开发规范

后台管理入口

后台管理入口，将admin.php修改成自定义字符.php

请求参数过滤

1、全局配置 D:\www\webroot\demo\www\fastadminDemo\application\config.php

```
//默认全局过滤方法 用逗号分隔多个
'default_filter'         => 'trim,strip_tags,htmlspecialchars',
```

或

2、控制器中增加

```
 //移除HTML标签
 $this->request->filter('trim,strip_tags,htmlspecialchars');
```

目录安全

我们建议在生产环境只开放uploads和runtime目录的读写权限，其次还需要关闭uploads目录执行PHP的权限，因为很多时候用户上传恶意脚本，而服务端uploads目录又未屏蔽PHP□导致用户数据泄漏丢失。

通常情况在生产环境下建议使用

```
chown www:www /var/www/yoursite -R
chmod 555 /var/www/yoursite -R
chmod u+w /var/www/yoursite/runtime -R
chmod u+w /var/www/yoursite/public/uploads -R
```

通过以上的配置还不够，我们还需要继续对服务器做WEB配置以限制PHP脚本的运行

SQL

1、非必要，不推荐直接编写原生SQL语句

```
//若使用原生SQL语句，请做参数预处理
$username = $this->request->request("username", "");
$username = htmlspecialchars($username, ENT_QUOTES);
\think\Db::query("SELECT * FROM fa_user WHERE username=:username",
['username'=>$username]);
```

2、推荐使用模型进行操作

```
//如
\app\common\model\User::where('username', $username)->find();
```