

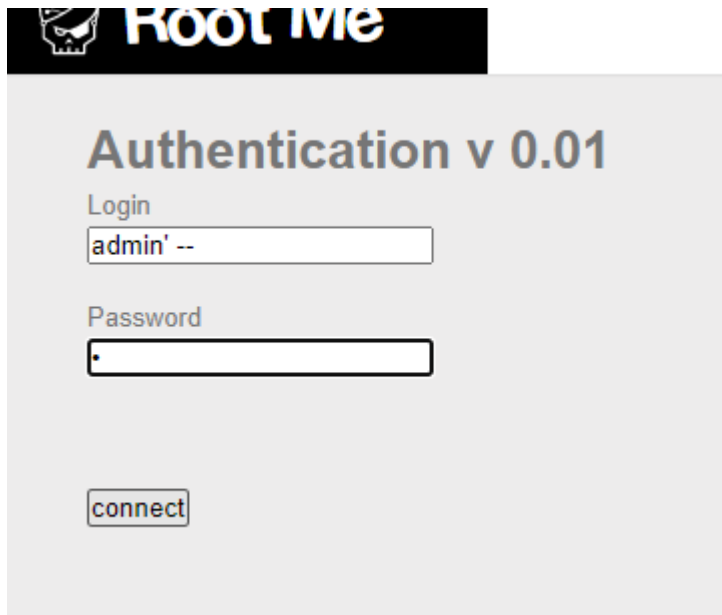
Write up challenge SQL injection - Authentication

Tác giả:

- **Nguyễn Mỹ Quỳnh**

[Link Challenge](#)

Truy cập challenge ta thấy có một form login. Thử tiến hành một sqli basic attack

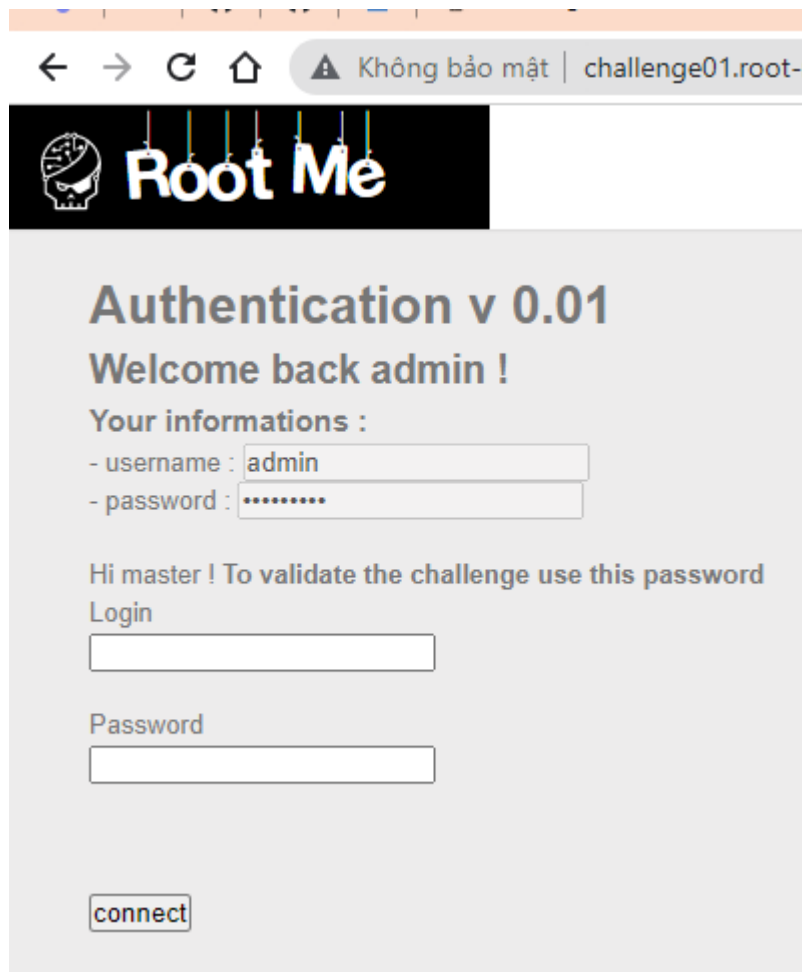


Authentication v 0.01

Login

Password

Thành công đăng nhập dưới quyền admin



← → ↻ 🏠 ⚠️ Không bảo mật | challenge01.root-

Root Me

Authentication v 0.01

Welcome back admin !

Your informations :

- username :
- password :

Hi master ! To validate the challenge use this password

Login

Password

Tat thấy có một form information chứa password bị hide, tiến hành inspect xem thử ta có được flag:

```
<html>
<body><link rel='stylesheet' property='stylesheet' id='s' 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 />
<form action="" 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/>
</form>
</body>
</html>
```

Submit thành công

SQL injection - Authentication

30 Points 

Authentication v 0.01

Author

g0uZ, 27 February 2011

Level 








Statement

Retrieve the administrator password

[Start the challenge](#)

13 related ressource(s)

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

Validation

Well done but you've already won the 30 Points

Don't forget to give your opinion on the challenge by voting :-)

Flag: t0_W34k!\$