

Лабораторная работа 3

Защита интеграционной платформы

Панченко Денис 1132229056

Савурская Полина 1132222827

Кочарян Никита 1132221541

Норсоян Шушаник 1132221545

Сухальская Ксения 1132229052

Умярова Камилла 1132229051

Содержание

1	Цель работы	3
2	Выполнение лабораторной работы	4
2.1	Уязвимость Bitrix vote RCE и последствие Bitrix deface	4
2.2	Уязвимость GitLab RCE и последствие GitLab meterpreter	7
2.3	Уязвимость WSO2 API-Manager RCE и последствие WSO2 User web . .	9
3	Выводы	12

1 Цель работы

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. Нужно защитить компанию от атаки.

2 Выполнение лабораторной работы

2.1 Уязвимость Bitrix vote RCE и последствие Bitrix deface

При входе на сайт компании, видим, что сайт взломан (рис. 2.1).

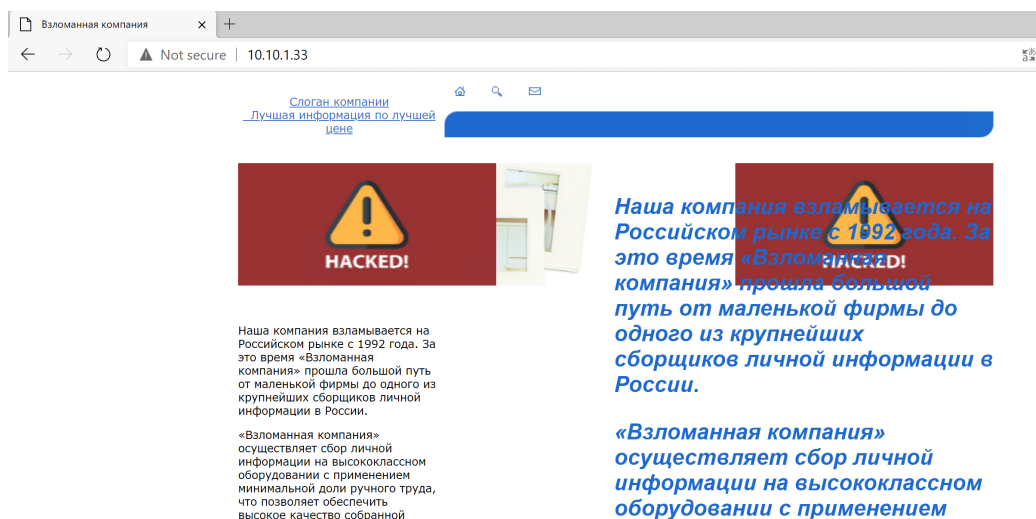


Рисунок 2.1: Взломанный сайт компании

Подключаемся к серверу Bitrix через SSH (рис. 2.2).

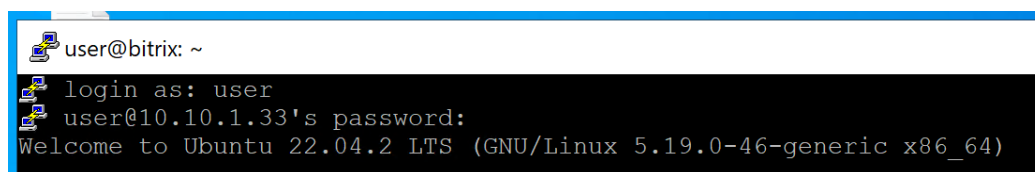


Рисунок 2.2: Подключение к серверу Bitrix

Закрываем локальное повышение привилегий, удалив файл `apache_restart` (рис. 2.3).

```
user@bitrix:~$ ls -la /var/www/html/
иторо 5640
drwxrwxr-x 12 www-data www-data 4096 окт 1 09:57 .
drwxr-xr-x 3 root root 4096 июл 7 2023 ..
-rw-r--r-- 1 www-data www-data 519 июл 7 2023 404.php
-rw-r--r-- 1 www-data www-data 216 июл 7 2023 .access.php
-rwsr-sr-x 1 root root 16048 июл 31 2023 apache_restart
drwxrwxr-x 25 www-data www-data 4096 сен 22 2023 bitrix
-rw-r--r-- 1 www-data www-data 265 июл 7 2023 .bottom.menu.php
-rw-r--r-- 1 www-data www-data 34 окт 1 09:55 caidao.php
drwxr-xr-x 2 www-data www-data 4096 июл 7 2023 company
drwxr-xr-x 2 www-data www-data 4096 июл 7 2023 contacts
-rw-r--r-- 1 www-data www-data 860 июл 7 2023 .htaccess
drwxr-xr-x 2 www-data www-data 4096 июл 7 2023 include
-rw-r--r-- 1 www-data www-data 1168 окт 1 10:44 index.php
drwxr-xr-x 2 www-data www-data 4096 июл 7 2023 login
drwxr-xr-x 2 www-data www-data 4096 июл 7 2023 news
-rw-r--r-- 1 root root 201 окт 1 09:57 password_recovery.php
drwxr-xr-x 2 www-data www-data 4096 июл 7 2023 products
-rw-r--r-- 1 root root 5661008 окт 1 10:44 RickRolled.mp4
-rw-r--r-- 1 www-data www-data 76 окт 1 09:56 script.sh
drwxr-xr-x 2 www-data www-data 4096 июл 7 2023 search
-rw-r--r-- 1 www-data www-data 611 июл 7 2023 .section.php
drwxr-xr-x 2 www-data www-data 4096 июл 7 2023 services
-rw-r--r-- 1 www-data www-data 496 июл 7 2023 .top.menu.php
drwxrwxr-x 4 www-data www-data 4096 окт 1 09:56 upload
-rw-r--r-- 1 www-data www-data 509 июл 7 2023 urlrewrite.php
user@bitrix:~$
```

Рисунок 2.3: Заккрытие локального повышения привилегий

```
user@bitrix:~$ sudo rm /var/www/html/apache_restart
```

Рисунок 2.4: Заккрытие локального повышения привилегий

Для закрытия уязвимости создаем файл `.htaccess` в директории, отклоняющий все запросы к директории `vote` (рис. 2.5).

```
GNU nano 6.2 /var/www/html/bitrix/tools/vote/.htaccess *
deny from all
```

Рисунок 2.5: Создание файла `.htaccess`

Закрываем все вредоносные сессии (рис. 2.6).

```

user@bitrix:~$ sudo ss -tp
State      Recv-Q      Send-Q       Local Address:Port      Peer Address:Port
ESTAB      0            64           10.10.1.33:ssh          10.10.1.253:38152
d",pid=5899,fd=4), ("sshd",pid=5774,fd=4))
user@bitrix:~$ sudo kill 4567

```

Рисунок 2.6: закрытие вредоносных сессий

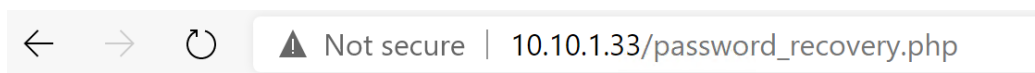
Сбрасываем пароль администратора при помощи специального скрипта (рис. 2.7).

```

GNU nano 6.2 /var/www/html/password_recovery.php
?
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');
?>

```

Рисунок 2.7: Скрипт



← → ↻ ⚠ Not secure | 10.10.1.33/password_recovery.php

Рисунок 2.8: Выполнение скрипта

Восстанавливаем сайт из бэкапа (рис. 2.9).

```

user@bitrix:~$ ls -la /var/bitrix_backups/
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

```

Рисунок 2.9: Бэкап

```

user@bitrix:~$ sudo tar xvfz /var/bitrix_backups/Bitrix_full_backup.tar.gz -C /var/www/html/

```

Рисунок 2.10: Восстановление сайта из бэкапа

Сайт воостановлен (рис. 2.11).

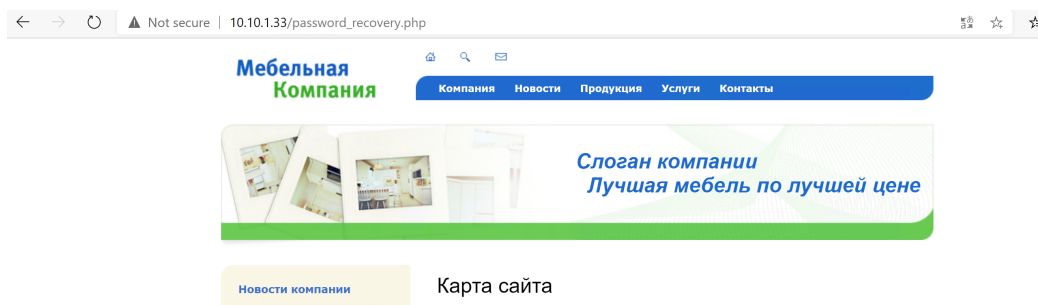


Рисунок 2.11: Восстановленный сайт компании

Уязвимость и последствие успешно устранены (рис. 2.12).



Рисунок 2.12: Устранение уязвимости и последствия

2.2 Уязвимость GitLab RCE и последствие GitLab meterpreter

Подключаемся к серверу GitLab (рис. 2.13).



Рисунок 2.13: Подключение к серверу GitLab

С локального ПК отправляем нужное обновление на сервер (рис. 2.14).


```

root@ampire-gitlab:/home# ss -tp
State      Recv-Q      Send-Q       Local Address:Port      Peer Address:Port
ESTAB      0            0            127.0.0.1:43498         127.0.0.1:9168
users:(("prometheus",pid=4511,fd=26))
ESTAB      0            0            10.10.2.18:46784        195.239.174.11:5559
users:(("SYn57A",pid=10578,fd=3))
ESTAB      0            0            127.0.0.1:9187         127.0.0.1:55410
users:(("postgres_export",pid=4502,fd=8))
ESTAB      0            0            127.0.0.1:8082         127.0.0.1:49876

```

Рисунок 2.17: Поиск вредоносных сессий

```

root@ampire-gitlab:/home# kill -9 10578

```

Рисунок 2.18: Завершение вредоносных сессий

Уязвимость и последствие успешно устранены (рис. 2.19).

GitLab RCE Не назначено	Устранено
GitLab meterpreter Не назначено	Устранено

Рисунок 2.19: Устранение уязвимости и последствия

2.3 Уязвимость WSO2 API-Manager RCE и последствие WSO2 User web

Подключаемся к WSO2 API-Manager (рис. 2.20).

```

Last login: Wed Sep 11 12:12:36 2024 from 10.10.2.254
user@wso2-virtual-machine:~$

```

Рисунок 2.20: Подключение к серверу

Для устранения уязвимости добавляем проверку уязвимого маршрута в конфигурационный файл deployment.toml (рис. 2.20).

```

GNU nano 2.9.3 /opt/wso2am-4.0.0/repository/conf/deployment.toml

enable_h2_console = "true"

[http_access_log]
useLogger = true

[catalina.valves.valve.properties]
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/"]

```

Рисунок 2.21: Добавление проверки в конфигурационный файл

Удаляем все эксплойты и полезные нагрузки с сервера (рис. 2.22).

```

user@wso2-virtual-machine:~$ cd /tmp
user@wso2-virtual-machine:/tmp$ sudo rm payload.elf
user@wso2-virtual-machine:/tmp$ cd /opt/wso2am-4.0.0/repository/deployment/server/webapps/authenticationendpoint/
user@wso2-virtual-machine:/opt/wso2am-4.0.0/repository/deployment/server/webapps/authenticationendpoint$ sudo rm exploit.jsp

```

Рисунок 2.22: Удаление вредоносных файлов

Подключаемся к веб-интерфейсу (рис. 2.22).

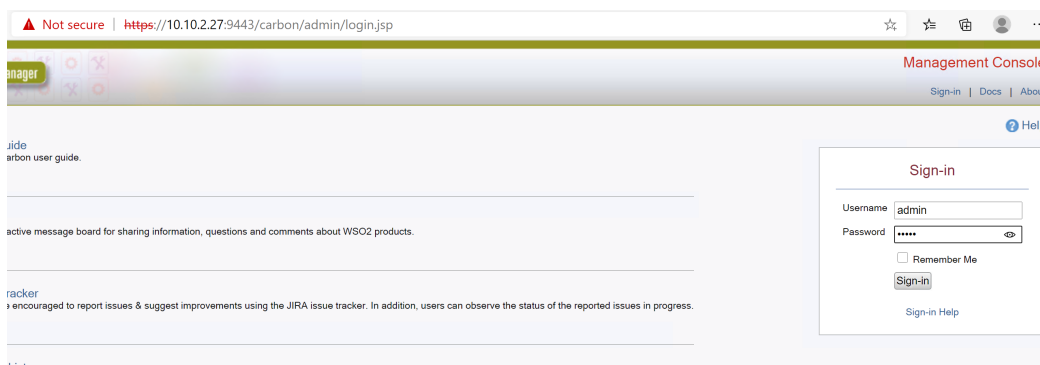


Рисунок 2.23: Подключение к веб-интерфейсу

Удаляем вредоносного пользователя веб-интерфейса (рис. 2.24).

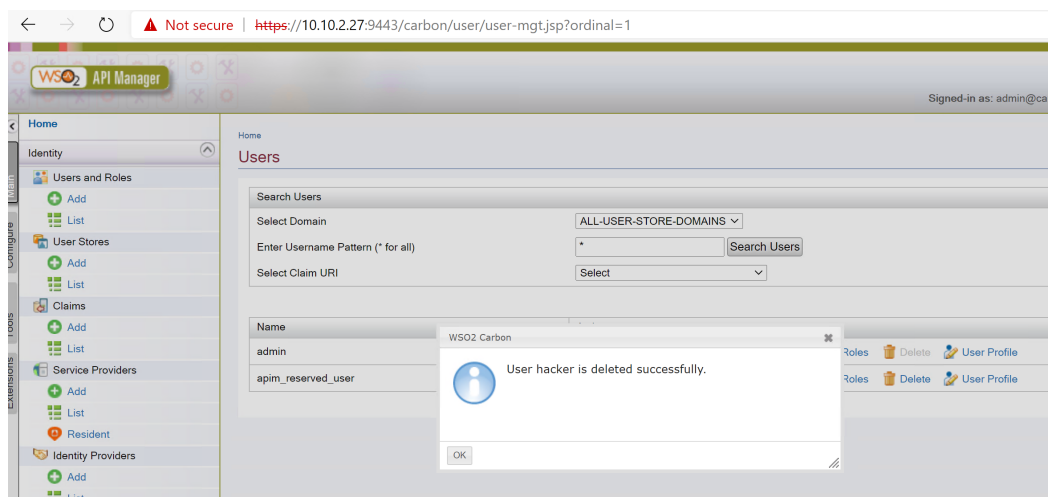


Рисунок 2.24: Удаление вредоносного пользователя

Уязвимость и последствие успешно устранены (рис. 2.25).

WSO2 API-Manager RCE	Устранено
Не назначено	
WSO2 User web	Устранено
Не назначено	

Рисунок 2.25: Устранение уязвимости и последствия

3 Выводы

В результате выполнения работы мы успешно устранили все уязвимости и их последствия (рис. 3.1).

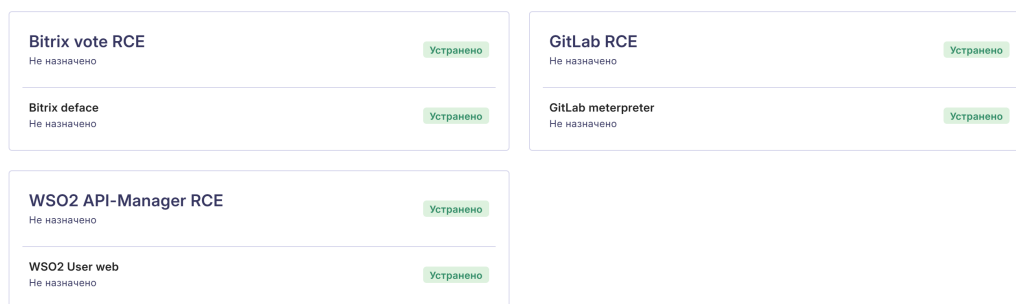


Рисунок 3.1: Успешное устранение всех уязвимостей и последствий