Отчет по практической работе

Эксплуатации уязвимости серверной части

Составил: Артем К. Telegram: @qlVwVlq

Лабораторная работа № 8, 17 модуль, Задание 8.4 (HW-04).

Общая информация:

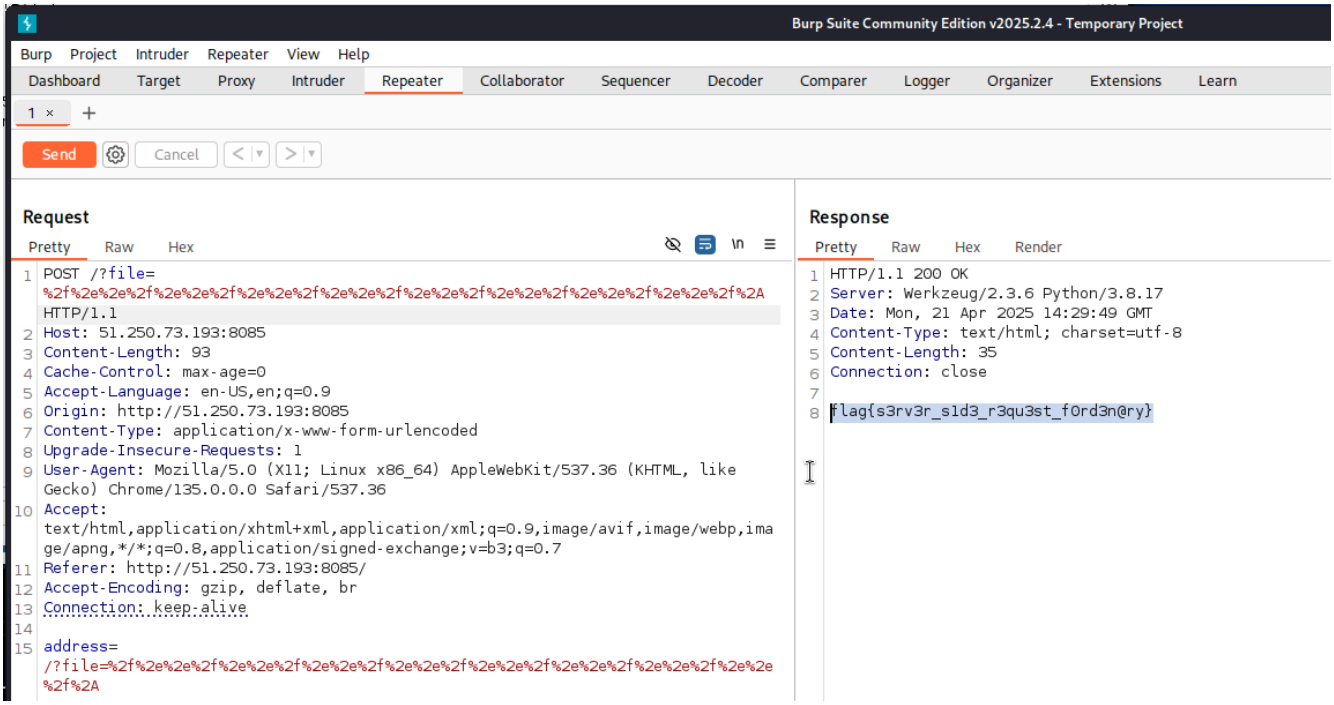
- Период тестирования: 17.04.2025-25.04.2025
- Объект тестирования:

1. http://51.250.73.193:8085 (Задание 8.1),
2. http://51.250.73.193:8086 (Задание 8.2),
3. http://51.250.73.193:8087 (Задание 8.3).

Описание действий и ход работы:

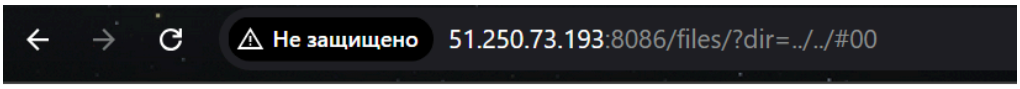
1. Тестирование первого объекта http://51.250.73.193:8085 (Задание 8.1), сайт с уязвимостью SSRF, для теста воспользуемся burpsuite, в запросе видим уязвимое пустое поле address=, подставить можно любое значение, сервер делает запрос по указаниям, на фото 1, в ответе сервера видим флаг задания 8.1.

Фото 1



2. Тестирование второго объекта http://51.250.73.193:8086 (Задание 8.2), сайт с по предоставлению услуг веб-дизайна, в проверках директорий страниц была выявлена уязвимость Directory Traversal, что позволяет нам получить доступ к директориям.

Это позволяет просматривать файлы, изменять их, а также проводить другие манипуляции.



This page in progress, but you can download some materials about ../../.

bin
dev
etc
home
lib
media
mnt
opt
proc
root
run
sbin
srv
sys
tmp
usr
var
.dockerenv
app
flag{D1r3ct0ry_is_d@ng3r0us}

3. Тестирование третьего объекта http://51.250.73.193:8087 (Задание 8.3) сервис по генерации pdf-документов, где каждый клиент может сгенерировать себе документ с любой надписью.

Выполнен перебор различных ID с использование инструмента burpsuite (Фото 2), по результатам сканирования была выявлена уязвимость insecure Direct Object Reference - IDOR.

Приложение показывает а также предоставляет доступ к внутреннему объекту, не проверяя, авторизован ли пользователь (Фото 3).

Фото 2 (перебор файлов, нахождение)

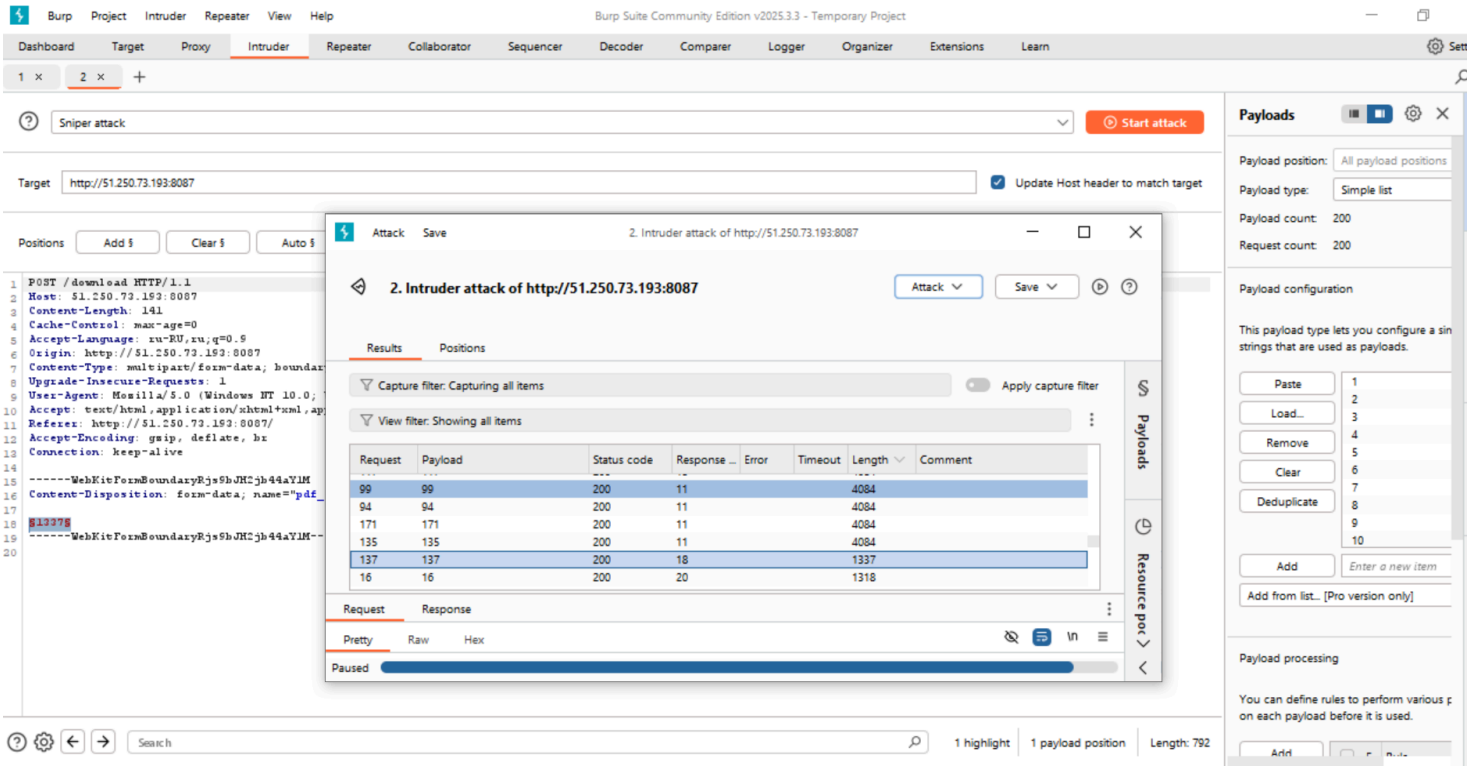
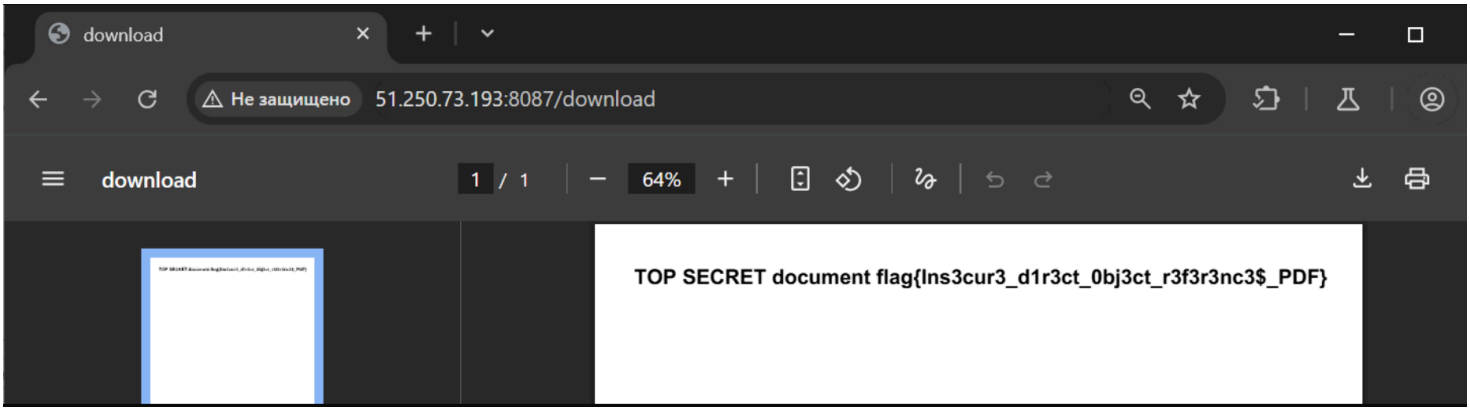


Фото 3 (секретный документ 137)



Итог:

- В процессе решения данной лабораторной работы были использованы инструменты (программы и утилиты): Burp Suite, Firefox browser, Chromium, инструменты Kali Linux.

Уязвимости, которые удалось обнаружить:

- SSRF (Server-Side Request Forgery)
- Directory Traversal (Path Traversal)
- IDOR - Insecure Direct Object Reference

Рекомендации по улучшению защиты:

- Для SSRF занести в белый список DNS-имя или IP-адрес, к которому ваше приложение должно получить доступ.
- Провести Chroot jail – операция изменения корневого каталога диска для запущенного процесса и его дочерних процессов. Программа, запущенная в таком окружении не может получить доступ к файлам вне нового корневого каталога для Directory Traversal (Path Traversal).
- IDOR Проверка авторизации, использовать UUID или хеши.