Лабораторная работа 2

Захват интернет-магазина компании

Панченко Денис 1132229056

Савурская Полина 1132222827

Кочарян Никита 1132221541

Норсоян Шушаник 1132221545

Сухальская Ксения 1132229052

Умярова Камилла 1132229051

Содержание

# 1. Цель работы

Произвести атаку на интернет-магазин компании и найти два флага.

# 2. Выполнение лабораторной работы

## 2.1 Исследование веб-директории магазина

Сайт магазина находится по адресу http://195.239.174.35/. Зайдем на этот сайт ([рис. 1](#fig-001)).

|  |
| --- |
| Рисунок 1: Интернет-магазин |

Исследуем веб-директории магазина с помощью утилиты DirBuster. Укажем URL сайта и выберем словарь из директории /usr/share/wordlists/dirbuster/ ([рис. 2](#fig-002)).

|  |
| --- |
| Рисунок 2: Утилита DirBuster |

После завершения сканирования переходим на вкладку с результатами, на которой отображены найденные файлы ([рис. 3](#fig-003)).

|  |
| --- |
| Рисунок 3: Результаты сканирования |

Для получения флага переходим по ссылке http://195.239.174.35/info.php ([рис. 4](#fig-004)).

|  |
| --- |
| Рисунок 4: Получение флага |

Флаг успешно найден ([рис. 5](#fig-005)).

|  |
| --- |
| Рисунок 5: Успешное нахождение флага |

## 2.2 Атака на веб-сайт магазина

На странице сайта есть ссылка на страницу с API ([рис. 6](#fig-006)).

|  |
| --- |
| Рисунок 6: Ссылка на страницу с API |

Переходим на страницу с API ([рис. 7](#fig-007)).

|  |
| --- |
| Рисунок 7: Страница с API |

На странице указаны примеры запросов. Попробуем произвести запрос ([рис. 8](#fig-008)).

|  |
| --- |
| Рисунок 8: Запрос |

Теперь изменяем запрос для проведения XXE-атаки ([рис. 9](#fig-009)).

|  |
| --- |
| Рисунок 9: Запрос для XXE-атаки |

Выполнив запрос, получаем искомый флаг в формате base64. Декодируем флаг ([рис. 10](#fig-010)).

|  |
| --- |
| Рисунок 10: Получение флага |

Флаг успешно найден ([рис. 11](#fig-011)).

|  |
| --- |
| Рисунок 11: Успешное нахождение флага |

# 3. Выводы

В результате выполнения работы мы успешно произвели атаку на интернет-магазин и нашли два флага.