Mysql注入新姿势---innodb存储引擎的利用

c1em0 / 2017-11-16 10:56:00 / 浏览数 2508 安全技术 技术讨论 顶(0) 踩(0)

作者：C1em0 @D0g3

前言

对于常见的mysql注入来说，我们常利用mysql中自带存储整个数据信息的information_schema数据库来注入查询数据。但是当我们遇到正则将其关键字，例如informatio

Mysql>5.6.x

在Mysql中，存储数据的默认引擎分为两类。一类是在5.5.x之前的MyISAM数据存储引擎，另一类是5.5.x版本后的innodb引擎。并且mysql开发团队在5.5.x版本后将innod

而在mysql 5.6.x版本起，innodb增添了两个新表，一个是innodb_index_stats,另一个是innodb_table_stats。查阅官方文档，其对这两个新表的解释如下图：

从官方文档我们可以发现两个有用的信息：

1. 从5.6.x版本开始，innodb_index_stats和innodb_table_stats数据表时自动设置的。
2. 两个表都会存储数据库和对应的数据表。

本地实验

那么我们来本地实验下，我是用mysql 5.7.2版本来实验

```
select @@innodb_version;
```

查看已有的数据库

查看innodb_table_stats表中的数据

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

表中只有两个系统数据库和一个user数据库和对应表名，以及最后更新时间。这个结果很是让人疑惑，既然有数据，但是为什么数据不全，单单只出现了一个数据库。再次查
Persistent Statistics
Tables（永久记录表）。观察表中显示user数据库是11月4号创建的，而笔者测试的时候是11月14号，中间相隔10天。那么这里我们再次创建一个inno_test的数据库。

发现也被记录了下来。于是我们就有了取代information_schema的注入payload

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

就能够成功注入。

上一篇：某开源框架从信息泄露到后台失守 下一篇：某开源框架从信息泄露到后台失守

1. 1 条回复


hades 2017-11-21 10:23:28

@c1em0 思路还是挺不错的

0 回复Ta

目录