ISCC 2018 web writeup

原创

linlhf 于 2018-05-20 17:59:42 发布 1576 收藏
分类专栏： 网络安全

1.php是世界上最好的语言

看源码，我们可以看到MD5的0e漏洞，即0后面的数字都不识辨，值默认为0

```
<?php
header("content-type:text/html;charset=utf-8");
if(isset($_POST['username'])&isset($_POST['password'])){
    $username = $_POST['username'];
    $password = $_POST['password'];
}
else{
    $username="hello";
    $password="hello";
}
if(md5($password) == 0){
    echo "xxxxx";
}
show_source(__FILE__);

?>
```

用户名随便，密码使用0e开头的MD5值：

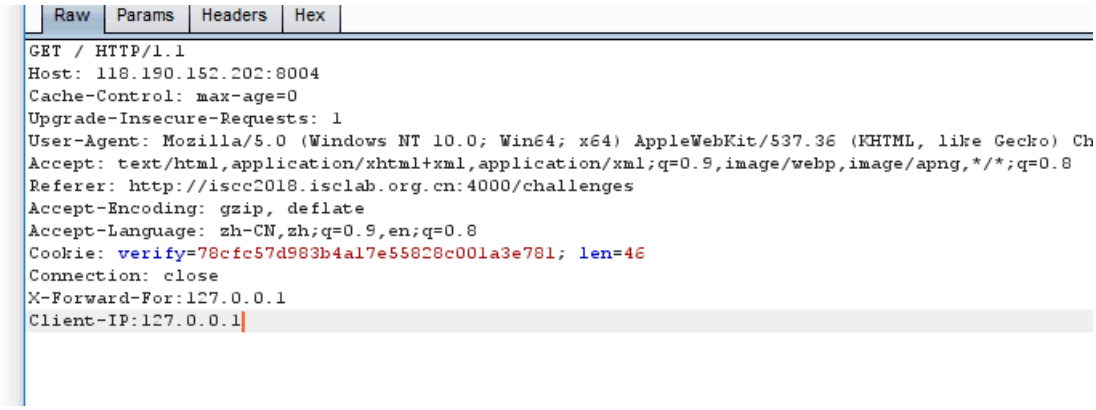
```
s878926199a
```

这里提供一个网站，里面归纳了一些0e开头的MD5值 http://www.219.me/posts/2884.html

之后需要将a的值变为Globals,使其变为全局变量，flag便出现了

2.web02

要求我们用本地IP访问。抓包，改请求头



注意：大小写一定要区分

3.你能跨过去吗？

将url进行解码，然后删除必要的符号，进行base64解码

http://www.test.com/NodeMore.jsp?

id=672613&page=2&pageCounter=32&undefined&callback=%2b/v%2b%20%2bADwAcwBjAHIAaQBwAHQAPgBhAGwAZQByAHQAKAAiAGsAZQB5A

&_=1302746925413

<script>alert("key:/%nsfocusXSStest%/")</script>

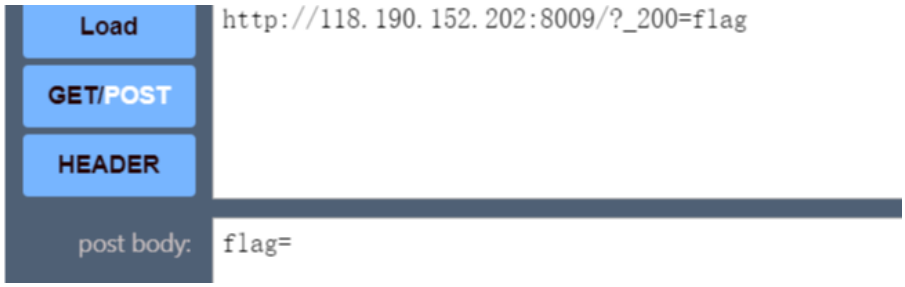
输入key，flag就出来了

4.一切都是套路

我们需要输入 http://118.190.152.202:8009/index.php.txt 才能看到代码

```php
<?php

include "flag.php";

if ($_SERVER["REQUEST_METHOD"] != "POST")
 die("flag is here");

if (!isset($_POST["flag"]) )
 die($_403);

foreach ($_GET as $k => $v){
 $$k = $$v;
}

foreach ($_POST as $k => $v){
 $$k = $v;
}

if ( $_POST["flag"] !== $flag )
 die($_403);

echo "flag: ". $flag . "\n";
die($_200);

?>
```

这里需要post也需要get,直接post是不行的



flag: ISCC{taolu2333333....}