**知与教育详细设计文档**

目录

[1 目录 1](#_Toc8811006)

[2 Java技术架构 2](#_Toc8811007)

[3 移动端 3](#_Toc8811008)

[3.1 Android 3](#_Toc8811009)

[3.2 IOS 3](#_Toc8811010)

[4 信息安全策略 3](#_Toc8811011)

[4.1 数据安全 3](#_Toc8811012)

[4.2 运营安全 3](#_Toc8811013)

[4.2.1 安全监控 3](#_Toc8811014)

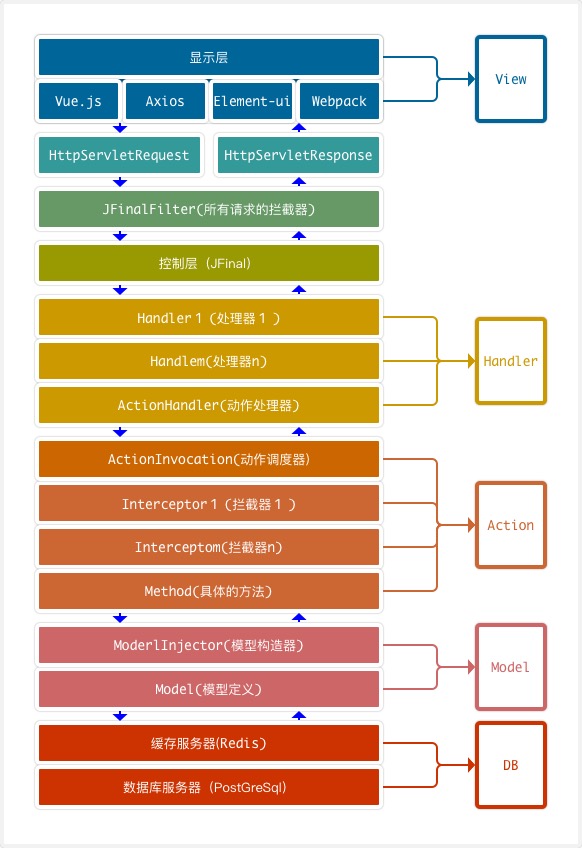
[4.2.2 入侵检测 3](#_Toc8811015)

[4.2.3 弱点分析 3](#_Toc8811016)

[4.2.4 日志分析 4](#_Toc8811017)

[5 服务器配置 4](#_Toc8811018)

# Java技术架构



# 移动端

## Android

## IOS

# 信息安全策略

主要集中使用了：密码学、安全协议、信息隐蔽、安全基础设施、系统安全、网络安全六个方面，

主要应用技术包括加密技术、身份认证、访问控制、防火墙技术、系统入侵检测技术、数据库安全等多门安全防护技术。

信息安全技术的核心是保护敏感信息不被非法窃取、更改、删除或破坏。

## 数据安全

第三方篡改

意思是说在数据由用户发到服务器的途中，数据被第三方篡改，造成发送的数据和接收的数据不一致，防止此类情况的发生的常用做法如下：

1）将要提交的参数先做加密

2）然后把加密的信息做一次md5摘要，也就是签名

3）然后把摘要连同参数一起回传给服务器

4）服务器拿到参数后，同样的方式加密做md5摘要

5）两个摘要做对比，如果不相等参数便是被篡改了，否则可信。

数据库单例访问

数据库运行访问应用进行IP绑定，只允许制定IP可以访问

## 运营安全

### 安全监控

最快到秒级响应的安全监控能力

同时整合了网络和主机端的关联分析来减少误报。解决了企业安全人士最为头疼的问题之一

全面包含企业漏洞监控、开放端口监控、黑客入侵监控、web攻击监控、DDoS攻击监控、威胁情报监控、企业安全舆情监控等。

### 入侵检测

webshell检测，恶意病毒识别，准确且低误报。

识别可能的入侵行为，从流量特征、主机行为、主机操作日志中获取关联信息，再通过进一步建模分析，从而做到99.99%准确的入侵检测。

通过海量数据，对那些能够引发网络安全态势发生变化的要素进行全面、快速和准确地捕获和分析。

### 弱点分析

支持web漏洞，主机漏洞，配置隐患，弱口令检测

扫描SQL注入、XSS等各种web漏洞和第三方开源程序漏洞，并对主机ECS漏洞，甚至是配置项漏洞也能做到实时监控和发现。

可对漏洞进行实时回扫，提升漏洞修复周期和漏洞解决时间。

### 日志分析

相当于拥有了自己的大数据分析平台，可导入更多日志数据，并进行关联分析。

PB级的数据存储和分析能力，在DT时代用更智能的方法做安全。

通过分析网络日志数据来侦测正在进行的攻击，并自动进行事件响应，识别关键的异常行为。

# 服务器配置

# 数据库设计