

Отчёт по пятому этапу индивидуального проекта

Burp Suite

Вакутайпа Милдред

Содержание

1	Цель работы	5
2	Выполнение лабораторной работы	6
3	Выводы	15
	Список литературы	16

Список иллюстраций

2.1	Запуск сервера	6
2.2	Запуск Burp suite	6
2.3	сетевые настройки сервера	7
2.4	настройки проху	7
2.5	Включение intercept	7
2.6	Установка параметра локального хоста	8
2.7	Пытка зайти в dvwa	8
2.8	вкладка проху	8
2.9	окно dvwa	9
2.10	Измененные данные	10
2.11	Тип атака	10
2.12	Список 1	11
2.13	Список 2	12
2.14	Правильная пара	13
2.15	Окна repeater и response	13
2.16	Полученная страница	14

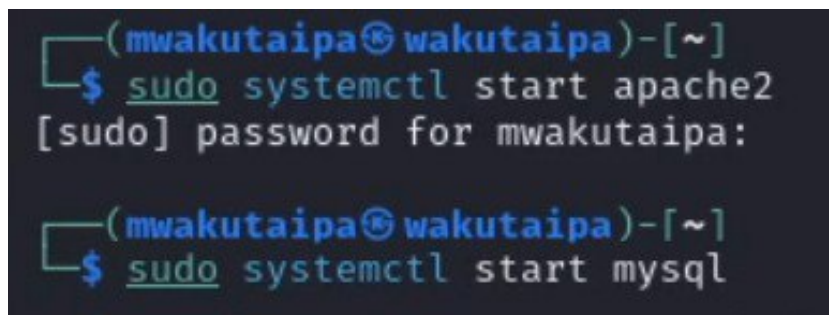
Список таблиц

1 Цель работы

Научиться использовать Burp Suite.

2 Выполнение лабораторной работы

Запускаю локальный сервер DVWA:



```
(mwakutaipa@wakutaipa)-[~]  
$ sudo systemctl start apache2  
[sudo] password for mwakutaipa:  
  
(mwakutaipa@wakutaipa)-[~]  
$ sudo systemctl start mysql
```

Рис. 2.1: Запуск сервера

Запускаю burp suite:



```
(mwakutaipa@wakutaipa)-[~]  
$ burpsuite  
Picked up _JAVA_OPTIONS: -Dawt.useSystemAAFontSettings=on -Dswing.aatext=true  
Your JRE appears to be version 23.0.1 from Debian  
Burp has not been fully tested on this platform and you may experience problems.
```

Рис. 2.2: Запуск Burp suite

Открываю сетевые настройки браузера и изменяю настройки сервера для работы с прокси и захватом данных с burp suite:

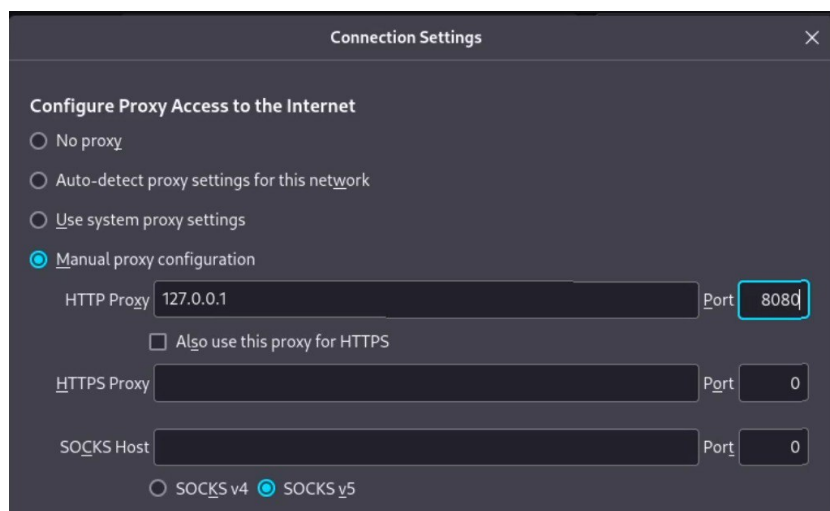


Рис. 2.3: сетевые настройки сервера

Изменяю настройки проху инструмента burp suite:

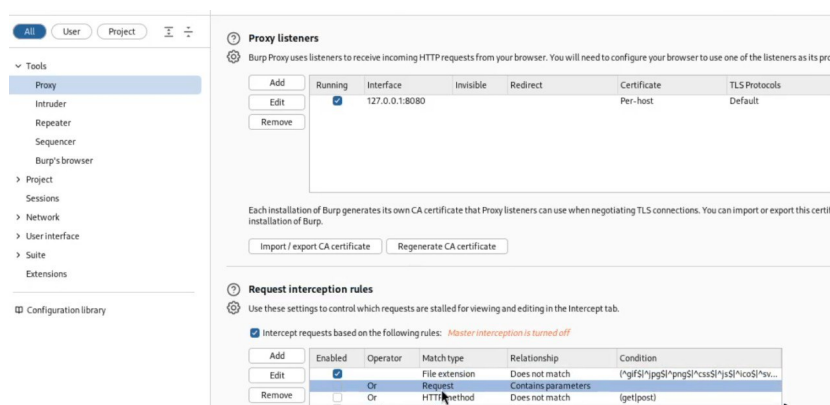


Рис. 2.4: настройки проху

Включаю intercept во вкладке проху:

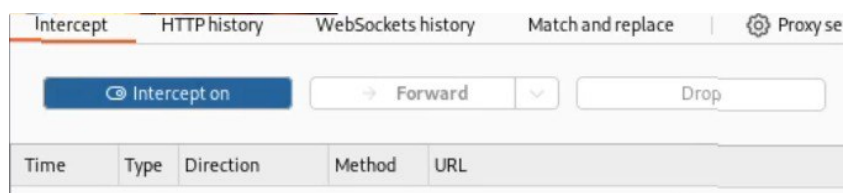


Рис. 2.5: Включение intercept

Необходимо установить параметр `network_allow_hijacking_localhost` на `true`, чтобы burp suite работал с локальным сервером. Я это и делала:

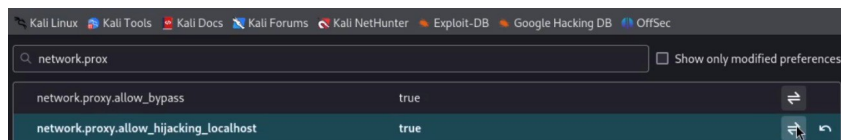


Рис. 2.6: Установка параметра локального хоста

Пытаюсь зайти на dvwa в браузере и во вкладки проху появляется запрос. Нажимаю forward, чтобы загрузить страницу:

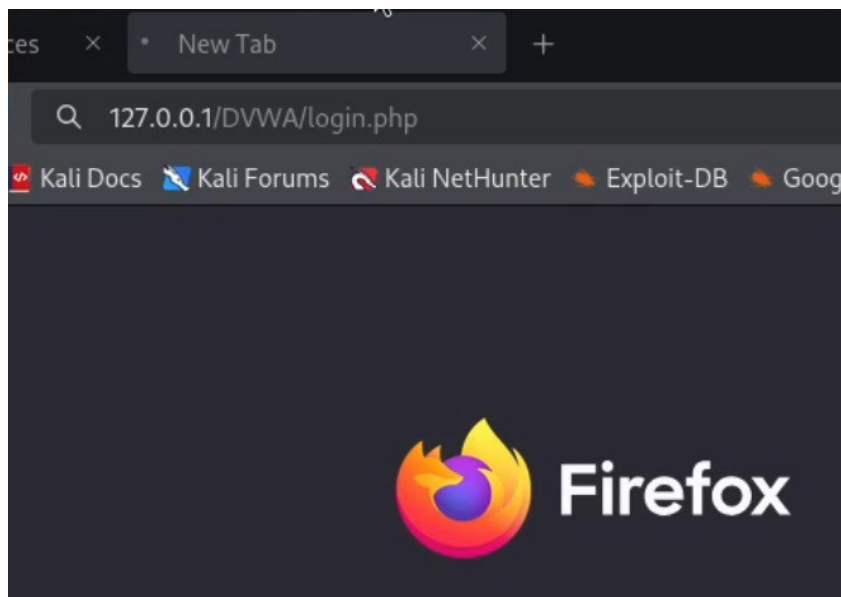


Рис. 2.7: Пытка зайти в dvwa

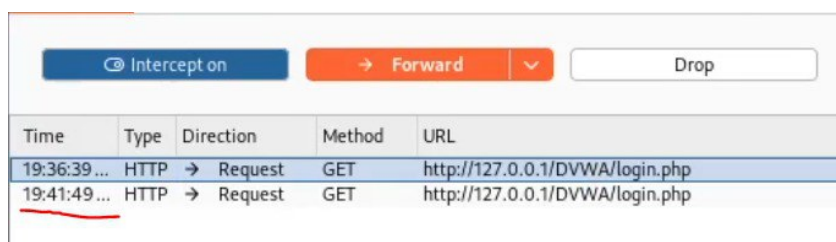


Рис. 2.8: вкладка проху



Username

Password

Login

Рис. 2.9: окно dvwa

Когда пытаюсь ввести неправильные логин и пароль, в запросе появляется строка, в которой отображается введенные данные. Этот же запрос ,во вкладке target, отправила к злоумышленнику (send to intruder). Во вкладке intruder, изменяю тип атаки (на cluster bomb) и данные для входа.

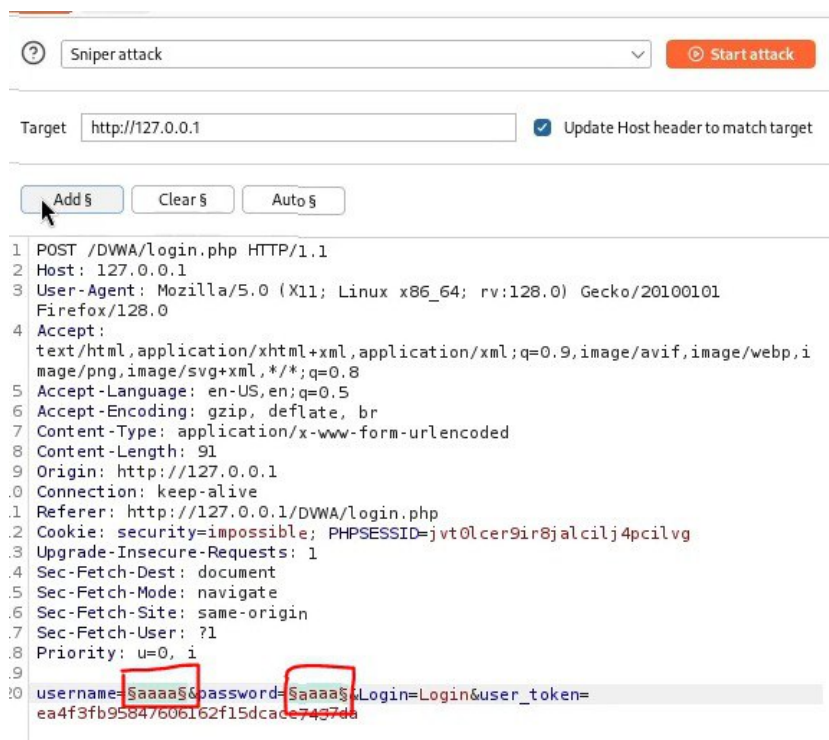


Рис. 2.10: Измененные данные

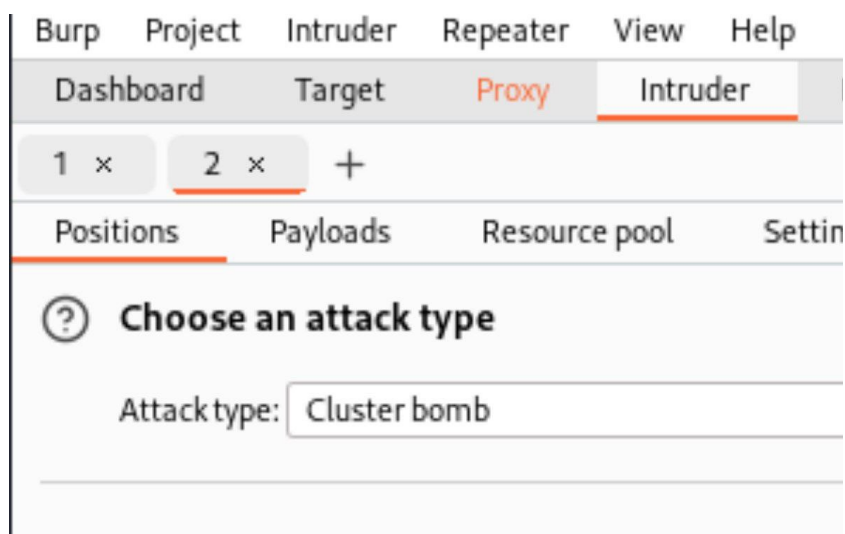


Рис. 2.11: Тип атаки

Отметила два параметра для подбора, поэтому создала два списка со значениями для подбора в payload:

DashboardTargetProxyIntruderRepeaterCollaboratorSequenc

1 x2 x+

PositionsPayloadsResource poolSettings

?

Payload sets

You can define one or more payload sets. The number of payload sets depends on the attack type c ways.

Payload set:

1

Payload count:

6

Payload type:

Simple list

Request count:

24

?

Payload settings [Simple list]

This payload type lets you configure a simple list of strings that are used as payloads.

Paste

Load ...

Remove

Clear

Deduplicate

admin

password

psswd

123456

dddddd

fffff

Add

Enter a new item

Add from list ... [Pro version only]

Рис. 2.12: Список 1

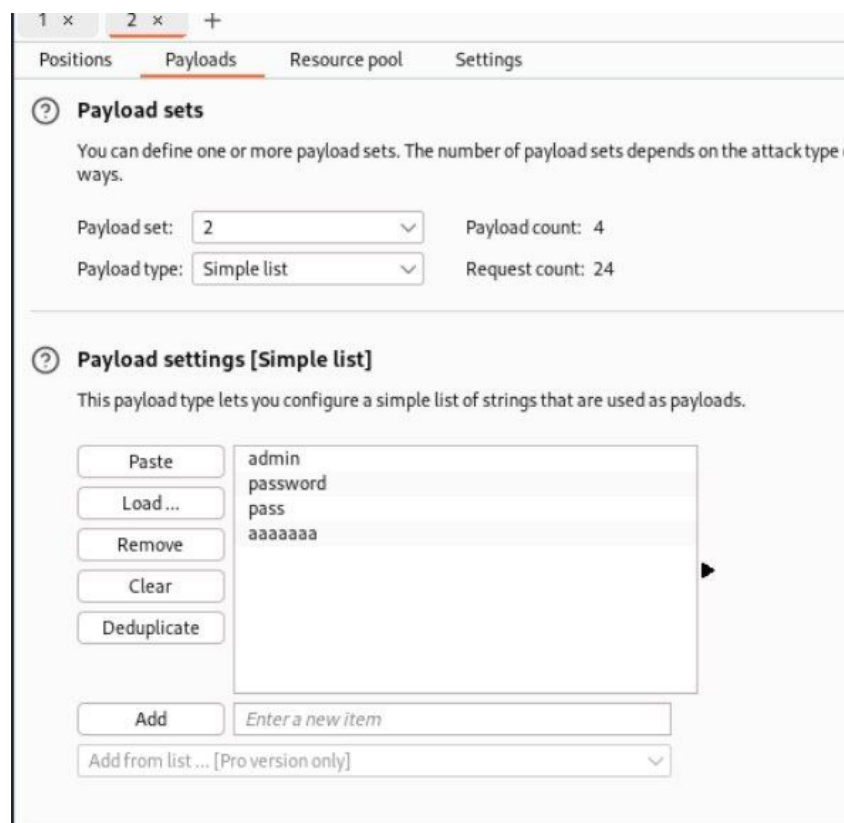


Рис. 2.13: Список 2

Далее запускаю атаку и начинаю подбор. При открытии каждого post-запроса можно увидеть полученный get-запрос, в нем видно, куда нас перенаправило после выполнения ввода пары пользователь-пароль. В этом случае с подбором пары нас перенаправило на страницу index.php, значит пара должна быть верной:

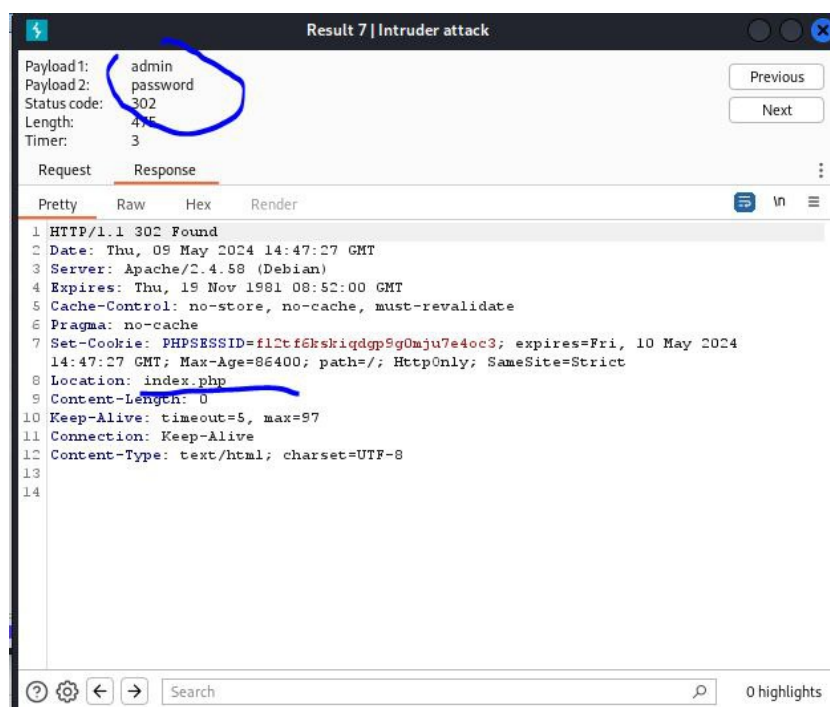


Рис. 2.14: Правильная пара

С использованием repeater делаю дополнительную проверку. Нажимаю send и в response получаю результат перенаправления на index.php.

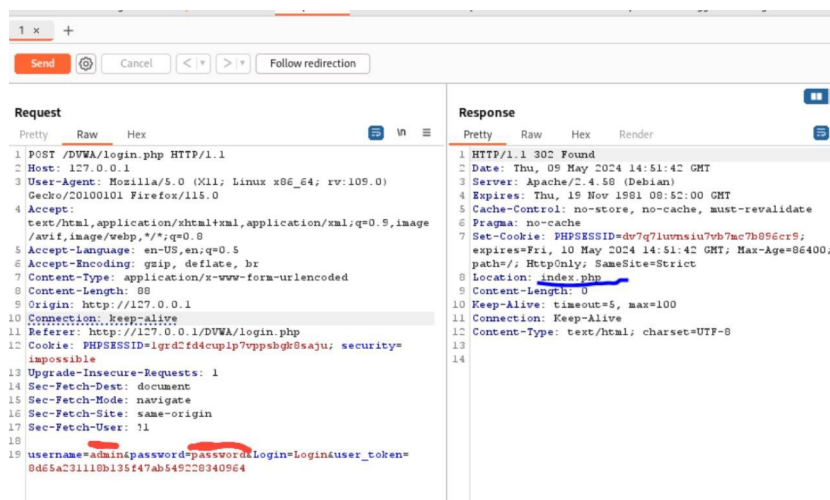


Рис. 2.15: Окна repeater и response

В подокне Render получаю то, как выглядит полученная страница:

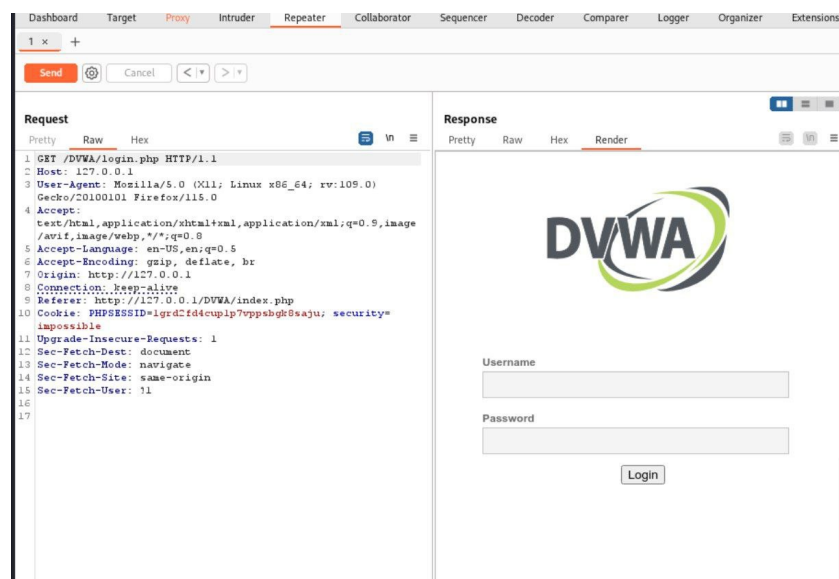


Рис. 2.16: Полученная страница

3 Выводы

Научилась использовать Burp Suite.

Список литературы