

Отчёт по лабораторной работе №2 по кибербезопасности.

Последовательность устранения уязвимостей в Ampire.

Дурдалыев Максат

Содержание

1	Выполнение лабораторной работы.....	2
2	Выполнение лабораторной работы.....	2
3	Выполнение лабораторной работы.....	3
4	Выполнение лабораторной работы.....	3
5	Выполнение лабораторной работы.....	3
6	Выполнение лабораторной работы.....	4
7	Выполнение лабораторной работы.....	4
8	Выполнение лабораторной работы.....	4
9	Выполнение лабораторной работы.....	4
10	Выполнение лабораторной работы	5
11	Выполнение лабораторной работы	5
12	Выполнение лабораторной работы	5
13	Выполнение лабораторной работы	6
14	Выполнение лабораторной работы	6
15	Выполнение лабораторной работы	6
16	Выводы	6

Список иллюстраций

Рис. 1: События, связанные с эксплуатацией уязвимости.....	2
Рис. 2: Ошибка восстановления.	2
Рис. 3: Успешное выполнение восстановления.	3
Рис. 4: Последствие WordPress Deface устранено.	3
Рис. 5: Закрытие сессии.	3
Рис. 6: Уязвимость WordPress wpDiscuz устранена.	4
Рис. 7: Настройка конфигурации БД для отключения операций с кодами на JavaScript на стороне сервера.....	4
Рис. 8: Перезагрузка RocketChat.	4
Рис. 9: Закрытие сессии с нарушителем.....	4

Рис. 10: Уязвимость RocketChat RCE и последствие RocketChat meterpreter устранены. . 5

Рис. 11: Окно Internet Information Services (ISS) Manager. 5

Рис. 12: IP Address and Domain Restrictions. 5

Рис. 13: Устранение последствия Exchange China Chopper. 6

Рис. 14: Обнаружение Exchange China Chopper последствия в приведенном на скриншоте пути.) 6

Рис. 15: Устранение уязвимости Proxylogon и последствия Exchange China Chopper. 6

Список таблиц

Элементы списка иллюстраций не найдены.

1 Выполнение лабораторной работы

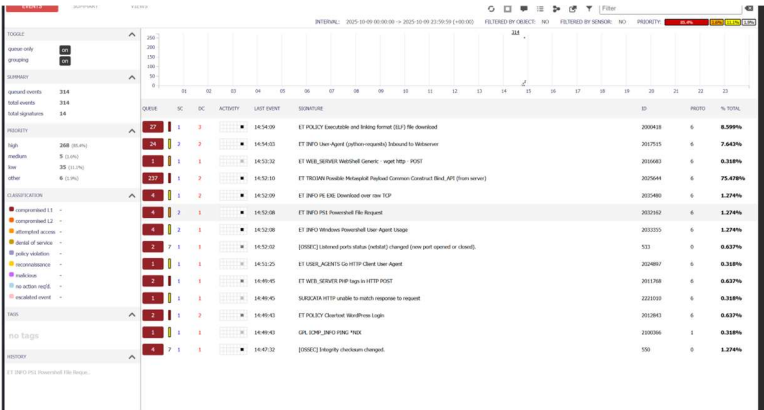


Рис. 1: События, связанные с эксплуатацией уязвимости.

2 Выполнение лабораторной работы

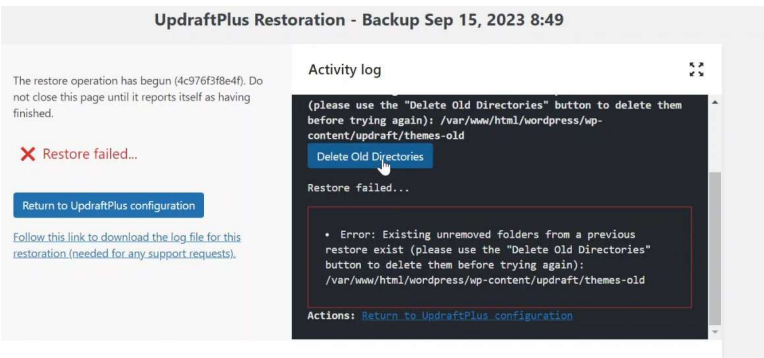


Рис. 2: Ошибка восстановления.

3 Выполнение лабораторной работы

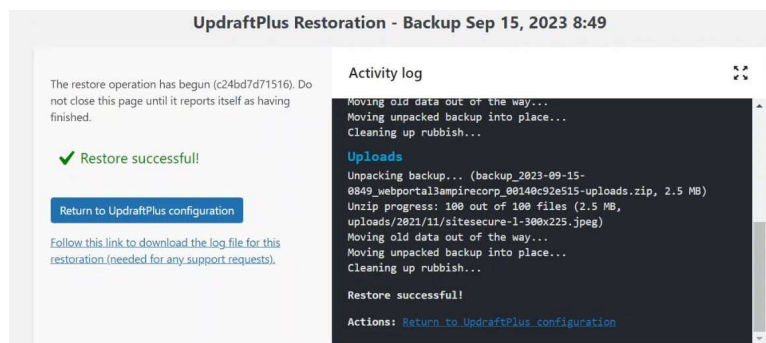


Рис. 3: Успешное выполнение восстановления.

4 Выполнение лабораторной работы

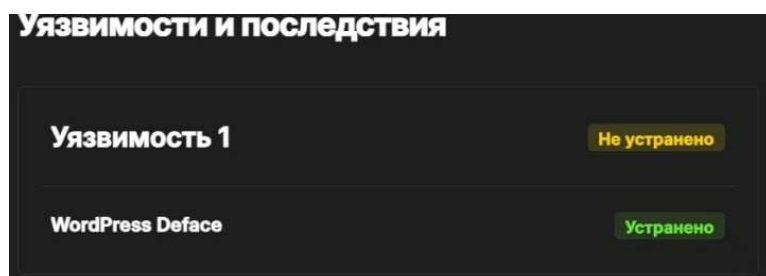


Рис. 4: Последствие WordPress Deface устранено.

5 Выполнение лабораторной работы

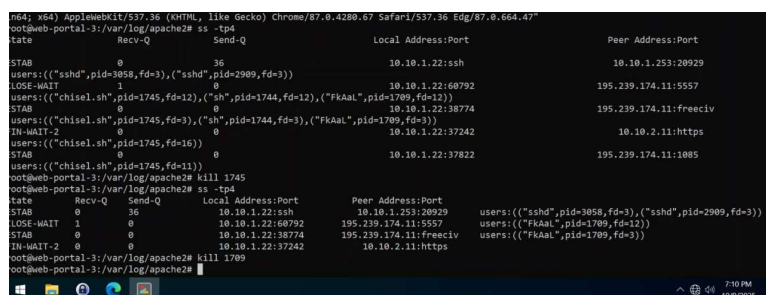


Рис. 5: Закрытие сессии.

6 Выполнение лабораторной работы

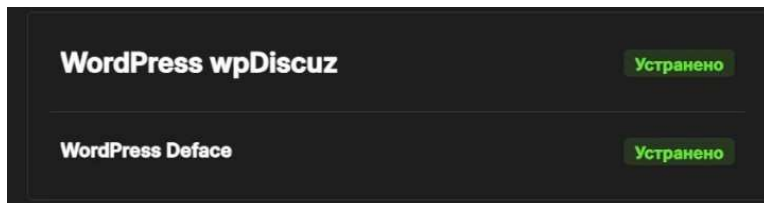


Рис. 6: Уязвимость WordPress wpDiscuz устранена.

7 Выполнение лабораторной работы

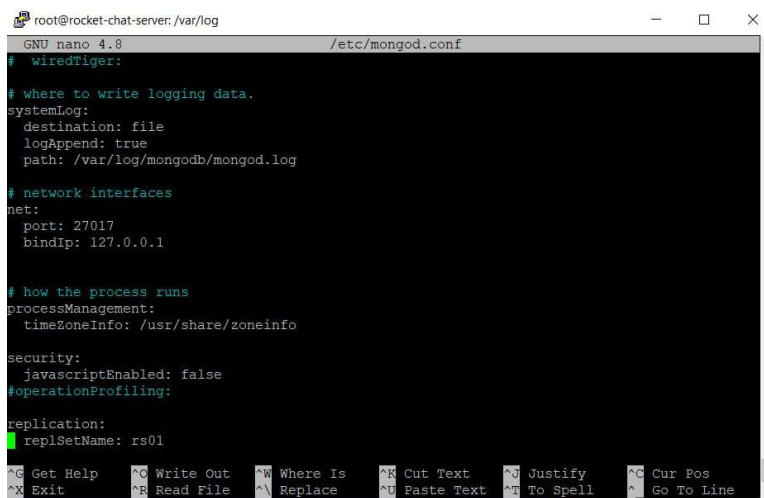


Рис. 7: Настройка конфигурации БД для отключения операций с кодами на JavaScript на стороне сервера.

8 Выполнение лабораторной работы

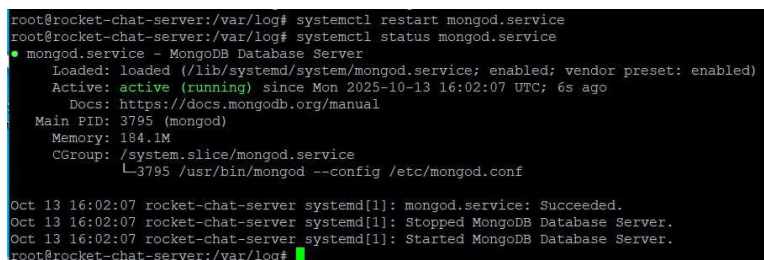


Рис. 8: Перезагрузка RocketChat.

9 Выполнение лабораторной работы

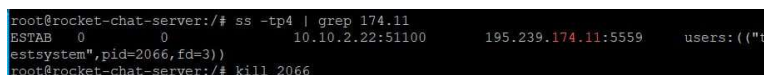


Рис. 9: Закрытие сессии с нарушителем.

10 Выполнение лабораторной работы

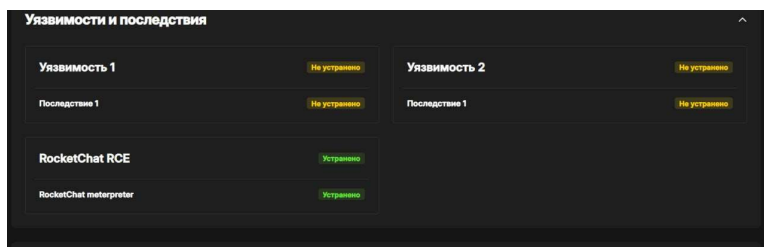


Рис. 10: Уязвимость RocketChat RCE и последствие RocketChat meterpreter устранены.

11 Выполнение лабораторной работы

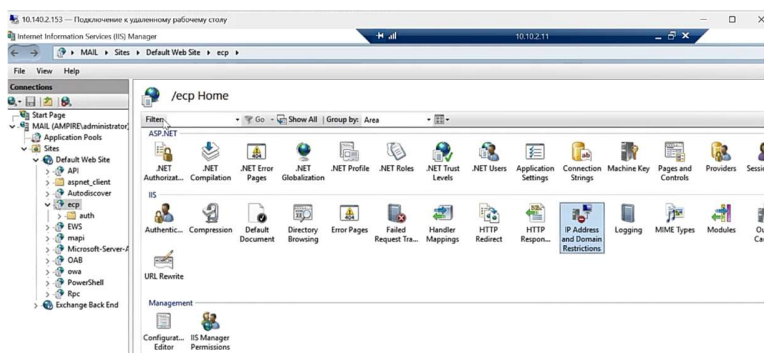


Рис. 11: Окно Internet Information Services (IIS) Manager.

12 Выполнение лабораторной работы

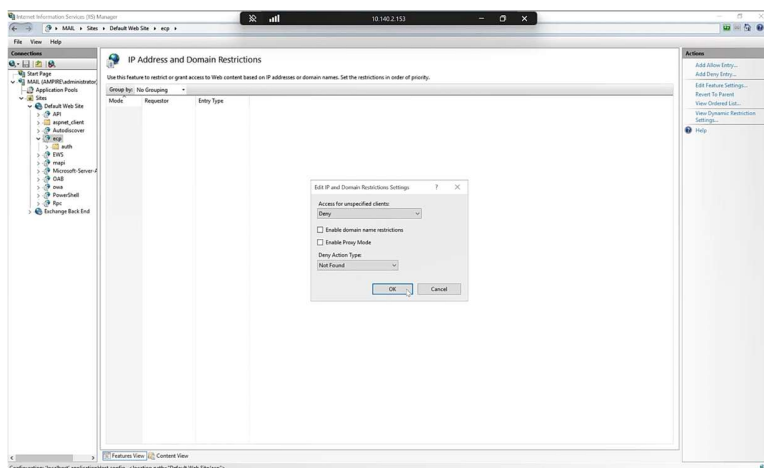


Рис. 12: IP Address and Domain Restrictions.

13 Выполнение лабораторной работы

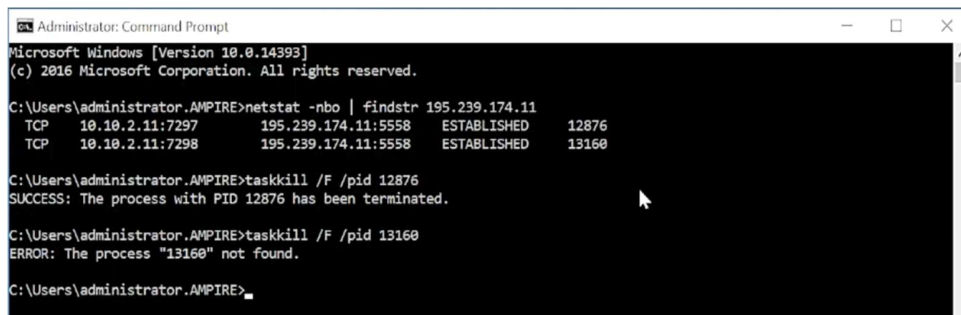


Рис. 13: Устранение последствий Exchange China Chopper.

14 Выполнение лабораторной работы

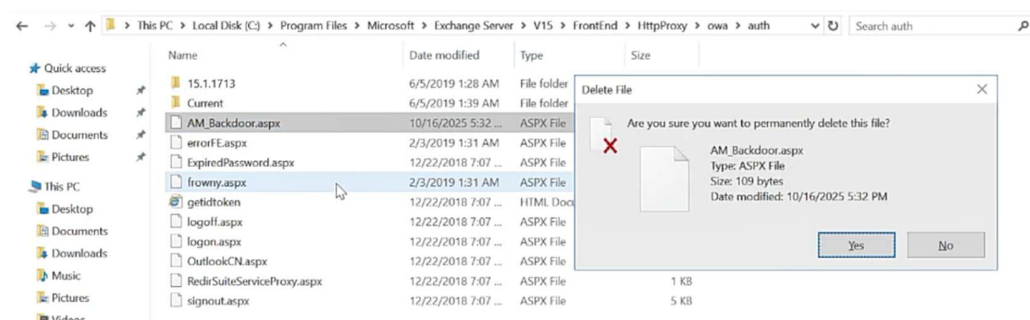


Рис. 14: Обнаружение Exchange China Chopper последствия в приведенном на скриншоте пути.)

15 Выполнение лабораторной работы

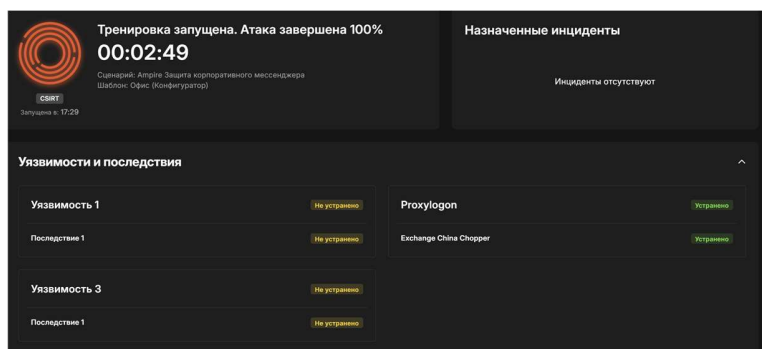


Рис. 15: Устранение уязвимости Proxylogon и последствия Exchange China Chopper.

16 Выводы

В ходе данной лабораторной мы устранили 3 уязвимости и 3 последствия.