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

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

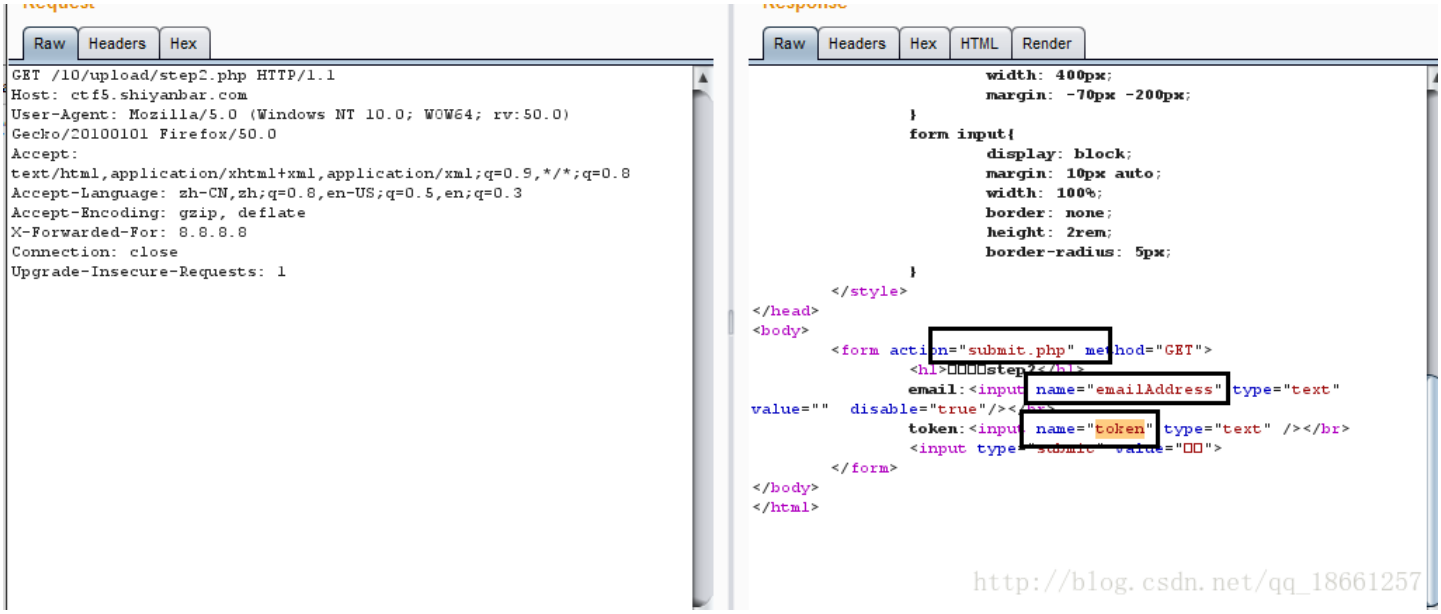
1.忘记密码了

> 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，然后我们通过抓包，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

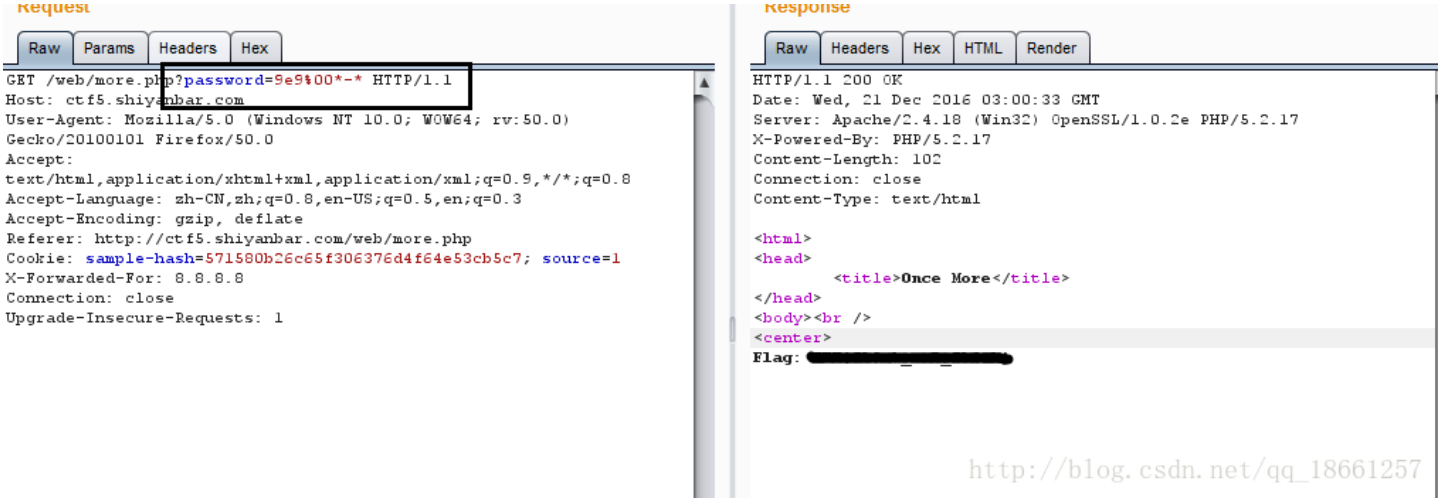
> 题解

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：



3.Guess Next Session

> 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

FALSE 分值：10

来源： iFurySt 难度：易 参与人数：2290人 Get Flag：722人 答题人数：726人 解题通过率：99%

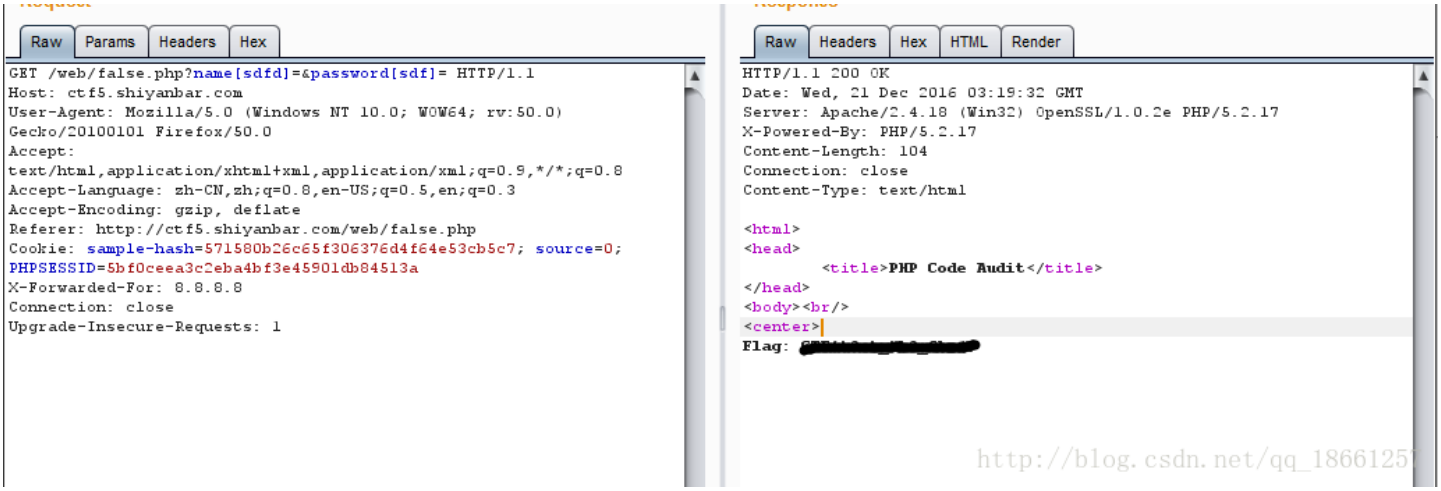
PHP代码审计
hint：sha1函数你有认真了解过吗？听说也有人用md5碰撞o(〃□〃)o
格式：CTF{}

解题链接： http://ctf5.shiyanbar.com/web/false.php 通过

提交

题解

又是有源码的题目，啊，有点不想写了，题目给出两个name和password不相同，同时 后面判断了sha1是否相同，嘿，sha1处理数组会返回false，然后两个false相等就是true，如此得到flag,但是数组要注意，name[x]=&password[y]=，x字符串和y字符串是不能相等，不然第一个判断语句是过不了的，嘿，如下图。



哎，写完啦，辛苦啊