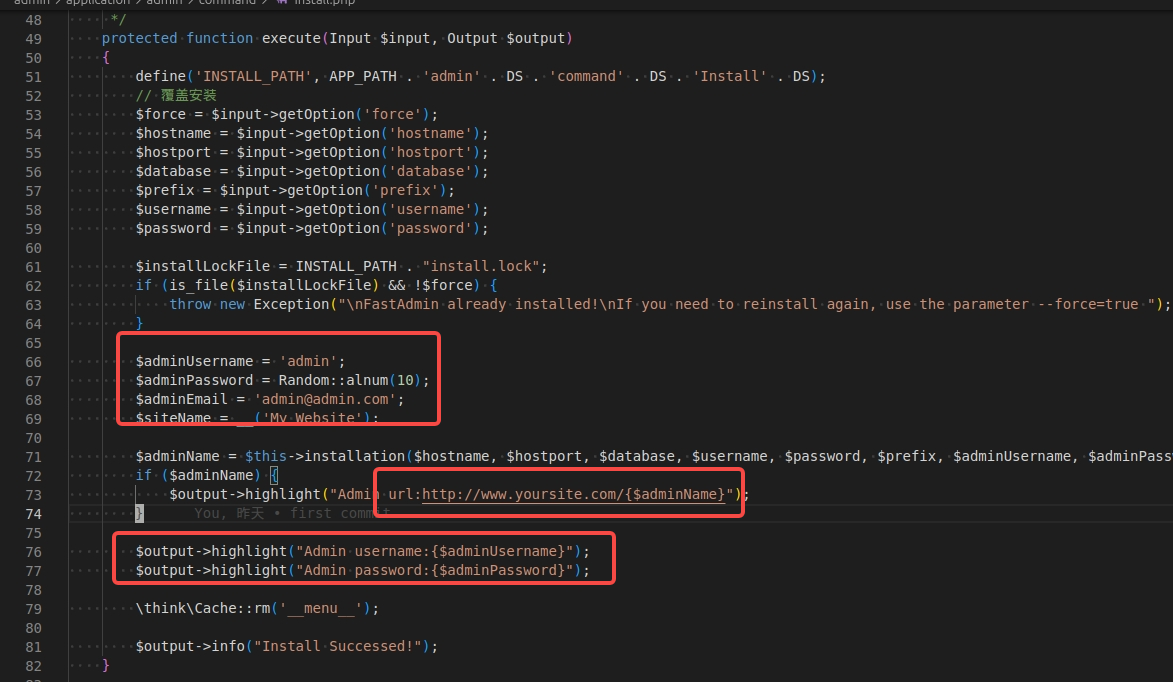
## 问题1： 账户名和密码

代码路径：admin/application/admin/command/Install.php

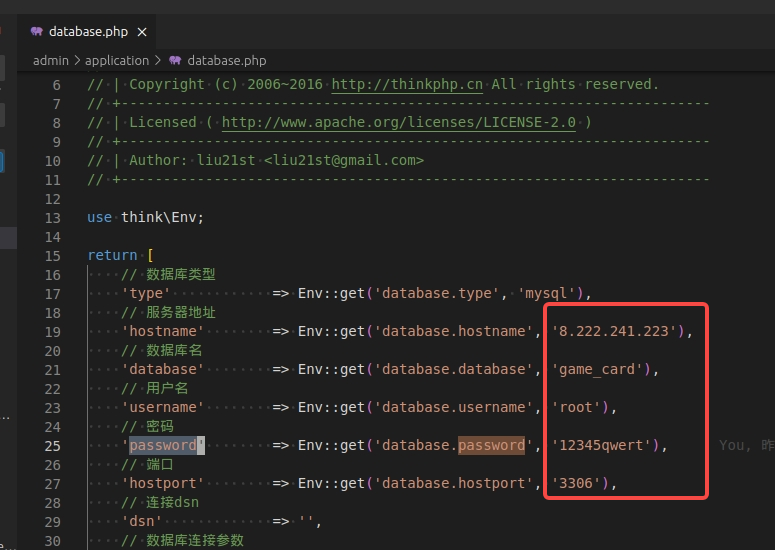


修改建议:

* 密码应该从环境变量中读取，不能打印到log或控制台
* 密码应该包含特殊符号，使用更长的密码，防止暴力破解
* 账户名不要用admin， admin太过于常见
* 管理台的链接，避免使用 xxxxx/admin这样普遍的url路径, 因为很容易被扫描和暴力破解

## 问题2： 默认数据库密码，存在密码泄漏风险

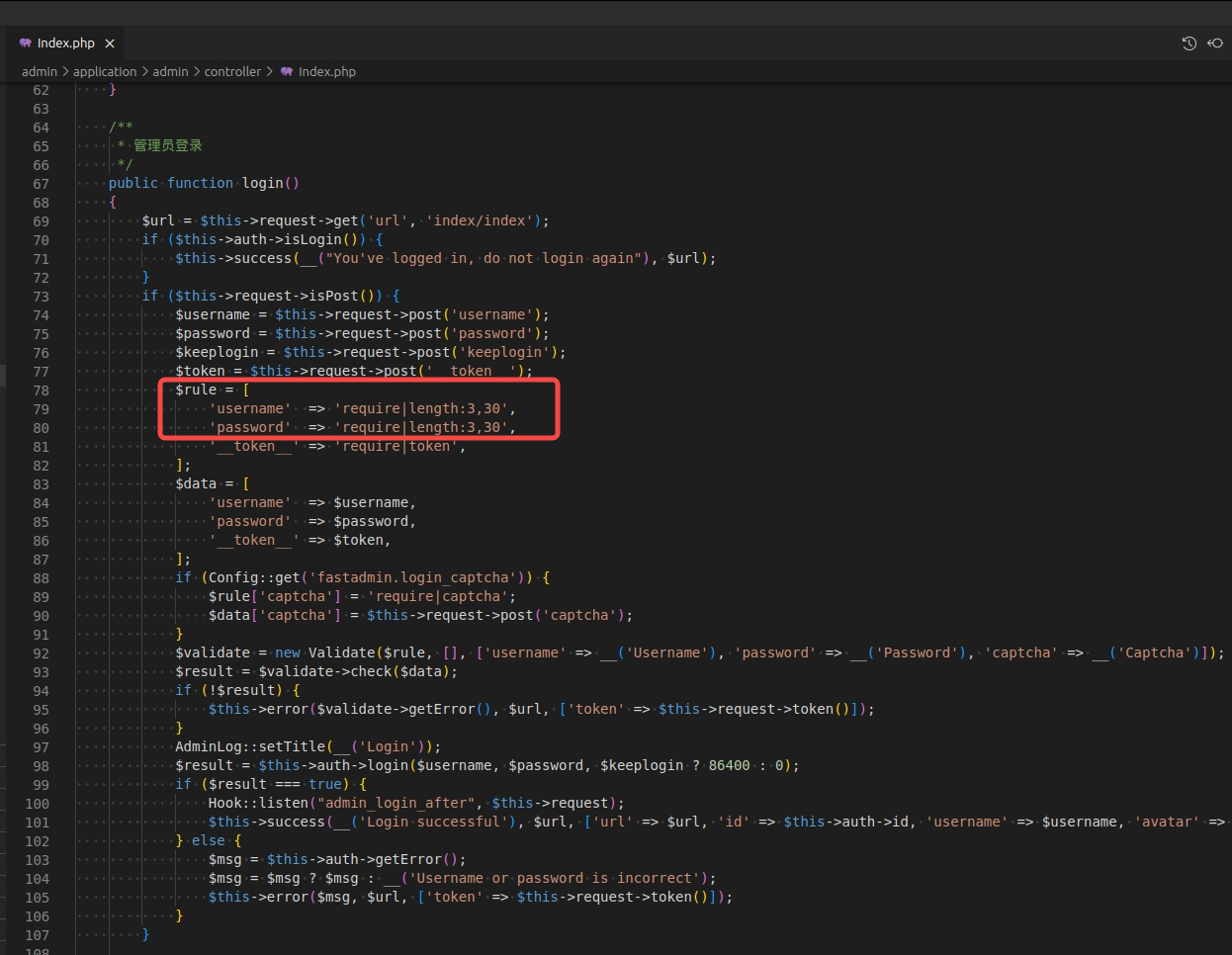
代码路径：admin/application/database.php



修改建议：

* 将缺省的默认值统一设置为**空字符串**，如果环境环境变量中没有设置相应变量，会引发应用程序报错。必须**强制**设置环境变量
* 数据库服务器应该采用ip白名单,禁止非白名单的ip进行连接
* 随机生成复杂的数据库密码，不要使用弱密码

## 问题3： 密码验证

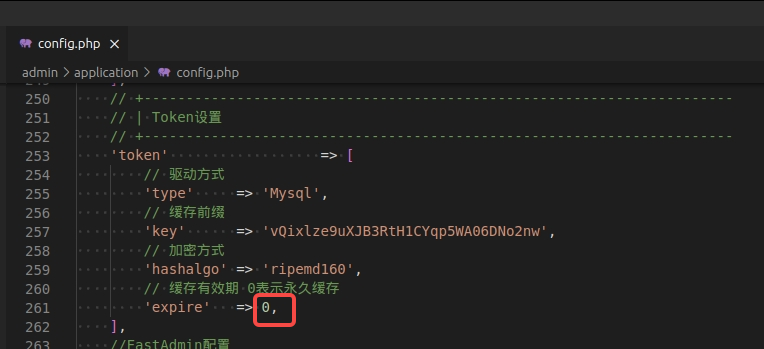


修改建议：

应该与其他地方保持统一，长度6～30

## 问题4： token无限有效期

代码路径：admin/application/config.php

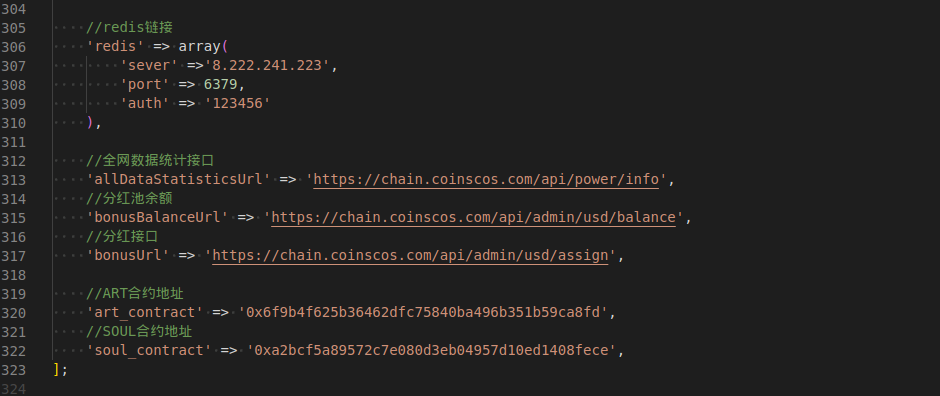


修改建议：

应该设置有限的token有效期

## 问题5： redis密码

代码路径：admin/application/config.php

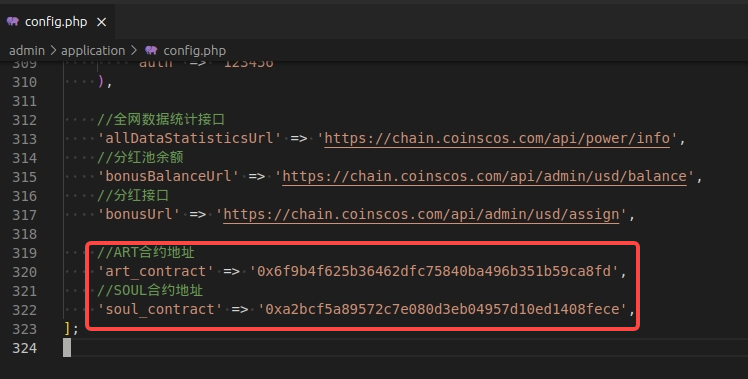


修改建议：

从环境变量中读取redis ip 和 redis密码

redis密码应该随机生成，禁止使用弱密码

## 问题6： （**BUG**）硬编码测试链的代币合约地址



修改建议：

应该根据环境，设置测试环境或生产环境的合约地址。