

Отчет по выполнению индивидуального проекта. Этап №5

Основы информационной безопасности

Авдадаев Джамал, НКАбд-01-23

Содержание

1	Цель работы	1
2	Теоретическое введение.....	1
3	Выполнение лабораторной работы.....	1
4	Выводы.....	11
	Список литературы	11

1 Цель работы

Научиться использовать Burp Suite.

2 Теоретическое введение

Burp Suite представляет собой набор мощных инструментов безопасности веб-приложений, которые демонстрируют реальные возможности злоумышленника, проникающего в веб-приложения. Эти инструменты позволяют сканировать, анализировать и использовать веб-приложения с помощью ручных и автоматических методов. Интеграция интерфейсов этих инструментов обеспечивает полную платформу атаки для обмена информацией между одним или несколькими инструментами, что делает Burp Suite очень эффективной и простой в использовании платформой для атаки веб-приложений. [1].

3 Выполнение лабораторной работы

Запускаю локальный сервер, на котором открою веб-приложение DVWA для тестирования инструмента Burp Suite (рис. 1).

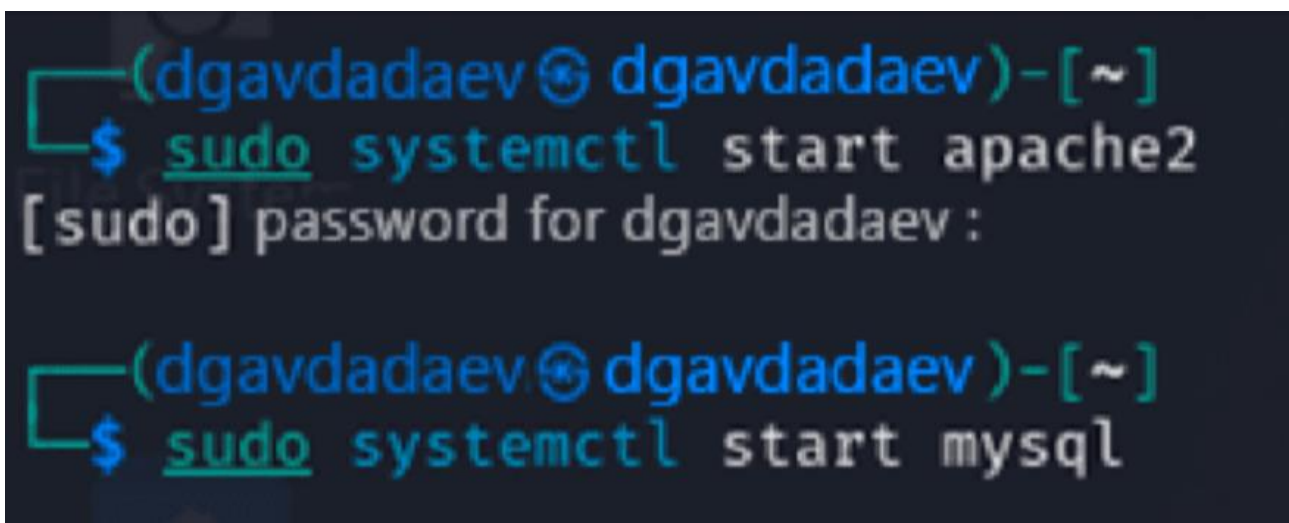


Рис. 1: Запуск локального сервера

Запускаю инструмент Burp Suite (рис. 2).

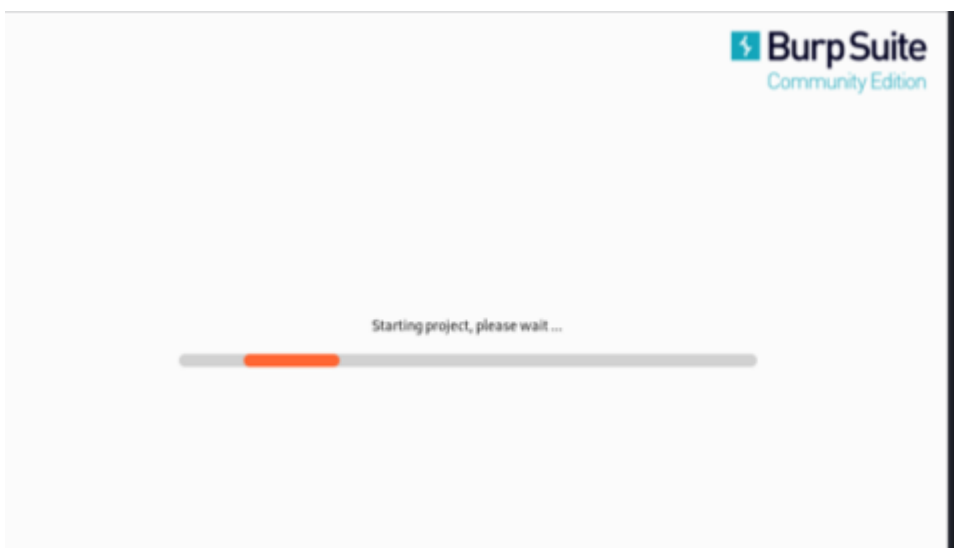


Рис. 2: Запуск приложения

Открываю сетевые настройки браузера, для подготовке к работе (рис. 3).

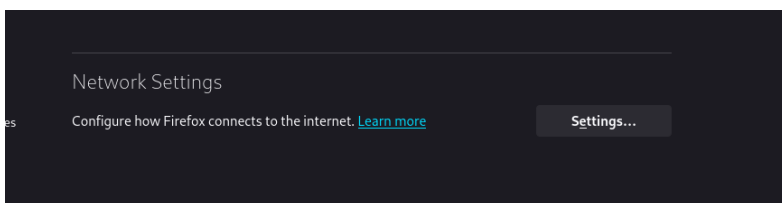


Рис. 3: Сетевые настройки браузера

Изменение настроек сервера для работы с прокси и захватом данных с помощью Burp Suite (рис. 4).

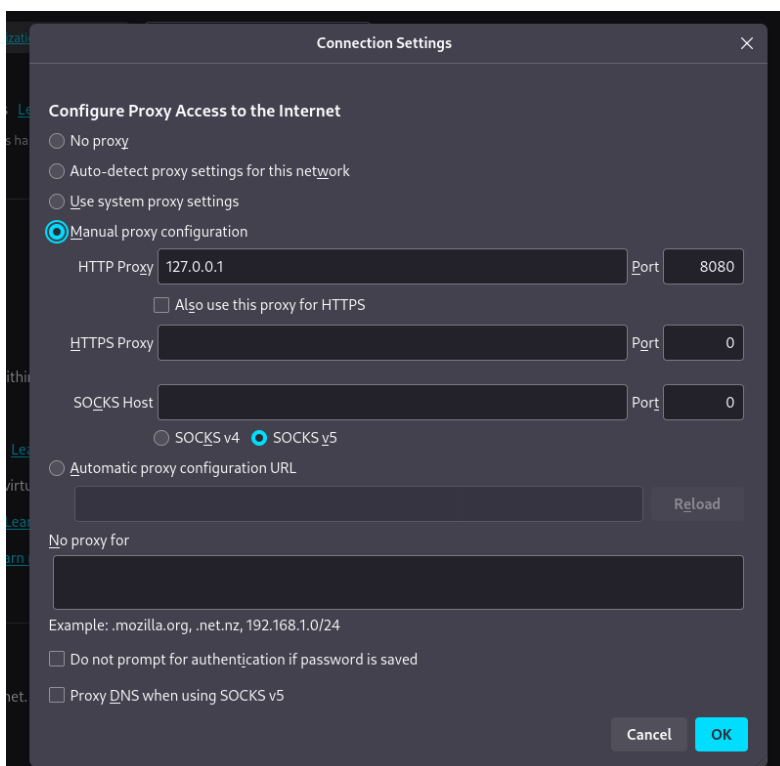


Рис. 4: Настройки сервера

Изменяю настройки Прoxy инструмента Burp Suite для дальнейшей работы (рис. 5).

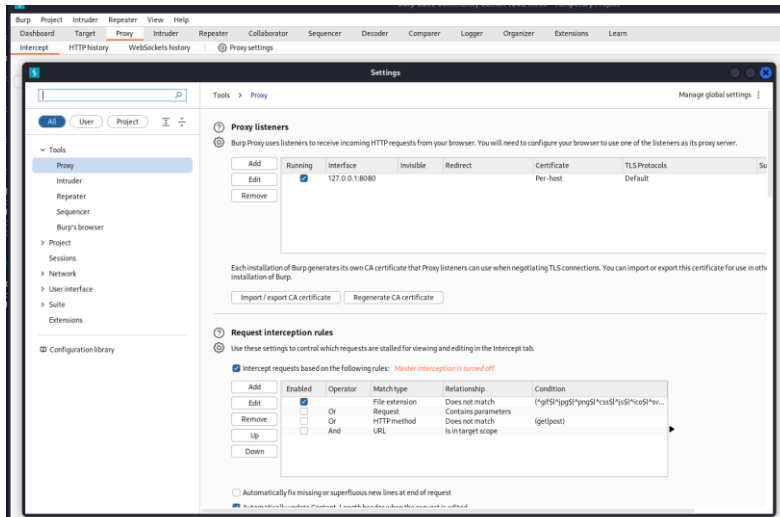


Рис. 5: Настройки Burp Suite

Во вкладке Proxy устанавливаю “Intercept is on” (рис. 6).

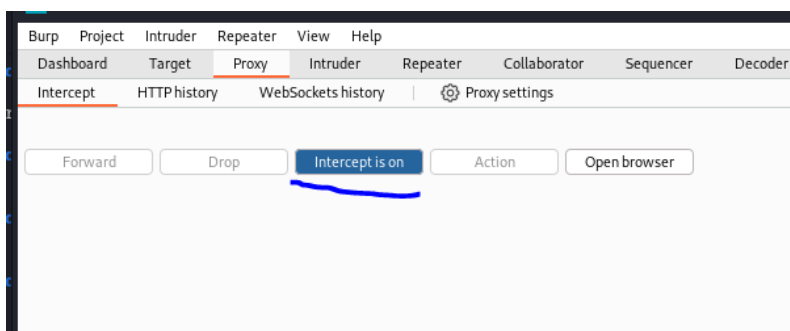


Рис. 6: Настройки Proxy

Чтобы Burp Suite исправно работал с локальным сервером, необходимо установить параметр `network_allow_hijacking_localhost` на `true` (рис. 7).

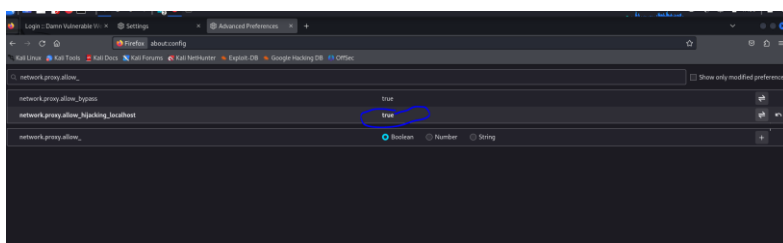


Рис. 7: Настройки параметров

Пытаюсь зайти в браузере на DVWA, тут же во вкладки Proxy появляется захваченный запрос. Нажимаем "Forward", чтобы загрузить страницу (рис. 8).

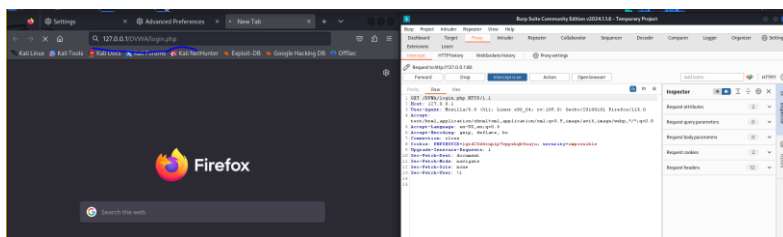


Рис. 8: Получаемые запросы сервера

Загрузилась страница авторизации, текст запроса поменялся (рис. 9).

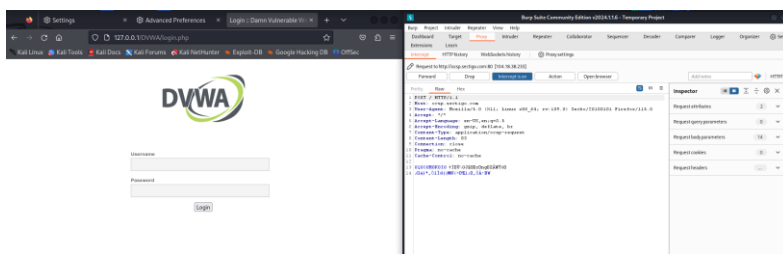


Рис. 9: Страница авторизации

История запросов хранится во вкладке Target (рис. 10).

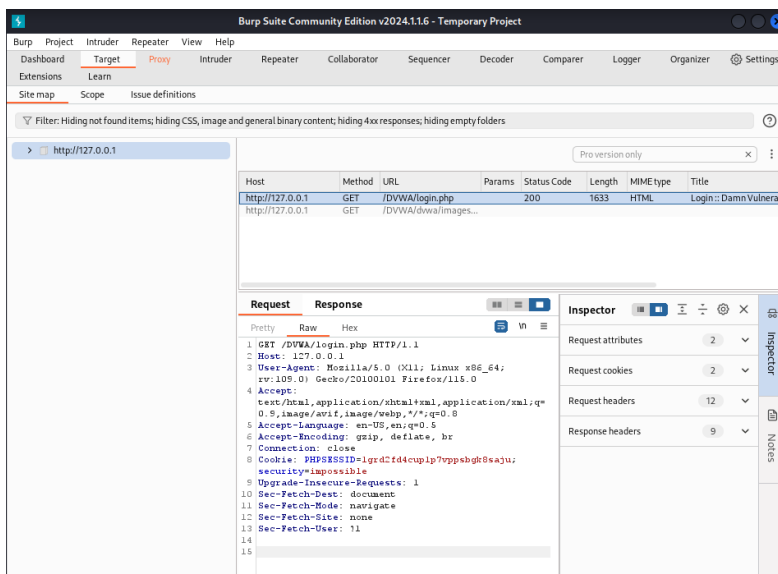


Рис. 10: История запросов

Попробуем ввести неправильные, случайные данные в веб-приложении и нажмем Login. В запросе увидим строку, в которой отображаются введенные нами данные, то есть поле для ввода (рис. 11).

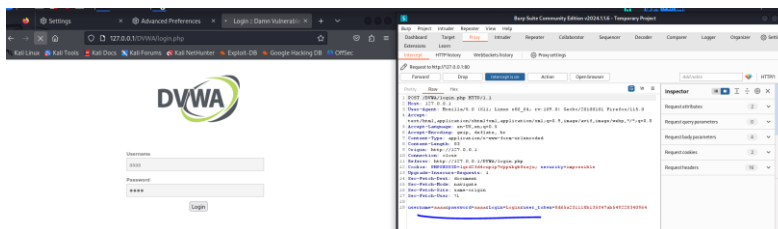


Рис. 11: Ввод случайных данных

Этот запрос так же можно найти во вкладке Target, там же жмем правой кнопкой мыши на хост нужного запроса, и далее нажимаем “Send to Intruder” (рис. 12).

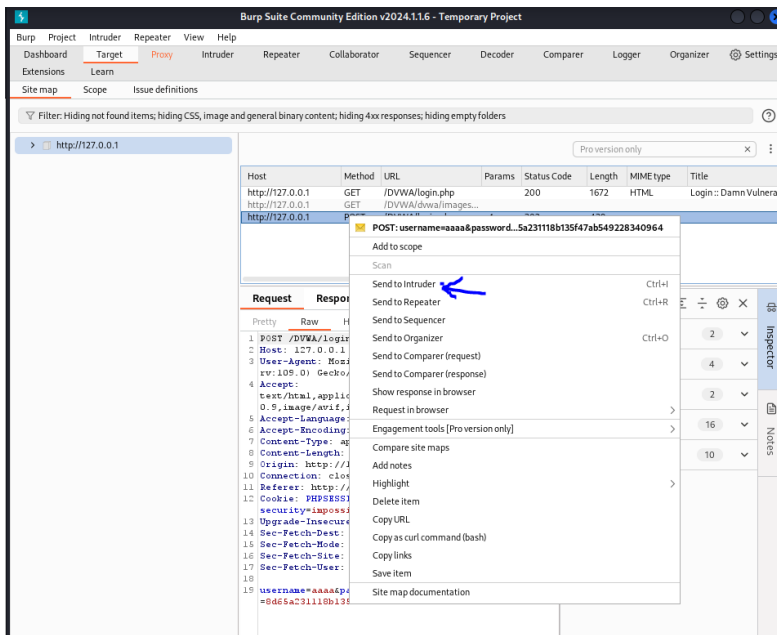


Рис. 12: POST-запрос с вводом пароля и логина

Попадаем на вкладку Intruder, видим значения по умолчанию у типа атаки и наш запрос (рис. 13).

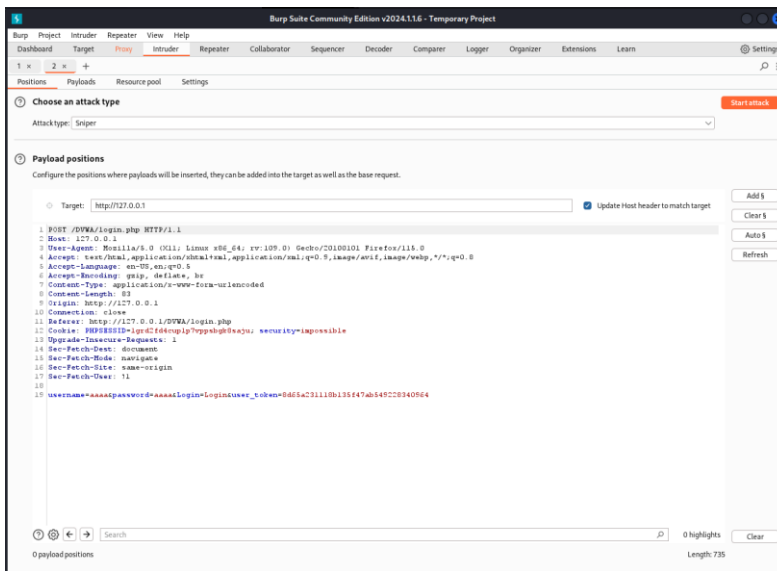


Рис. 13: Вкладка Intruder

Изменяем значение типа атаки на Cluster bomb и проставляем специальные символы у тех данных в форме для ввода, которые будем пробивать, то есть у имени пользователя и пароля (рис. 14).

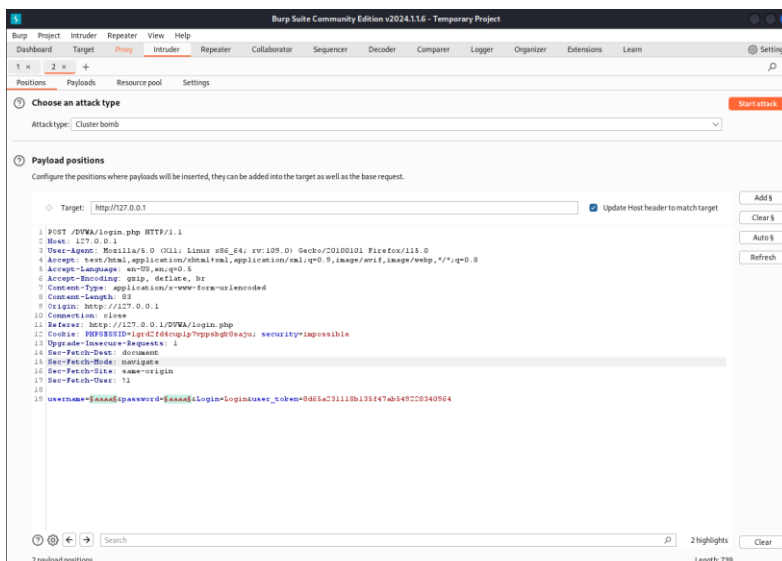


Рис. 14: Изменение типа атаки

Так как мы отметили два параметра для подбора, то нам нужно два списка со значениями для подбора. Заполняем первый список в Payload setting (рис. 15).

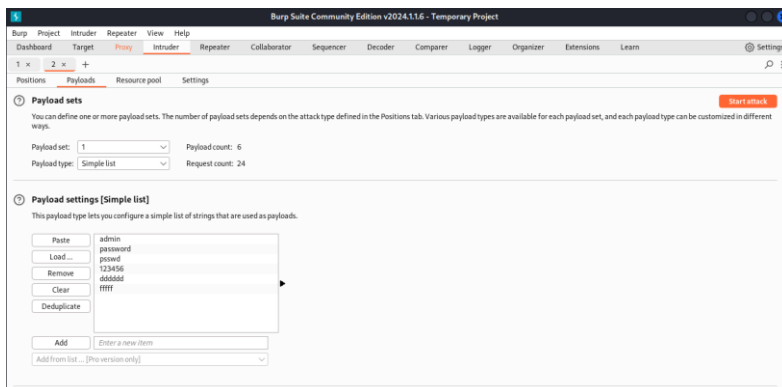


Рис. 15: Первый Simple list

Переключаемся на второй список и добавляем значения в него. В строке request count видим нужное количество запросов, чтобы проверить все возможные пары пользователь-пароль (рис. 16).

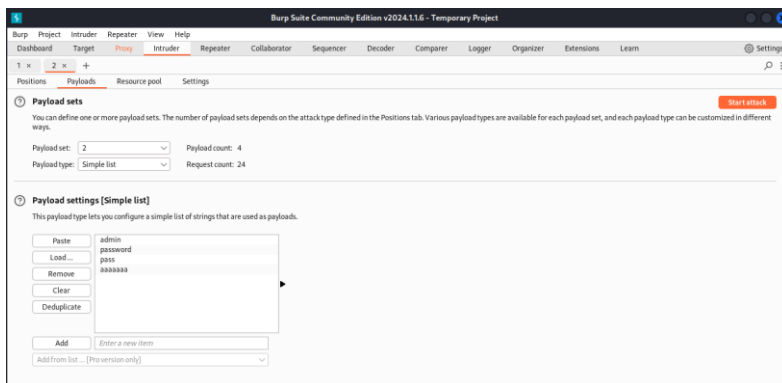
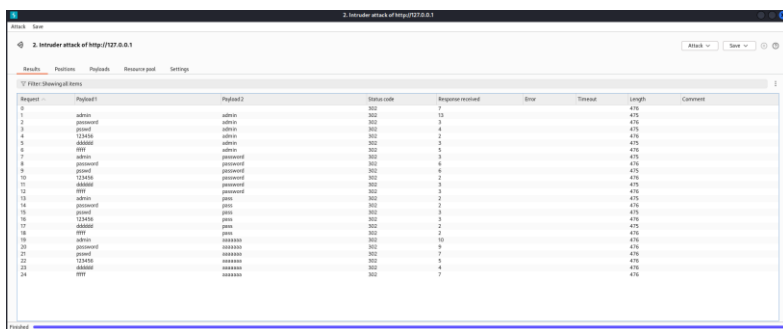


Рис. 16: Второй Simple list

Запускаю атаку и начинаю подбор (рис. 17).



The screenshot shows the 'Results' tab of an Intruder attack in Burp Suite. The table lists 24 requests with columns for Request, Payload1, Payload2, Status code, Response received, Error, Timeout, Length, and Comment. The status codes are 302 for all requests, indicating a redirect.

Request	Payload1	Payload2	Status code	Response received	Error	Timeout	Length	Comment
0			302	7			475	
1	admin	admin	302	10			475	
2	password	admin	302	3			475	
3	password	admin	302	4			475	
4	123456	admin	302	3			475	
5	admin	admin	302	3			475	
6	admin	admin	302	3			475	
7	admin	password	302	3			475	
8	password	password	302	6			475	
9	password	password	302	6			475	
10	123456	password	302	3			475	
11	admin	password	302	3			475	
12	admin	password	302	3			475	
13	admin	password	302	3			475	
14	password	password	302	2			475	
15	password	password	302	2			475	
16	123456	password	302	3			475	
17	admin	password	302	3			475	
18	admin	password	302	3			475	
19	password	password	302	10			475	
20	password	password	302	9			475	
21	password	password	302	7			475	
22	123456	password	302	6			475	
23	admin	password	302	4			475	
24	admin	password	302	7			475	

Рис. 17: Запуск атаки

При открытии результата каждого post-запроса можно увидеть полученный get-запрос, в нем видно, куда нас перенаправило после выполнения ввода пары пользователь-пароль. В представленном случае с подбором пары admin-admin нас перенаправило на login.php, это значит, что пара не подходит (рис. 18).

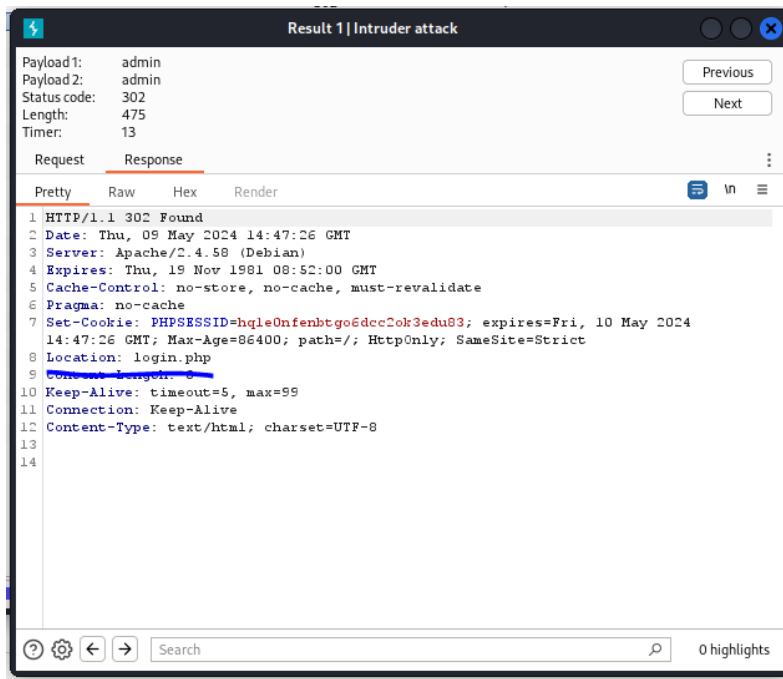


Рис. 18: Результат запроса

Проверим результат пары admin-password во вкладке Response, теперь нас перенаправляет на страницу index.php, значит пара должна быть верной (рис. 19).

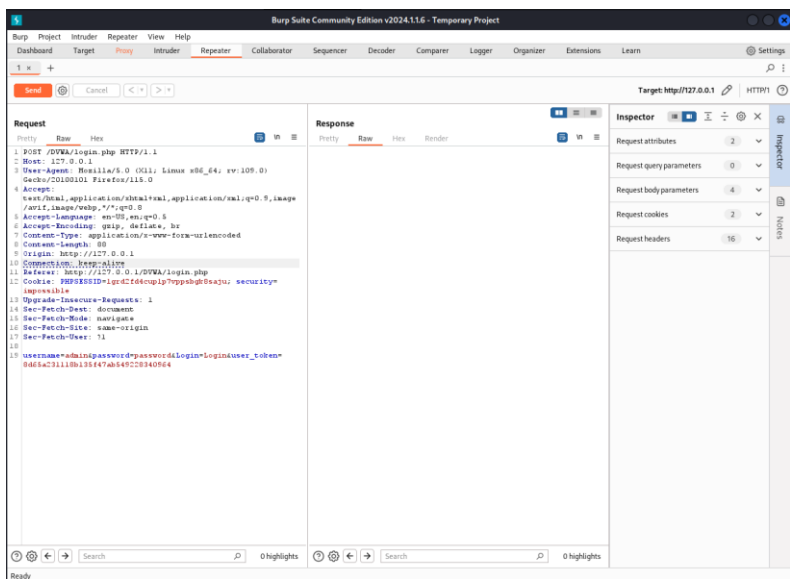


Рис. 21: Вкладка Repeater

Нажимаем “send”, получаем в Response в результат перенаправление на index.php (рис. 22).

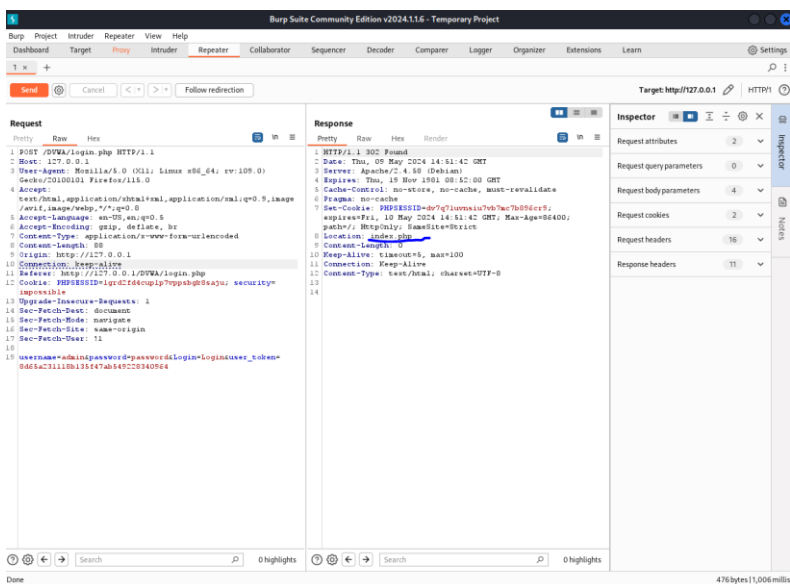


Рис. 22: Окно Response

После нажатия на Follow redirection, получим неcompiled html код в окне Response (рис. 23).

