ISCC2018部分WriteUp

原创

江左盟宗主 于 2018-05-06 21:45:02 发布 17609 收藏
文章标签： ISCC CTF CTF WriteUp ISCC2018 PHP代码审计

一、比较数字大小

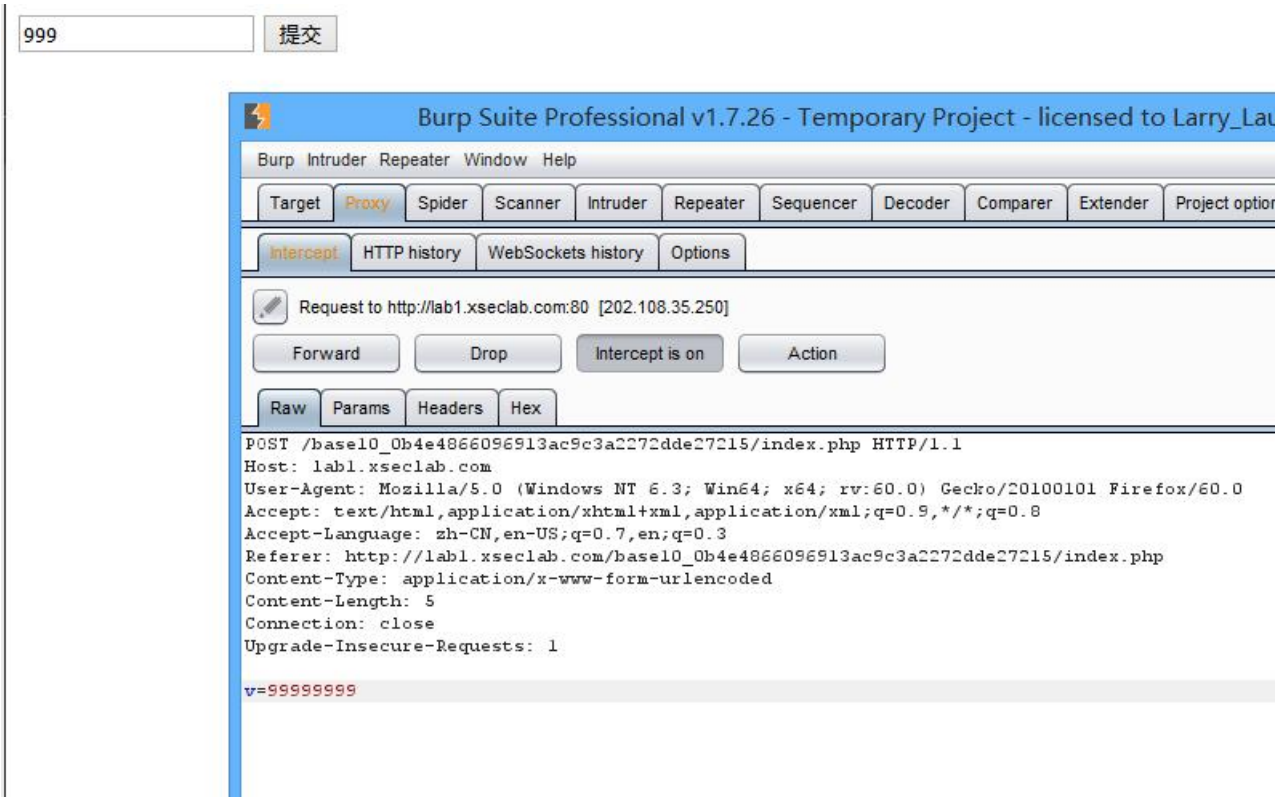
只要比服务器上的数字大就好了

题目地址：http://118.190.152.202:8014/

打开之后很简洁，一个提交框，首先查看源代码：

```
<!-- saved from url=(0073)http://lab1.xseclab.com/base10_0b4e4866096913ac9c3a2272dde27215/index.php -->
<html><head><meta http-equiv="Content-Type" content="text/html; charset=UTF-8">

    </head>
    <body>
                <form action="http://lab1.xseclab.com/base10_0b4e4866096913ac9c3a2272dde27215/index.php" me
            <input type="text" maxlength="3" name="v">
            <input type="submit" value="提交">
        </form>


</body></html>
```

点开提示的链接没发现和这个差别不大，在提交框随便输入，发现只能输入3位，然后提交,发现必须填数字，而且就算是数字999也显示数字太小了，然后开启浏览器代理，打开BurpSuite,再次输入999提交，BurpSuite拦截http请求，然后修改999为很多个9就可以啦，然后点forward，得到flag



key is 768HKyu678567&*&K

二、web01

题目地址: http://118.190.152.202:8003/

点开之后是源代码：

```
<?php
highlight_file('2.php');
$flag='{***************}';
if (isset($_GET['password'])) {
    if (strcmp($_GET['password'], $flag) == 0)
        die('Flag: '.$flag);
    else
        print 'Invalid password';
}

?>
```

分析代码发现：php中strcmp函数存在弱类型，如果是一个数组和字符串比较，函数会报错，但依然会返回0，因此可以利用这歌漏洞来绕过验证得到flag。


```
<?php
highlight_file('2.php');
$flag='{***************}';
if (isset($_GET['password'])) {
        if (strcmp($_GET['password'], $flag) == 0)
                die('Flag: '.$flag);
        else
                print 'Invalid password';
}
?> Flag: ISCC{iscc_ef3w5r5tw_5rg5y6s3t3}
```

三、本地的诱惑

小明扫描了他心爱的小红的电脑，发现开放了一个8013端口，但是当小明去访问的时候却发现只允许从本地访问，可他心爱的小红不敢让这个诡异的小明触碰她的电脑，可小明真的想知道小红电脑的8013端口到底隐藏着什么秘密(key)？（签到题）
题目地址: http://118.190.152.202:8013/

打开之后显示只能从本地访问，肯定想到修改ip了吧？被套路了吧？我也被套路了(-_-)。看题！！最后又对括号（签到题），打开源码发现flag。

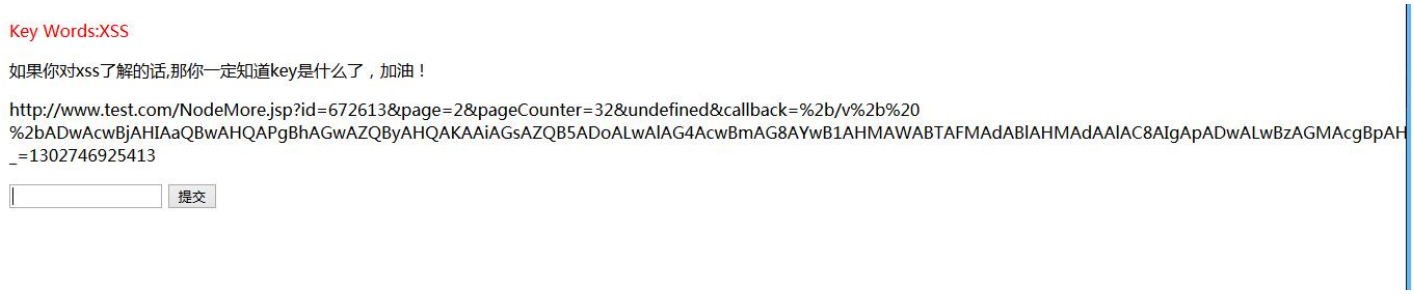
```
<html>
    <head>
        <meta charset="gb2312" />
    </head>
    <body>

必须从本地访问!      </body>
</html>



<html>
    <head>
        <meta charset="utf-8" />
    </head>
    <body>

<?php
//print_r($_SERVER);
$arr=explode(',',$_SERVER['HTTP_X_FORWARDED_FOR']);
if($arr[0]=='127.0.0.1'){
    //key
    echo "key is ISCC{`&*(UIHKJjkadshf}";
}else{
    echo "必须从本地访问！";
}
?>    </body>
</html>
```

四、你能跨过去吗？

如果你对xss了解的话,那你一定知道key是什么了，加油！

题目地址: http://118.190.152.202:8010/

打开看到：



这个框是可以xss的但是机关算尽都没得到flag。这个URL挺奇怪的，把callback的值用URL解码，发现+/v+ ，显然是UTF-7编码，然后打开XSSEE网站，把callback的值复制，UTF-7解码得：+/v+ <script>alert("key:/%nsfocusXSStest%/")</script>-&_然后就是提交key了：

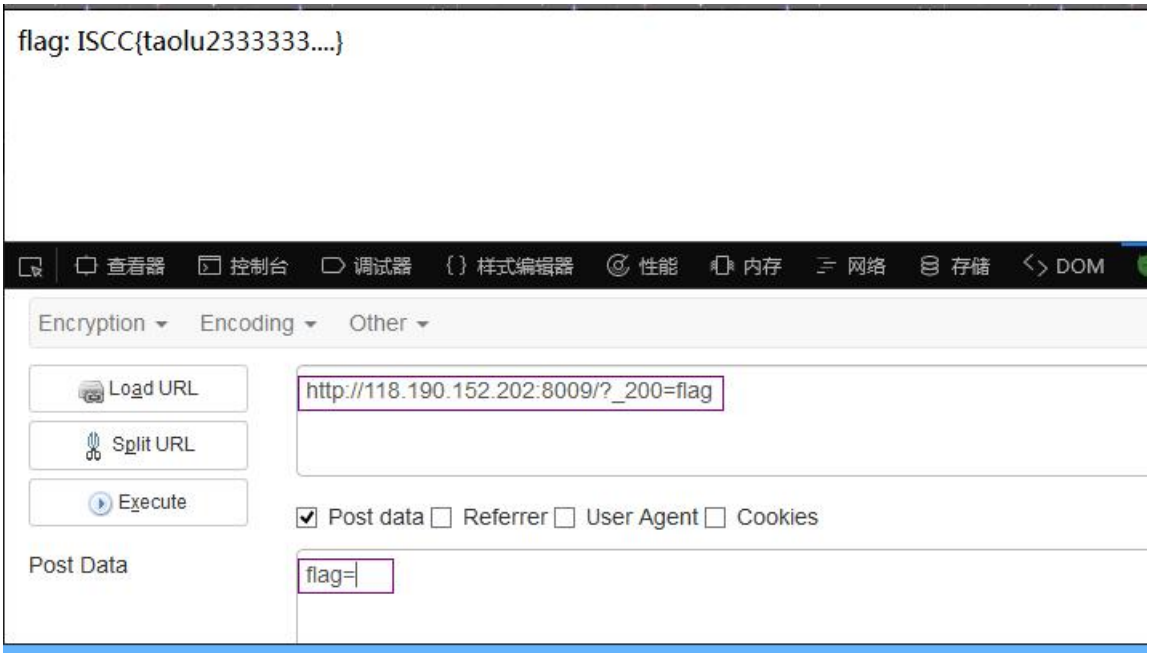
五、一切都是套路

好像有个文件忘记删了
题目地址: http://118.190.152.202:8009/

打开之后发现只有一行`flag is here`，查看源码也是只有这一行，看到提示好像有个文件忘记删了，是什么文件呢？我用御剑后台扫描发现存在`index.php`，`flag.php`，然后我输入`index.php.txt`惊喜的发现了忘删的文件：

```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);
?>
```

分析代码，如果是POST提交最后就会显示出flag，然后我屁颠屁颠的直接POST提交flag，结果输出的不是真正的flag。然后继续分析，如果POST没有提交flag就会输出$_403的值，然后是两个foreach函数，这两个函数会替换$flag的值。然后如果POST提交的flag类型或值不一样时输出$_403的值，最后输出$flag，和$_200的值，所以我们可以提交的时候把flag的值赋值给$_200或者$_403就可以了。经过测试只有把flag的值赋给$_200可以得到flag。

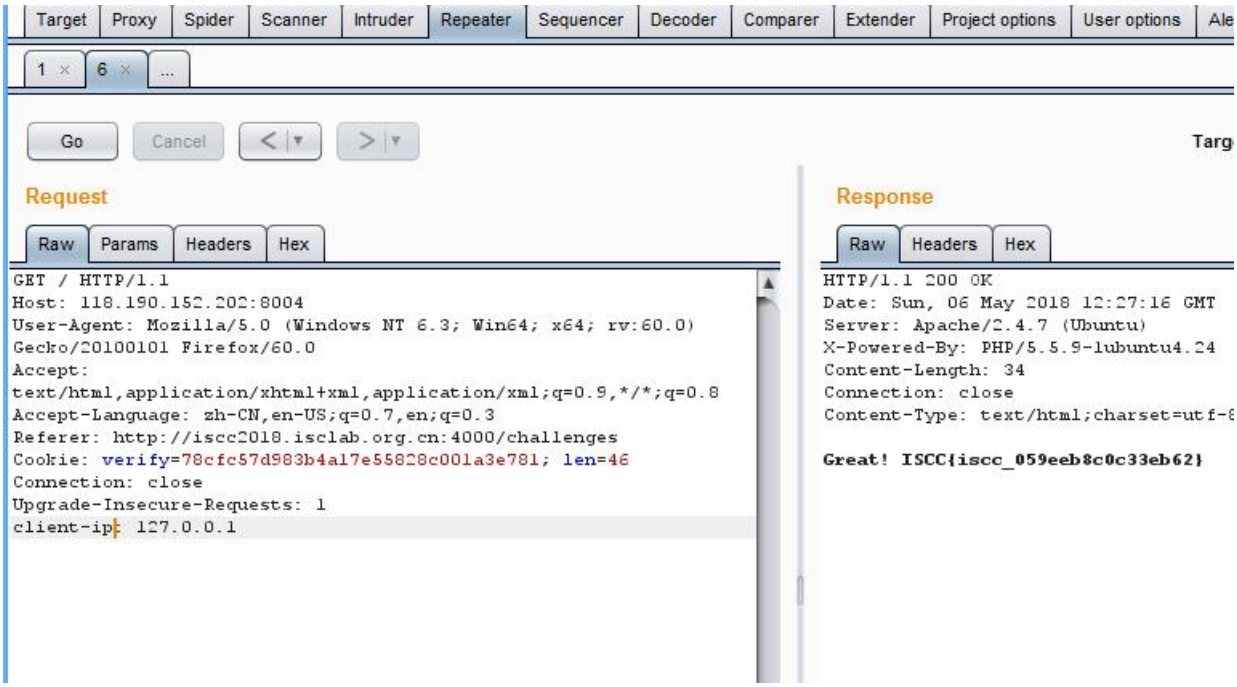


六、web02

题目地址：http://118.190.152.202:8004/

打开后显示：错误！你的IP不是本机ip！

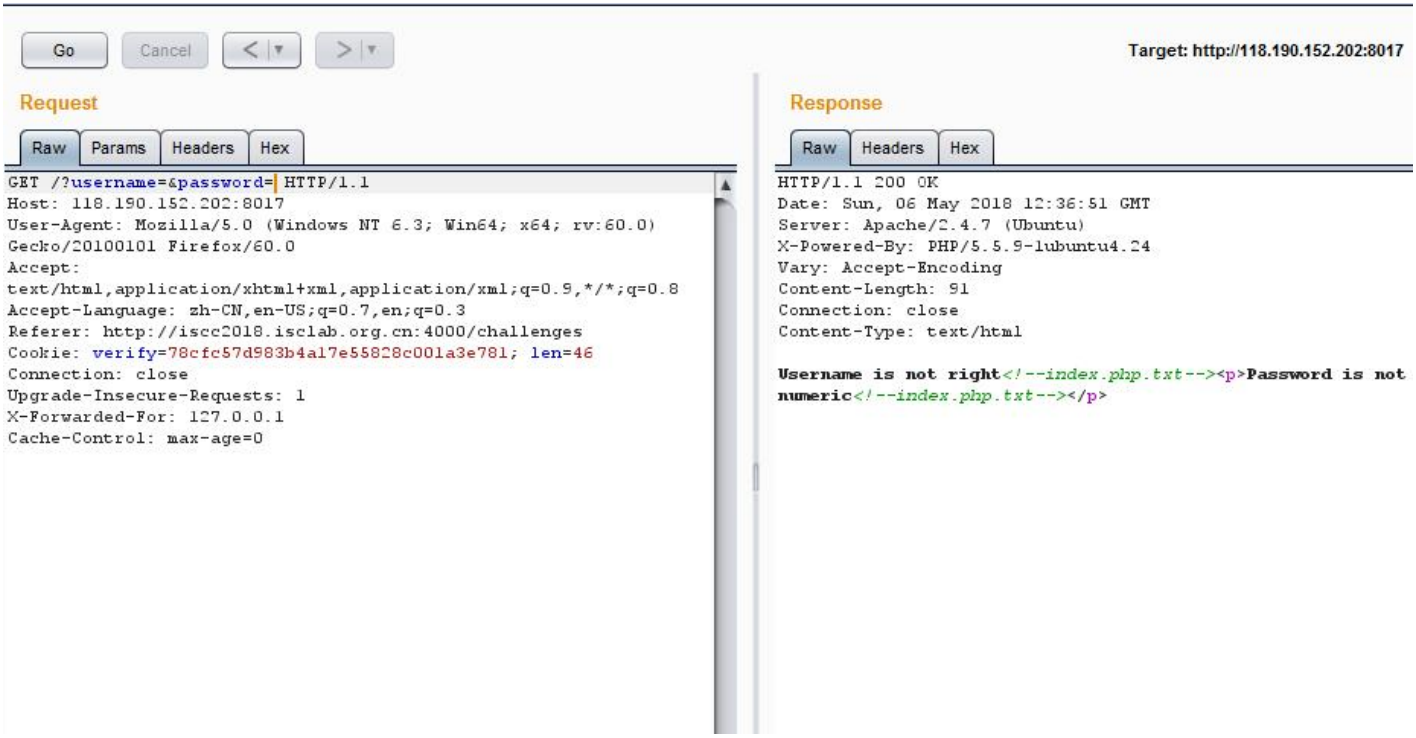
显然，修改http请求头的ip呗，不过发现用X-Forwarded-For修改后没用，用Client-Ip修改后成功得到flag



七、Please give me username and password!

题目地址：http://118.190.152.202:8017/

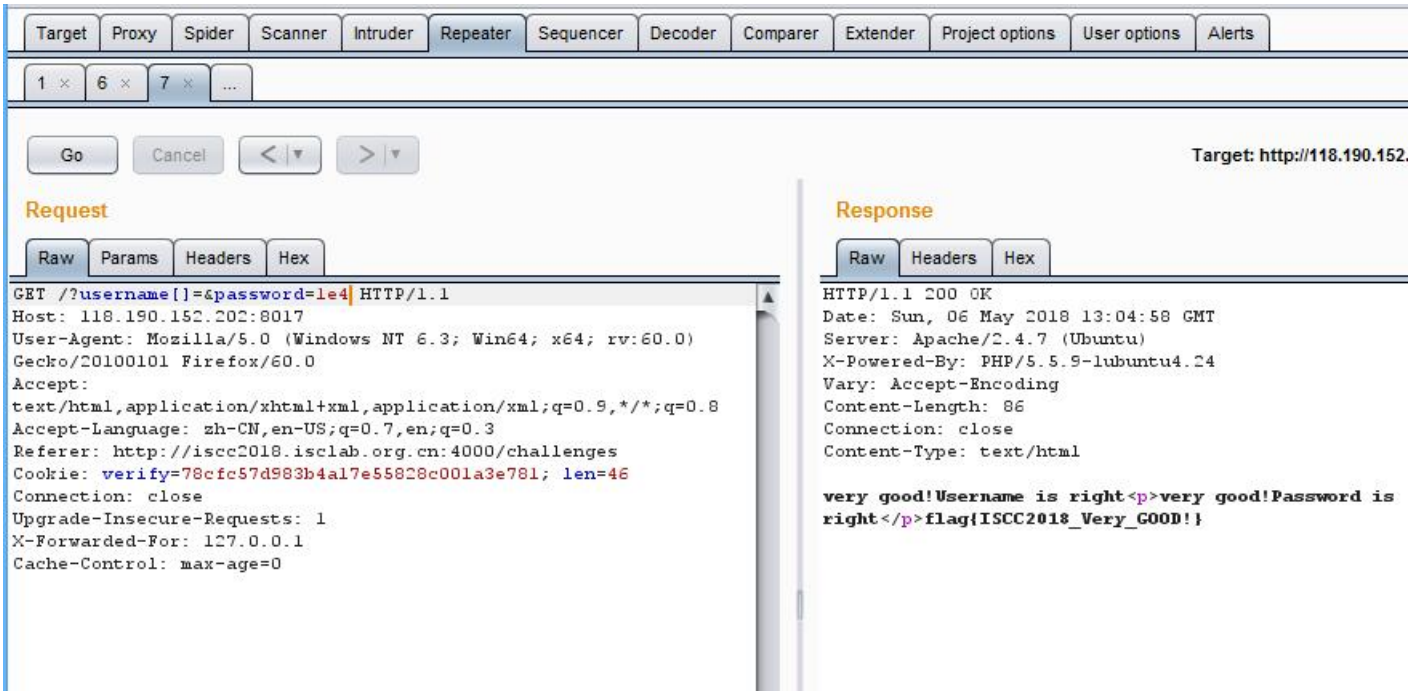
打开发现只有这句话，查看源码也一样。打开BurpSuite，设置浏览器代理，刷新页面，在BurpSuite中修改请求头，添加GET请求的参数提交，发现返回Username is not right<!--index.php.txt-->
Password is not numeric<!--index.php.txt-->



在浏览器URL后加入index.php.txt，发现源代码

```php
<?php
error_reporting(0);
$flag = "***********";
if(isset($_GET['username'])){
 if (0 == strcasecmp($flag,$_GET['username'])){
 $a = fla;
 echo "very good!Username is right";
 }
 else{
 print 'Username is not right<!--index.php.txt-->';}
}else
print 'Please give me username or password!';
if (isset($_GET['password'])){
 if (is_numeric($_GET['password'])){
  if (strlen($_GET['password']) < 4){
   if ($_GET['password'] > 999){
   $b = g;
   print '<p>very good!Password is right</p>';
  }else
   print '<p>Password too little</p>';
  }else
  print '<p>Password too long</p>';
 }else
 print '<p>Password is not numeric</p>';
}
if ($a.$b == "flag")
 print $flag;
?>
```

分析代码发现，提交的username和$flag的值进行比较用的是strcasecmp函数它和strcmp的区别是他的比较不区分大小写，但是已经存在漏洞，传入数组依旧会得到0，轻松绕过。输入的password需要是字母或数字，并且长度最大是3位值要大于999，最后就可以得到flag。因此构造GET提交的参数username[]=&password=1e4成功得到flag



八、秘密电报

知识就是力量：ABAAAABABBABAAAABABAAABAAABAAABAABAAAABAAAABA

密文长度是45，并且由2种字符组成，我先想到的是摩斯密码，但是并不是，然后问了度娘发现是培根密码，培根什么时候成精了，还发明了培根密码。

培根密码加密方式：

A：aaaaa　B：aaaab　C：aaaba　D：aaabb E aabaa　F：aabab　G：aabba　H：aabbb　I：abaaa　J：abaab　K：ababa　L：ababb　M：abbaa　N：abbab　O：abbba　P：abbbb　Q：baaaa　R：baaab S：baaba T：baabb　U：babaa　V：babab　W：babba　X：babbb　Y：bbaaa　Z：bbaab

5个一组解密后：ILIKEISCC