云演CTF: 007.blog

转载

wangguixiu 于 2021-06-09 22:57:45 发布 291 收藏

原文链接：https://www.wangguixiu.top/%E4%BF%A1%E6%81%AF%E6%94%B6%E9%9B%86/%E4%BA%91%E6%BC%94CTF-007-blog.html

版权

云演CTF: 007.blog

- 作者: admin
- 时间: 2021-05-28
- 分类: 信息收集

打开就是登录界面，直接'123456'，出现弹窗，还以为是js验证(想多了)，CTRL+u打开源码

```
$(function(){
    var $login = $("#login");
    $login.on(
        "click",function(){
            try{
                $.ajax({
                    url: '/admin/checklogin.php',
                    type: 'POST',
                    dataType:'json',
                    cache: false,
                    data: new FormData($('#form-login')[0]),
                    processData: false,
                    contentType: false
                    }).done(function(res){
                        if(data.result=='true'){
                            alert('登陆成功');
                        }else{
                            alert('登陆失败');
                        }
                    }).fail(function(res){
                        alert('登陆失败');
                    });
            }catch(e){
                alert(e);
            }
        }
    );
});
```

打开checklogin.php，出现一个链接，点进去，源码里有checklogin.txt，又是代码审计(应该是checklogin.php的源码),内容如下：

```
session_start();
$_SESSION['pwd']=time();
foreach(array_keys($_REQUEST) as $v){
        $key = $v;
        $$key = $_REQUEST[$v]; # 重点在这，可变变量
    }
if (isset ($_POST['password'])) {
    if ($_SESSION['pwd'] == $pwd)
        die('Flag:'.$flag);
    else{
        print '<p>猜测错误.</p>';
        $_SESSION['pwd']=time().time();
    }
}
```

array_keys函数的作用的读取给定数组的键，比如POST发送"password=123456"，在后端就是$_REQUEST['password']='123456'，那么$_key的值就是'password'，"$$key=$_REQUEST[$v]"就是"$password=$REQUEST['password']

同理，POST发送"_SESSION[pwd]=123456"，$_key的值就是"_SESSION[pwd]"，得到$_SESSION[pwd]='123456'

所以最终payload是"_SESSION[pwd]=1&pwd=1&password="

标签: none