Выполнил Мешечкин Д. Инфобез-2837 (Ранее 2345)

Задание 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.

В данном случае, эту комбинацию логин/пароль безопасной считать нет возможности. По "последним рекомендациям создания безопасного пароля" состоящей из:

- Как минимум 12 символов (чем больше - тем безопаснее)
- Использование нижнего и верхнего регистра, чисел, специальных символов.
- Не состоит из запоминаемых комбинаций клавиш клавиатуры.
- Не имеет под собой личной информации.
- Пароль должен быть уникальным для каждого аккаунта у человека.

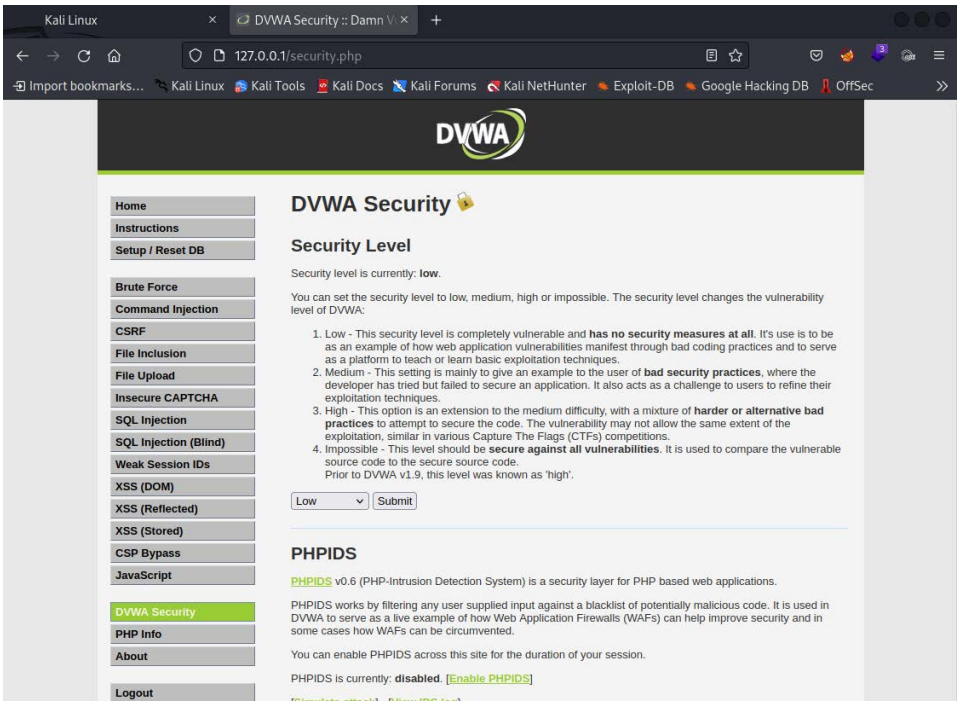
Даже при условии соблюдения большей части "условий" главным фактором является длина пароля, при наличии 8 символов - слабоват, брутфорсом открывается достаточно быстро. При "дополнительных уязвимостях" ещё быстрее. Ограничение количества попыток ввода, 2FA - возможности которые могут "спасти" аккаунт на время.

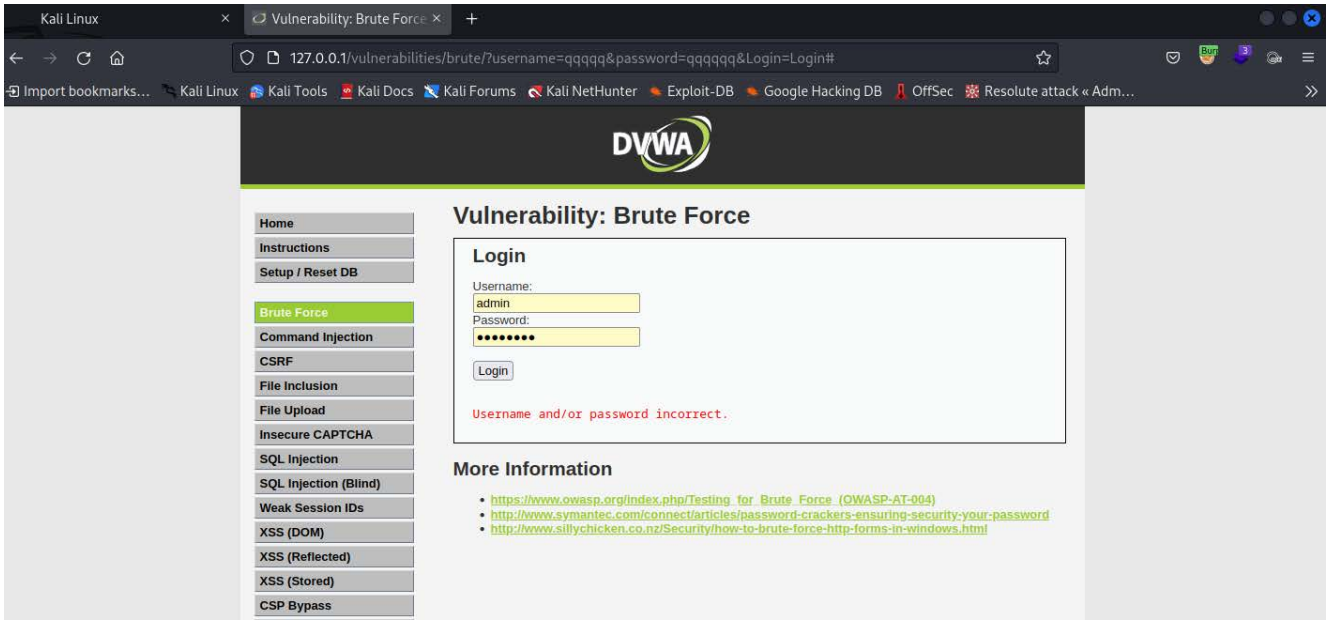
Задание 2: Подберите логин и пароль к странице bruteforce-сервиса dvwa на уровне сложности LOW. Приложите к ответу описание решения задания и скриншот(ы), подтверждающие решение.

С ВМ уже работал, для выполнения задач был взят отдельный ноут, DVWA в докере, BurpPro ну и далее по списку, необходимое для выполнения дз.

Установку-настройку-запуск описывать не буду, уже были установлены.

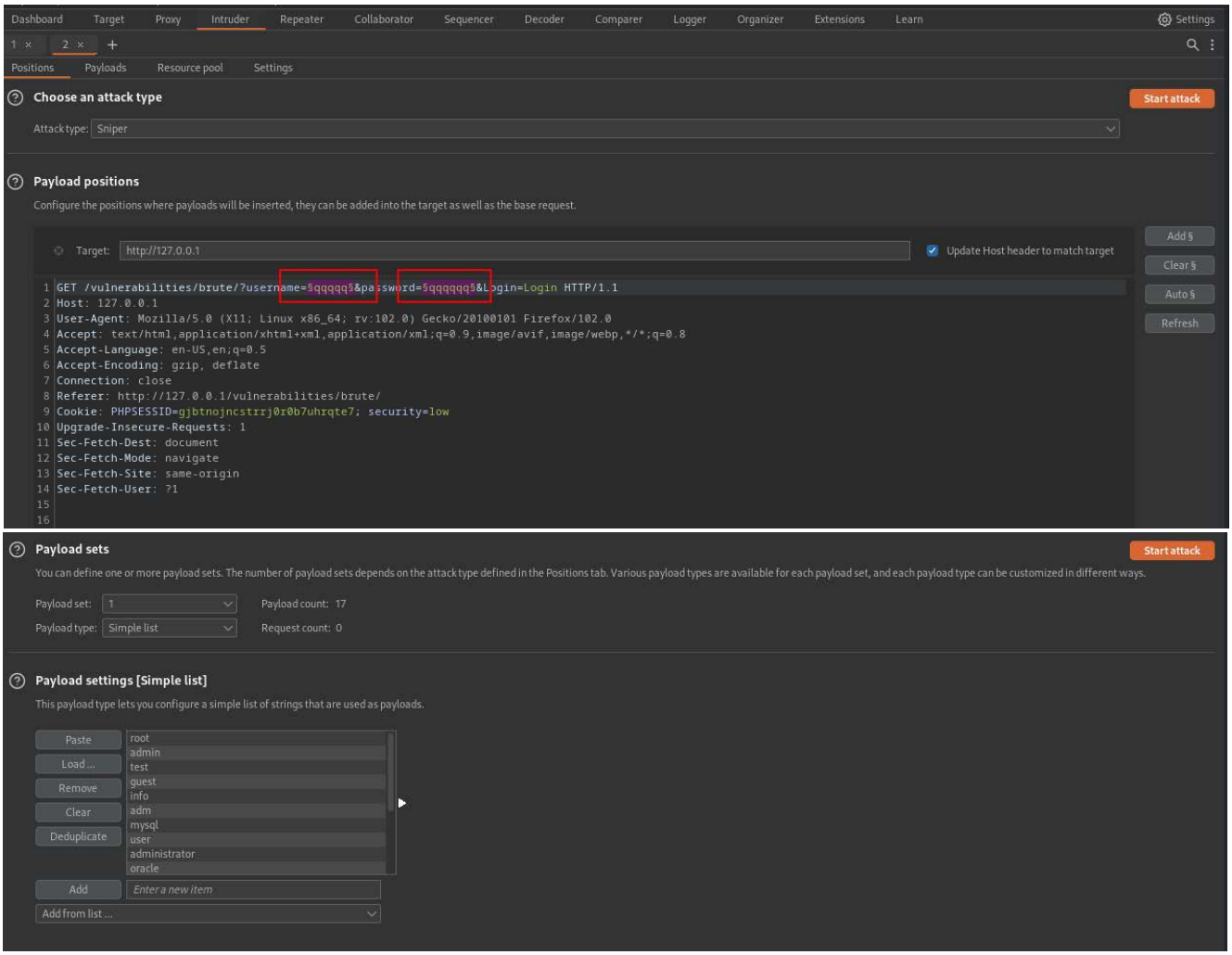
Далее запуск DVWA на сложности LOW. Brute Force.

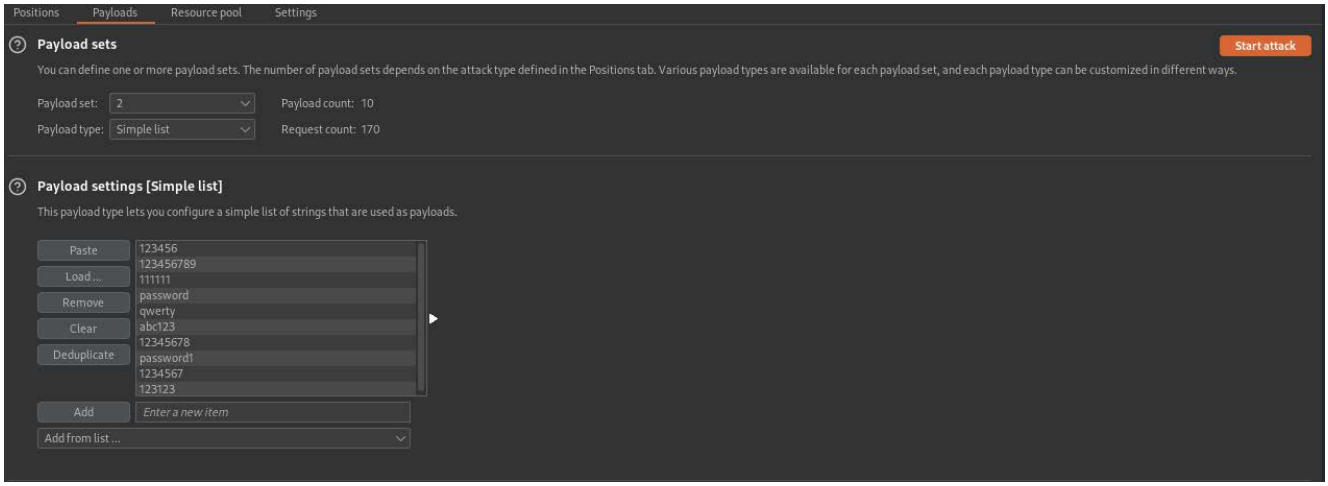


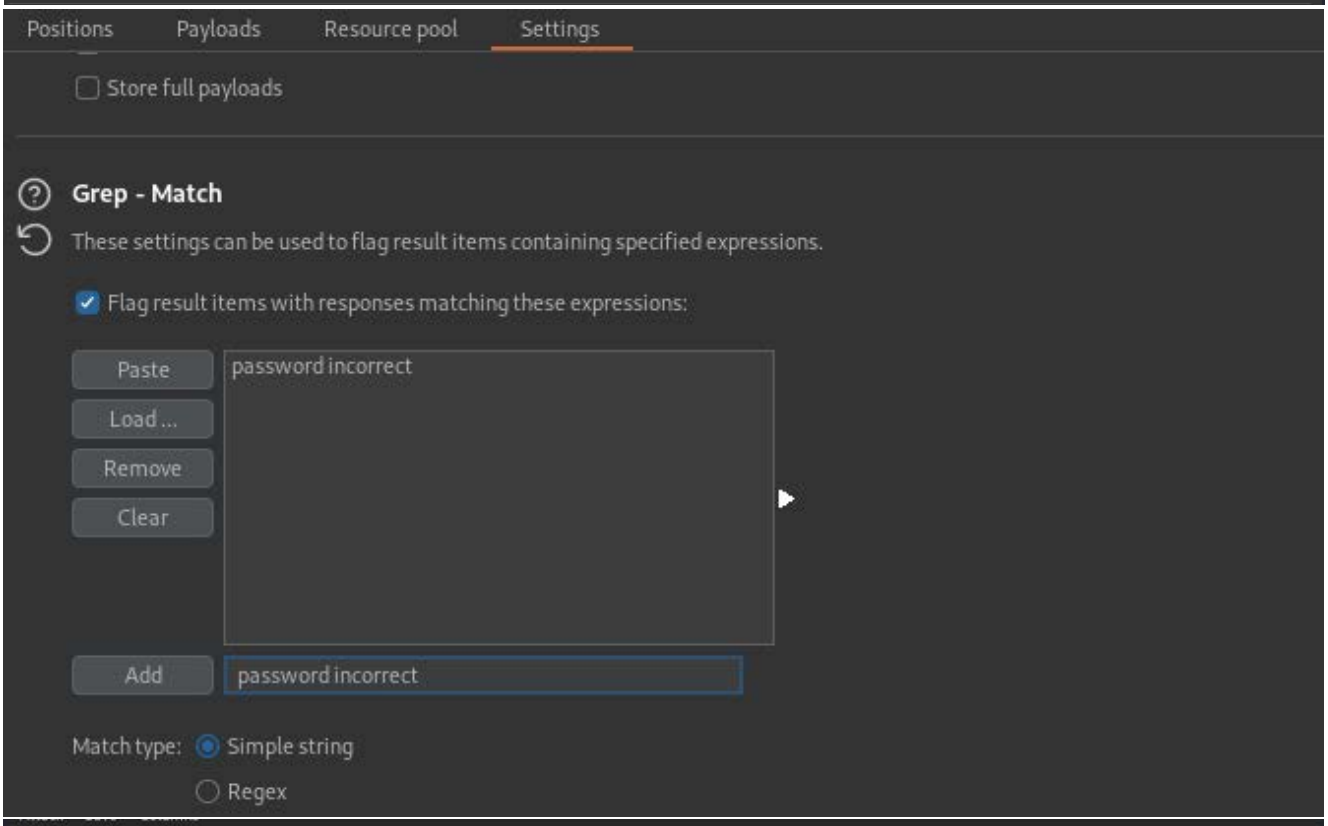


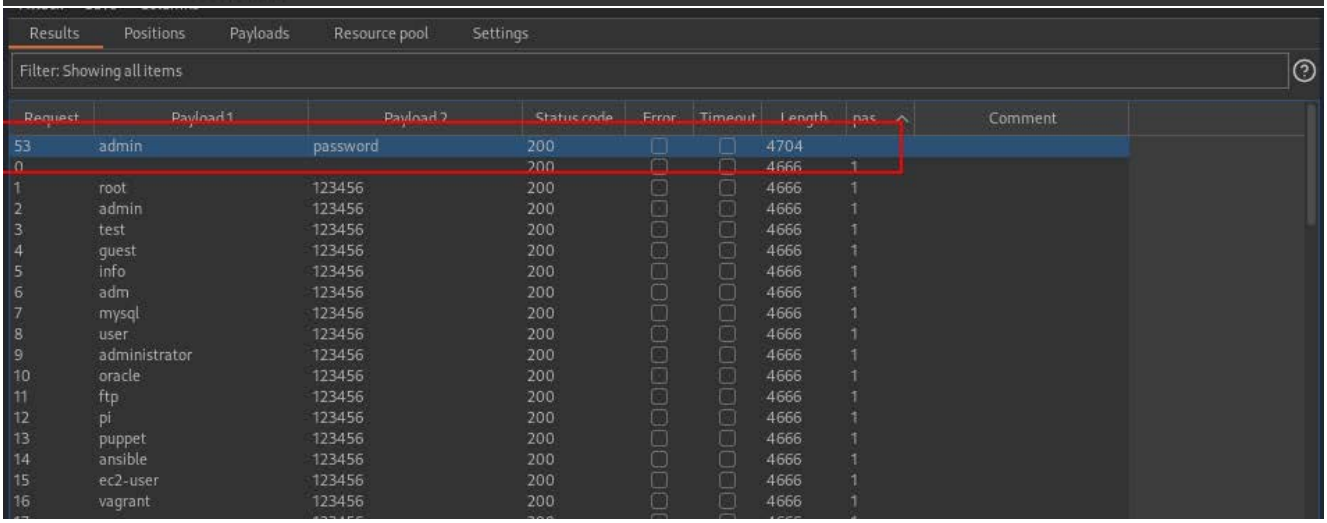
Вводятся абсолютно любые значения в поля. При не верном вводе имеем строку "password incorrcet" её далее буду использовать для фильтрации вывода.

В бёрпе пойманый запрос отправляю в интрудер, устанавливаю тип атаки на "cluster bomb"
Настраиваю 2 точки нагрузки.
1 - имя - по словарям seclist
2 - пароль - по словарям seclist
В настройках забиваю строку для отсева данных и прогоняю интрудером.



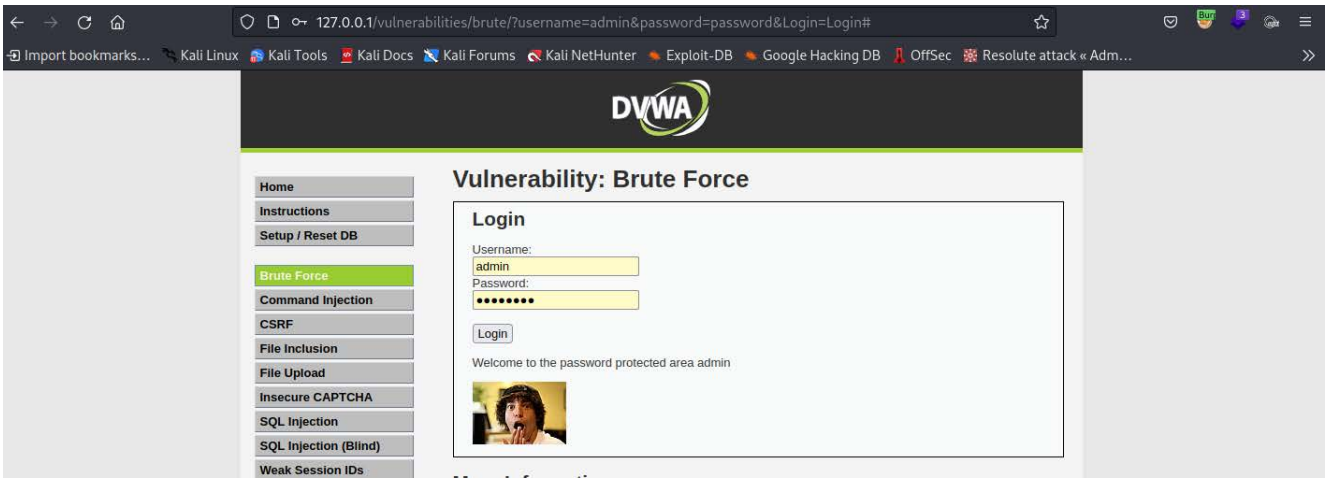






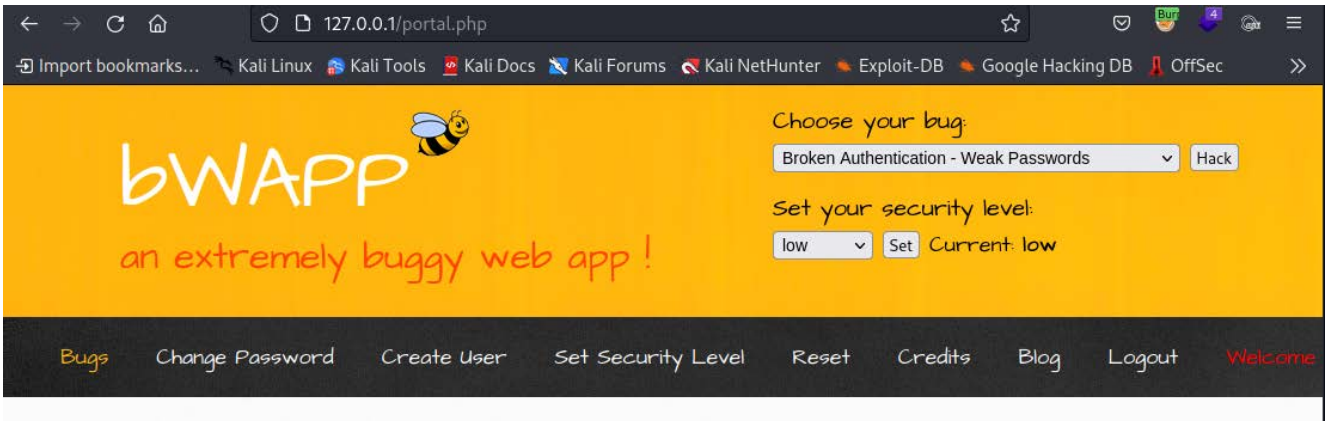
Request	Payload 1	Payload 2	Status code	Error	Timeout	Length	pas	Comment
53	admin	password	200			4704		
0			200			4666	1	
1	root	123456	200			4666	1	
2	admin	123456	200			4666	1	
3	test	123456	200			4666	1	
4	guest	123456	200			4666	1	
5	info	123456	200			4666	1	
6	adm	123456	200			4666	1	
7	mysql	123456	200			4666	1	
8	user	123456	200			4666	1	
9	administrator	123456	200			4666	1	
10	oracle	123456	200			4666	1	
11	ftp	123456	200			4666	1	
12	pi	123456	200			4666	1	
13	puppet	123456	200			4666	1	
14	ansible	123456	200			4666	1	
15	ec2-user	123456	200			4666	1	
16	vagrant	123456	200			4666	1	

Найден вариант. Проверяю его. Подходит.

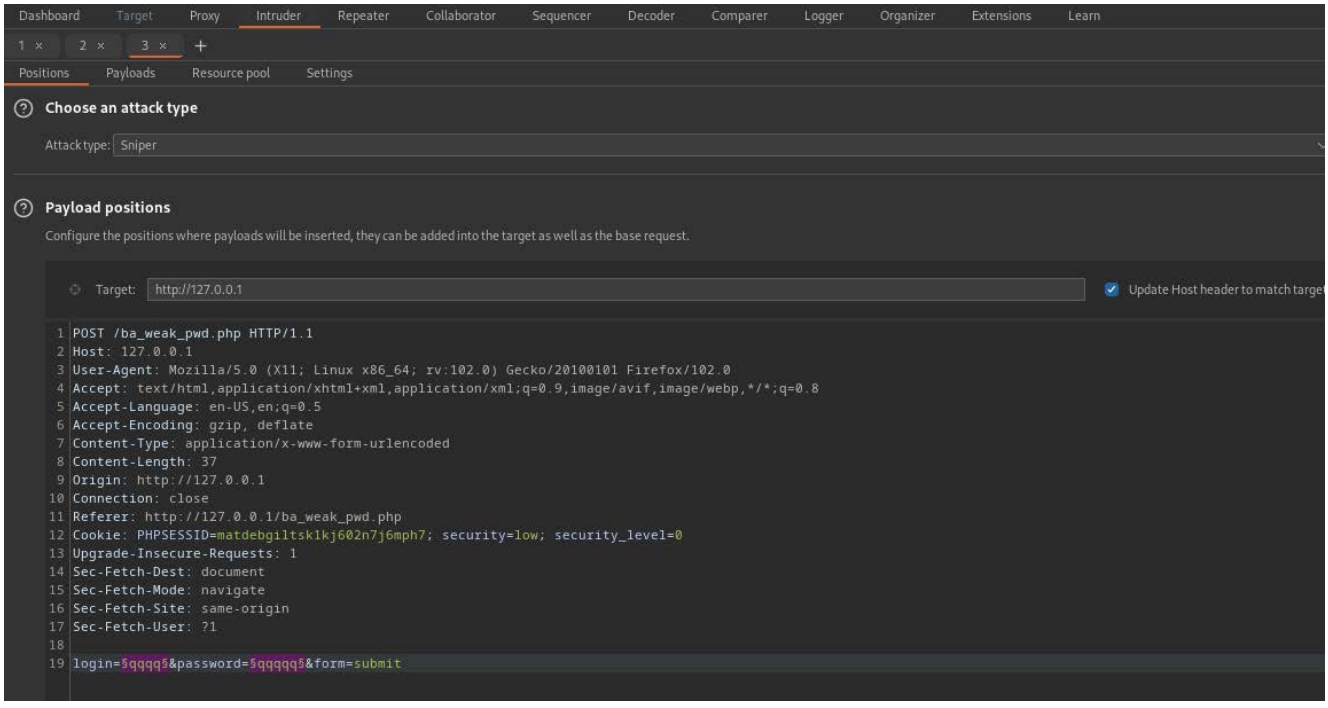


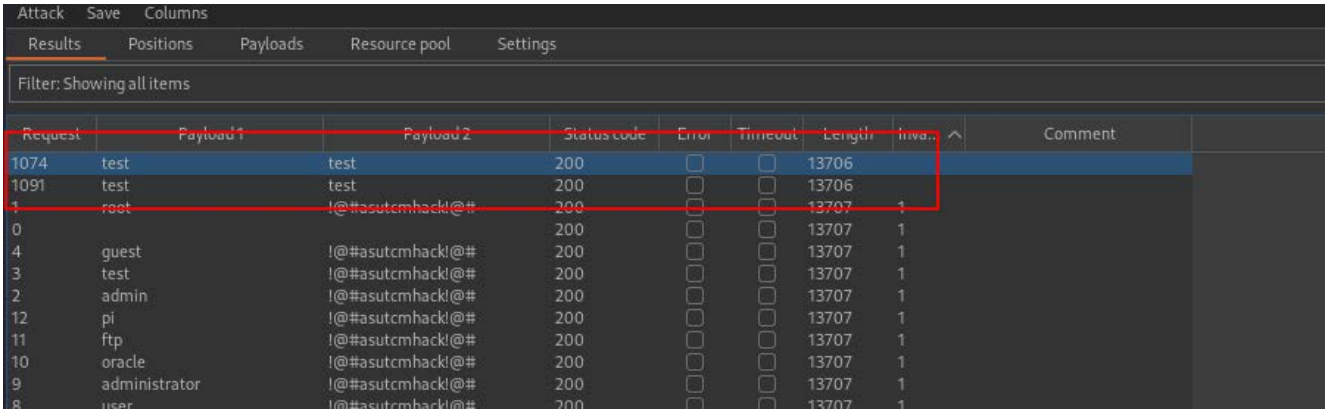
Задание 3: Подберите логин и пароль к странице Broken Auth. - Weak Passwords сервиса bwapp на уровне сложности LOW. Приложите к ответу описание решения задания и скриншот(ы), подтверждающие решение.

Задание выполняется аналогично в докере.
Заполняется идентично Бёрп, используемые словари по логину и паролю - seclist.
Дополнительно указывается строка "Invalid credentials!" для отсева непригодных комбинаций.




Kali Linux
bWAPP - Broken Authenti
127.0.0.1/ba_weak_pwd.php
Import bookmarks...
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
bWAPP
an extremely buggy web app !
Choose yo
Set your s
low
Bugs
Change Password
Create User
Set Security Level
Reset
/ Broken Auth. - Weak Passwords /
Enter your credentials.
Login:
Password:
Login
Invalid credentials!


Dashboard
Target
Proxy
Intruder
Repeater
Collaborator
Sequencer
Decoder
Comparer
Logger
Organizer
Extensions
Learn
1 ×
2 ×
3 ×
Positions
Payloads
Resource pool
Settings
Choose an attack type
Attack type: Sniper
Payload positions
Configure the positions where payloads will be inserted, they can be added into the target as well as the base request.
Target: http://127.0.0.1
Update Host header to match target
1 POST /ba_weak_pwd.php HTTP/1.1
2 Host: 127.0.0.1
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 Content-Type: application/x-www-form-urlencoded
8 Content-Length: 37
9 Origin: http://127.0.0.1
10 Connection: close
11 Referer: http://127.0.0.1/ba_weak_pwd.php
12 Cookie: PHPSESSID=matdebgiltsk1kj602n7j6mph7; security=low; security_level=0
13 Upgrade-Insecure-Requests: 1
14 Sec-Fetch-Dest: document
15 Sec-Fetch-Mode: navigate
16 Sec-Fetch-Site: same-origin
17 Sec-Fetch-User: ?1
18
19 login=§qqqq§&password=§qqqqq§&form=submit



По вордлистам нашлось два совпадения. Проверяю - зелёненькая "Successful login!"

Задание на этом выполнено.

Задания 4* и 5* - не выполнялись.