New issue

Jump to bottom

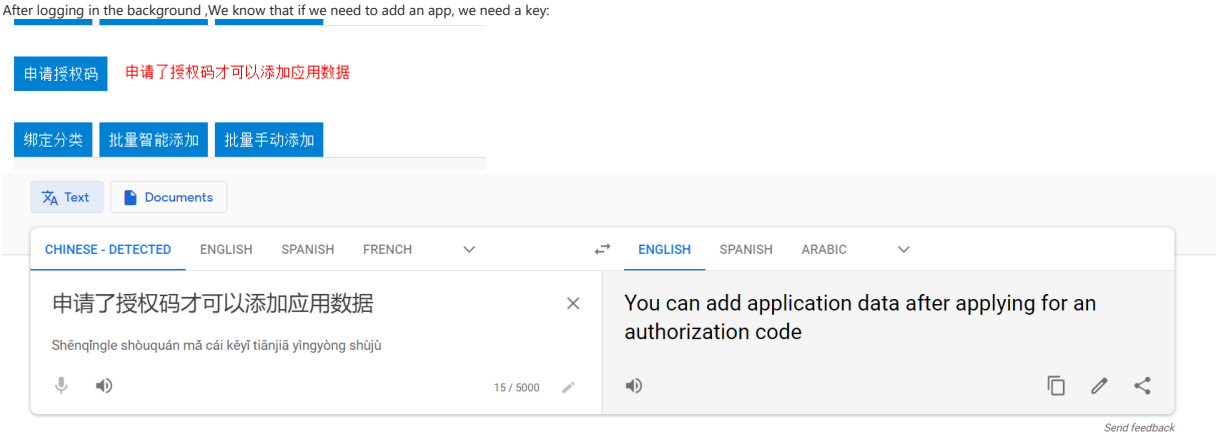
SQL injection vulnerability exists in /admin/download_frame.php(Login required) #2

Open **H9dawn** opened this issue on Dec 18, 2020 · 0 comments

H9dawn commented on Dec 18, 2020

First, the loopholes should be reappeared, and then the reasons should be analyzed :

After logging in the background ,We know that if we need to add an app, we need a key:



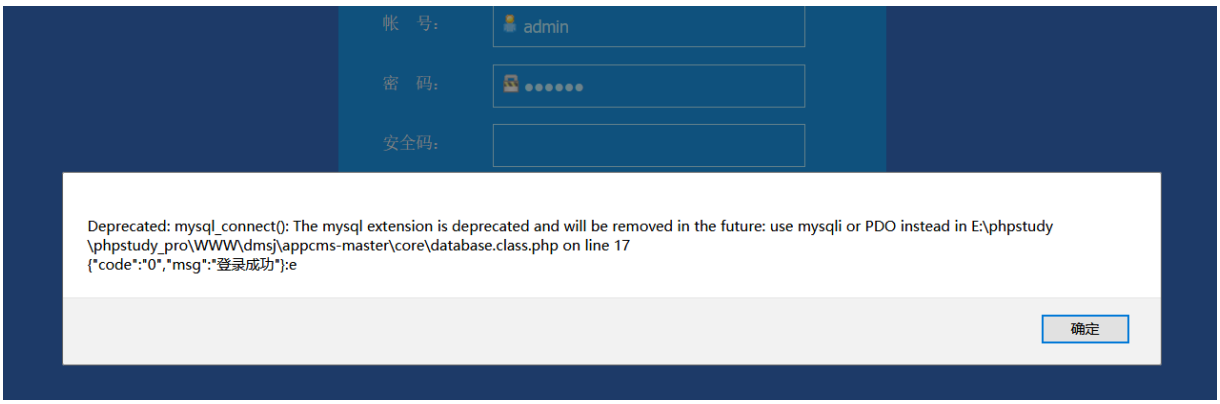
So before testing, I need to create a new table in the database and add data .

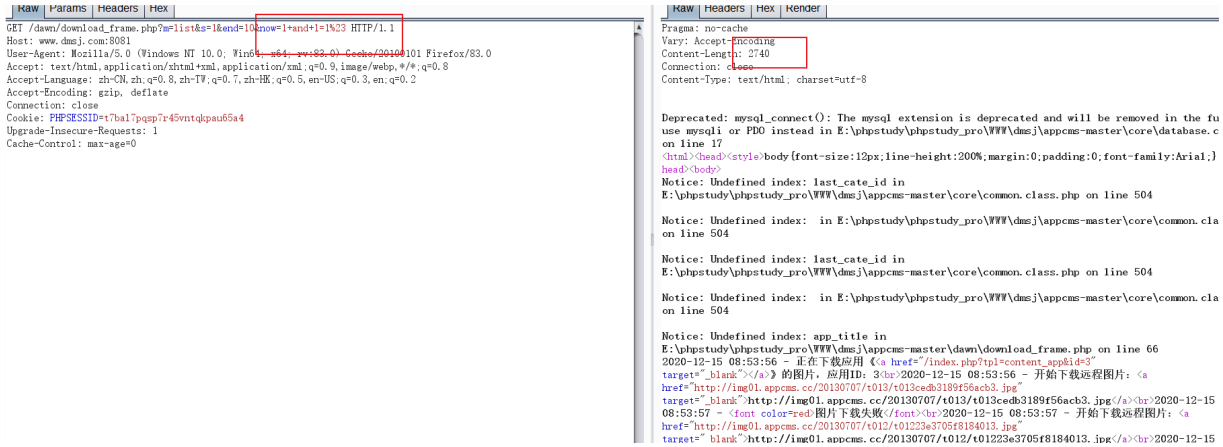
The table name is "app"_ cms_list" , It then contains two pieces of data, as shown in the figure.

Next, we can visit this link to perform blind SQL injection in the "now":("dawn" is the original "admin", but the system needs us to change the background name)

http://www.dmsj.com:8081/dawn/download_frame.php?m=list&s=1&end=10&now=1+and+1=1%23

Pay attention to the use of "+" instead of "space", and unsuccessful words will lead to 302. At the same time, remember to log in to the background.





Little surprise, we also found that its cookie did not change before and after login, but it was in the header, interesting.

Next, we analyze the code :

dawn\download_frame.php

We can control them completely,Then go to "get_ List":

Our "$now" was handed over to "$params['where']"

```
41      global $c, $dbm, $page;
42      //header("Content-type: multipart/x-mixed-replace;boundary=endofsection");
43      $start = isset($_GET['s'])?$_GET['s']:1;
44      $end = isset($_GET['end'])?$_GET['end']:10;
45
46      echo('<html><head>');
47      echo('<style>body{font-size:12px;line-height:200%;margin:0;padding:0;font-family:Arial;}</style>');
48      echo('</head><body>');
49
50      if(!is_numeric($start)) die('<font color=red>开始ID必须是数字</font>');
51      if(!is_numeric($end)) die('<font color=red>结束ID必须是数字</font>');
52      if(intval($start)>intval($end)) die('<font color=red>开始ID必须小于结束ID</font>');
53
54      $params['type'] = 0; //0表示取应用列表
55      $params['resource'] = 1;
56      $params['count'] = 0 ; //计算总数
57      $params['pagesize'] = 2;
58      $now = isset($_GET['now'])?$_GET['now']:$start;
59      if ($now > $end) die('<font color=green><b>全部下载完毕！</b></font>');
60      $params['where'] = " app_id >=" . $now . " ";
61      $params['order'] = " order by app_id asc";
62      $apps = $c -> get_list($params, no_cache: 1);
63
64      if (count($apps['list']) == 0) die('<font color=red>没有需要下载图片的应用</font>');
65      if (count($apps['list']) > 0) {
66          helper::print_state( str: '正在下载应用《<a href="'.$apps['list'][0]['surl'].'" target="_blank">'.$apps
67          // 下载缩略图
```

core\common.class.php

```php
public function get_list($params, $no_cache = 0)
{
    $type = isset($params['type']) ? $params['type'] : 0;
    if ($type == 0) {
        $tbname = 'app';
    } else {
        $tbname = 'info';
    }
    $cate_id = isset($params['cate_id']) ? $params['cate_id'] : '';
    $where = isset($params['where']) ? $params['where'] : '';
    $order = isset($params['order']) ? $params['order'] : ' order by ' . $tbname . '_update_time desc
    $pagesize = isset($params['pagesize']) ? $params['pagesize'] : PAGESIZE;
    $p = isset($params['p']) ? $params['p'] : 1;
    $count = isset($params['count']) ? $params['count'] : 0;
    $rewrite = isset($params['rewrite']) ? $params['rewrite'] : 2;
    $resource = isset($params['resource']) ? $params['resource'] : 0;
    $history = isset($params['history']) ? $params['history'] : 0;
    $fields = isset($params['fields']) ? $params['fields'] : '';
    $node = isset($_GET['tpl']) ? $_GET['tpl'] : 'index';
    $strip_tags_desc = isset($params['strip_tags_desc']) ? $params['strip_tags_desc'] : 1;
    if (isset($_GET['cpy'])) $node = 'cpy_' . $node;

    if ($fields == '') {
```

In any case, our $where is not filtered and goes directly into the SQL statement :

```php
        // 分类ID为空，或者为终极分类，无需联表查询
        if ($cate_id == '' || (isset($this->categories[$cate_id]) && $this->categories[$cate_id]['son'] == 0)
            if ($cate_id == '') { // 分类ID为空
                $sql = "select $fields from " . TB_PREFIX . $tbname . "_list as b";
                if (strlen($where) > 0) {
                    $sql .= " where $where";
                }
                if ($count == 1) $count = 1;
            } else { // 分类ID不为空
                $sql = "select $fields from " . TB_PREFIX . $tbname . "_list as b  where last_cate_id=$cate_
                if (strlen($where) > 0) {
                    $sql .= " and $where";
                    if ($count == 1) $count = 1;
                } else {
                    $total = $this->categories[$cate_id]['cdata'];
                    $count = 0;
                }
            }
        } else { // 分类ID不为空,也不是终极分类
            $order = preg_replace( pattern: '~' . $tbname . '_~', replacement: 'id_', $order);
            $user_index = ''; //echo($order);
            if (strpos($order, needle: 'id_update_time') > 0 && strpos($order, needle: 'id_order') <= 0) $user_
            if (strpos($order, needle: 'id_down') > 0 && strpos($order, needle: 'id_order') <= 0) $user_index =
            $sql = "select * from " . TB_PREFIX . "cate_relation as a $user_index left join " . TB_PREFIX . $
            if (strlen($where) > 0) {
                $sql .= " and $where";
                if ($count == 1) $count = 1;
            } else {
                $total = $this->categories[$cate_id]['cdata'];
```

common › get_list()

We follow the "query":

```php
                }
            } else {
                $result = $this->dbm->query($sql, $suffix, $count);
            }
        } else {
            $result = $this->dbm->query($sql, $suffix, $count);
        }
        // print_r($result['sql']);echo('<br>');print_r($result['sql_time']);
```

core\database.class.php

```
46          }
47          #var_dump($sql . ' ' . $suffix);
48          // 查询取得记录列表
49          $rs = mysql_query( query: $sql . ' ' . $suffix);
50          $this -> query_count++;
51          $i = 0;
52          $list = array();
53          if ($rs) {
54              while ($rows = mysql_fetch_assoc($rs)) {
55                  $list[$i] = $rows;
56                  $i++;
57              }
58          }
59          // 返回该查询的记录总数和记录列表
```

nice!

H9dawn changed the title ~~SQL injection vulnerability exists in /dawn/download_frame.php(Login required)~~ SQL injection vulnerability exists in /admin/download_frame.php(Login required) on Dec 18, 2020

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant