

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

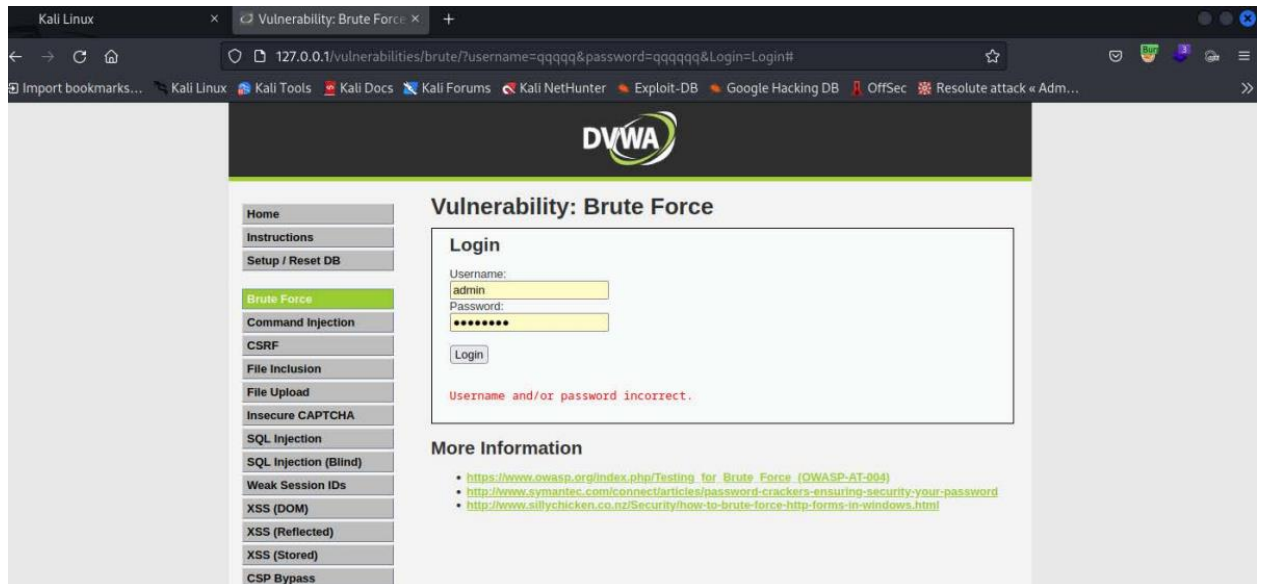
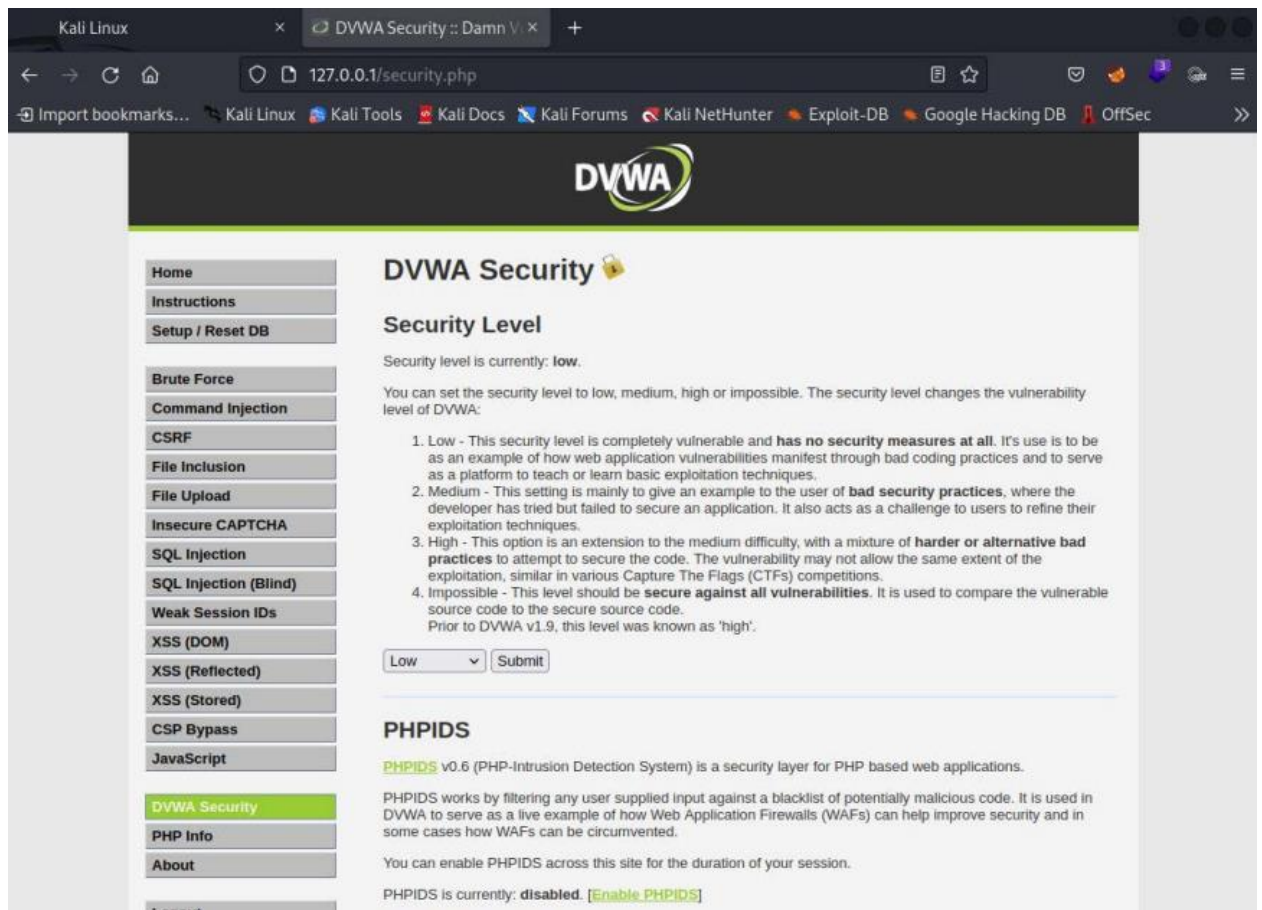
- Как минимум 12 символов
- Использование нижнего и верхнего регистра, чисел, специальных символов.
- Не состоит из запоминаемых комбинаций клавиш клавиатуры.
- Не имеет под собой личной информации.
- Пароль должен быть уникальным для каждого аккаунта у человека.

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.

2. С VM уже работала, для выполнения задач был взят отдельный ноут, DVWA в докере, BurpPro ну и по списку, все 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 неверном вводе имеем строку "password incorrcet" её далее буду использовать для фильтрации вывода.

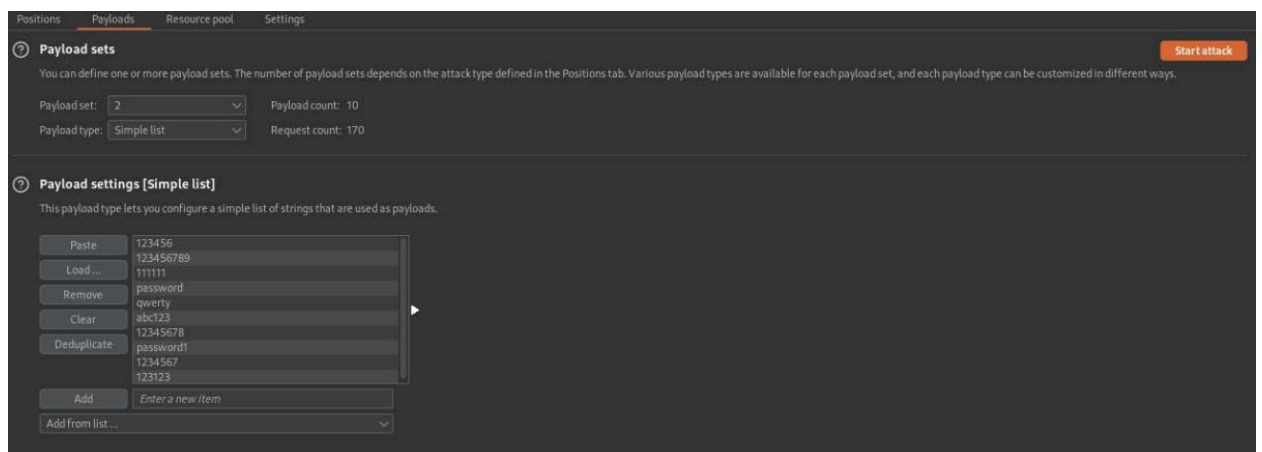
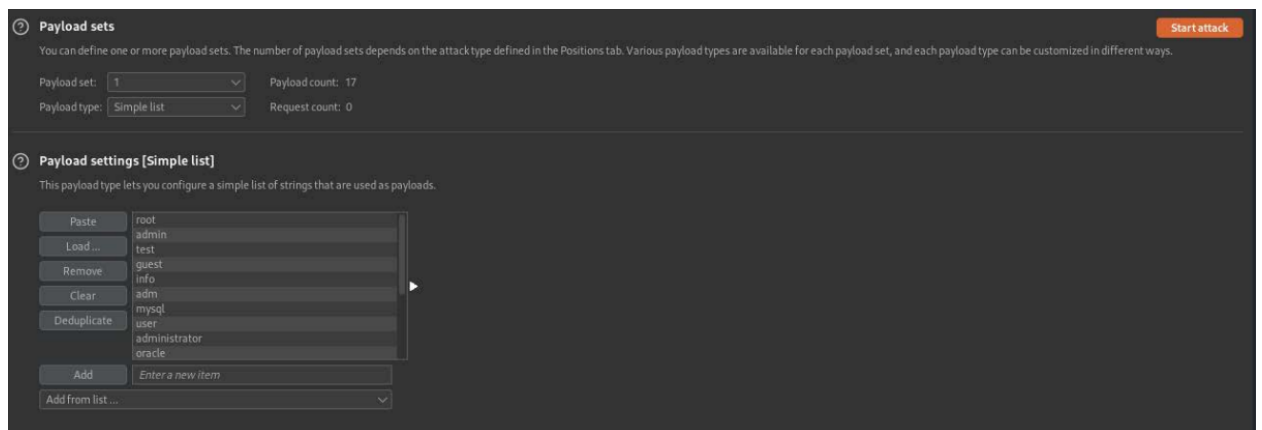
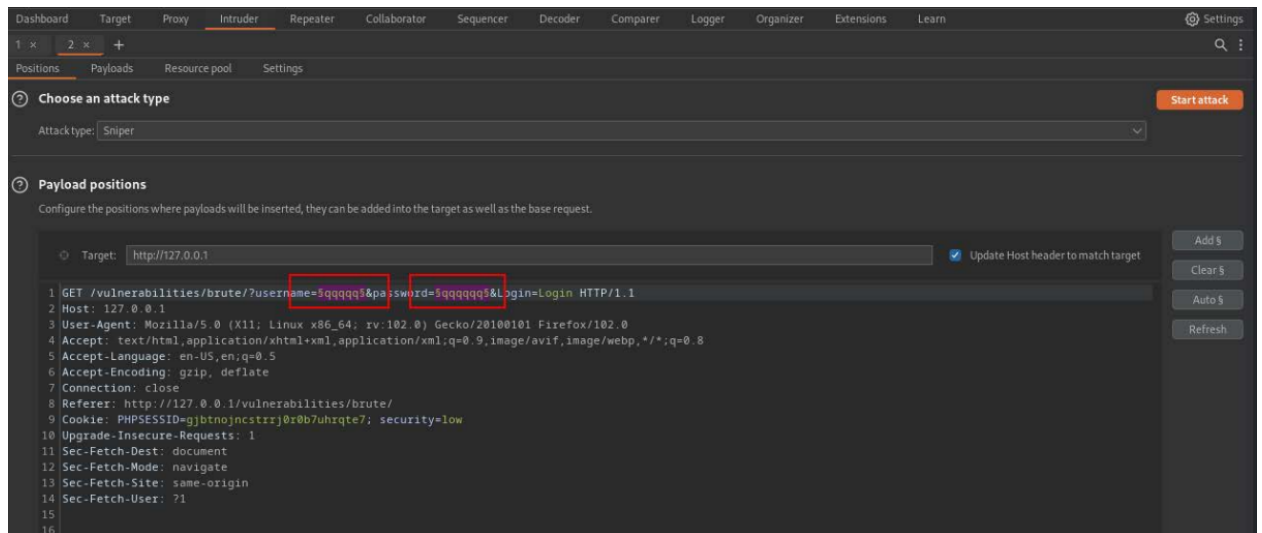
В бёрпе пойманный запрос отправляю в интродер, устанавливаю тип атаки на "cluster bomb"

Настраиваю 2 точки нагрузки.

1 - имя - по словарям seclst

2 - пароль - по словарям seclist

В настройках забиваю строку для отсева данных и прогоняю интродером.



Positions
Payloads
Resource pool
Settings

☐ Store full payloads

? **Grep - Match**

↻ These settings can be used to flag result items containing specified expressions.

☒ Flag result items with responses matching these expressions:

Paste
Load ...
Remove
Clear

password incorrect

Add password incorrect

Match type: ☒ Simple string
☐ Regex

Results
Positions
Payloads
Resource pool
Settings

Filter: Showing all items

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

Найден вариант. Проверяю его, он подходит.

DVWA

Home
Instructions
Setup / Reset DB
Brute Force
Command Injection
CSRF
File Inclusion
File Upload
Insecure CAPTCHA
SQL Injection
SQL Injection (Blind)
Weak Session IDs

Vulnerability: Brute Force


Login

Username: admin

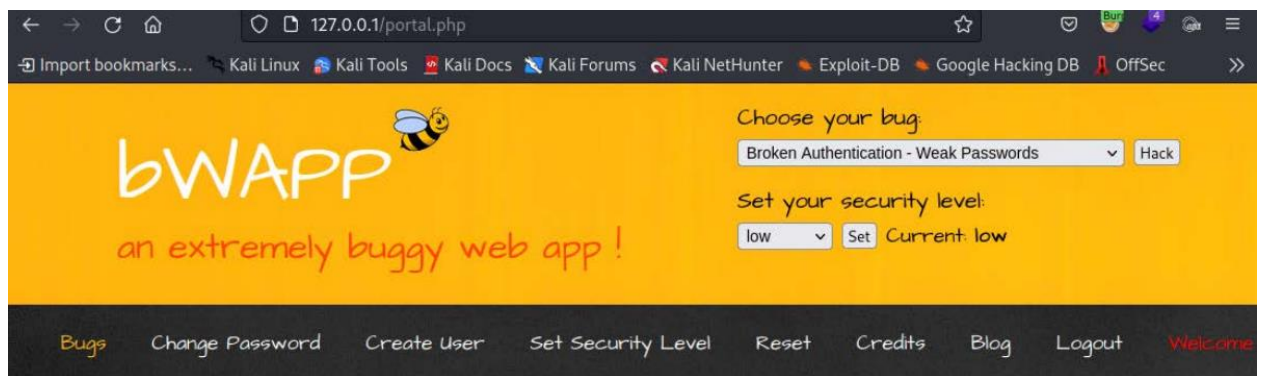
Password:

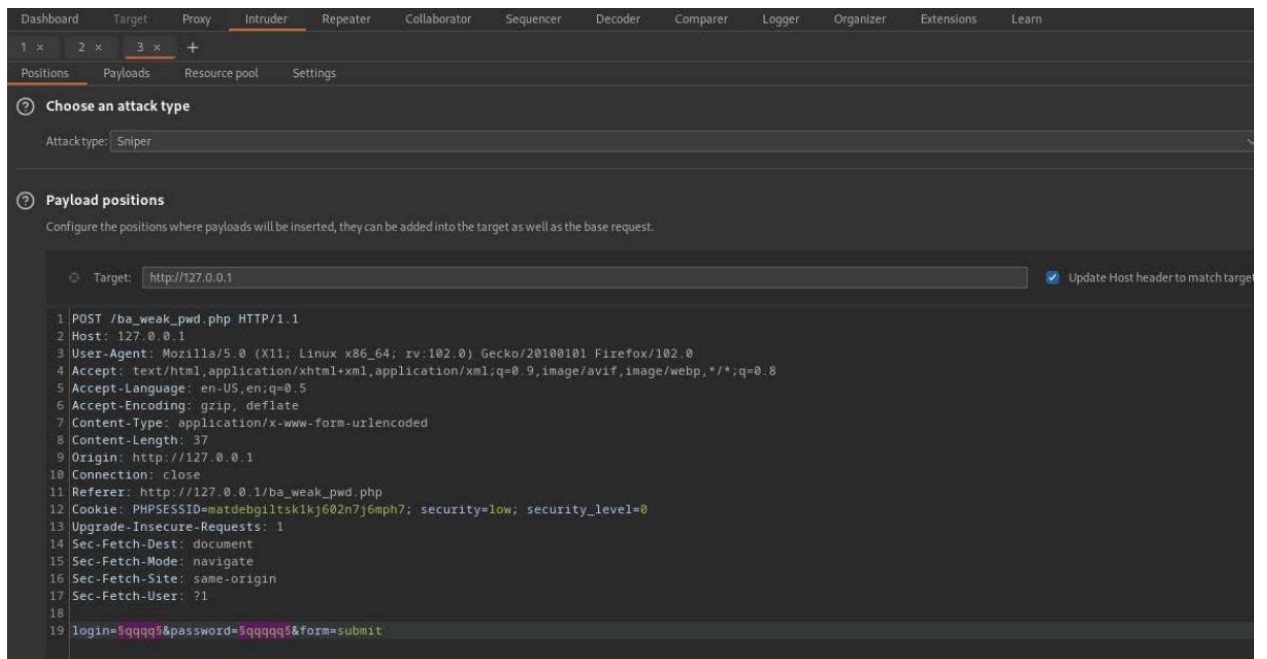
Login

Welcome to the password protected area admin



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





| Attack Save Columns | | | | | | | | | |
|---|---------------|------------------|-------------|--------------------------|--------------------------|--------|--------|--|---------|
| Results Positions Payloads Resource pool Settings | | | | | | | | | |
| Filter: Showing all items | | | | | | | | | |
| Request | Payload 1 | Payload 2 | Status code | Error | Timeout | Length | Inva.. | | Comment |
| 1074 | test | test | 200 | <input type="checkbox"/> | <input type="checkbox"/> | 13706 | | | |
| 1091 | test | test | 200 | <input type="checkbox"/> | <input type="checkbox"/> | 13706 | | | |
| 1 | root | !@#asutcmhack!@# | 200 | <input type="checkbox"/> | <input type="checkbox"/> | 13707 | 1 | | |
| 0 | | | 200 | <input type="checkbox"/> | <input type="checkbox"/> | 13707 | 1 | | |
| 4 | guest | !@#asutcmhack!@# | 200 | <input type="checkbox"/> | <input type="checkbox"/> | 13707 | 1 | | |
| 3 | test | !@#asutcmhack!@# | 200 | <input type="checkbox"/> | <input type="checkbox"/> | 13707 | 1 | | |
| 2 | admin | !@#asutcmhack!@# | 200 | <input type="checkbox"/> | <input type="checkbox"/> | 13707 | 1 | | |
| 12 | pi | !@#asutcmhack!@# | 200 | <input type="checkbox"/> | <input type="checkbox"/> | 13707 | 1 | | |
| 11 | ftp | !@#asutcmhack!@# | 200 | <input type="checkbox"/> | <input type="checkbox"/> | 13707 | 1 | | |
| 10 | oracle | !@#asutcmhack!@# | 200 | <input type="checkbox"/> | <input type="checkbox"/> | 13707 | 1 | | |
| 9 | administrator | !@#asutcmhack!@# | 200 | <input type="checkbox"/> | <input type="checkbox"/> | 13707 | 1 | | |
| 8 | user | !@#asutcmhack!@# | 200 | <input type="checkbox"/> | <input type="checkbox"/> | 13707 | 1 | | |

По вордлистам нашлось два совпадения. Проверяю - Successful login!