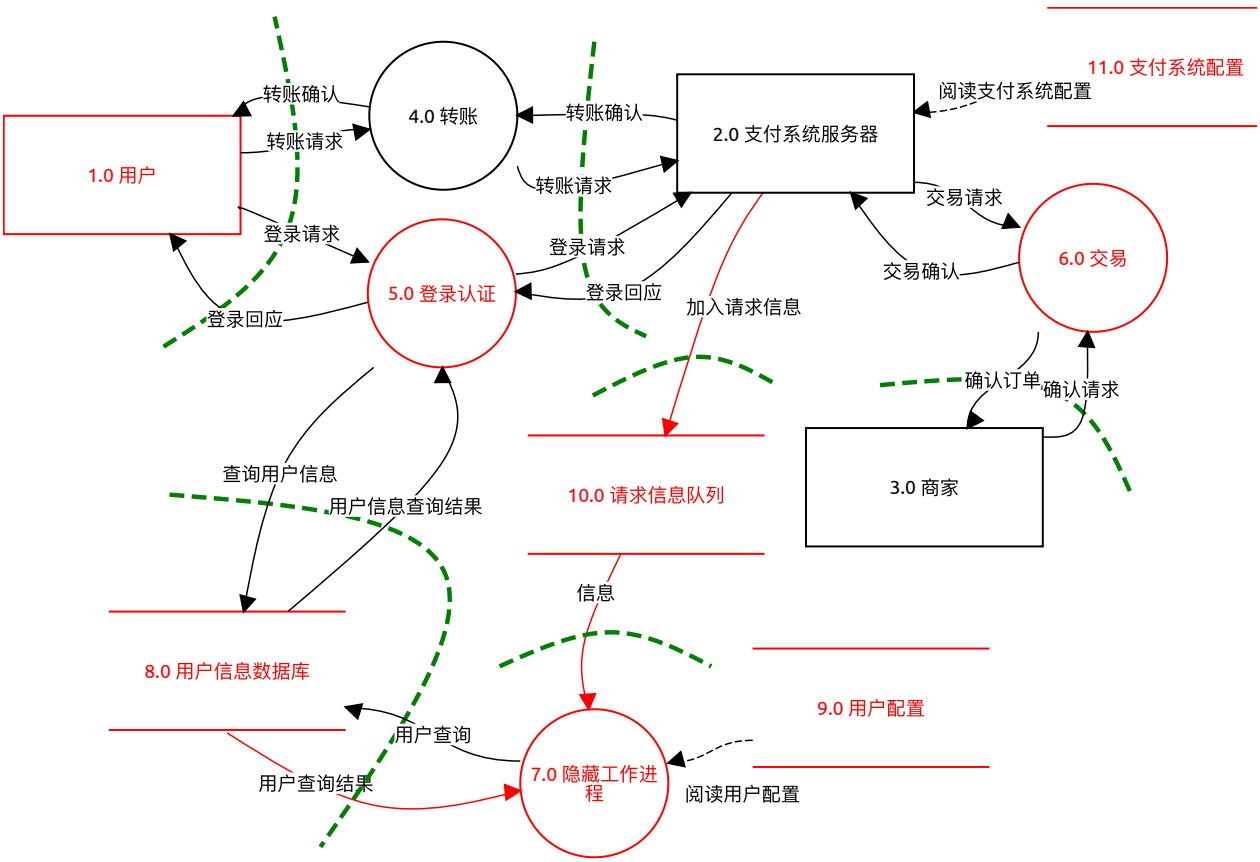
Threat model report for Threat Model

Owner:
Lyy
Reviewer:
Contributors:

High level system description

A sample model of a web application, online payment.

支付数据流图



9.0 用户配置 (Data Store)

Description:

非法访问数据库凭证

Information disclosure, Open, High Severity

Description:
后台工作人员配置并存储工作人员访问数据库所使用的凭据，攻击者可以攻击后台工作人员并访问数据库凭据

Mitigation:
· 在配置文件中加密数据库凭据。
· 定期过期并替换数据库凭据。

8.0 用户信息数据库 (Data Store)

Description:

攻击者可以通过执行SQL注入获得对用户信息的访问权

Information disclosure, Open, High Severity

Description:
SQL注入是一种攻击，它将恶意代码插入到字符串中，然后传递给SQL Server实例进行解析和执行。SQL注入的主要形式是将代码直接插入到用户输入变量中，这些变量与SQL命令连接并执行。不那么直接的攻击则将恶意代码注入到存储在表中或作为元数据的字符串中。当存储的字符串随后连接到一个动态SQL命令时，将执行恶意代码。

Mitigation:
要求所有查询都经过身份验证，确保在SQL Server上启用了登录审核。

11.0 支付系统配置 (Data Store)

Description:

非法访问系统配置凭证

Information disclosure, Open, High Severity

Description:
Web应用程序配置存储Web应用程序用于访问消息队列的凭据，它们可能被攻击者窃取，用于读取机密数据或在队列上放置有害消息

Mitigation:
应该对支付系统消息队列凭据进行加密

10.0 请求信息队列 (Data Store)

Description:

读取请求信息

Information disclosure, Open, Low Severity

Description:
Web应用程序和后台管理员之间的数据流不是点对点的，因此在传输层不能提供端到端保密。消息可以被攻击者在消息队列中读取。

Mitigation:
对消息中的高敏感性数据(例如安全令牌)使用消息级加密

攻击者篡改请求信息

Tampering, Open, Medium Severity

Description:
队列上的消息可能会被篡改，从而导致后台工作人员进行不正确的处理

Mitigation:
· 对Web服务器上的所有队列消息添加数字签名。在后台工作人员验证消息签名并拒绝任何缺少或无效签名的消息。
· 记录任何失败的消息。

攻击者可能放置假消息在队列中

Tampering, Mitigated, High Severity

Description:
攻击者可能会在队列中放置假消息，导致后台工作人员进行不正确的处理

Mitigation:
· 将对队列的访问限制为Web服务器和后台工作人员的IP地址
· 在队列端点上实现身份验证

攻击者破坏请求信息

Tampering, Open, Medium Severity

Description:
攻击者可能利用缺乏入侵检测和异常数据库活动的阻止，破坏用户的请求信息，使用户无法与服务器交互

Mitigation:
· 启用威胁检测
· 配置防火墙

7.0 隐藏工作进 程 (Process)

Description:

恶意消息

Denial of service, Open, Medium Severity

Description:
攻击者可能生成后台工作程序无法处理的恶意消息

Mitigation:
实现一个恶意消息队列，其中的消息在经过固定次数的重试后放置

大量访问数据

Denial of service, Open, Medium Severity

Description:
攻击者可能生成大量访问数据，使应用程序拒绝服务

Mitigation:
· 在处理之前验证所有消息的内容
· 拒绝任何含有无效内容的邮件，并记录拒绝记录
· 不要记录恶意内容，而是记录错误的描述

5.0 登录认证 (Process)

Description:

由于松散的授权规则，攻击者可能获得对数据库的未授权访问

Elevation of privilege, Open, Medium Severity

Description:
数据库应该确保使用最低特权帐户或了解原则的较高权限连接到数据库服务器

Mitigation:
确保使用特权最少的帐户连接到数据库服务器

由于缺乏网络访问保护，攻击者可能获得对数据库的未经授权的访问

Elevation of privilege, Open, Medium Severity

Description:
如果在网络或主机防火墙级别上没有访问数据库的限制，那么任何人都可以尝试从未授权的位置连接到数据库

Mitigation:
为数据库引擎访问配置Windows防火墙，限制只有后台管理员可以访问

1.0 用户 (External Actor)

Description:

攻击者欺骗计算机执行用户请求
Spoofing, Open, High Severity

Description:
攻击者进行非法访问，使用另一用户的身份登录支付页面；或破坏服务器，使恶意服务器冒充有效服务器

Mitigation:
· 考虑使用标准身份验证机制向支付网页进行身份验证
· 网页必须安全处理失败的身份验证方案
· 启用升级或自适应的身份验证
· 确保适当锁定管理界面
· 安全实施忘记密码功能
· 确保实施密码和帐户策略
· 实施控制来防止用户名枚举

由于缺乏审计，攻击者可能否认对数据库的操作
Repudiation, Open, Medium Severity

Description:
正确地记录所有安全事件和用户操作，在系统中构建可跟踪性，并否认任何可能的否认问题。如果没有适当的审计和日志控制，就不可能在系统中实现任何责任。

Mitigation:
确保在SQL Server上启用了登录审核。

加入请求信息 (Data Flow)

Description:

数据流应使用HTTP/S
Information disclosure, Open, High Severity

Description:
这些请求是通过公共Internet发出的，攻击者可能会拦截这些请求

Mitigation:
请求应该需要HTTP/S，这将提供机密性和完整性。HTTP不应该被支持

信息 (Data Flow)

Description:

数据流应该使用 HTTP/S

Information disclosure, Open, High Severity

Description:
信息是通过公共网络发出的，攻击者可能会拦截这些请求

Mitigation:
信息传递应该需要HTTP/S。这将提供机密性和完整性。HTTP不应该被支持

用户查询结果 (Data Flow)

Description:

中间人攻击

Information disclosure, Open, Low Severity

Description:
攻击者可以在传输过程中拦截数据库查询并获取敏感信息，如数据库凭证、查询参数或查询结果（可能性较低，因为数据流是通过私有网络进行的）

Mitigation:
在数据库服务器上执行加密连接，使用SSL/TLS保护与事件中心的加密

查询用户信息 (Data Flow)

Description:

No threats listed.

用户信息查询结果 (Data Flow)

Description:

No threats listed.

用户查询 (Data Flow)

Description:

No threats listed.

4.0 转账 (Process)

Description:

No threats listed.

转账请求 (Data Flow)

Description:

No threats listed.

转账确认 (Data Flow)

Description:

No threats listed.

登录请求 (Data Flow)

Description:

No threats listed.

登录回应 (Data Flow)

Description:

No threats listed.

2.0 支付系统服务器 (External Actor)

Description:

No threats listed.

登录请求 (Data Flow)

Description:

No threats listed.

转账请求 (Data Flow)

Description:

No threats listed.

转账确认 (Data Flow)

Description:

No threats listed.

登录回应 (Data Flow)

Description:

No threats listed.

3.0 商家 (External Actor)

Description:

No threats listed.

6.0 交易 (Process)

Description:

商家否认已支付

Repudiation, Open, Medium Severity

Description:
由于缺乏审计，商家否认用户已支付账单

Mitigation:
· 正确地记录所有安全事件和用户操作，在系统中构建可跟踪性，并否认任何可能的否认问题。
· 使用数字签名确保信息真实性的有效证明
· 使用时间戳记录支付时间，确保不可抵赖

交易请求 (Data Flow)

Description:

No threats listed.

交易确认 (Data Flow)

Description:

No threats listed.

确认订单 (Data Flow)

Description:

No threats listed.

确认请求 (Data Flow)

Description:

No threats listed.

阅读支付系统配置 (out of scope Data Flow)

Description:

Out of scope reason:
This data flow represents a read from the file system

阅读用户配置 (out of scope Data Flow)

Description:

Out of scope reason:
This data flow represents a read from the file system