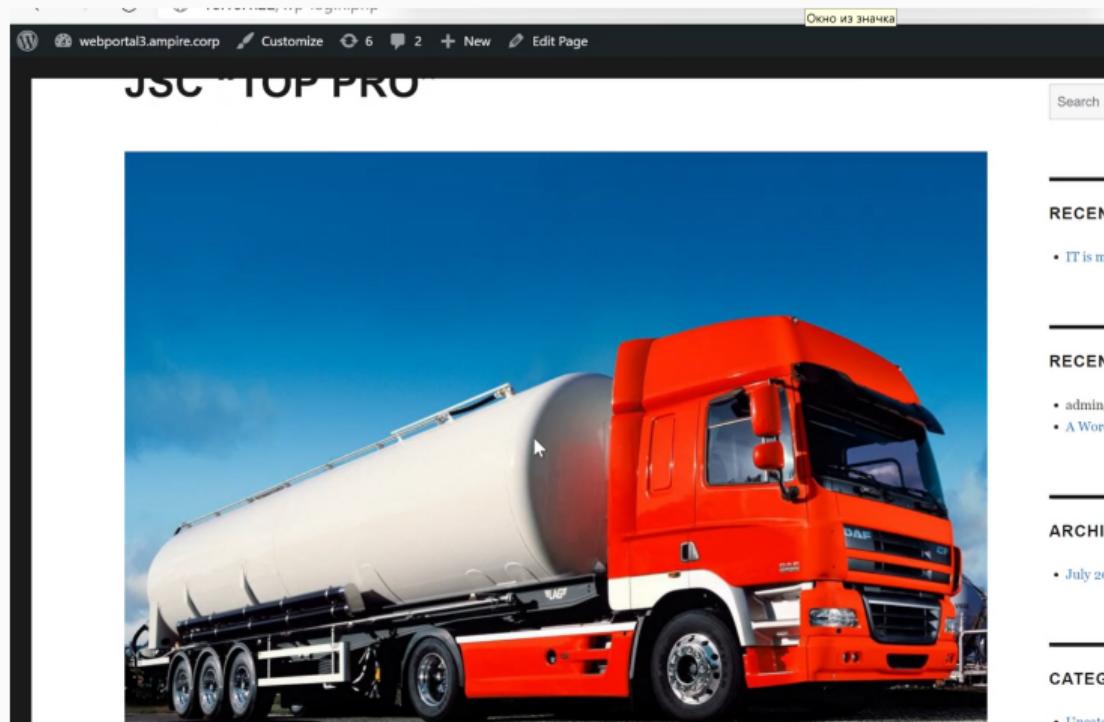
Уязвимость WordPress-wpDiscuz

Когда директории удалились, нажали “Return to UpdraftPlus configuration”

The screenshot shows a web interface for UpdraftPlus. At the top, there is a yellow banner with the text "WordPress 5.9.2 is available! [Please update now.](#)". Below the banner, the title "UpdraftPlus - Remove old directories" is displayed. A list of directory deletions is shown, each followed by the status "OK":
Delete: plugins-old-old: OK
Delete: uploads-old: OK
Delete: plugins-old: OK
Delete: uploads-old-old-old: OK
Delete: index.php-old: OK
Delete: uploads-old-old: OK
Delete: themes-old-old: OK
Delete: themes-old: OK
Delete: plugins-old: OK
Delete: themes-old: OK
Delete: uploads-old: OK
At the bottom, a message states "Old directories successfully removed."

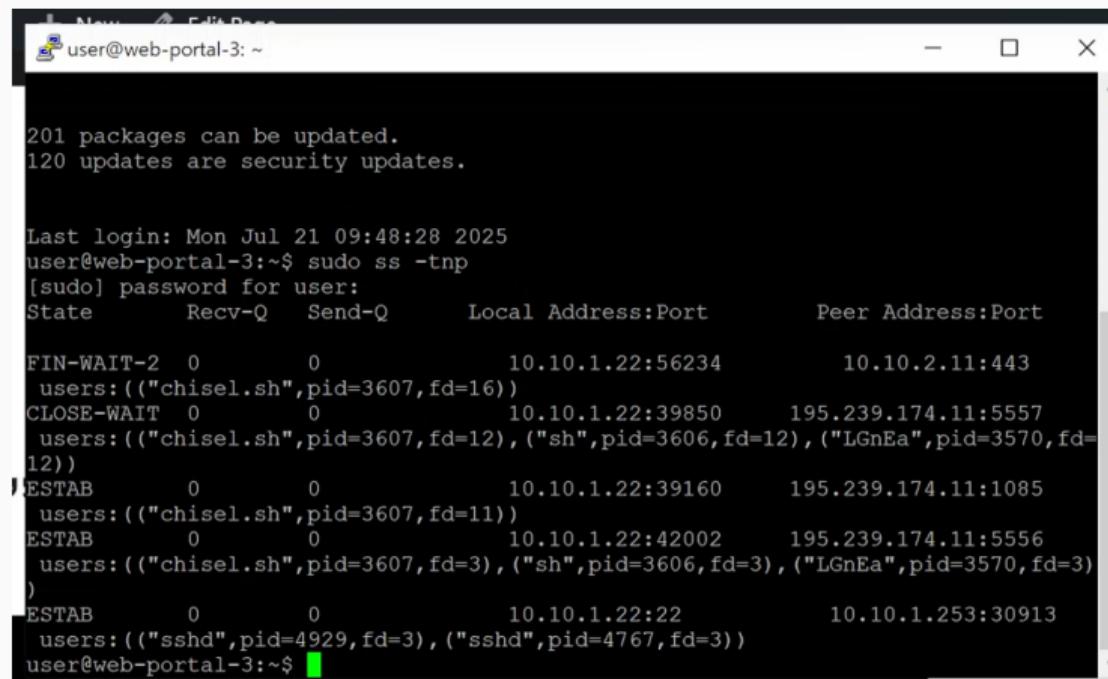
Уязвимость WordPress-wpDiscuz

Обновили страницу сайта. Убедились, что последствие Deface успешно устранено.



Уязвимость WordPress-wpDiscuz

Перешли в Putty web-portal, чтобы проверить сокеты на наличие подозрительных процессов с помощью утилиты ss.



```
user@web-portal-3: ~
201 packages can be updated.
120 updates are security updates.

Last login: Mon Jul 21 09:48:28 2025
user@web-portal-3:~$ sudo ss -tnp
[sudo] password for user:
State      Recv-Q      Send-Q      Local Address:Port      Peer Address:Port
FIN-WAIT-2    0          0          10.10.1.22:56234      10.10.2.11:443
users:(("chisel.sh",pid=3607,fd=16))
CLOSE-WAIT    0          0          10.10.1.22:39850      195.239.174.11:5557
users:(("chisel.sh",pid=3607,fd=12),("sh",pid=3606,fd=12),("LGN Ea",pid=3570,fd=12))
ESTAB        0          0          10.10.1.22:39160      195.239.174.11:1085
users:(("chisel.sh",pid=3607,fd=11))
ESTAB        0          0          10.10.1.22:42002      195.239.174.11:5556
users:(("chisel.sh",pid=3607,fd=3),("sh",pid=3606,fd=3),("LGN Ea",pid=3570,fd=3))
ESTAB        0          0          10.10.1.22:22          10.10.1.253:30913
users:(("sshd",pid=4929,fd=3),("sshd",pid=4767,fd=3))
user@web-portal-3:~$
```

Уязвимость WordPress-wpDiscuz

Уничтожили вредоносные соединения с помощью команды kill {pid}. Убедились в их отсутствии.

```
user@web-portal-3:~$ sudo kill 3607
user@web-portal-3:~$ sudo ss -tnp
State      Recv-Q Send-Q      Local Address:Port          Peer Address:Port
FIN-WAIT-2 0          0          10.10.1.22:56234        10.10.2.11:443
CLOSE-WAIT 0          0          10.10.1.22:39850        195.239.174.11:5557
users:(("LGnEa",pid=3570,fd=12))
ESTAB     0          0          10.10.1.22:42002        195.239.174.11:5556
users:(("LGnEa",pid=3570,fd=3))
ESTAB     0          64         10.10.1.22:22          10.10.1.253:30913
users:(("sshd",pid=4929,fd=3),("sshd",pid=4767,fd=3))
FIN-WAIT-2 0          0          [:ffff:10.10.1.22]:80    [:ffff:10.10.1.253]:45442

user@web-portal-3:~$ sudo kill 3570
user@web-portal-3:~$
```

Рис. 17: Уничтожение вредоносных процессов

Уязвимость WordPress-wpDiscuz

Первая уязвимость с ее последствием успешно устранены

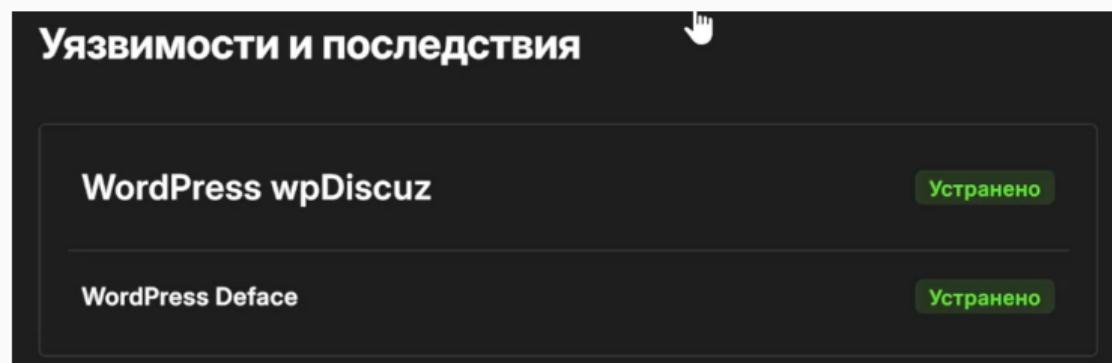


Рис. 18: Успех

Уязвимость Proxylogon

Вернулись в ViPNet для обнаружения подозрительной активности в журнале событий.

16:33.807 29....	2025644	1	ET TROJAN Possible Metas...	trojan-activity
16:33.807 29....	2025644	1	ET TROJAN Possible Metas...	trojan-activity
16:33.804 29....	2035480	1	ET INFO PE EXE Download ...	misc-activity
16:33.804 29....	2035480	1	ET INFO PE EXE Download ...	misc-activity

Рис. 19: Журнал событий

Уязвимость Proxylogon

Изучили информацию об обнаруженной уязвимости.

Результаты поиска по IOC
CVE-2021-26855

Основное Правила обнаружения вторжений 3 Взаимосвязи 0 Граф

Основное

Метрики CVSS версии 3.1

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 03.03.2021 03:15 Последнее изменение NVD 03.03.2021 03:15

Описание Microsoft Exchange Server Remote Code Execution Vulnerability

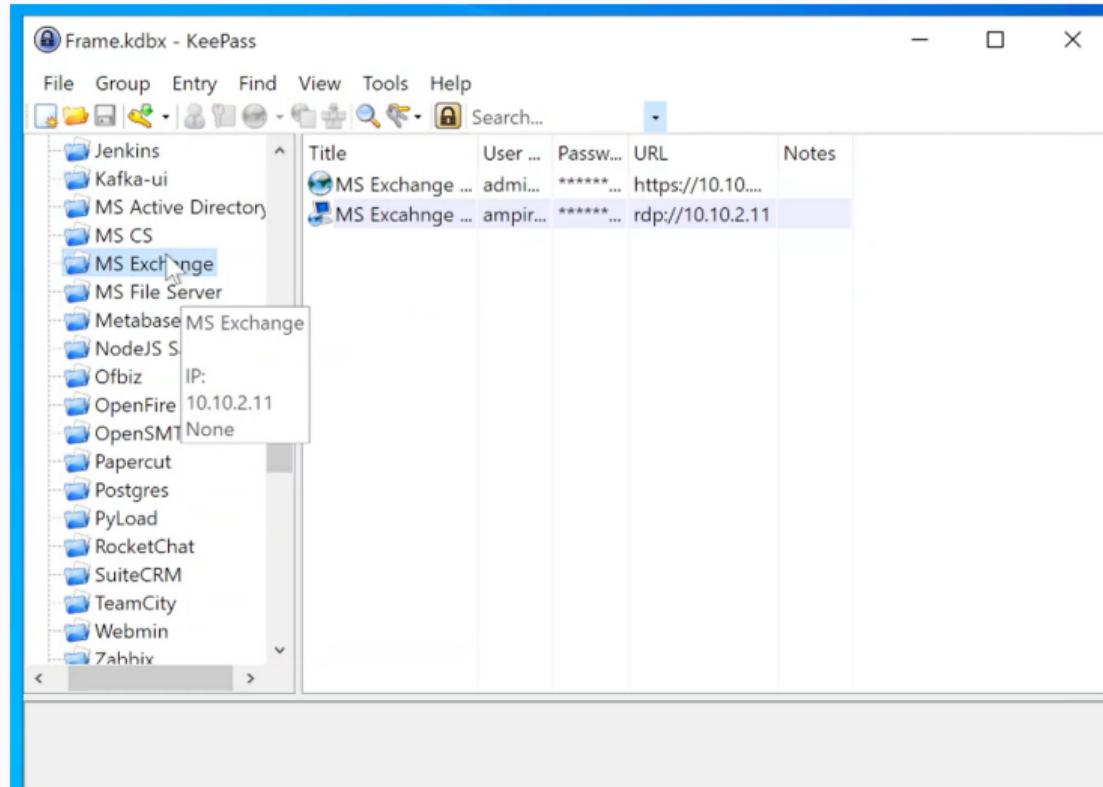
Уровень серьезности

Оценка воздействия 5.9
Оценка эксплуатируемости 3.9
Вектор атаки Сетевой
Сложность атаки Низкая
Уровень привилегий Не требуется

Рис. 20: Обзор уязвимости

Уязвимость Proxylogon

В соответствии с вектором атаки в KeePass нашли MS Exchange.



Уязвимость Proxylogon

Подключились к удаленному рабочему столу по адресу в соответствии с вектором атаки.
Открыли Internet Information Services Manager.

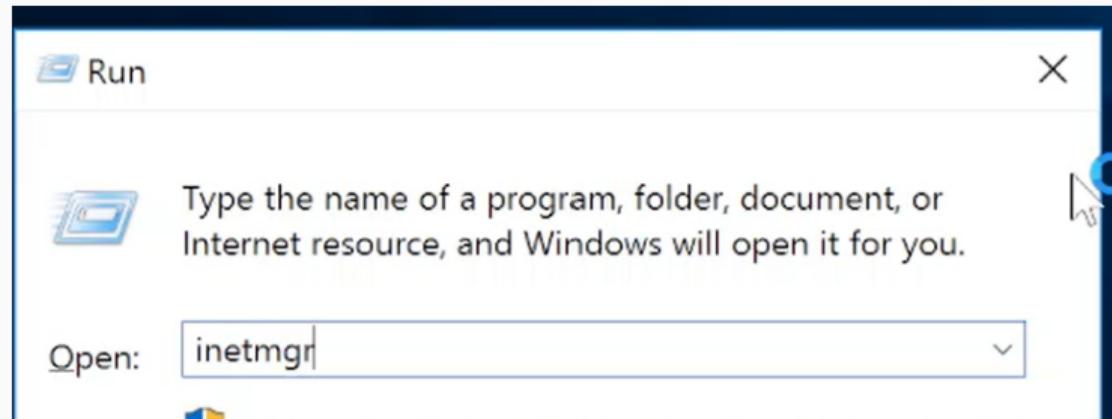
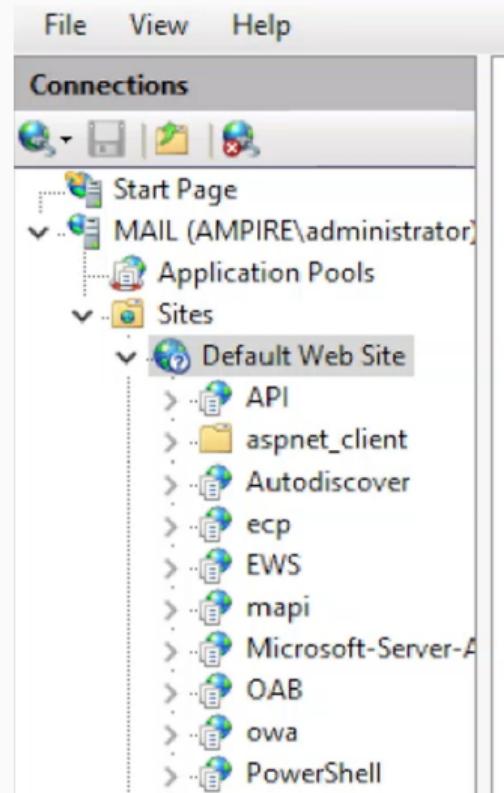


Рис. 22: inetmgr

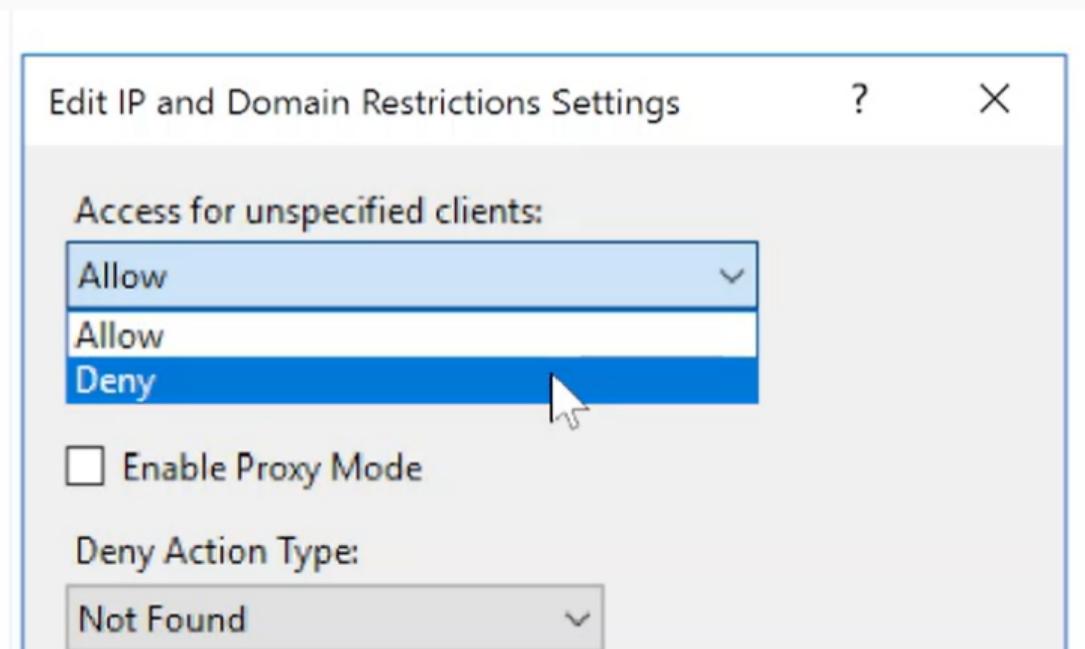
Уязвимость Proxylogon

Перешли в /MAIL/Sites/Default Web Site/ecp



Уязвимость Proxylogon

Перешли в IP Address and Domain Restrictions, в “Actions” выбрали “Edit Feature Settings”, в открывшемся окне в параметре “Access for unspecified clients” выбрали “Deny”.



Уязвимость Proxylogon

Далее открыли терминал, чтобы обнаружить вредоносные процессы с помощью утилиты netstat.

```
C:\Users\administrator.AMPIRE>netstat -b -o

Active Connections

  Proto  Local Address          Foreign Address        State      PID
  TCP    10.10.2.11:443        10.10.1.22:56234    CLOSE_WAIT  4
```

Рис. 25: Вредоносные процессы

Уязвимость Proxylogon

[w3wp.exe]	TCP	10.10.2.11:13923	195.239.174.11:5558	ESTABLISHED	14832
[powershell.exe]	TCP	10.10.2.11:13924	195.239.174.11:5558	ESTABLISHED	13016
[powershell.exe]					

Рис. 26: Вредоносные процессы

Уязвимость Proxylogon

Остановили эти процессы и проверили их отсутствие.

```
C:\Users\administrator.AMPIRE>taskkill /PID 14832 /F  
SUCCESS: The process with PID 14832 has been terminated.  
  
C:\Users\administrator.AMPIRE>taskkill /PID 14832 13016 /F  
ERROR: Invalid argument/option - '13016'.  
Type "TASKKILL /?" for usage.  
  
C:\Users\administrator.AMPIRE>taskkill /PID 13016 /F  
ERROR: The process "13016" not found.  
  
C:\Users\administrator.AMPIRE>netstat -b -o
```

Рис. 27: Вредоносные процессы

Уязвимость Proxylogon

Далее в директории /C:/Program Files/Microsoft/Exchange Server/V15/FrontEnd/HttpProxy/owa/auth удалили файл AM_Backdoor.aspx

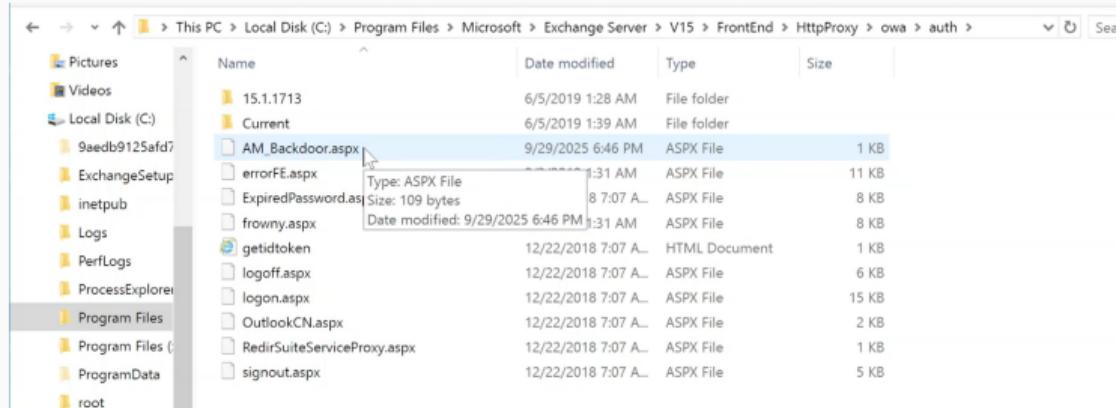


Рис. 28: Удаление файла .aspx

Уязвимость Proxylogon

Уязвимость Proxylogon и ее последствие China Chopper успешно устранены.

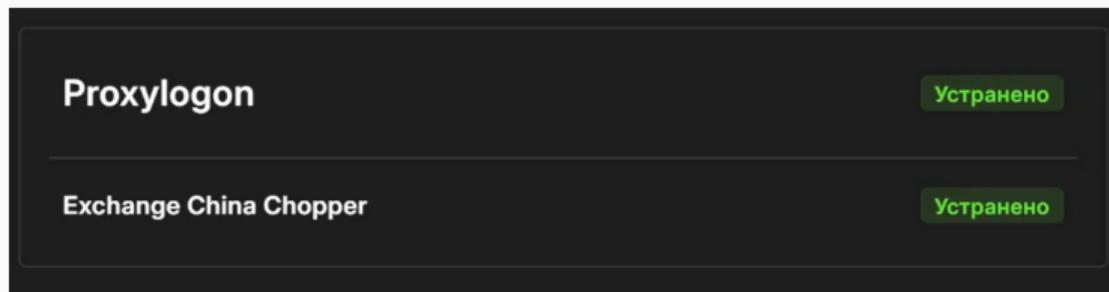


Рис. 29: Успех

Уязвимость Rocket.Chat

Вернулись в ViPNet для обнаружения подозрительной активности в журнале событий.

I8:33.030 29....	3121915	1	ET POLICY Executable and I... policy-violation	TCP	195.239.174.11	5559	10.10.2.22	45770
I8:33.030 29....	3121915	1	ET POLICY Executable and linking format (ELF)	TCP	195.239.174.11	5559	10.10.1.253	1548
I8:22.912 29....	3129327	1	ET POLICY Executable and linking format (ELF) file download var1	TCP	195.239.174.11	8010	10.10.2.22	47362
I8:22.912 29....	3129327	1	ET POLICY Executable and I... policy-violation	TCP	195.239.174.11	8010	10.10.1.253	37775

Рис. 30: Журнал событий

Уязвимость Rocket.Chat

Изучили информацию об обнаруженной уязвимости.

Результаты поиска по IOC
CVE-2021-22911

Основное Правила обнаружения вторжений ⓘ Взаимосвязи ⓘ Граф

Обзор CVE-2021-22911

Название уязвимости: RocketChat RCE

Описание уязвимости: 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

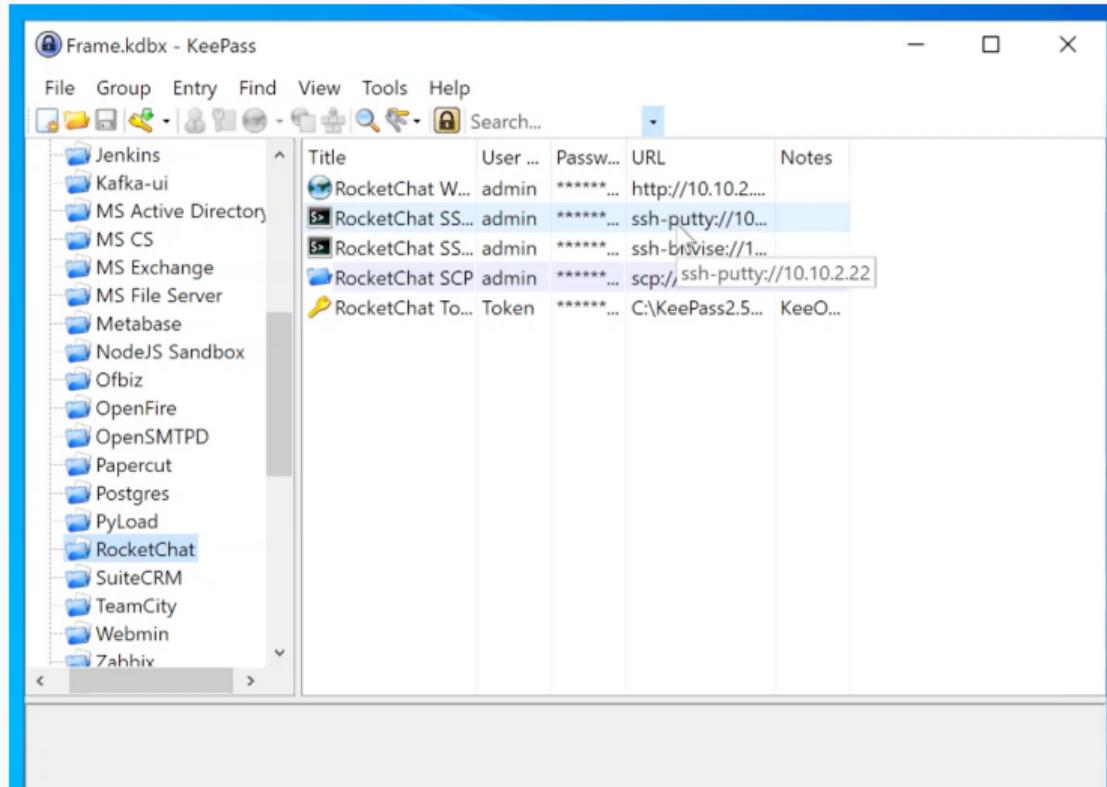
Рекомендации по нейтрализации:

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

Рис. 31: Обзор уязвимости

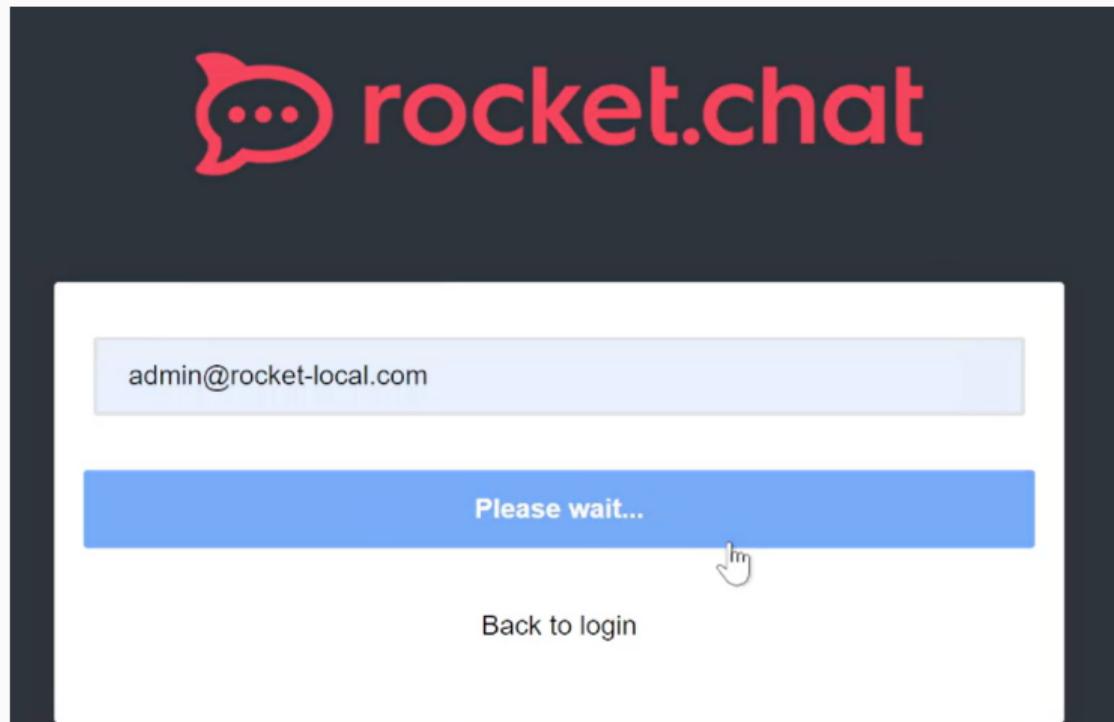
Уязвимость Rocket.Chat

В соответствии с вектором атаки в KeePass нашли RocketChat.



Уязвимость Rocket.Chat

Открыли веб-версию Rocket.Chat и нажали на сброс пароля для указанной учетной записи.



Уязвимость Rocket.Chat

На почту администратора Rocket.Chat было направлено email-письмо с инструкциями по сбросу пароля.

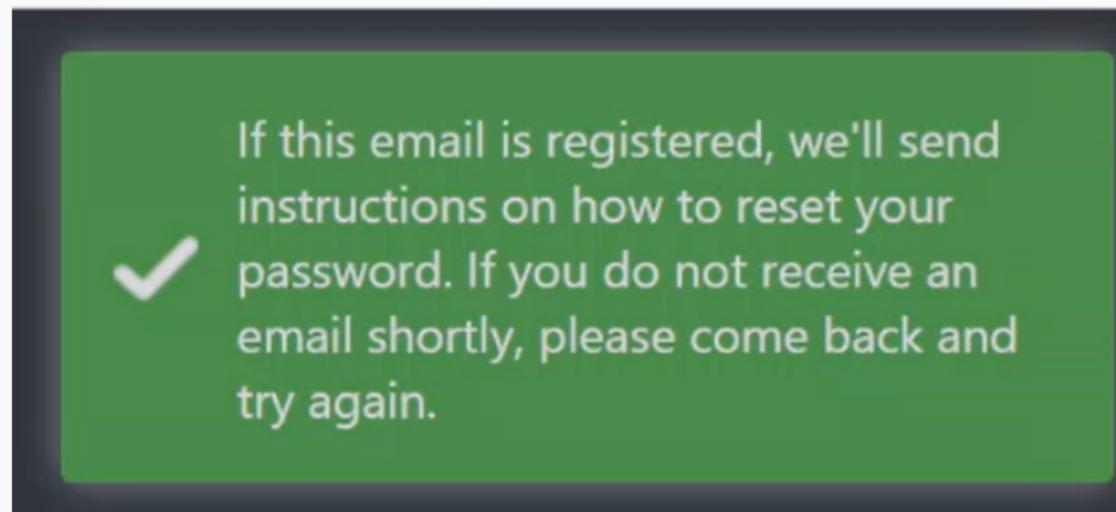


Рис. 34: Сообщение об отправке email

Уязвимость Rocket.Chat

В консоли от администратор просмотрели это письмо. Скопировали ссылку со сгенерированным токеном для сброса пароля.

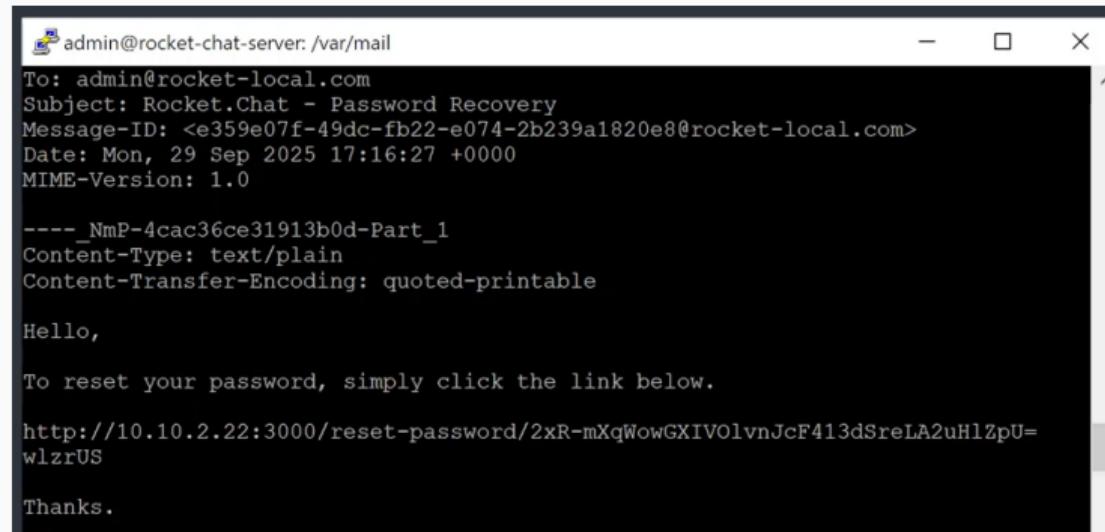


Рис. 35: Инструкция по сбросу пароля

Уязвимость Rocket.Chat

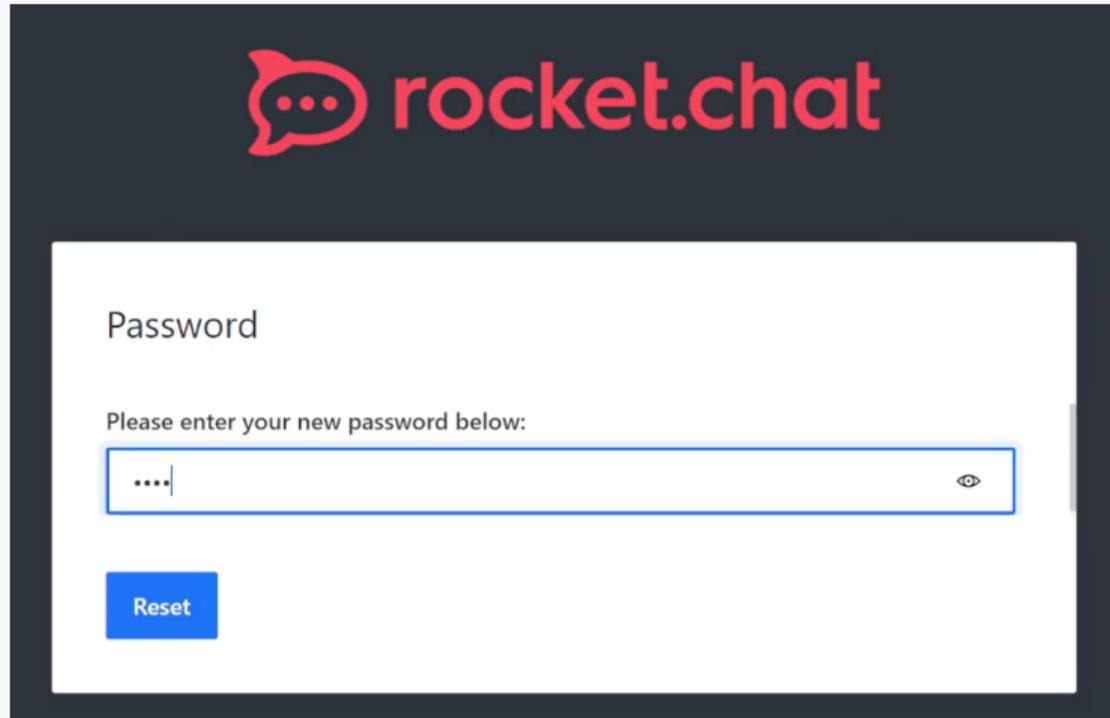
Перешли по скопированному адресу в браузере



Рис. 36: Сброс пароля

Уязвимость Rocket.Chat

Задали новый пароль для пользователя



Уязвимость Rocket.Chat

Просмотрели /home/user/backup_codes для прохождения двухфакторной аутентификации при сбросе пароля.

```
admin@rocket-chat-server:/$ cat /home/user/backup_codes
backup codes for admin Rocket Chat:
iFdDR68y kpMifh9E 43PxEyom jho4DGdw RiuwYGrg LohP2b4A 9tiK2Sca THHC87gf mnPEZACy
rdhcBy8B DvPHRnTz ZZPgeko2
admin@rocket-chat-server:/$
```

Рис. 38: Backup_codes

Уязвимость Rocket.Chat

Ввели один из них в соответствующее поле ввода.

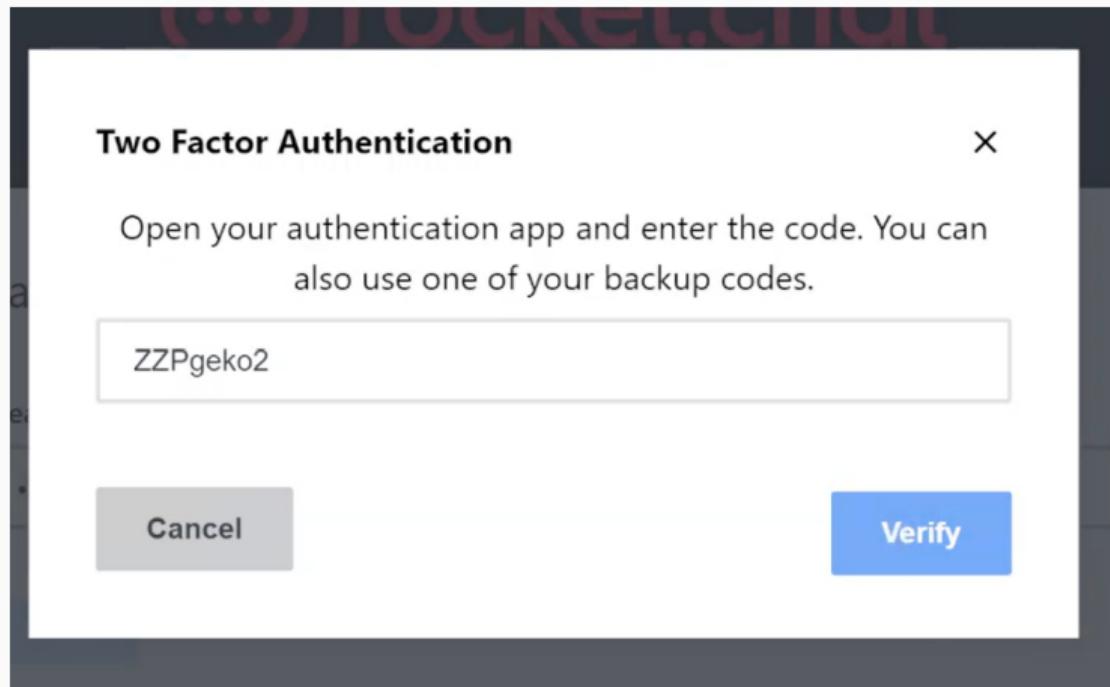
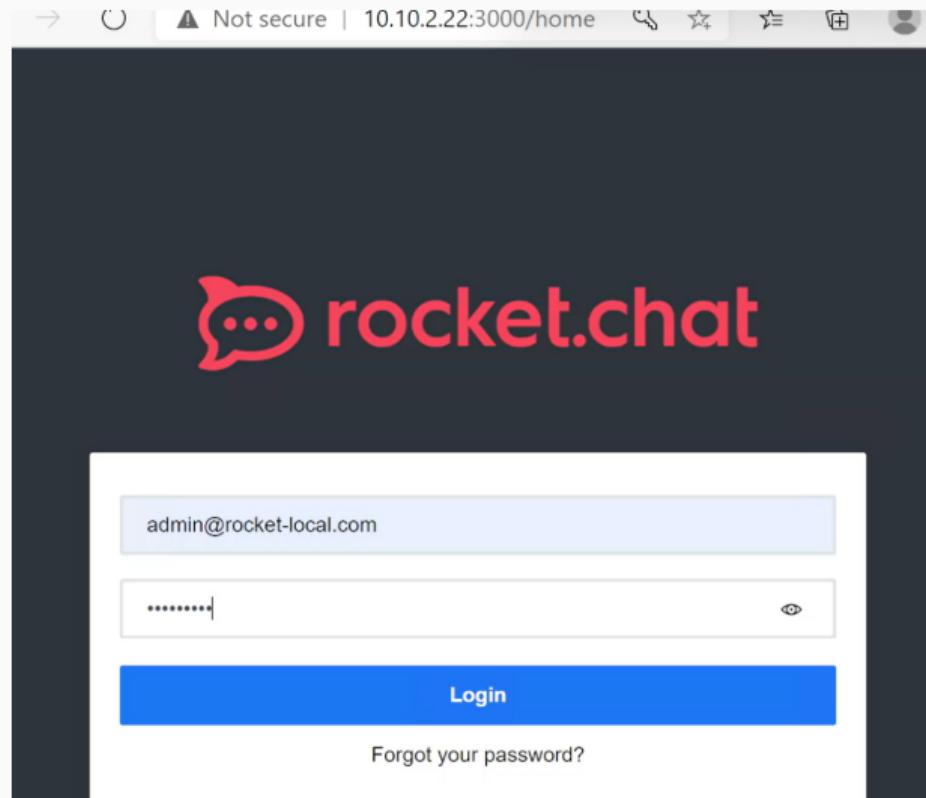


Рис. 39: Сброс пароля

Уязвимость Rocket.Chat

Залогинились с измененным паролем.



Уязвимость Rocket.Chat

В панели администрирования перешли в “Права доступа”, и для роли “User” поставили флагок “User must use Two factor Authentication”.

The screenshot shows two panels from the Rocket.Chat administration interface. On the left is the 'Permissions' screen, which lists various administrative tasks with checkboxes for Admin, Moderator, Leader, and Owner roles. On the right is the 'Role Editing' dialog for the 'user' role, showing the 'Scope' set to 'Global' and the 'Users must use Two Factor Authentication' checkbox checked. A 'Save' button is at the bottom of the dialog.

Name	Admin	Moderator	Leader	Owner
Access Mailer Screen	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Access Permissions Screen	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Modify setting-based permissions	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Add Omnichannel Agents to Departments	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Add Oauth Service	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Add User to Any Public Channel	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Add User to Any Private Channel	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Add User to Any Joined Channel	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Bypass rate limit for REST API	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Рис. 41: Права доступа

Уязвимость Rocket.Chat

Перешли во вкладку “Учетные записи” и настроили подтверждение адреса электронной почты при регистрации для роли “User” и автоматическую настройку двухфакторной аутентификации по электронной почте для новых пользователей.

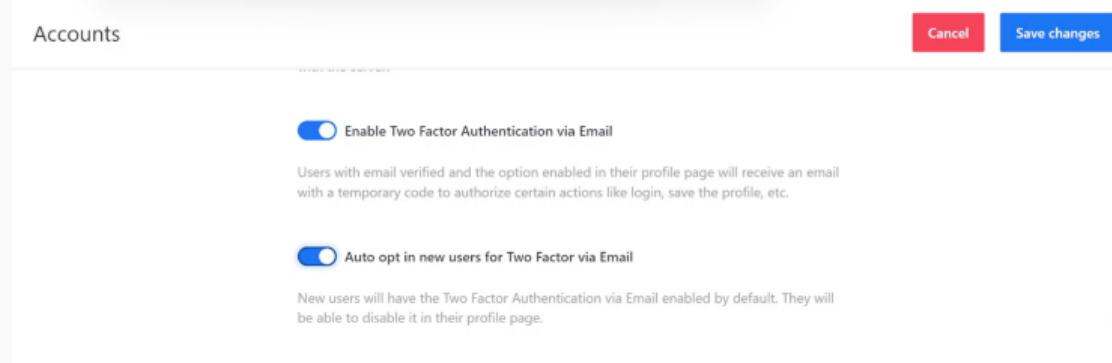


Рис. 42: Настройки двухфакторной аутентификации

Уязвимость Rocket.Chat

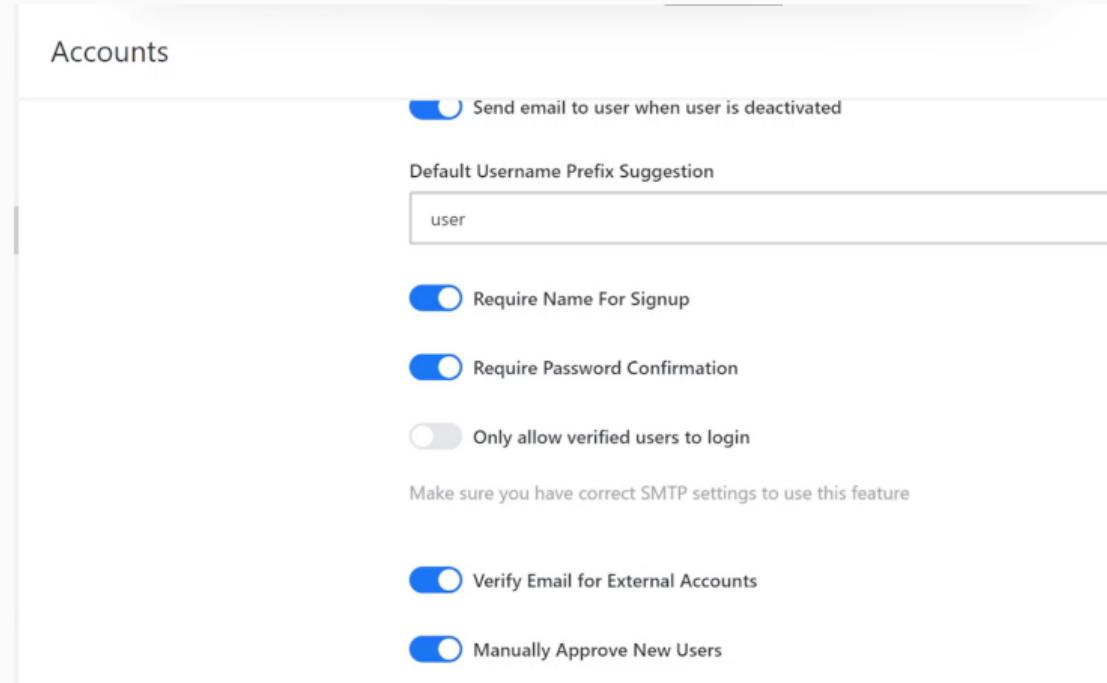
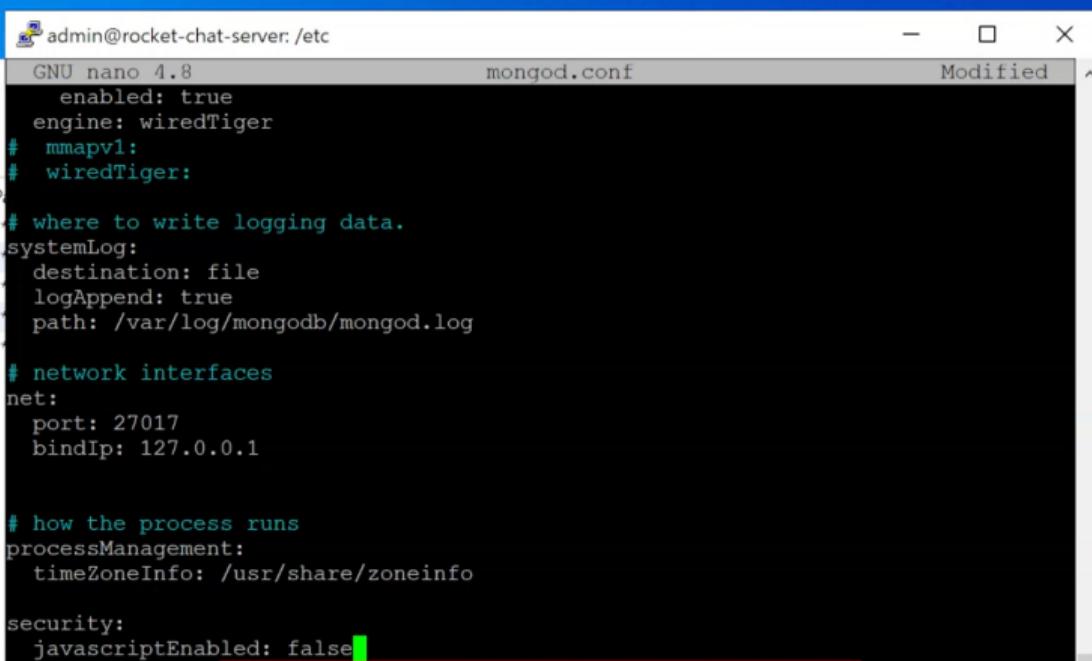


Рис. 43: Настройки регистрации

Уязвимость Rocket.Chat

В терминале администратора Rocket.Chat-server отредактировали файл mongod.conf, расскомментировав параметр “security:” и прописав отключение выполнения JavaScript на стороне сервера базы данных “javascriptEnabled: False”.



```
admin@rocket-chat-server: /etc
GNU nano 4.8                                     mongod.conf                                         Modified
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
```

Уязвимость Rocket.Chat

Перезапустили службу mongod.service

```
admin@rocket-chat-server:/etc$ sudo systemctl restart mongod.service
```

Рис. 45: Restart mongod.service

Уязвимость Rocket.Chat

С помощью утилиты ss обнаружили и остановили вредоносные процессы.

```
admin@rocket-chat-server:/etc$ sudo ss -tp4 | grep 174.11
ESTAB      0      0          10.10.2.22:45770      195.239.174.11:5559
  users:(("testsystem",pid=3384,fd=3))
admin@rocket-chat-server:/etc$ sudo kill 3384
admin@rocket-chat-server:/etc$
```

Рис. 46: Уничтожение вредоносных соединений

Уязвимость Rocket.Chat

Уязвимость RocketChat RCE и ее последствие meterpreter успешно устранены.

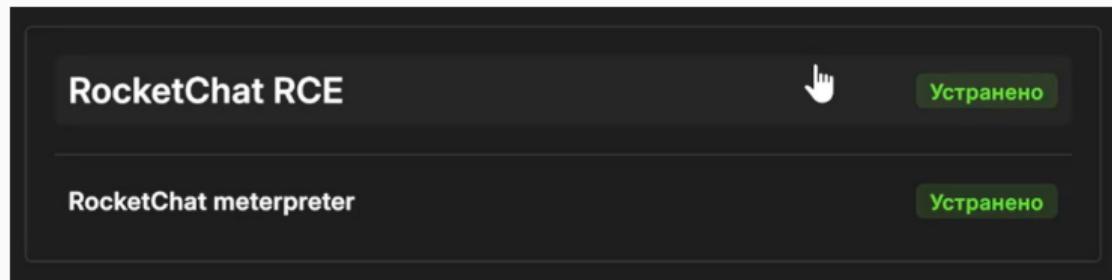


Рис. 47: Успех

Завершение выполнения лабораторной работы

Заполнили карточки инцидентов для уязвимостей и их последствий.

Лабораторная 1-D (НФИ-2) 29_09
Группа: НФИбд-02-22 (D) - пятница

Основная информация Инциденты Цепочки кибератаки Beta Схема шаблона Материалы

Поиск Фильтр

В работе Уязвимость WordPress-wpDiscuz

Автор Доберштейн Алина @1132226448@pfur.ru

Ответственный Доберштейн Алина @1132226448@pfur.ru

Сообщений 0 29.09.2025 18:44

Новый Последствие WordPress-wpDiscuz → Deface

Автор Доберштейн Алина @1132226448@pfur.ru

Сообщений 0 29.09.2025 18:44

Новый Уязвимость WordPress-wpDiscuz

Автор Доберштейн Алина @1132226448@pfur.ru

Сообщений 0

Новый Последствие Proxylogon → Exchange China Chopper

Автор

Новый Уязвимость RocketChat

Автор

Новый Последствие Meterpreter

Автор

Выводы

В результате выполнения лабораторной работы мы получили навыки обнаружения и устранение уязвимостей WordPress-wpDiscuz, Proxylogon, Rocket.Chat и их последствий.