

BÀI TẬP CTF

Bảo mật web và ứng dụng – NT213.M21.ANTN

Giảng viên hướng dẫn: *Đỗ Hoàng Hiển*

Sinh viên thực hiện: *19520199 – Lê Tôn Nhân*

Challenge 1: SQL injection - Authentication (level medium)

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

- Bài này yêu cầu lấy mật khẩu của administrator

SQL injection - Authentication

30 Points 🌐

Authentication v 0.01

Author

g0uZ, 27 February 2011

Level ⓘ



Statement

Retrieve the administrator password

- Truy cập vào challenge ta có trang web như bên dưới

Root Me


Authentication v 0.01

Login

Password

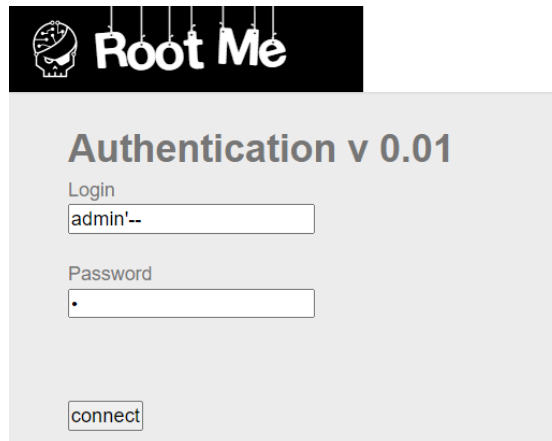
connect

- Thử đăng nhập với user/password là 19520199/1 thì xuất hiện dòng **Error : no such user/password**



The screenshot shows a web interface titled "Authentication v 0.01". Below the title, an error message "Error : no such user/password" is displayed. There are two input fields: "Login" and "Password". Below the "Password" field is a "connect" button.

- Thử tấn công bằng cách nhập user là admin '-- và password bất kỳ (ở đây ta nhập 1). Với ' để đóng giá trị của username và -- để cho phần sau trở thành đoạn comment.



The screenshot shows the same "Authentication v 0.01" interface. The "Login" field now contains "admin'--" and the "Password" field contains a single dot ".". The "connect" button is still visible.

- Bấm connect và ta thu được kết quả như bên dưới

Authentication v 0.01

Welcome back admin !

Your informations :

- username :

- password :

Hi master ! To validate the challenge use this password

Login

Password

- Xem mã nguồn ta thấy giá trị của password là **t0_W34k!\$**. Sử dụng password này để vượt qua thử thách này

Authentication v 0.01

Welcome back admin !

Your informations :

- username :

- password :

Hi master ! To validate the challenge use this password

Login

DevTools is now available in Vietnamese! [Always match Chrome's language](#) [Switch DevTools to Vietnamese](#) [Do](#)

Elements Console Recorder Sources Network Performance Memory Application

```
<html>
<head>...</head>
<body data-new-gr-c-s-check-loaded="14.1056.0" data-gr-ext-installed>
  <link rel="stylesheet" property="stylesheet" id="s" type="text/css" href="/template/s.css" m...
  <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> == $0
  </p>

```

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 \(Exploitation - Web\)](#)
-  [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 \(Exploitation - Web\)](#)

[0](#) 5

Validation

Well done, you won 30 Points

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

FLAG: t0_W34k!\$