实验吧-忘记密码了 Writeup

原创

baynk 于 2019-08-22 02:16:36 发布 121 收藏 1

分类专栏： # 实验吧 Writeup 文章标签： CTF 实验吧 忘记密码了

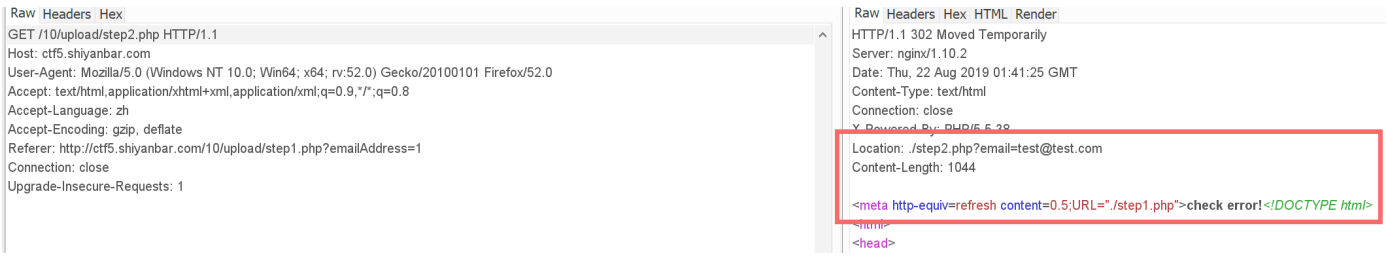
本文链接：https://blog.csdn.net/u014029795/article/details/100006582

两天没写了，来练练手，不过这玩意是真的把我难住了一会，由于没太多时间去想，所以直接去看了writeup，没看完就知道自己问题出在哪了，记录一下。

过程

- 链接：http://ctf5.shiyanbar.com/10/upload/step1.php
- 随便填了一个，丢到Burpsutie中去的repeater看。

- 只看到这两个内容，不过有新的页面出现了，继续访问下，html header的内容可能是提示吧，先记下来，去访问setup2。

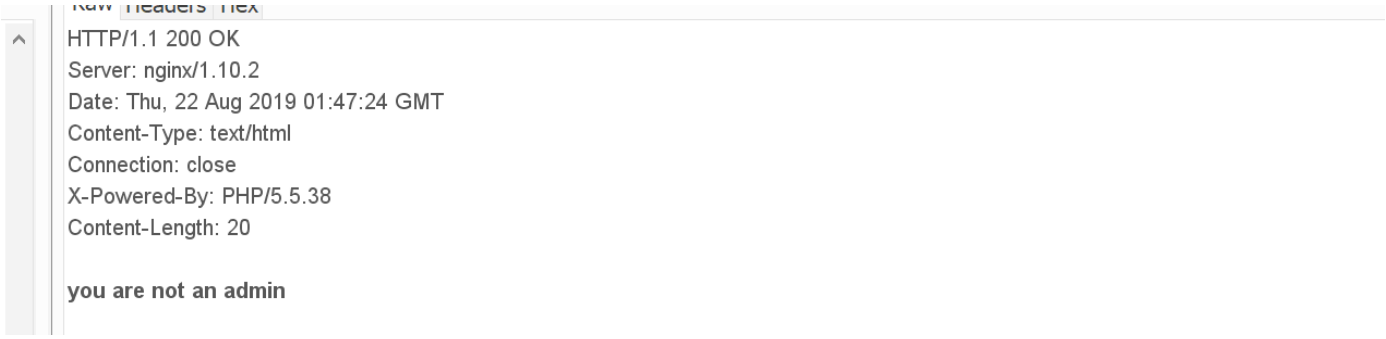


- 由于没有提交参数，所以就自动刷新到setup1了。当然在刷新前还有一个test@test.com，暂时也没找到好用的地方，源码中最后一行还有提示，表单中会有要提交数据的文件，比较容易忽略的。

```
</head>
<body>
    <form action="submit.php" method="GET">
        <h1>找回密码step2</h1>
```

```
            email:<input name="emailAddress" type="text" value=""  disable="true"/></br>
            token:<input name="token" type="text" /></br>
            <input type="submit" value="提交">
        </form>
</body>
</html>
```

- 这里有告诉，要往submit.php中提交emailAddress参数和token参数，接着去访问submit.php。



- 提示不是管理员，用之前的test@test.com不行，又试了之前html header中的admin@simplexue.com。

- 结果显示空白，可能是没有token的问题，这里就随便试了两个token，要么是空白的要么就是fail。。。

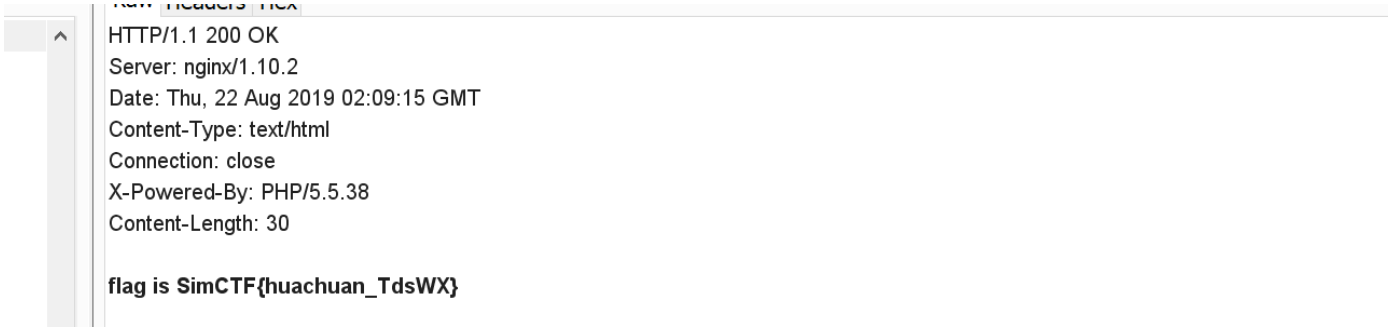
- 关键是这种绕过题，没有源码提示如何才能绕过。。。就卡在这了，于是才去看的writeup，经过“作弊”，才知道要利用html header中的editor是vim这个提示，vim如果使用完没有正常退出，会留下一个隐藏的swp文件，这里就是利用这一点，去看submit.php的源码。访问的文件为`.sumbit.php.swp`，这里一定要在前面加上一个点，因为linux中的隐藏文件就是以.开头的。

```
INSERT INTO `user` (`id`, `username`, `email`, `token`) VALUES
(1, '****不可见***', '***不可见***', 0);
*/


.....这一行是省略的代码.....
```

```
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 "失败了呀";
        }
}
```

- 终于能看到源码了，token是为0，但是下面也有判断token长度一定要为10，而且不能等于0，这就奇怪了，明明token就是0，还不能这样写0，仔细看了下原来是$token!='0'，字符串0，不是数字0，所以这里可以直接写'0000000000'这样的10个0来绕过，最后提交的语句为`/10/upload/submit.php?emailAddress=admin@simplexue.com&token=0000000000`



总结

- 多注意表单的名字，再仔细点
- 以后可以利用这个vim的隐藏文件看到更多的东西，GET。
-