代码安全审计报告

共发现 4 个安全问题

database.php:7

使用不安全的加密算法 (HIGH)

代码中使用了mcrypt扩展，该扩展自PHP 7.1.0起已被弃用，并在PHP 7.2.0中移除。使用已弃用的加密库可能导致安全风险，因为已知存在漏洞且不再维护。

修复建议：建议改用OpenSSL扩展，并选择现代加密算法如AES-256-CBC，确保使用安全的密钥和IV生成方法。

database.php:4

硬编码密钥和IV不安全 (HIGH)

代码中直接硬编码了加密密钥'PanGuShi'，且IV生成方式不安全（使用SHA1哈希截取前16字节）。硬编码密钥易泄露，IV生成缺乏随机性，降低加密强度。

修复建议：应使用安全的随机数生成器生成密钥和IV，并将密钥存储在安全配置文件中，避免硬编码。例如，使用openssl_random_pseudo_bytes生成IV。

database.php:11

缺少填充验证 (MEDIUM)

解密后的数据使用trim()函数去除空白字符，但未正确验证和处理加密填充，可能导致填充Oracle攻击或数据截断问题。

修复建议：应在解密后显式验证并移除PKCS7填充，使用如OpenSSL的openssl_decrypt函数自动处理填充，避免手动处理错误。

database.php:6

弱加密模式使用 (HIGH)

代码使用CBC模式但未结合消息认证码（MAC），无法保证密文的完整性，易受到篡改攻击。

修复建议：采用经过验证的加密模式如AES-GCM，或在使用CBC模式时结合HMAC进行完整性验证。