

Домашняя работа № 2

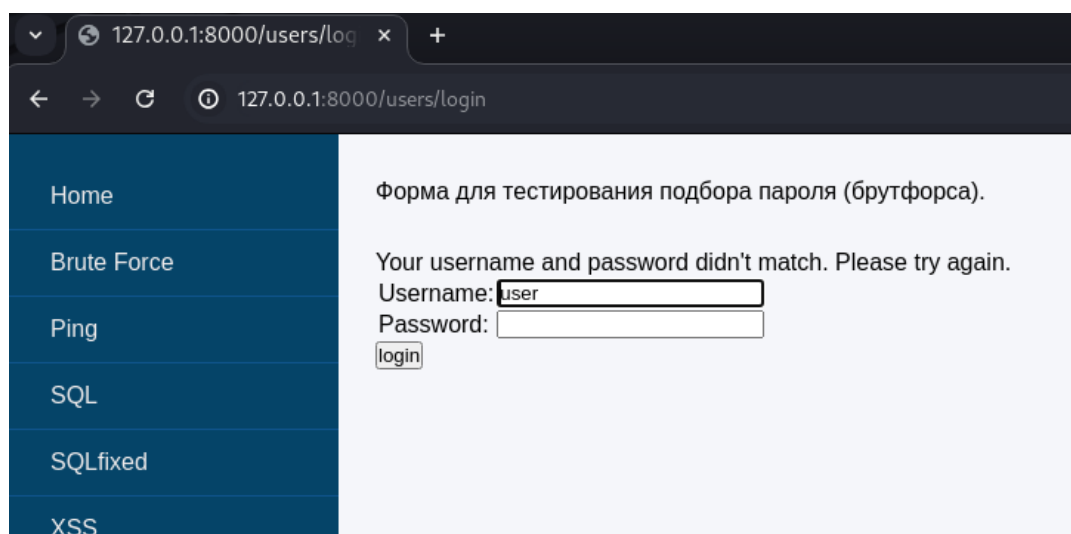
Выполнила Вишняк Евгения

1. С использованием BurpSuite выполнить подбор пароля для пользователя user в приложении test_app . Для формирования payload считать известным, что пароль имеет длину 4 символа и содержит только буквы 'a', 'b', 'c', 'd'. Прикрепить найденный пароль, скрин интродера и скрин настройки payload.

Запускаю сервер при помощи команды:

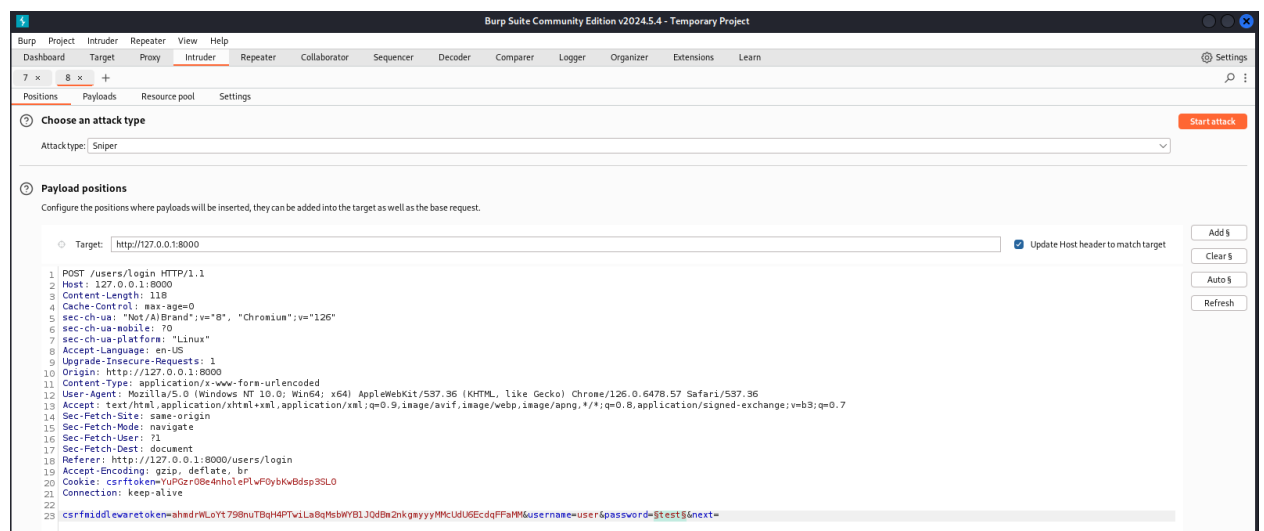
```
python3 manage.py runserver 0.0.0.0:8000
```

Проверяю работоспособность в браузере:



Запускаю BurpSuite, открываю браузер и делаю попытку входа. После чего нахожу нужный пакет в Dashboard и настраиваю брутфорс:

Скриншот интродера:



Скриншот настройки payload:

Burp Suite Community Edition v2024.5.4 - Temporary Project

Dashboard Target Proxy **Intruder** Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn

7 x 8 x +

Positions **Payloads** Resource pool Settings

1 Payload sets

You can define one or more payload sets. The number of payload sets depends on the attack type defined in the Positions tab. Various payload types are available for each payload set, and each payload type can be customized in different ways.

Payload set: 1 Payload count: 256
Payload type: Brute forcer Request count: 256

2 Payload settings [Brute forcer]

This payload type generates payloads of specified lengths that contain all permutations of a specified character set.

Character set: abcd
Min length: 4
Max length: 4

3 Payload processing

You can define rules to perform various processing tasks on each payload before it is used.

Add Enabled Rule
Edit
Remove
Up
Down

4 Payload encoding

This setting can be used to URL-encode selected characters within the final payload, for safe transmission within HTTP requests.

☒ URL-encode these characters: /!<>?+&*;"'{}|^`#

Запускаю и жду окончания перебора. Результат:

8. Intruder attack of http://127.0.0.1:8000

Attack Save

Results Positions Payloads Resource pool Settings

Intruder attack results filter: Showing all items

Request	Payload	Status code	Response received	Error	Timeout	Length	Comment
247	cbdd	200	449			2038	
248	dbdd	200	425			2038	
249	acdd	200	433			2038	
250	bcdd	200	405			2038	
251	rcdd	200	479			2038	
252	dcdd	200	444			2038	
253	addd	200	424			2038	
254	bddd	200	433			2038	
255	cddd	200	410			2038	
256	dddd	200	417			2038	

Request Response

Pretty Raw Hex **Render**

Home Форма для тестирования подбора пароля (брутфорса).

Brute Force Your username and password didn't match. Please try again.

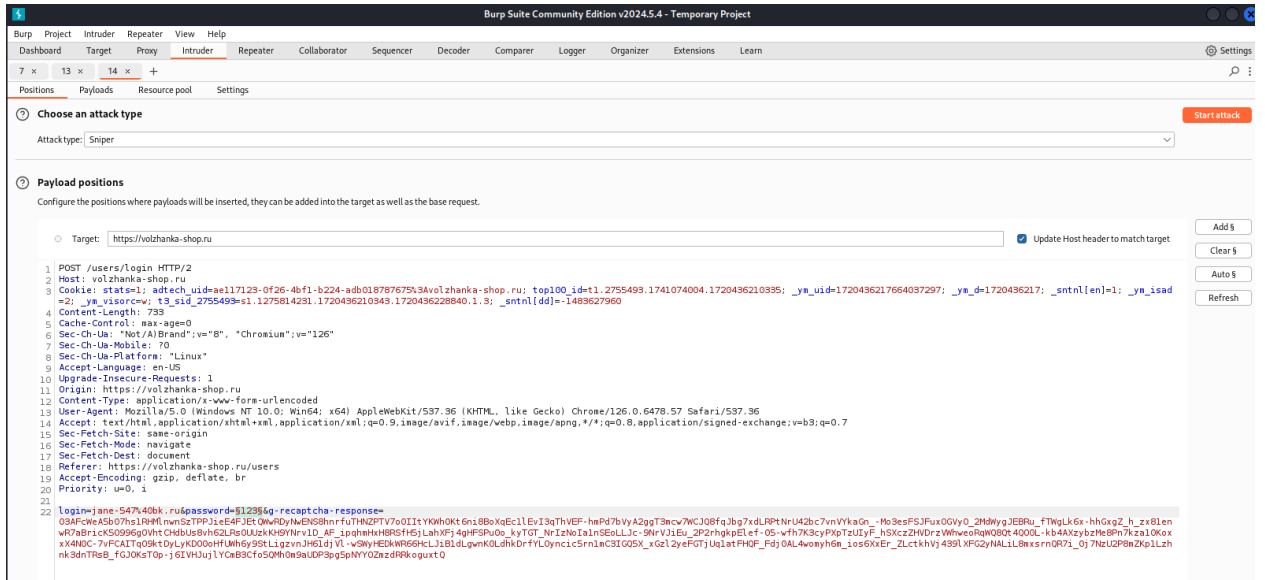
Ping Username: user Password: login

SQL

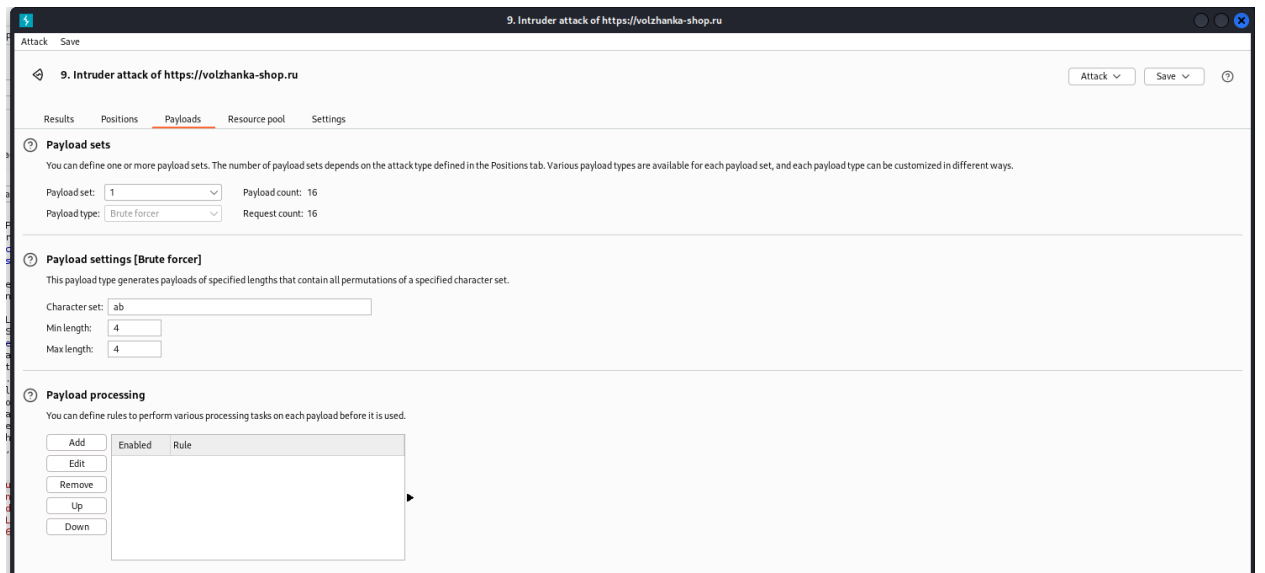
SQLfixed

XSS

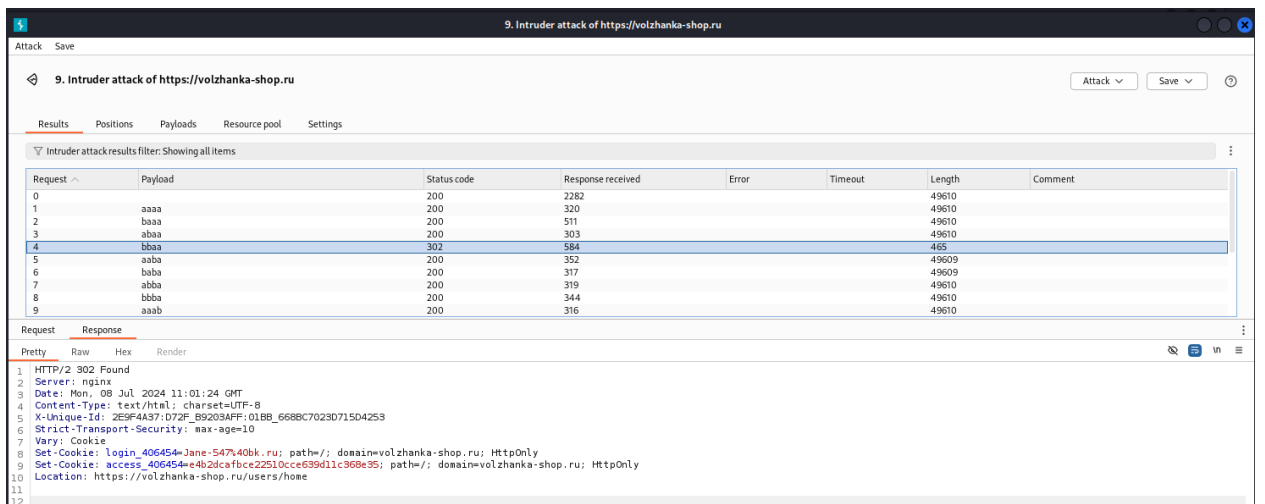
Поскольку на тестовом сервере нет заданных учетных данных, попробую протестировать другой произвольный сайт, использующий протокол http. Например, volzhanka-shop.ru. Прохожу простую регистрацию и использую простой пароль. Запускаю брутфорс:



Настройки payload:



Результат:



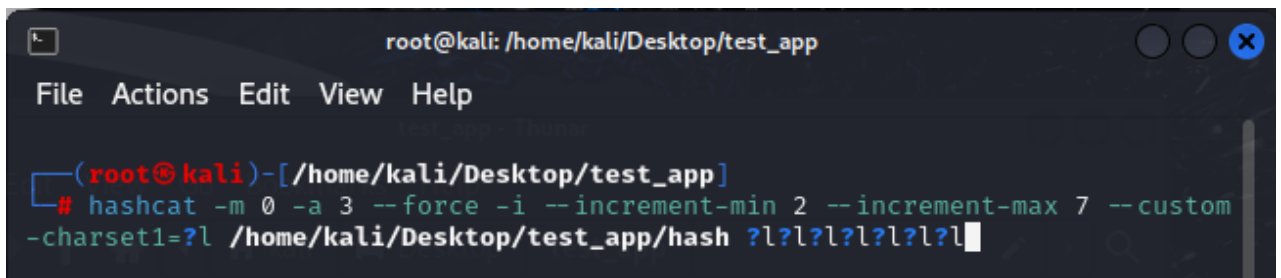
Пароль подобран верно. Status code при этом имеет значение 302, что отличает текущее значение от всех остальных.

2. Имеется md5 хеш: 1ea55264488aa89e8f9cb13eca5a792e .

Записать его в файл, перенести на Kali Linux и выполнить расшифровку, с использованием Hashcat если известно, что исходное слово содержит от 2 до 7 строчных латинских букв. Прикрепить расшифрованное значение, скрин команды запуска и скрин настройки результата расшифровки.

Я создала в текущей директории файл с заданным хешем, после этого запустила команду:

```
hashcat -m 0 -a 3 --force -i --increment-min 2 --increment-max 7 --custom-charset1=?l /home/kali/Desktop/test_app/hash ?l?l?l?l?l?l
```



The screenshot shows a terminal window titled 'root@kali: /home/kali/Desktop/test_app'. The window has a menu bar with 'File', 'Actions', 'Edit', 'View', and 'Help'. The terminal prompt is '(root@kali)-[/home/kali/Desktop/test_app]'. The command being executed is '# hashcat -m 0 -a 3 --force -i --increment-min 2 --increment-max 7 --custom-charset1=?l /home/kali/Desktop/test_app/hash ?l?l?l?l?l?l'. The cursor is at the end of the command line.

Здесь:

- ✓ -m 0 означает алгоритм md5
- ✓ -a 3 режим подбора брутфорсом без словаря
- ✓ - -force игнорирование ошибок
- ✓ -i, --increment-min 2 --increment-max 7 ограничения на длину
- ✓ --custom-charset1=?l - указание состава пароля (только латинские строчные буквы)
- ✓ ?l?l?l?l?l?l - маска пароля (7 латинских строчных букв).

Первая попытка запуска была неудачной: недостаточно памяти. Выключила виртуальную машину, исправила и запустила снова:

```
root@kali: /home/kali
File Actions Edit View Help
(root@kali)-[/home/kali]
# hashcat -m 0 -a 3 --force -i --increment-min 2 --increment-max 7 --custom
-charset1=?l /home/kali/Desktop/test_app/hash ?l?l?l?l?l?l
hashcat (v6.2.6) starting

You have enabled --force to bypass dangerous warnings and errors!
This can hide serious problems and should only be done when debugging.
Do not report hashcat issues encountered when using --force.

OpenCL API (OpenCL 3.0 PoCL 6.0+debian Linux, None+Asserts, RELOC, LLVM 17.0
.6, SLEEP, DISTRO, POCL_DEBUG) - Platform #1 [The pocl project]

=====
* Device #1: cpu-sandybridge-AMD Ryzen 5 3400G with Radeon Vega Graphics, 126
7/2599 MB (512 MB allocatable), 2MCU

Minimum password length supported by kernel: 0
Maximum password length supported by kernel: 256

Hashes: 1 digests; 1 unique digests, 1 unique salts
Bitmaps: 16 bits, 65536 entries, 0x0000ffff mask, 262144 bytes, 5/13 rotates

Optimizers applied:
* Zero-Byte
* Early-Skip
* Not-Salted
* Not-Iterated
* Single-Hash
* Single-Salt
* Brute-Force
* Raw-Hash

ATTENTION! Pure (unoptimized) backend kernels selected.
Pure kernels can crack longer passwords, but drastically reduce performance.
If you want to switch to optimized kernels, append -O to your commandline.
See the above message to find out about the exact limits.

Watchdog: Temperature abort trigger set to 90c
```

На этот раз получен результат:

```
root@kali: /home/kali
File Actions Edit View Help

Approaching final keyspace - workload adjusted.

Session.....: hashcat
Status.....: Exhausted
Hash.Mode.....: 0 (MD5)
Hash.Target.....: 1ea55264488aa89e8f9cb13eca5a792e
Time.Started.....: Mon Jul 8 07:25:06 2024, (0 secs)
Time.Estimated...: Mon Jul 8 07:25:06 2024, (0 secs)
Kernel.Feature...: Pure Kernel
Guess.Mask.....: ?l?l?l?l?l [5]
Guess.Charset....: -1 ?l, -2 Undefined, -3 Undefined, -4 Undefined
Guess.Queue.....: 4/6 (66.67%)
Speed.#1.....: 32824.3 kH/s (0.26ms) @ Accel:256 Loops:26 Thr:1 Vec:8
Recovered.....: 0/1 (0.00%) Digests (total), 0/1 (0.00%) Digests (new)
Progress.....: 11881376/11881376 (100.00%)
Rejected.....: 0/11881376 (0.00%)
Restore.Point....: 456976/456976 (100.00%)
Restore.Sub.#1...: Salt:0 Amplifier:0-26 Iteration:0-26
Candidate.Engine.: Device Generator
Candidates.#1....: spgqx → xqxvq
Hardware.Mon.#1...: Util: 73%

1ea55264488aa89e8f9cb13eca5a792e:gbtest

Session.....: hashcat
Status.....: Cracked
Hash.Mode.....: 0 (MD5)
Hash.Target.....: 1ea55264488aa89e8f9cb13eca5a792e
Time.Started.....: Mon Jul 8 07:25:06 2024, (0 secs)
Time.Estimated...: Mon Jul 8 07:25:06 2024, (0 secs)
Kernel.Feature...: Pure Kernel
Guess.Mask.....: ?l?l?l?l?l [6]
Guess.Charset....: -1 ?l, -2 Undefined, -3 Undefined, -4 Undefined
Guess.Queue.....: 5/6 (83.33%)
Speed.#1.....: 61357.4 kH/s (5.30ms) @ Accel:256 Loops:676 Thr:1 Vec:8
Recovered.....: 1/1 (100.00%) Digests (total), 1/1 (100.00%) Digests (new)
Progress.....: 1730560/308915776 (0.56%)
Rejected.....: 0/1730560 (0.00%)
Restore.Point....: 2048/456976 (0.45%)
Restore.Sub.#1...: Salt:0 Amplifier:0-676 Iteration:0-676
Candidate.Engine.: Device Generator
Candidates.#1....: saxyle → xqbvon
Hardware.Mon.#1...: Util: 76%

Started: Mon Jul 8 07:25:01 2024
Stopped: Mon Jul 8 07:25:07 2024
```

Искомое значение - gbtest.