php带帽接口_一道php代码审计的writeup

原创

函明 于 2021-01-12 11:51:40 发布 14 收藏
文章标签： php带帽接口

@Szrzvdny的题

首先访问网站

http://118.89.157.11/code/

访问index.txt

我就直接复制到notepad++里了, 看着比较方便

看代码

md5解密结果: HaHa

HTTP_BGROTNYSPXPD在http包中也没有, 尝试直接构造

返回 man,your need Crack Md5

来到下一段if语句

md5解密结果: !#%ASFASDY#$&ASF

在burp中构造

Go

hash先不管, 看下一段if

$pass=unserialize(base64_decode($_GET['pass']));

它是先解密然后再反序列化, 那么我们就要先序列化在加密

if($pass!==" &&is_array($pass)){

$a=$pass['a'];

$b=$pass['b'];

$c=$pass['c'];

同时这里的$pass要是数组

直接在本地echo序列化的内容

那么初始代码就是这样的

$arr = array('a'=>'a','b'=>'b','c'=>'c');

echo base64_encode(serialize($arr));

?>

不过下面的if就有点变态了

if((md5($a) == md5($b) && $a !== $b)){

echo "WOW!
";

$v1=1;

http://www.cnblogs.com/Primzahl/p/6018158.html

PHP在处理哈希字符串时，会利用"!="或"=="来对哈希值进行比较，它把每一个以"0E"开头的哈希值都解释为0，所以如果两个不同的密码经过哈希以后，其哈希值都是以"0E"开头的，那么PHP将会认为他们相同，都是0。

原来要利用php的一个缺陷

用这两个字符串

s878926199a

0e545993274517709034328855841020

s1091221200a

0e940624217856561557816327384675

更改代码

$arr = array('a'=>'s878926199a','b'=>'s1091221200a','c'=>'c');

echo base64_encode(serialize($arr));

?>

echo输出

YTozOntzOjE6ImEiO3M6MTE6InM4Nzg5MjYxOTlhIjtzOjE6ImliO3M6MTI6InMxMDkxMjIxMjAwYSI7czoxOiJjIjtzO

构造参数

提交

出现WOW!

还是if

```
if(strlen($c)<4 && $c>99999999){
echo "666666!";
$v2=1;
}
```

$c要小于4并大于99999999

这里虽然是strlen, 但没说$c一定要是字符串

回到本地测试

```
$arr = array('a'=>'s878926199a','b'=>'s1091221200a','c'=>array('aaa'));
$c = $arr['c'];
if(strlen($c)<4 && $c>99999999){
echo "666666!";
}
echo base64_encode(serialize($arr));
?>
```

访问

出现Warning并输出666666!

YTozOntzOjE6ImEiO3M6MTE6InM4Nzg5MjYxOTIhIjtzOjE6ImliO3M6MTI6InMxMDkxMjIxMjAwYSI7czoxOiJjIjthC

burp构造 提交

继续看代码

```
$aa = base64_decode($_GET['file']);
$bb = base64_decode($_GET['file1']);
if((md5($aa) == md5($bb) && $aa !== $bb)){
if(encodeSecret($_GET['onet']) == $encodedSecret){
echo $flag;
```

}else{

echo 'come on baby';

}

}else{

echo "On On On";

}

get传递file1 file2, 同时要用base64加密, 然后是比较md5

依然用这两个

s878926199a

s1091221200a

Go

输出come on baby

if(encodeSecret($_GET['onet']) == $encodedSecret){

echo $flag;

}else{

echo 'come on baby';

查看encodeSecret

function encodeSecret($secret) {

return bin2hex(strrev(base64_encode($secret)));

}

Hash:3d3d516343746d4d6d6c315669563362

bin2hex 转16进制

转回去 pack("H*",bin2hex($str))

strrev 翻转字符串

只要再翻转一次就可以了

回到本地

function decodeSecret($str){

return base64_decode(strrev(pack("H*",$str)));

}

```
echo decodeSecret('3d3d516343746d4d6d6c315669563362');
?>
```

burp构造, 得到了flag