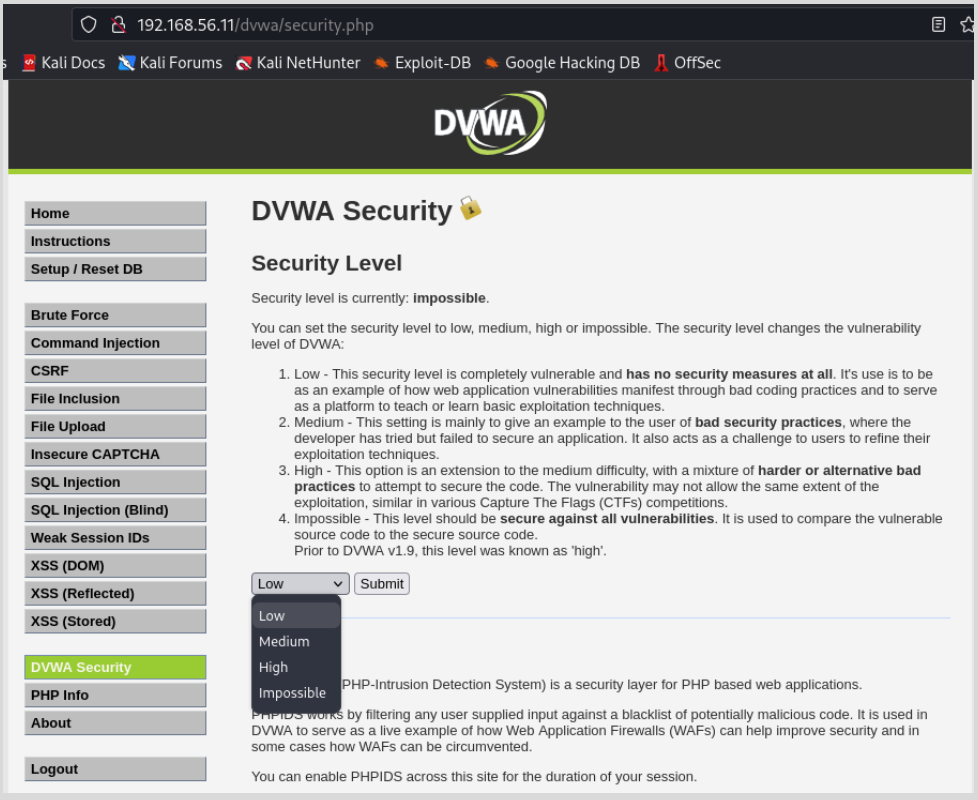
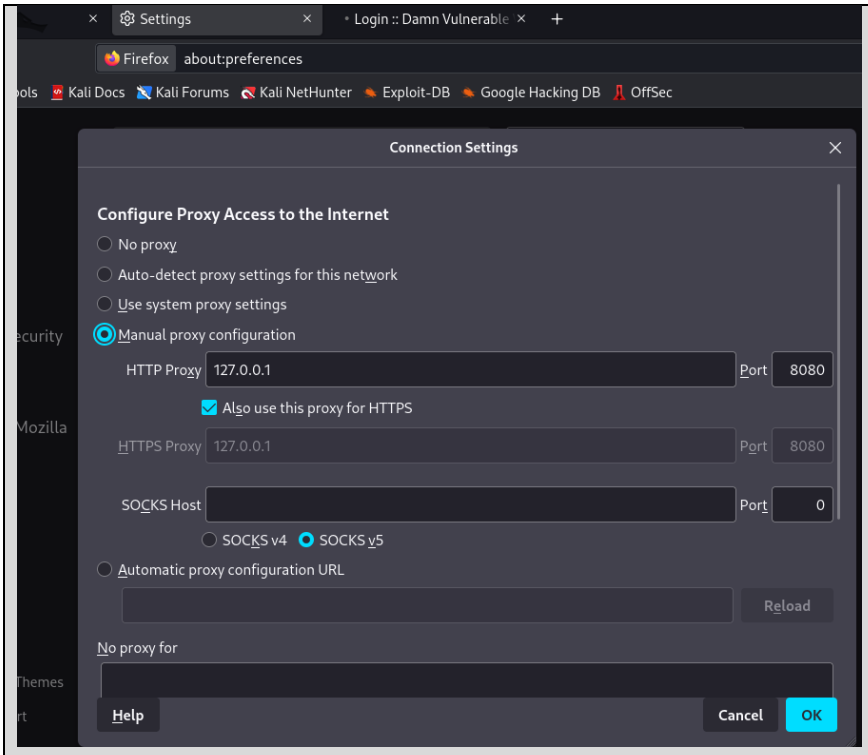
**Задание выполнил студент группы 2345 Романенко К.Д.**

1. Имеется логин **admin** и пароль **yo30E#jb**, которые были заданы администратором для входа в систему с использованием веб-формы. Можно ли считать такую комбинацию логина и пароля безопасной для защиты от брутфорса? Ответ обоснуйте.

> Я считаю, что данная комбинация небезопасна.
>
> Логин admin – стандартный. В 99% случаев эта учётная запись имеет права sudo. Злоумышленник, на этапе разведки пробежится по словарям и обнаружит, что такой логин есть. Далее брутфорсом подберет пароль.
>
> Да, можно выставить ограничение на 5 попыток входа в течение n-ого времени, но рассуждения на данную тему не входят в тело вопроса.

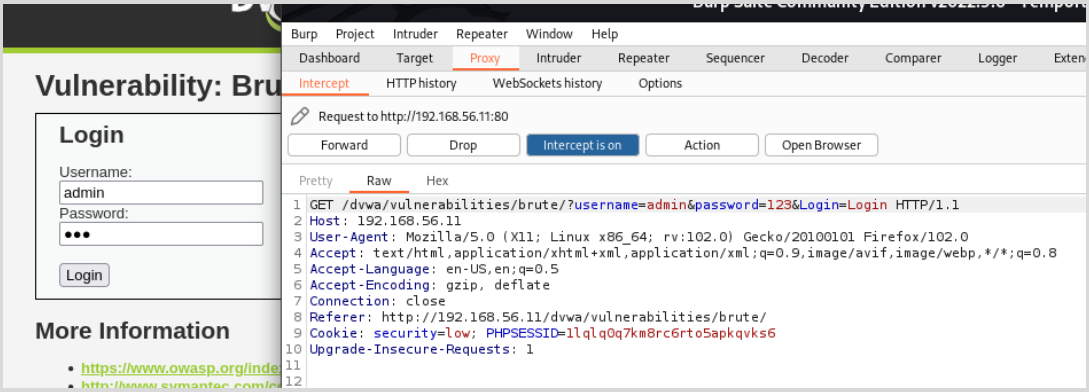
2. Подберите логин и пароль к странице bruteforce-сервиса **dvwa** на уровне сложности LOW. Приложите к ответу описание решения задания и скриншот(ы), подтверждающие решение.

> Открыл браузер на kali. Подключился к 192.168.56.11. Выбрал DVWA.
>
> Ввёл логин – пароль: admin – password. Изменил уровень сложности на Low
>
> 
> 
>
> Открыл BurpSuite. Настроил Proxy в браузере

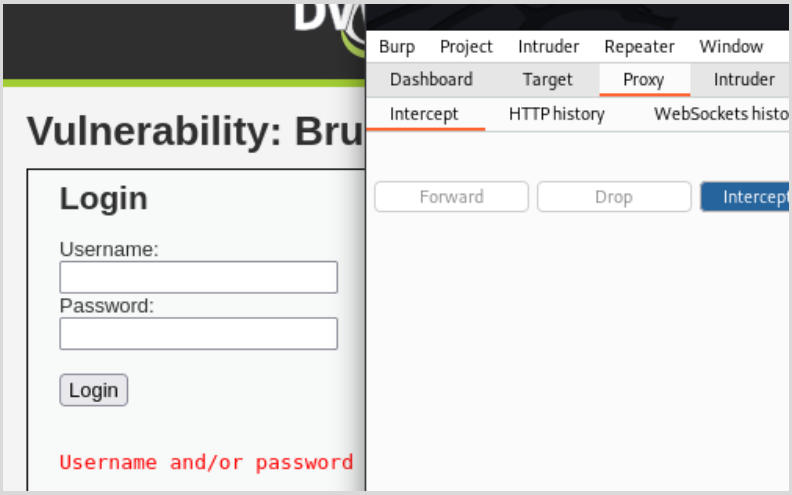



Открыл сайт вкладку Brute Force на сайте DVWA

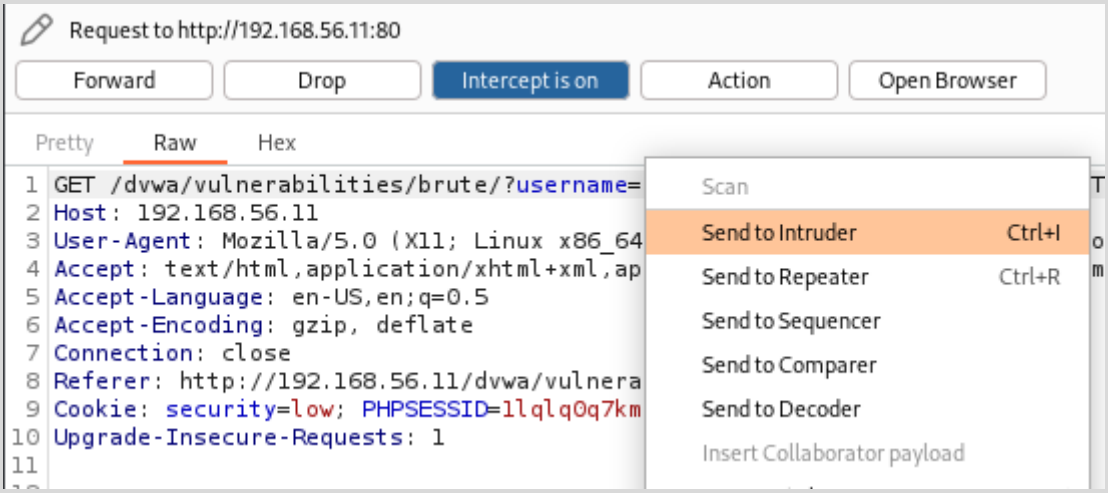
Открыл Burp Suite и запустил proxy. В форму на dvwa ввёл логин - пароль: admin - 123.



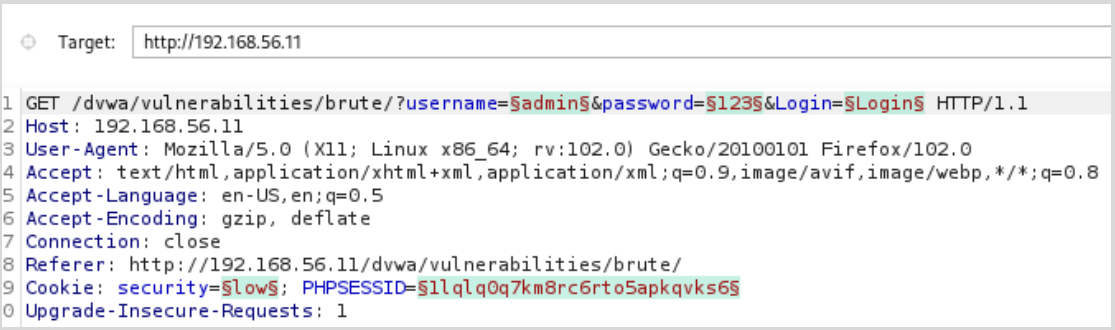

В Burp нажал Forward. Итог: комбинация логин/пароль неверна



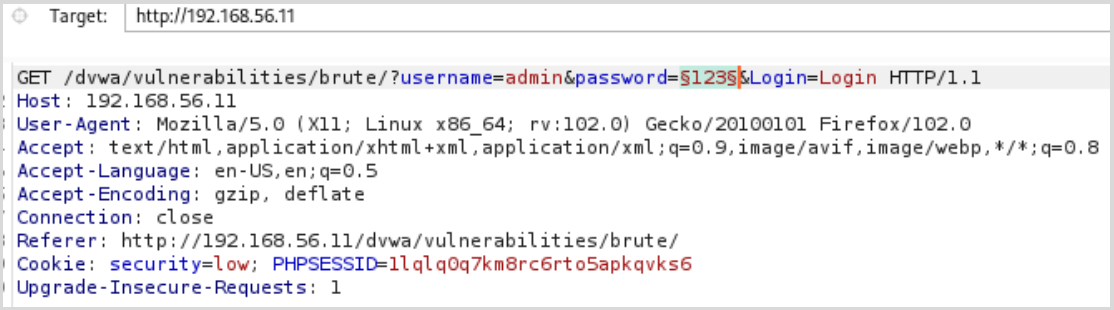
ПКМ в burp и Send to Intruder



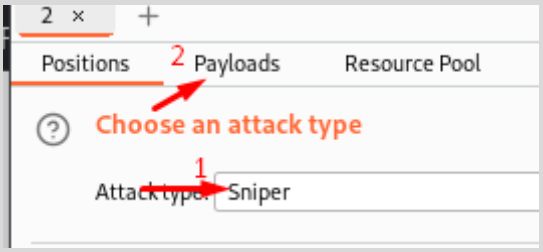

Вывод Intruder'a:



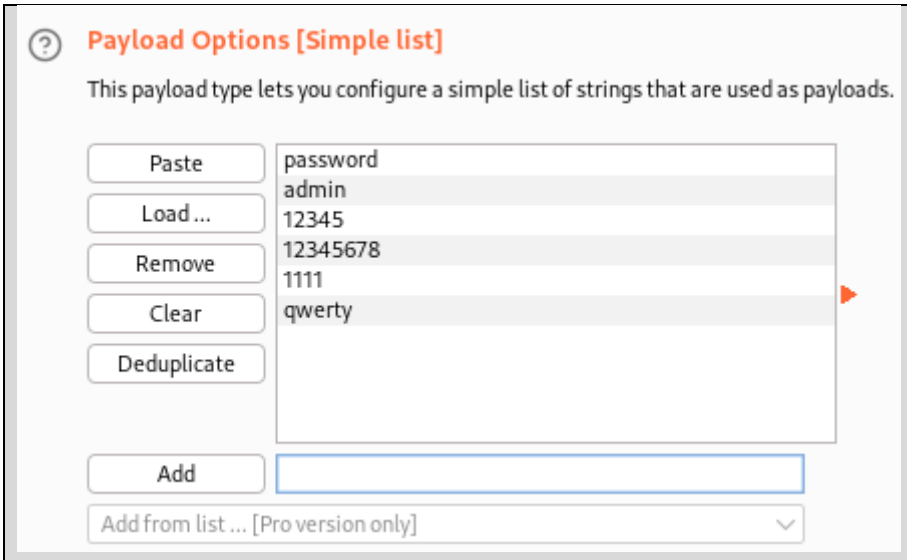

Очистил выделение переменных с помощью Clear. Выделил значение password и нажал Add




Выбрал тип атаки Sniper, открыл вкладку Payloads

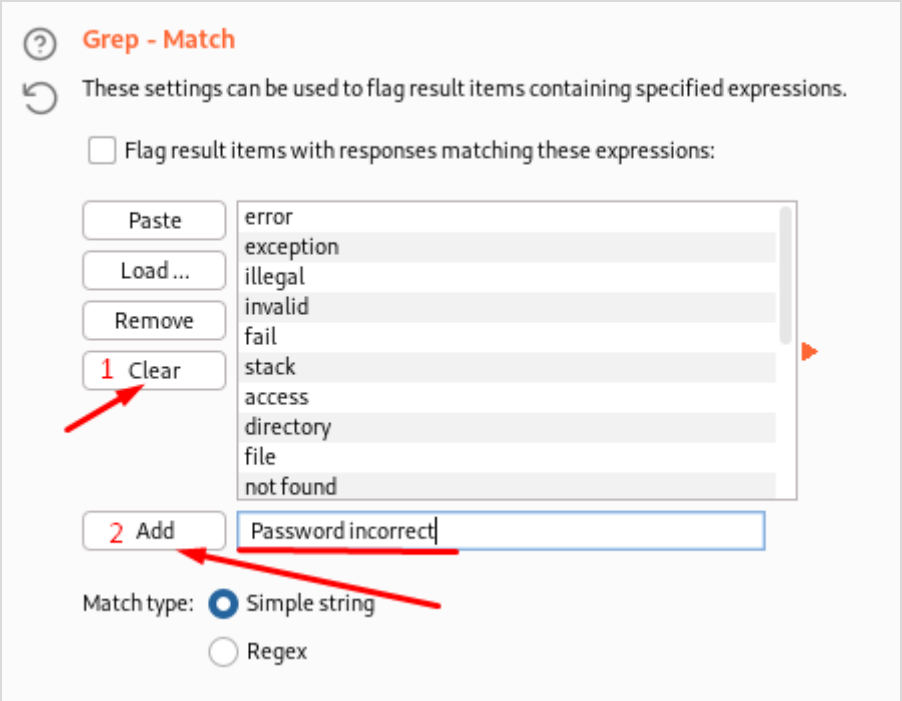



Задал payload set (1 переменная, Simple list) Наполнил payload options данными, т.е. паролями, которые надо подставить методом bruteforce




Вкладка Options. Пункт Grep-Match

Здесь ввёл все варианты вывода ответа, которые нужно отсеять из результатов. Сначала очистил фильтр




>>> Start Attack <<<

Результат:

Filter: Showing all items

| Request | Payload | Status | Error | Timeout | Length | Passwor... | Comment |
|---|---|---|---|---|---|---|---|
| 0 | | 200 | | | 5486 | 1 | |
| 1 | password | 200 | | | 5524 | | |
| 2 | admin | 200 | | | 5486 | 1 | |
| 3 | 12345 | 200 | | | 5486 | 1 | |
| 4 | 12345678 | 200 | | | 5486 | 1 | |
| 5 | 1111 | 200 | | | 5486 | 1 | |
| 6 | qwerty | 200 | | | 5486 | 1 | |

Из всего списка выбивается password с Length = 5524

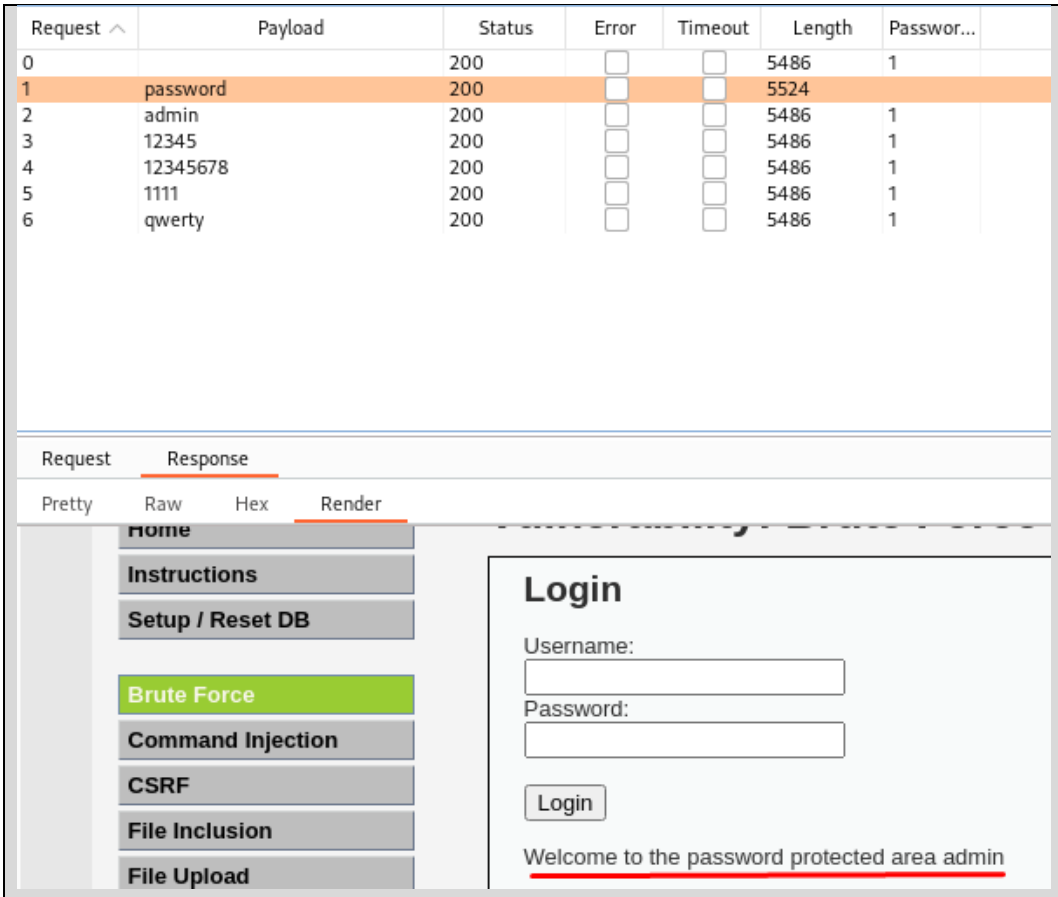
| Request | Payload | Status | Error | Timeout | Length | Passwor... | Comment |
|---|---|---|---|---|---|---|---|
| 0 | | 200 | | | 5486 | 1 | |
| 1 | password | 200 | | | 5524 | | |
| 2 | admin | 200 | | | 5486 | 1 | |
| 3 | 12345 | 200 | | | 5486 | 1 | |
| 4 | 12345678 | 200 | | | 5486 | 1 | |
| 5 | 1111 | 200 | | | 5486 | 1 | |
| 6 | qwerty | 200 | | | 5486 | 1 | |

Request Response

Pretty Raw Hex

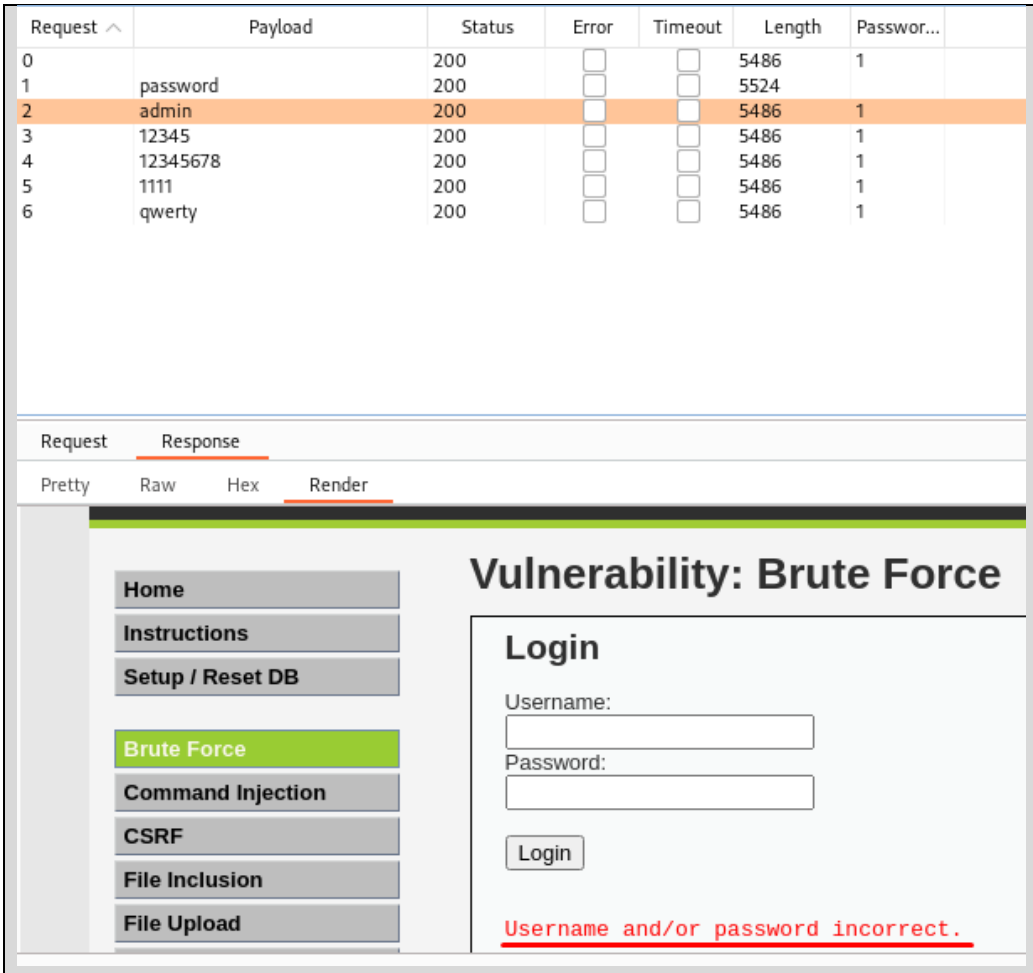
```
1 GET /dvwa/vulnerabilities/brute/?username=admin&password=password&Login=Login HTTP/1.1
2 Host: 192.168.56.11
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Connection: close
8 Referer: http://192.168.56.11/dvwa/vulnerabilities/brute/
9 Cookie: security=low; PHPSESSID=1lqlq0q7km8rc6rto5apkqvks6
10 Upgrade-Insecure-Requests: 1
```

Нажал Response -> Render




Готово. Сочетание admin – password рабочее.

Для самопроверки чекнул другое сочетание с Length = 5486

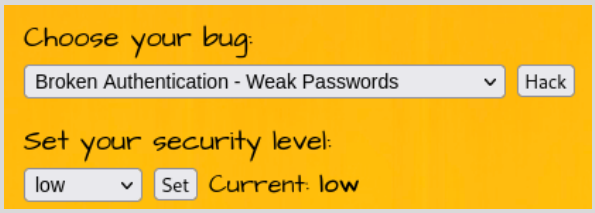



Все отработало верно.

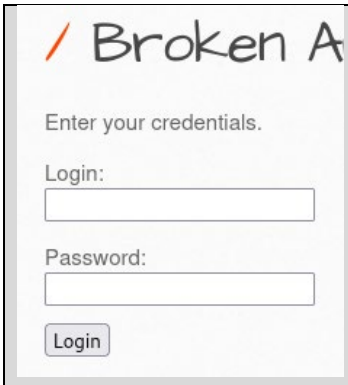
P.S. Не понял, как работает grep, т.к. в выводе были все пароли. Нашел нужный лишь по Lenght. Пробовал разные стоп-слова записать, не помогло

3. Подберите логин и пароль к странице Broken Auth. - Weak Passwords сервиса bwapp на уровне сложности LOW. Приложите к ответу описание решения задания и скриншот(ы), подтверждающие решение.

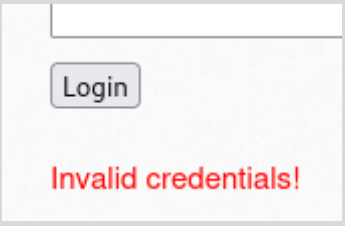
Открыл bwapp. Ввёл логин/пароль – bee/bug. В правом верхнем углу выбрал нужный пункт и уровень сложности




Результат подготовки:

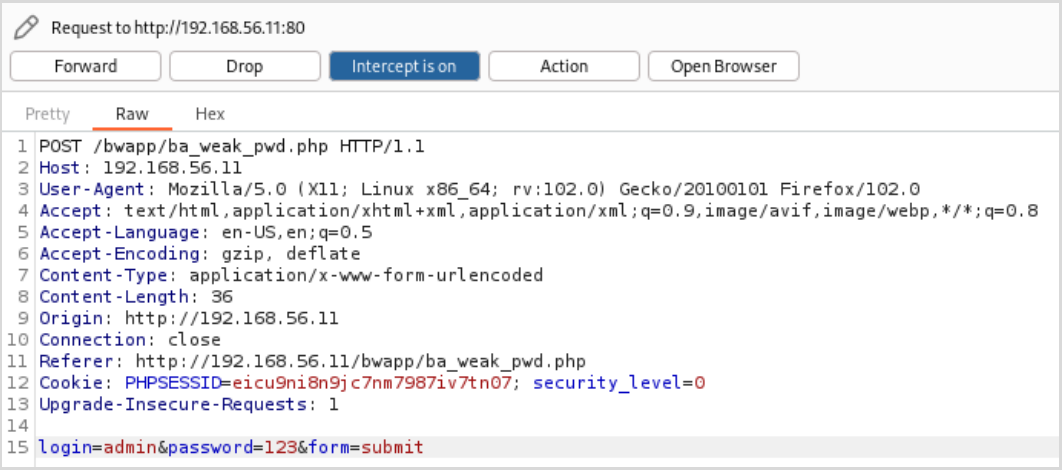



Попробовал различные варианты логин-пароль, ответ один:

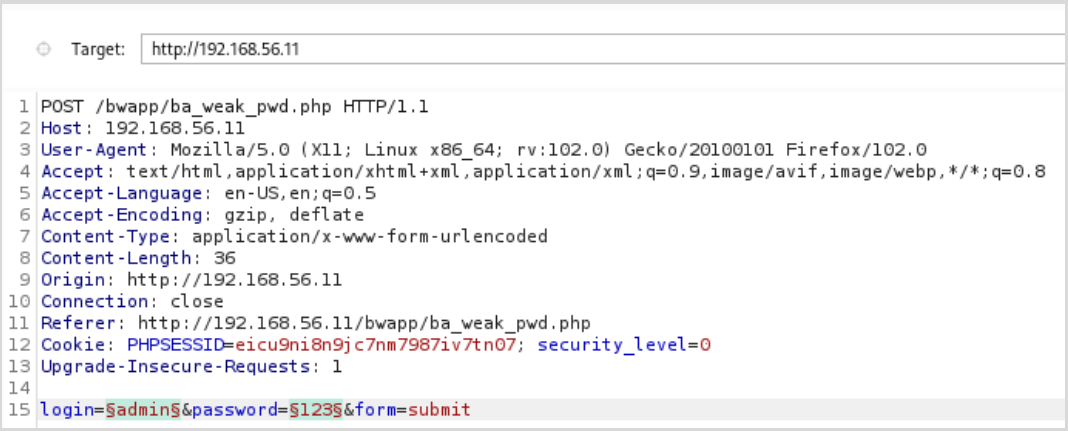



Значит надо подбирать обе переменные. Поехали

Включил Proxy в Burp Suite

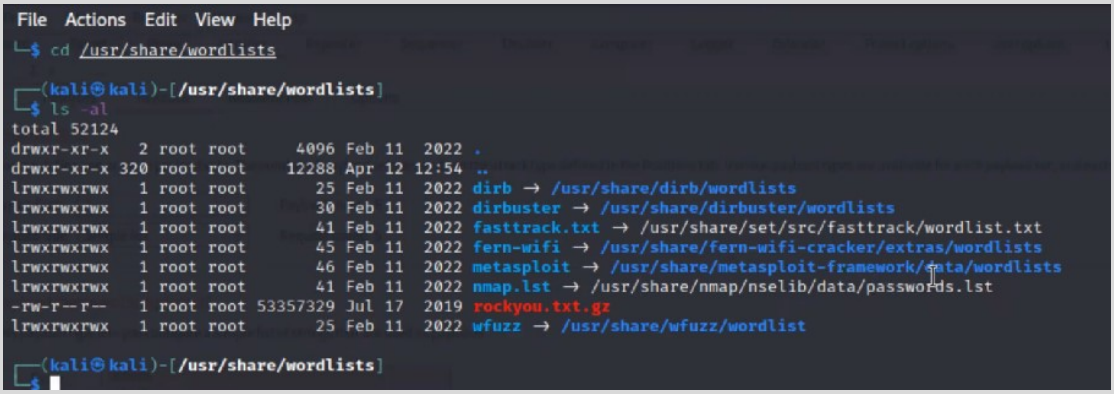



Залил в Intruder. Задал переменные для брут форса




Тип атаки Sniper

В Kali есть заготовленные словари в директории /usr/share/wordlists

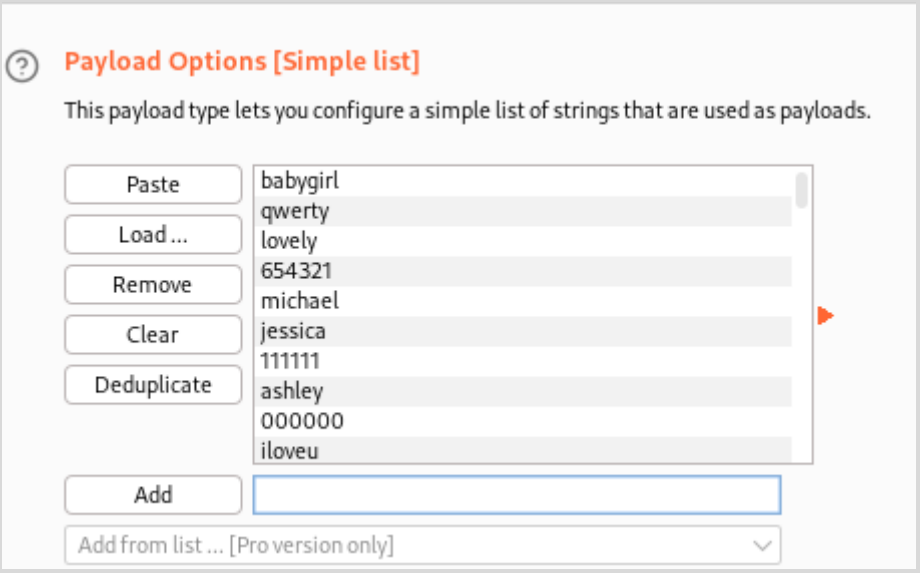



Выбрал словарь nmap

*Также есть большой словарь **fuzzdb** на гитхабе*

Выбрал Payload Set = 1, Simple list

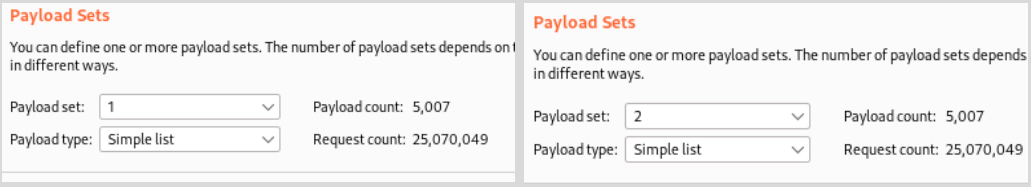
Подставил словарь в Payload Options через Load




Вкладка Options. Пункт Grep-Match

Оставил со значениями по умолчанию. Среди них есть invalid.

Для Payload Set = 2 сделал аналогично

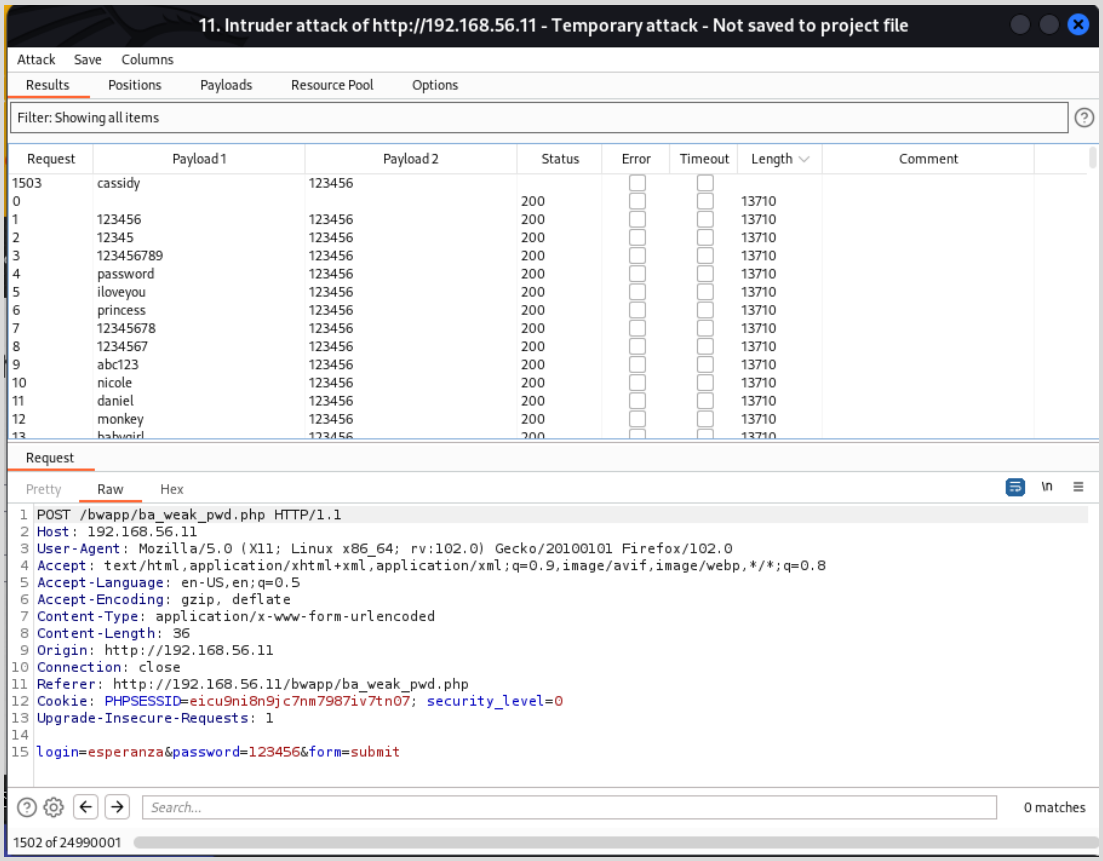



25 млн кобинаций

>>> Start Attack <<<

Старт 02.03.23 в 12:06

24 990 001 комбинация




Очень низкая скорость перебора. 300 комбинаций/час

Ждать, пока он все подберет, времени нет. Оставлю так

*Есть возможность ускорить процесс брут форса?*

- Через консольные утилиты быстрее, GET быстрее POST
- Вообще, конечно, такой брут не делают обычно, это слишком заметно. Делают ну 500 максимум

4. * Протестируйте пример 3 на практике. Приложите к ответу описание решения задания и скриншот(ы), подтверждающие решение.

5. * Решите задание http://challenge01.root-me.org/web-serveur/ch3/ методом брутфорса. Приложите к ответу описание решения задания и скриншот(ы), подтверждающие решение.