实验吧 WEB题目题解

原创

buchiyexiao. 于 2019-05-08 20:29:10 发布 259 收藏

分类专栏： ctf 文章标签： ctf writeup

本文链接：https://blog.csdn.net/qq_43647462/article/details/89972135

Shiyanbar WEB题目WriteUp

- 天网管理系统

天网你敢来挑战嘛
格式：ctf{ }

我们打开题目，发现了一个的登录界面，既然告诉我们账号密码，那我们就尝试登陆一下

天网管理系统

安全与你同在

账户:admin 密码:admin

就是这么光明正大的放置用户名和密码,爸爸说我们再也不会忘记密码啦。

大家请放心使用我们的产品。

用户名: admin

密码: admin

登入系统

果不其然，没什么用，查看下源代码
发现注释部分藏着信息

$test= $_GET['username'];
$test= md5(test); if($test=='0')
就是把username进行md5变换后与0进行比较，而经过查阅我们可以发现PHP在处理哈得到地址
进入后查看源码发现是一个简单的反序列化然后进行简单的判断

进入后查看源码发现是一个简单的反序列化然后进行简单的判断

```
$unserialize_str = $_POST['password'];
      $data_unserialize = unserialize($unserialize_str);
      if($data_unserialize['user'] == '???' && $data_unserialize['pass']=='???')
      {
        print_r($flag);
      }
伟大的科学家php方言道：成也布尔，败也布尔。
回去吧骚年
```

然后我们输入数组并且保证其判断可以绕过，传入一个数组，含有两个变量，一个变量
PS：自己开始的时候一直以为会有__wakeup()防绕过所以找了半天

- 忘记密码了

（我前脚写完这个题目，刚要写WP，后脚实验吧服务器就挂了？？？）

首先我们打开题目二话不说直接先随便输入个邮箱进去发现弹出来提示我们去看step2.php，而step2.php我们打开后发现直接跳转到step1.php，拿bp抓一下，看一下step2.php的源码，会发现其实step2.php是把信息传入到submit.php

```
<body>
    <form action="submit.php" method="GET">
        <h1>找回密码step2</h1>
        email:<input name="emailAddress" type="text" <br />
<b>Notice</b>: Use of undefined constant email - assumed 'email' in <b>C:\h43a1W3\phpstudy\WWW\10\upload\step2.php</b> on line <b>49</b><br />
<br />
<b>Notice</b>: Undefined index: email in <b>C:\h43a1W3\phpstudy\WWW\10\upload\step2.php</b> on line <b>49</b><br />
value="" disable="true"/></br>
        token:<input name="token" type="text" /></br>
        <input type="submit" value="提交">
    </form>
</body>
</html>
```

然后我们去访问下submit.php，本以为过了，发现还是不行，我们回来再把step1.php抓一下，对比看一下step1.php和step2.php，发现编辑器是Vim，经过面向百度做题，我们知道了Vim中如果文件非正常退出会产生一个临时文件，临时文件名字为.文件名.swp，因此我们去访问.submit.php.swp，看到页面的源码，发现一堆乱码，在乱码中找到我们所需要的代码

```
if(!empty($token)&&!empty($emailAddress)){
        if(strlen($token)!=10) die('fail');
        if($token!='0') die('fail');
        $sql = "SELECT count(*) as num from `user` where token='$token' AND email='$emailAddress'";
        $r = mysql_query($sql) or die('db error');
        $r = mysql_fetch_assoc($r);
        $r = $r['num'];
        if($r>0){
                echo $flag;
        }else{
                echo "瀹辫触浜嗗悆";
        }
}
```

其中我们需要两个参数，一个是emailAddress这个我们可以从step2中看到admin@simplexue.com，而token需要我们自己构造，token长度为10且值为0，最简单就是0000000000,即可以完成判断，将这两个参数传入即可获得flag

（如果无法确定自己传入的token是否满足要求，可以自己写几行代码去测试下~）