


斑马网络外包供应商云端 应用安全开发部署管理规范

版本 1.0

斑马网络版权所有



修 订 历 史

版本号	修订日期	修订者	修订内容
V1.0	2018-12-13	陈胜楠	初始草稿

1. 前言	4
1.1 背景	4
1.2 适用范围	4
2. 应用安全编码规范	4
2.1 前端应用安全编码规范	4
2.1.1 HTML 页面渲染	4
2.1.2 Form 表单提交	4
2.1.3 AJAX 接口	4
2.1.4 JSONP 接口	5
2.1.5 CORS 跨域	5
2.1.6 URL 重定向	5
2.2 服务端应用安全编码规范	5
2.2.1 文件上传	5
2.2.2 执行系统命令	6
2.2.3 HTTP Header 读写	6
2.2.4 SQL 编写	6
2.2.5 服务器处理 XML 文件	6
2.2.6 服务器解析序列化数据	6
3. 业务流程安全规范	7
3.1 账号相关业务安全规范	7
3.1.1 登录注册	7
3.1.2 权限设计	7

3.2	短信、邮件、电话等外呼接口业务安全规范	7
3.2.1	频率限制	7
4.	部署环境安全基本要求	8
4.1	PHP 环境安全基本要求	8
4.1.1	PHP 版本控制要求	8
4.1.2	PHP 参数安全要求	8
4.2	Apache 环境安全基本要求	8
4.2.1	Apache 安全配置参数要求	8
4.3	Tomcat 环境安全基本要求	9
4.3.1	删除默认管理后台页面	9

1. 前言

1.1 背景

为保护斑马互联网汽车相关平台应用的运行安全，特参考业界安全编码相关规范与最佳实践制定本规范内容，旨在针对可能导致安全漏洞或风险的常见场景，规范应用在开发、部署过程中需要遵循的安全基线，以减少各项基本常见安全问题的发生。

1.2 适用范围

本规范适用范围包括但不限于斑马网络技术有限公司与外部供应商合作开发的平台应用、外部供应商独立提供的平台应用等云端应用的安全管理。

2. 应用安全编码规范

2.1 前端应用安全编码规范

2.1.1 HTML 页面渲染

- **【强制】** 禁止向 HTML 页面输出未经安全过滤或未正确转义的外部输入数据
- **【推荐】** 建议使用 `xssfilter`、`htmlencode` 等方式 对外部输入数据进行过滤和转码

2.1.2 Form 表单提交

- **【强制】** Form 表单提交必须使用 CSRF Token 并执行过滤
- **【强制】** 涉及用户数据后台修改的接口必须使用 CSRF Token 并执行过滤

2.1.3 AJAX 接口

- **【强制】** 统一使用 POST 方式提交 AJAX 请求，禁止 GET 请求
- **【强制】** 如果涉及对后端数据的增删改，则必须在后端通过框架配置或单独验证的方式进行 CSRF 验证
- **【强制】** AJAX 接口返回头必须正确设置 Content-Type

- 【强制】AJAX 接口输出 JSON 字符串禁止通过字符串拼接构造，且输出的 JSON 需要经过安全过滤
- 【强制】JSONP 接口必须对 REFERER 进行白名单校验
- 【强制】如果涉及对后端数据的增删改，则必须在后端通过框架配置或单独验证的方式进行 CSRF 验证

2.1.4 JSONP 接口

- 【强制】JSONP 接口 Callback 必须验证有效性
- 【强制】JSONP 接口返回头必须 JSONP 接口返回头必须正确设置 Content-Type
- 【强制】JSONP 接口输出 JSON 字符串禁止通过字符串拼接构造，且输出的 JSON 需要经过安全过滤
- 【强制】JSONP 接口返回内容首行必须为空行或者注释

2.1.5 CORS 跨域

- 【强制】支持 CORS 跨域的接口，返回头 Access-Control-Allow-Origin 必须使用白名单验证，禁止直接返回

2.1.6 URL 重定向

- 【强制】URL 外部重定向的目标地址必须执行白名单过滤

2.2 服务端应用安全编码规范

2.2.1 文件上传

- 【强制】禁止将外部上传文件存储到本地。如果有存储需求，则使用 OSS 进行存储。
- 【强制】禁止从服务器本地读取文件传输到外部。
- 【强制】如必须读取，则需要对传入的路径用安全包函数做安全过滤

- **【强制】**如果上传的文件为图片，需要对其进行内容校验

2.2.2 执行系统命令

- **【强制】**尽量避免执行系统命令。如果应用必须通过系统命令获取信息，则务必不要通过外部输入获取命令。通过外部输入获取命令参数时，需要使用安全函数对其进行包装。

2.2.3 HTTP Header 读写

- **【强制】**禁止直接读取、使用 HTTP Header(X-Forwarded-For)头中的 IP 地址
- **【强制】**服务器向响应 HTTP Header 写入用户输入数据时必须做 CRLF 过滤或者转义

2.2.4 SQL 编写

- **【强制】**编写的 SQL 必须预编译，不允许通过字符串拼接的方式合成
- **【强制】**部分特殊场景，必须通过拼接合成，则拼接的变量必须经过处理，只允许[a-zA-Z0-9_-.]+字符

2.2.5 服务器处理 XML 文件

- **【强制】**服务器处理外部传输的 XML 时，请务必禁止 DOCTYPE 解析。

2.2.6 服务器解析序列化数据

- **【推荐】**请尽量避免使用序列化功能。特别是使用语言自身的序列化功能，或对象序列化功能
- **【推荐】**如果一定要使用序列化功能完成业务需求，优先考虑 JSON 序列化
- **【强制】**如果序列化数据中包含敏感数据，则序列化后，需要对其进行对称加密后，再进行传输使用
- **【强制】**如未使用加密，则需要使用 HMAC(input)+SERIALIZE(INPUT)的方式存储数据，

3. 业务流程安全规范

3.1 账号相关业务安全规范

3.1.1 登录注册

- 【强制】注册页面有验证码，登录失败 3 次后，需要出现验证码。
- 【推荐】登录页面使用安全控件
- 【强制】登录过程使用 https 安全通道。
- 【强制】检查登录成功后跳转的 URL，是否在白名单内。

3.1.2 权限设计

- 【强制】明确用户身份的操作权限，客户端中有标志用户权限的 cookie 选项需做加密处理或者把权限控制放在服务端
- 【强制】垂直权限控制：数据权限做严格分级，用户只能访问自己具有相应权限的数据，防止用户越权
- 【强制】水平权限控制：对数据的访问加拥有者判断，用户只能访问自己拥有授权的数据，防止用户访问到和自己同等权限的其他用户数据

3.2 短信、邮件、电话等外呼接口业务安全规范

3.2.1 频率限制

- 【推荐】必须做疲劳度控制。单用户，通常一分钟限制 5 次以内，一天限制 15 次以内。
- 【推荐】超出限制部分，在超出额定 200%范围内，采用验证码进行校验；超出 200%后，统一拒绝服务。
- 【强制】短信验证码长度至少 6 位。

4. 部署环境安全基本要求

4.1 PHP 环境安全基本要求

4.1.1 PHP 版本控制要求

- 【强制】必须使用已修复历史安全漏洞的最新 PHP 相关版本

4.1.2 PHP 参数安全要求

- 【强制】安全模式必须开启

```
safe_mode = on  
safe_mode_gid = off
```

- 【强制】禁止部分高危参数

```
disable_functions=exec,passthru,popen,proc_open,shell_exec,system  
,phpinfo,assert  
expose_php = Off
```

- 【强制】php.ini 的文件权限安全设置，只允许 root、admin 进行修改，其他用户不应该有权限修改

4.2 Apache 环境安全基本要求

4.2.1 Apache 安全配置参数要求

- 【强制】Apache 禁止配置为 HTTP 正向代理

```
ProxyRequests Off
```

- 【强制】目录禁止配置为可浏览、关闭服务端 SSI 包含

```
Options -Indexes -Includes
```

- 【强制】配置覆盖控制

AllowOverride None

- **【强制】**配置 Apache 不回显版本、关闭错误回显

ServerSignature Off

ServerTokens ProductOnly

- **【推荐】**对错误页面（如：404、500、501、502、503 等）进行定制，避免暴露系统、应用的相关信息

4.3 Tomcat 环境安全基本要求

4.3.1 删除默认管理后台页面

- **【强制】**删除 Tomcat 安装目录\webapps 下 manager 目录