

# 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

## Цель лабораторной 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.

### **Легенда. Защита корпоративного мессенджера**

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.

### **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.

## Подключение VPN WireGuard

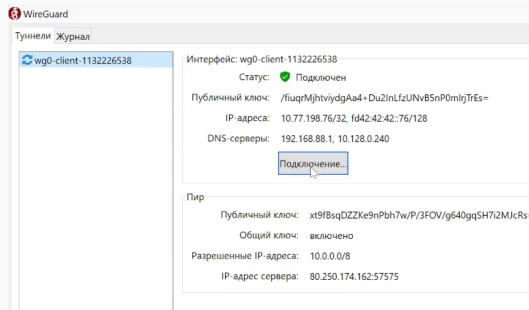


Рисунок 1: Подключение к серверу



### 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.

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

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.

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

Сетевой сенсор ViPNet IDS NS зафиксировал события, связанные с эксплуатацией уязвимости:

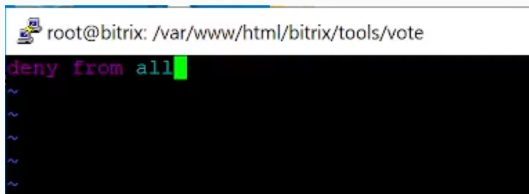
- AM EXPLOIT Possible Bitrix CMS below v21.0.100 RCE in module vote (CVE-2022-27228)
- ET EXPLOIT php script base64 encoded Remote Code Execution 2
- ET POLICY Executable and linking format (ELF) file download

## Заккрытие вектора LPE (Local Privilege Escalation)

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

Рисунок 2: Заккрытие вектора LPE

## Заккрытие уязвимости CVE-2022-27228



The screenshot shows a terminal window with a title bar. The title bar contains a small icon of a computer and the text "root@bitrix: /var/www/html/bitrix/tools/vote". The terminal content shows the command "deny from all" being entered, followed by four tilde characters (~) on separate lines, indicating a multi-line command or a list of entries.

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

Рисунок 3: Добавление директивы deny from all

## Нейтрализация последствий

```
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
lsuro 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 xvf /var/bitrix_backups/Bitrix_full_backup.tar.gz -C /var/www/html
```

Рисунок 4: Нейтрализация последствий

### 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`).

## 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`.



## Изменение политики безопасности

```
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
```

Рисунок 5: Удаление учетных записей, созданных злоумышленником

## Нейтрализация последствий:

```
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
```

Рисунок 6: Нейтрализация последствий

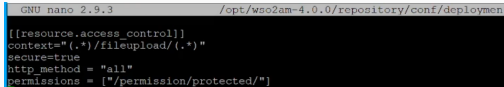
### Обнаружение уязвимости

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/authenticationen`
- Сгенерированный файл `payload.elf` в директории `/tmp`.
- Активные meterpreter-сессии, установленные через выполнение `payload.elf`.

## Изменение конфигурации



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

Рисунок 7: Изменение конфигурации

## Нейтрализация последствий:

```
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
```

Рисунок 8: Нейтрализация последствий

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.