[极客大挑战 2019]BuyFlag

原创

Sk1y 于 2020-12-29 20:59:21 发布
分类专栏： CTF刷题记录 文章标签： php 字符串 安全

[极客大挑战 2019]BuyFlag

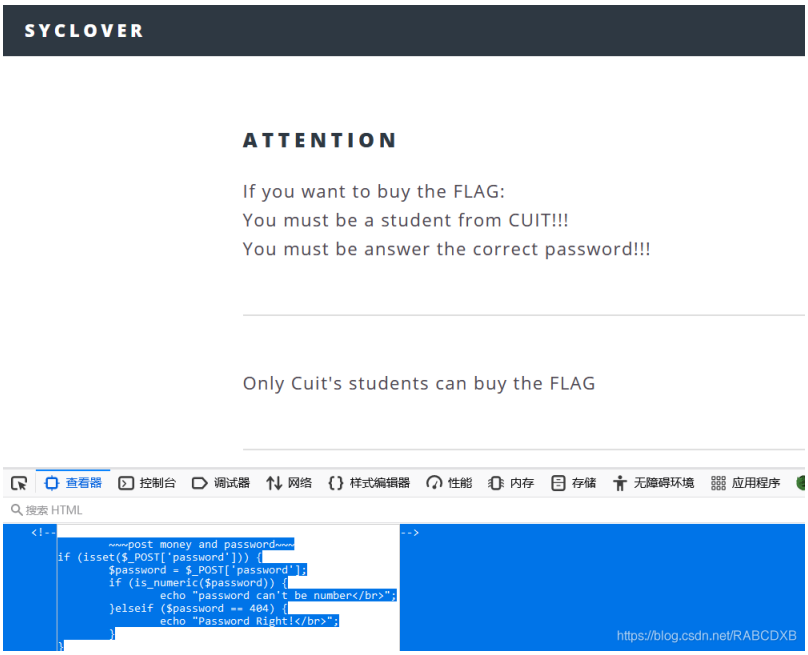
一点小记：

本题不错哎，学到了挺多的知识，php strcmp()漏洞，is_numeric()漏洞，并且在本地复现了一下，并且做了总结。

题目分析：

题目是下面这个样子滴

在点击PAYFLAG，我们可以在f12中发现了一些线索



代码审计一下：需要我们POST传值money和password，并且要求password不能全是字符，并且money要是100000000，这就涉及两个php函数的漏洞了。

```
 ~~~post money and password~~~
if (isset($_POST['password'])) {
 $password = $_POST['password'];
 if (is_numeric($password)) {
  echo "password can't be number</br>";
 }elseif ($password == 404) {
  echo "Password Right!</br>";
 }
}
```

一、php is_numeric()漏洞

is_numeric(str)函数会对传入的str字符进行判断，有以下几类情况会返回1：

is_numeric(str)返回1的情况	举例
str为纯数字（+-只允许在开头str头部出现一次）	123，+123，-123
16进制的字符串	0x61646D696E(admin的16进制),0x20(空格的16进制)

所以可以将password的值设为404%00（%00是空字符的url加码）

注意：password的值也可以是%00404,404%20,因为is_numeric()函数对%00不论是在字符串前面还是后面都判定为字符，而对%20只有当%20位于字符后面时才判定为字符

但是%20404，is_numeric()函数会对第一个空格字符跳过，对接下来的字符进行判断

```php
<?php
echo '传入:404 :' . is_numeric('404 ');  //注意404后面有一个空格
echo '<hr>';
echo '传入: 404:' . is_numeric(' 404');  //注意404前面有一个空格
echo '<hr>';
echo '传入:404%00:' . is_numeric('404%00');
echo '<hr>';
echo '传入:%00404:' . is_numeric('%00404');
echo '<hr>';
```

结果如下：

传入:404 :

传入: 404:1

传入:404%00:

传入:%00404:

二、php == 弱类型比较

接下俩会对$password与404进行比较，因为php的弱类型比较，404%00==404 返回值为1；

404%00==404

404%20==404

以上两种情况返回值都为真

本地相关实验代码如下：

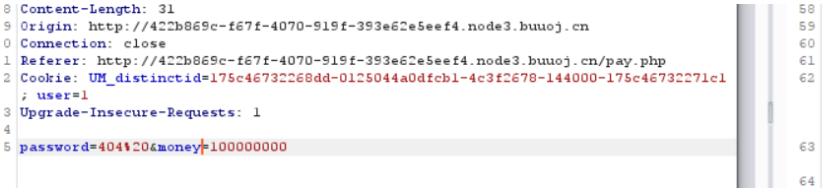
```php
<?php
$a='404%00';
$b='%00404';
$c='404%20';
$d='%20404';
if($a==404)
{
    echo"$a==404成立";
}
if($b==404)
{
    echo"$b==404成立";
}
if($c==404)
{
    echo"$c==404成立";
}
if($d==404)
{
    echo"$d==404成立";
}
```

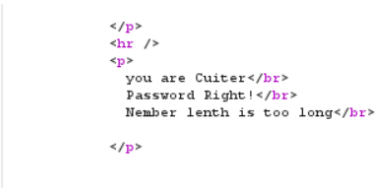
执行的结果是

404%00==404成立404%20==404成立

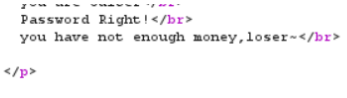
三、php strcmp()漏洞

经过上面的判断，将password=404%20&money=100000000传入，抓包，（注意将user=0改为user=1）,但是





回显number length is too long.所以就试试减个0



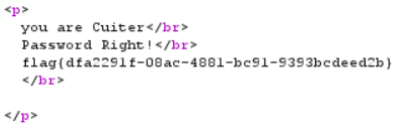
但是又显示钱不够,loser.

所以猜测这个题目是将我们传入的money与100000000进行对比，如果小就返回Money不够，但是又不能真的是100000000，会显示长度过长。所以猜测是strcmp()函数

strcmp(str1,str2)函数，参数是两个字符串，相等返回为零；str1大于str2，返回大于零；str1小于str2，返回小于零。

传入的类型是字符串类型的数据，如果传入其他类型会报错，但是会认为两个字符串相等，直接返回0！！！！一般可以采用传入数组或者对象进行绕过。

如本题目中可以采用money[]=1



总结

本题目中的很多地方在本地环境进行了复现，掌握了新的知识。