# WeChall-writeup-4-11.17(Register Globals;Baconian;LSB;Limited Access)

原创

MeliodasC 于 2018-11-17 23:02:20 发布 461 收藏

分类专栏： WeChall 文章标签： WeChall writeup 安全



本文链接：https://blog.csdn.net/Crystal_bing/article/details/84194201





今天有时间来更新新的writeup！刚刚写完的！

前两天在看《达芬奇密码》，所以做的题稍微少了一点~丹布朗是真的很厉害！宗教，密码和文学被他融合成了他独特的一种文风。对我来说真的超有吸引力！

---

### Training: Register Globals

```php
# Send request?
if (isset($_POST['password']) && isset($_POST['username']) && is_string($_POST['password']) && is_string($_POST['username']) )
{
        $uname = GDO::escape($_POST['username']);
        $pass = md5($_POST['password']);
        $query = "SELECT level FROM ".GWF_TABLE_PREFIX."wc_chall_reg_glob WHERE username='$uname' AND password='$pass'";
        $db = gdo_db();
        if (false === ($row = $db->queryFirst($query))) {
                echo GWF_HTML::error('Register Globals', $chall->lang('err_failed'));
        } else {
                # Login success
                $login = array($_POST['username'], (int)$row['level']);
        }
}

if (isset($login))
{
        echo GWF_HTML::message('Register Globals', $chall->lang('msg_welcome_back', array(htmlspecialchars($login[0]), htmlspecial
        if (strtolower($login[0]) === 'admin') {
                $chall->onChallengeSolved(GWF_Session::getUserID());
        }
}
```



这一段是用来判断用户是否成功登陆的。第一个if中验证用户名和密码，如果匹配的话就set $ login；第二个if用来判断$ login是否被set，如果是的话就判断登陆成功。

所以可以通过传一个值给$ login，来绕开第一个if的验证。

Tip:关于Register Globals

---

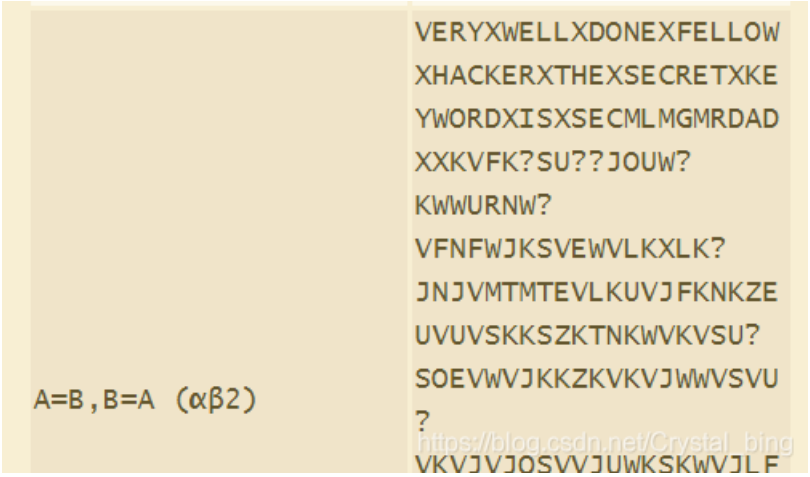
### Training: Baconian

```
#include<iostream>
#include<string.h>
using namespace std;
int main()
{
    char upper='A';
    char lower='B';
    string s;
    while(cin>>s){
        for(int i=0;i<s.size();i++)
    {

        if(s[i]>='A'&&s[i]<='Z'){cout<<'A';}
        else{cout<<'B';}
    }
    }

    return 0;
}
```

代码的大小写分别看作A与B，先写一个程序将密文转成AB序列。

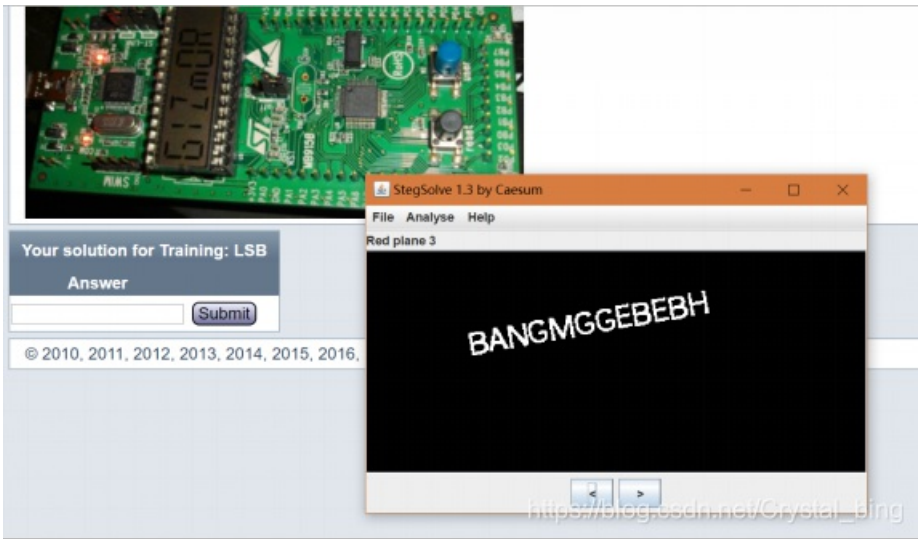



用这个在线工具dcode解码，找到keyword。

### Training: LSB

是你！隐写术！

用了一下Stegsolve

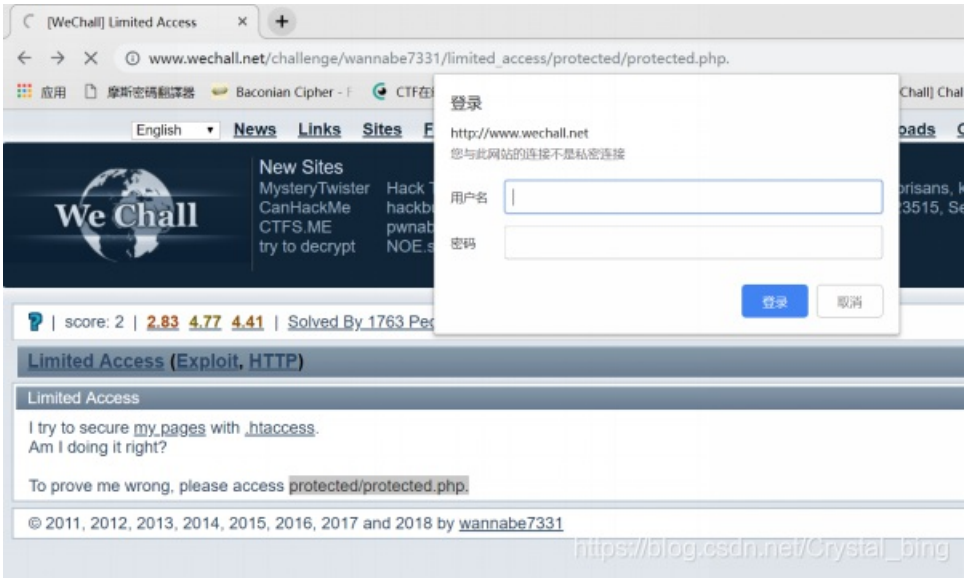



(每次keyword都不一样喔)

---

### Limited Access

首先发现访问给出的地址会出现账户的验证。（我们当然不知道啦）




看了一下网上大家的一些思路，选了一个现在手头能马上做出来的实现了一下:通过Firefox浏览器的Hackbar插件。