实验吧-忘记密码了？writeup

转载

怀念_过去 于 2017-11-26 19:54:57 发布 1800 收藏

分类专栏： CTF 文章标签： vim


CTF 专栏收录该内容

13 篇文章 0 订阅

订阅专栏

知识点：vim产生的备份文件.swp

1.打开链接发现就是页面,什么提示也没有
http://ctf5.shiyanbar.com/10/upload/step1.php?emailAddress=

2.我们直接构造了一个邮箱发送:它显示
你邮箱收到的重置密码链接为 ./step2.php?email=youmail@mail.com&check=???????

3.然后访问这个地址,发现它会马上跳转到step1,所以我们直接查看这个step2.php的源代码.
http://ctf5.shiyanbar.com/10/upload/./step2.php

4.发现一些重要的东西:
<meta name=”admin” content=”admin@simplexue.com” />
<meta name=”editor” content=”Vim” />
<form action=”submit.php” method=”GET”>
<h1>找回密码step2</h1>
email:<input name=”emailAddress” type=”text” value=”test@test.com” disable=”true”/></br>
token:<input name=”token” type=”text” /></br>
<input type=”submit” value=”提交”>
</form>
发现它是发送到submit.php这个页面去进行验证的,所以说我们只需要可以查看到这个页面的php代码就解决了一切.

5.访问这个页面:http://ctf5.shiyanbar.com/10/upload/submit.php
发现显示you are not an admin

6.抓取数据包从setp2开始分析,发现我们应该传递两个Get数据参数给这个submit.php才可以
这个时候就要用到我们前面看到的admin@simplexue.com
http://ctf5.shiyanbar.com/10/upload/submit.php?emailAddress=admin@simplexue.com&token=
没有显示错误,说明admin@simplexue.com是这个邮箱 , 但是我们给token赋值时还是有错误 , 所以要想办法得得token的值.
但是怎么得到呢?这个时候我就不会了…..
查百度吧,发现了其中的奥秘,
通过源代码，发现是通过vim编写的，一般的vim编写可能会产生遗留问题，就是一个备份文件.swp;

7.既然vim编写有这样的bug,所以我们可以利用一下,看看是否能利用上:
http://ctf5.shiyanbar.com/10/upload/./submit.php.swp
浏览器显示:Not Found
继续百度:
VIM产生的备份文件和临时文件如何访问:

1.http://www.cnblogs.com/zwfc/p/5466885.html
2.http://www.jb51.net/article/110312.htm(没有讲清楚,但是你按着它讲的每一种方法去结合使用就成功了)

找到文章后,立马去测试:
访问:http://ctf5.shiyanbar.com/10/upload/.submit.php.swp
发现可以查看源代码了,哈哈,既然可以查看 , 那么基本上就解决了问题.

8.分析它的源代码:
INSERT INTO `user` (`id`, `username`, `email`, `token`) VALUES
(1, '****涓嶅彲瑙佸***', '***涓嶅彲瑙佸***', 0); ->token为0插入到数据库中

if(!empty(token)&&!empty(emailAddress)){ ->邮箱和token都不可以为空
if(strlen(出错误)