

# Лабораторная работа №2

Кибербезопасность предприятия

Аскеров Александр Эдуардович

Замбалова Дина Владимировна

Кузнецова София Вадимовна

Поляков Глеб Сергеевич

Скандарова Полина Юрьевна

Тарутина Кристина Еленовна

Цвелев Сергей Андреевич

Шулуужук Айраана Вячеславовна

Учебная группа: НПИбд-01-22

# Содержание

Цель работы	4
Теоретическое введение	5
Легенда. Защита интеграционной платформы . . . . .	5
Описание уязвимостей . . . . .	6
CVE-2022-27228 (1C-Битрикс) . . . . .	6
CVE-2021-22204/GitLab (CVE-2021-22205) . . . . .	6
CVE-2022-29464 (WSO2 API Manager) . . . . .	6
Выполнение лабораторной работы	7
Уязвимый узел Bitrix (CVE-2022-27228) . . . . .	7
Обнаружение уязвимости . . . . .	7
Устранение уязвимости и последствий . . . . .	8
Уязвимый узел GitLab (CVE-2021-22204) . . . . .	9
Обнаружение уязвимости . . . . .	9
Устранение уязвимости и последствий . . . . .	10
Уязвимый узел WSO2 API Manager (CVE-2022-29464) . . . . .	11
Обнаружение уязвимости . . . . .	11
Устранение уязвимости и последствий . . . . .	11
Вывод	13
Список литературы	14

## Список иллюстраций

0.1	Подключение к серверу . . . . .	7
0.2	Закрытие вектора LPE . . . . .	8
0.3	Добавление директивы deny from all . . . . .	8
0.4	Нейтрализация последствий . . . . .	9
0.5	Удаление учетных записей, созданных злоумышленником . . . . .	10
0.6	Нейтрализация последствий . . . . .	10
0.7	Изменение конфигурации . . . . .	11
0.8	Нейтрализация последствий . . . . .	12

## Цель работы

Целью лабораторной работы является исследование сценария целевой атаки на инфраструктуру компании, включая эксплуатацию уязвимостей в веб-сервисе Bitrix, сервере GitLab и платформе управления API WSO2. Задачи работы включают обнаружение, анализ и нейтрализацию последствий атаки, а также восстановление работоспособности и безопасности компрометированных систем.

# Теоретическое введение

## 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.

Проексплуатировав 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, предназначенной 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.

## Описание уязвимостей

### CVE-2022-27228 (1С-Битрикс)

Уязвимость в модуле «vote» системы управления содержимым сайтов (CMS) «1С-Битрикс: Управление сайтом» позволяет нарушителю удаленно записывать произвольные файлы в систему и выполнять произвольный код, используя небезопасную десериализацию. Уязвимость присутствует в версиях Bitrix до 22.0.400.

### CVE-2021-22204/GitLab (CVE-2021-22205)

Критическая уязвимость в GitLab CE/EE, затрагивающая все версии начиная с 11.9. Уязвимость заключается в неправильной проверке файлов изображений, передаваемых в парсер ExifTool, что приводит к удаленному выполнению команд (RCE) при загрузке специально сформированного файла.

### CVE-2022-29464 (WSO2 API Manager)

Уязвимость платформы для интеграции интерфейсов прикладного программирования, приложений и веб-служб WSO2 связана с возможностью загрузки произвольного JSP-файла на сервер без надлежащей аутентификации. Эксплуатация уязвимости позволяет удаленно выполнить произвольный код.

# Выполнение лабораторной работы

Подключили vpn WireGuard, чтобы открыть сайт Ampire с лабораторной работой.

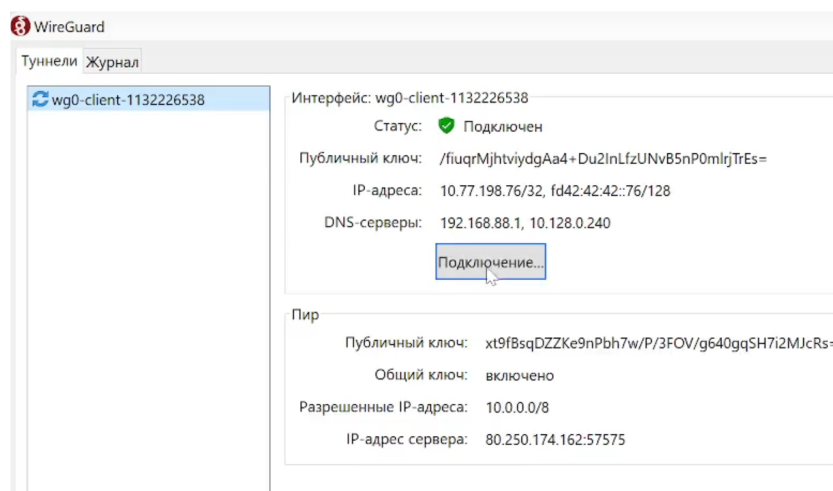


Рис. 0.1: Подключение к серверу

## Уязвимый узел Bitrix (CVE-2022-27228)

### Обнаружение уязвимости

Эксплуатация уязвимости CVE-2022-27228 была обнаружена по наличию в лог-файле `/var/log/apache2/access.log` записей с обращением к файлу `/bitrix/tools/vote/uf.php` и внедрением полезной нагрузки.

Были обнаружены артефакты атаки: 1. POST-запросы к `uf.php` с передачей вредоносного PHAR-файла (`payload2.phar`). 2. Файл веб-шелла `/var/www/html/caidao.php`, загруженный в результате выполнения уязвимости. 3. Наличие в директории

/var/www/html/ файлов apache\_restart (с SUID-битом) и systemctl, используемых для повышения привилегий и поддержания доступа.

Сетевой сенсор ViPNet IDS NS зафиксировал события, связанные с эксплуатацией уязвимости: - AM EXPLOIT Possible Bitrix CMS below v21.0.100 RCE in module vote (CVE-2022-27228) - ET EXPLOIT php script base64 encoded Remote Code Execution 2 - ET POLICY Executable and linking format (ELF) file download

## Устранение уязвимости и последствий

### 1. Закрытие вектора LPE (Local Privilege Escalation):

- Удален SUID-бит у файла /var/www/html/apache\_restart командой `chmod -s apache_restart`, после чего файл был удален.
- Удален файл /var/www/html/upload/systemctl.

```
root@bitrix:/var/www/html# chmod -s apache_restart
root@bitrix:/var/www/html# rm apache_restart
```

Рис. 0.2: Закрытие вектора LPE

### 2. Закрытие уязвимости CVE-2022-27228:

- В файл /var/www/html/bitrix/tools/vote/.htaccess добавлена директива `deny from all`, блокирующая все запросы к уязвимому модулю.

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

Рис. 0.3: Добавление директивы deny from all



### 3. Нейтрализация последствий:

- Завершены вредоносные meterpreter-сессии с помощью команды `kill -9 <PID>` для процессов, установивших соединение с IP-адресом злоумышленника.
- Удален веб-шелл `caidao.php`.
- Для восстановления доступа к панели администратора использован скрипт `password_recovery.php`, который сбросил пароль учетной записи администратора. После входа скрипт был удален.
- Веб-сайт восстановлен из резервной копии `Bitrix_full_backup.tar.gz`, расположенной в `/var/bitrix_backups/`.

```
root@bitrix:/var/www/html# vim password_recovery.php
root@bitrix:/var/www/html# rm password_recovery.php
root@bitrix:/var/www/html# cd /var/bitrix_backups
root@bitrix:/var/bitrix_backups# ls -al
итого 412112
drwxr-xr-x  2 root root    4096 дек 11  2023 .
drwxr-xr-x 16 root root    4096 дек 11  2023 ..
-rw-r--r--  1 root root 420715270 сен 15  2023 Bitrix_full_backup.tar.gz
-rw-r--r--  1 root root  1270146 дек 11  2023 Bitrix_sitemanager_DB.tar.gz
root@bitrix:/var/bitrix_backups# rm -r /var/www/html/*
root@bitrix:/var/bitrix_backups# tar xvfz /var/bitrix_backups/Bitrix_full_backup.tar.gz -C /var/www/html
```

Рис. 0.4: Нейтрализация последствий

## Уязвимый узел GitLab (CVE-2021-22204)

### Обнаружение уязвимости

Эксплуатация уязвимости была обнаружена по записям в логах GitLab (`/var/log/gitlab/gitlab-rails/production_json.log`), указывающим на загрузку файла с расширением `.jpg`, который содержал вредоносную нагрузку для RCE.

Сетевой сенсор ViPNet IDS NS зафиксировал событие: AM EXPLOIT GitLab CE/EE 11.9-13.10.3 Unauthenticated Remote ExifTool Command Injection (CVE-2021-22205).

Были обнаружены последствия атаки: - Наличие на сервере подозрительных пользовательских аккаунтов, созданных злоумышленником. - Факт создания и выгрузки резервной копии базы данных (`evil_*_gitlab_backup.tar`).

## Устранение уязвимости и последствий

### 1. Обновление GitLab:

- GitLab был обновлен до версии 13.10.3 с помощью пакета gitlab-ce\_13.10.3-ce.0\_amd64.deb командой `sudo dpkg -i`.

### 2. Изменение политики безопасности:

- В панели администратора GitLab в разделе Settings -> General -> Sign-up restrictions активирована опция, требующая подтверждения регистрации новых пользователей администратором.
- Удалены все учетные записи, созданные злоумышленником.

```
ESTAB 0 0 10.10.2.18:58860 195.239.174.11:5559
users: (("2FW4zI",pid=3626,fd=3))
ESTAB 0 0 10.10.2.18:ssh 10.10.2.254:26191
users: (("ssh",pid=22489,fd=3), ("ssh",pid=22325,fd=3))
ESTAB 0 0 127.0.0.1:9100 127.0.0.1:57000
users: (("node_exporter",pid=23543,fd=7))
ESTAB 0 0 127.0.0.1:48666 127.0.0.1:8060
users: (("prometheus",pid=23659,fd=31))
ESTAB 0 0 127.0.0.1:41978 127.0.0.1:9229
users: (("prometheus",pid=23659,fd=28))
ESTAB 0 0 127.0.0.1:8060 127.0.0.1:48666
users: (("nginx",pid=23538,fd=14))
ESTAB 0 0 127.0.0.1:9187 127.0.0.1:36498
users: (("postgres_export",pid=23549,fd=8))
ESTAB 0 0 10.10.2.18:http 10.10.2.18:43674
users: (("nginx",pid=23538,fd=13))
root@ampire-gitlab:/var/opt/gitlab/backups# kill 3626
```

Рис. 0.5: Удаление учетных записей, созданных злоумышленником

### 3. Нейтрализация последствий:

- Удалена оставленная нарушителем резервная копия базы данных (`evil_*_gitlab_backup.tar`).
- Завершены вредоносные соединения (meterpreter-сессии) с помощью команды `kill -9 <PID>`.

```
root@ampire-gitlab:~# cd /var/opt/gitlab/backups/
root@ampire-gitlab:/var/opt/gitlab/backups# ls
stable_gitlab_backup.tar
root@ampire-gitlab:/var/opt/gitlab/backups# gitlab-ctl stop puma && gitlab-ctl stop sidekiq
ok: down: puma: 0s, normally up
ok: down: sidekiq: 0s, normally up
root@ampire-gitlab:/var/opt/gitlab/backups# sudo gitlab-backup restore BACKUP=stable
```

Рис. 0.6: Нейтрализация последствий

# Уязвимый узел WSO2 API Manager (CVE-2022-29464)

## Обнаружение уязвимости

Эксплуатация уязвимости была обнаружена по записям в логах доступа (/var/log/wso2\_http\_access.log), указывающим на загрузку файла exploit.jsp на уязвимый маршрут fileupload.

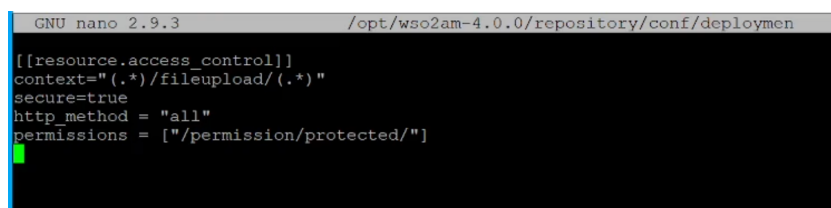
На сервере были обнаружены артефакты: - Файл exploit.jsp по пути /opt/wso2am-4.0.0/repository/deployment/server/webapps/authenticationendpoint/. - Сгенерированный файл payload.elf в директории /tmp. - Активные meterpreter-сессии, установленные через выполнение payload.elf.

## Устранение уязвимости и последствий

### 1. Изменение конфигурации:

- В конфигурационный файл /opt/wso2am-4.0.0/repository/conf/deployment.toml добавлены правила контроля доступа для маршрута fileupload, требующие аутентификации и соответствующих разрешений: toml

```
[[resource.access_control]] context="(.*)/fileupload/(.*)" secure=true
http_method = "all" permissions = ["/permission/protected/"]
```
- Служба WSO2 перезапущена: systemctl restart wso2api.service.



```
GNU nano 2.9.3 /opt/wso2am-4.0.0/repository/conf/deployment.toml
[[resource.access_control]]
context="(.*)/fileupload/(.*)"
secure=true
http_method = "all"
permissions = ["/permission/protected/"]
```

Рис. 0.7: Изменение конфигурации

### 2. Нейтрализация последствий:

- Удалены файлы, загруженные в ходе атаки: exploit.jsp и payload.elf.

- Завершены вредоносные meterpreter-сессии с помощью команды `kill -9 <PID>`.

```

ESTAB      0      0      10.10.2.27:54822      195.239.174.11:5561
users: (("payload.elf",pid=4108,fd=3))
ESTAB      0      0      10.10.2.27:60956      10.10.2.27:amqp
users: (("java",pid=771,fd=515))
ESTAB      0      0      10.10.2.27:amqp      10.10.2.27:60940
users: (("java",pid=771,fd=514))
SYN-SENT   0      1      10.10.2.27:39608      195.239.174.125:puppet
users: (("puppet",pid=4516,fd=6))
CLOSE-WAIT 1      0      10.10.2.27:9763      10.10.1.33:57438
users: (("java",pid=771,fd=398))
ESTAB      0      0      10.10.2.27:amqp      10.10.2.27:60996
users: (("java",pid=771,fd=580))
ESTAB      0      0      10.10.2.27:60938      10.10.2.27:amqp
users: (("java",pid=771,fd=451))
CLOSE-WAIT 0      0      10.10.2.27:9611      10.10.2.27:40912
users: (("java",pid=771,fd=201))
CLOSE-WAIT 0      0      10.10.2.27:9611      10.10.2.27:58064
users: (("java",pid=771,fd=495))
user@wso2-virtual-machine:~$ sudo kill 4108

```

Рис. 0.8: Нейтрализация последствий

## Вывод

В ходе выполнения лабораторной работы была успешно исследована многоэтапная целевая атака на корпоративную инфраструктуру. Были отработаны практические навыки по обнаружению, анализу и нейтрализации последствий эксплуатации критических уязвимостей в популярном веб-фреймворке (1С-Битрикс), системе контроля версий (GitLab) и платформе управления API (WSO2). В результате проведенных мероприятий безопасность всех компрометированных систем была восстановлена: уязвимости закрыты, последствия атаки устранены, работоспособность сервисов восстановлена из резервных копий. Работа продемонстрировала важность комплексного подхода к безопасности, включающего своевременное обновление ПО, мониторинг событий безопасности и наличие актуальных резервных копий.

## Список литературы

““