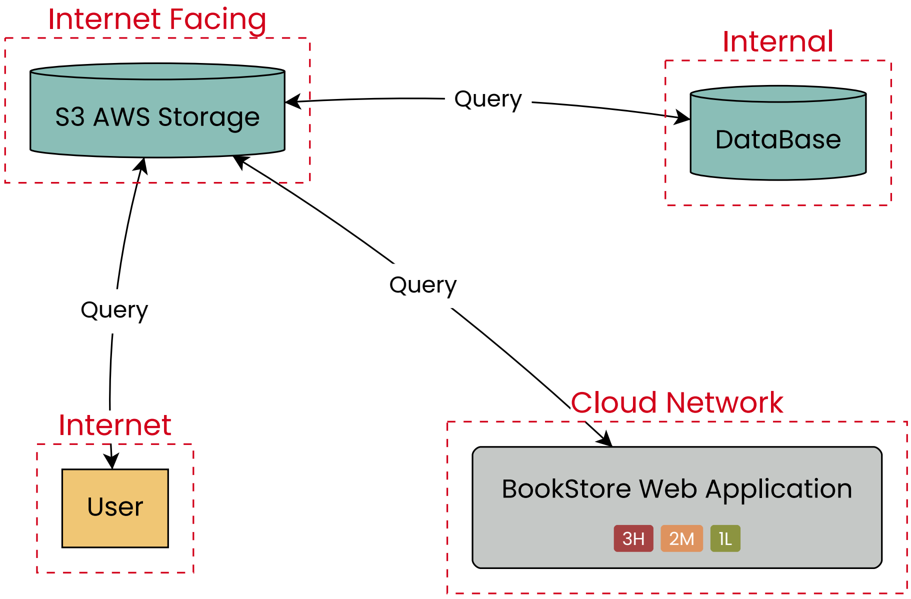
ThreatCanvas

by SecureFlag

My Threat Model

5/10/2025, 9:11:30 PM

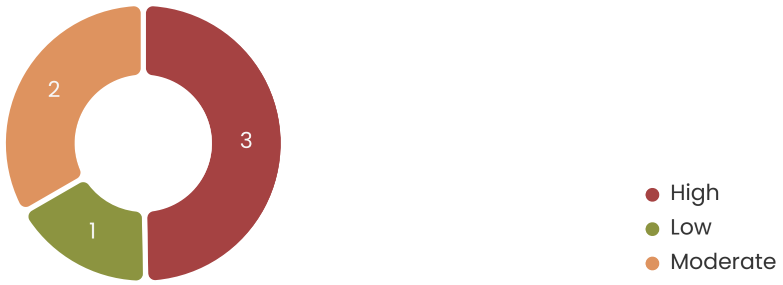
Diagram



Risk modifiers

Project type	Application

Open risks



Threat	Node	Risk rating
Abuse of Inadequate Authorization	BookStore Web Application	High
Password Brute-Force	BookStore Web Application	High
Upload of Malicious File	BookStore Web Application	High
Cross-Site Scripting (XSS)	BookStore Web Application	Moderate
Denial of Service	BookStore Web Application	Moderate
Insufficient Logging	BookStore Web Application	Low

Closed risks

Threat	Node	Risk rating
Abuse of Inadequate Authentication	BookStore Web Application	High
SQL Injection	BookStore Web Application	Low

Node analysis

BookStore Web Application

Component	Generic Process
Trust boundary	Cloud Network

Abuse of Inadequate Authentication

Risk rating	High
Status	Mitigated

Enforce Authentication

Implemented	Yes

Abuse of Inadequate Authorization

Risk rating	High
Status	Open

Enforce Authorization

Implemented	No

Unique User Identification

Implemented	No

Cross-Site Scripting (XSS)

Risk rating	Moderate
Status	Open

Input Sanitization

Implemented	No

Input Validation

Implemented	No

Output Encoding

Implemented	No

Denial of Service

Risk rating	Moderate

Status	Open

Firewall

Implemented	No

Mitigate Automated Attacks

Implemented	No

Insufficient Logging

Risk rating	Low
Status	Open

Logging and Monitoring

Implemented	No

Password Brute-Force

Risk rating	High
Status	Open

Mitigate Automated Attacks

Implemented	No

Password Policies

Implemented	No

SQL Injection

Risk rating	Low
Status	Risk accepted

Use of Parametrized SQL Queries

Implemented	No

Upload of Malicious File

Risk rating	High
Status	Open

Input Validation

Implemented	No

Restrict Software Execution	
Implemented	No

Use Antivirus Or Threat Response Software	
Implemented	No

Threat reference

Abuse of Inadequate Authentication

The node lacks proper authentication checks for functionalities or resources that require a provable user identity.

Abuse of Inadequate Authorization

The node does not perform an adequate authorization check against attackers when attempting to access data or perform actions they should not be allowed to perform.

Cross-Site Scripting (XSS)

The node uses untrusted input to build HTML content. Attackers can inject malicious scripts into the HTML content and induce the victim to browse it. This attack will force their browser to execute the client-side script in the context of the target website with the victim's privileges.

Denial of Service

The node is susceptible to DoS attacks, which can render the node unavailable or unresponsive to legitimate users.

Insufficient Logging

The node does not sufficiently log events such as logins, failed logins, high-value transactions, and errors.

Password Brute-Force

The node does not adequately protect against attackers who can perform an arbitrary number of authentication attempts using different passwords to gain access to the targeted account.

SQL Injection

The node uses untrusted input to build queries that are run on a back-end SQL database server. Attackers can submit malicious strings to manipulate statements and perform actions other than those intended by the application.

Upload of Malicious File

The node provides functionality that can be exploited to upload malicious files and potentially execute them.

Control reference

Enforce Authentication

Enforce robust authentication mechanism to access the node's resources and functionalities, such as passwords, pre-shared tokens, or digital certificates.

Enforce Authorization

Ensure that the node uses strict access policies against unauthorized access.

Firewall

Use network appliances to filter ingress or egress traffic. Configure software on endpoints to filter network traffic.

Input Sanitization

Check untrusted input and remove anything that might be potentially dangerous.

Input Validation

Ensure that only properly formed data is entered into the system.

Logging and Monitoring

Keep detailed audit logs with timestamps for activities such as user logins, sensitive data access, access control changes, and administrative actions.

Mitigate Automated Attacks

Protect against automated attacks such as content scraping, password brute-force, or denial of service attacks.

Output Encoding

Before displaying untrusted input, convert it to a safe form to prevent injection attacks that execute it as code in the browser.

Password Policies

Set and enforce secure password policies for accounts.

Restrict Software Execution

Block users from executing or installing unapproved software.

Unique User Identification

Assign a unique name and/or number for identifying and tracking user identity.

Use Antivirus Or Threat Response Software

Install antivirus or threat response software that use signatures or heuristics to detect malicious programs.

Use of Parametrized SQL Queries

Pre-compile SQL statements to prevent SQL Injection attacks.