web应用安全性分析

在开发的应用中，我们在三个方面为安全性提供了策略，分别是登陆验证，防止目录遍历以及注入式SQL攻击。

1. 登陆验证：

Web应用使用来自HTTP请求的输入来决定如何进行响应，攻击者可以篡改HTTP请求的任何部分，管理者和开发人员往往希望通过过滤恶意输入来保护自己，但是Web页面中存在多种信息编码方法且容易被绕过，因此必须使用服务器端的检查来对付参数篡改。我们采用登陆检查对用户进行验证，对其进行授权。

1. 防止目录遍历：

通过对任意目录添加“../”或者在有意义的目录附加“../”或者是“../”的一些变形都可能导致目录遍历。我们的开发的系统可以拒绝接受这种目录遍历访问。

1. 防止注入式SQL攻击：

注入式攻击包括对操作系统的调用，使用shell命令来调用外部程序以及通过SQL注入来调用后台程序。当Web应用将HTTP请求中的信息作为外部信息的一部分传送时，它必须被仔细检查。我们对一些必须使用的外部调用的输入数据进行了验证，保证不含任何恶意内容。