Student Website Threat Model

Owner: Teacher
Reviewer: Fahad Ibne Fahian
Contributors:
Date Generated: Fri Sep 12 2025

Executive Summary

High level system description

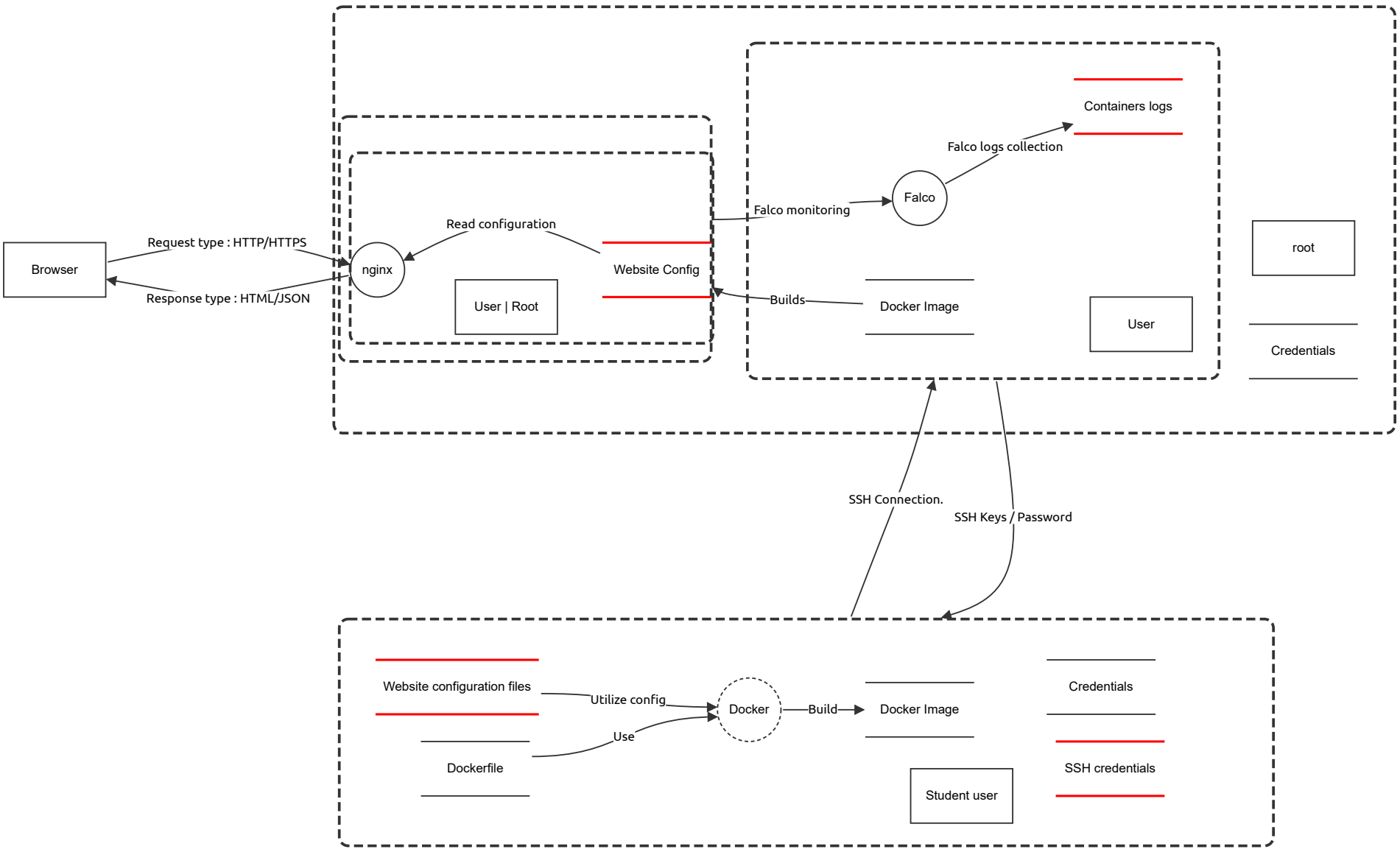
Whole system for a containerized website on cloud node.

Summary

Total Threats	10
Total Mitigated	6
Total Open	4
Open / Critical Severity	0
Open / High Severity	1
Open / Medium Severity	3
Open / Low Severity	0

System STRIDE

System includes: student's pc, cloud server and container.



System STRIDE

Browser (Actor)

Number	Title	Type	Severity	Status	Score	Description	Mitigations
1	Phishing Attack on Student Credentials	Spoofing	Medium	Mitigated		The attacker can use a phishing attack by creating a fake the student login page in to steal their credentials.	The user should check the URL carefully before using, avoid clicking on any suspicious links found online and also use 2FA, which can prevent the attacker from logging in even if they've stolen the credentials.

nginx (Process)

Description: Engine

Number	Title	Type	Severity	Status	Score	Description	Mitigations
22	Server Overload via DDoS Attack	Denial of service	High	Mitigated		The attackers may use Distributed Denial of Service (DDoS) method to flood the server with repeatedly high amount of auto-generated traffic to overload the server bandwidth, making the website unavailable to real users.	Rate-limiting and implementing a Content Delivery Network (CDN) like Cloudflare can be used to mitigate DDoS attacks and distribute the load.

Website Config (Store)

Description: HTML and CSS for the website

Number	Title	Type	Severity	Status	Score	Description	Mitigations
25	Impersonation via Fake SSH Key	Tampering	Medium	Open		An attacker may spoof their identity by creating a fake SSH key, allowing them to impersonate an authorized user or admin and access sensitive resources.	Need to maintain strict SSH key management policies and regularly audit and rotate SSH keys.

Read configuration (Data Flow)

Number	Title	Type	Severity	Status	Score	Description	Mitigations

Response type : HTML/JSON (Data Flow)

Number	Title	Type	Severity	Status	Score	Description	Mitigations

Request type : HTTP/HTTPS (Data Flow)

Number	Title	Type	Severity	Status	Score	Description	Mitigations
2	Man-in-the-Middle Attack (MITM) during HTTP Requests	Tampering	High	Mitigated		If the student is using public network (wifi) or if the website/application is using Unsecured connection (HTTP) instead of HTTPS, then an attacker can tamper with requests sent between the browser and server. They can manipulate and steal the data.	Use VPN or avoid using public Wifi and use HTTPS to encrypt all data for communication to ensure the security of the data during transmission.

Builds (Data Flow)

Number	Title	Type	Severity	Status	Score	Description	Mitigations

Falco monitoring (Data Flow)

Number	Title	Type	Severity	Status	Score	Description	Mitigations

Falco logs collection (Data Flow)

Number	Title	Type	Severity	Status	Score	Description	Mitigations

Build (Data Flow)

Number	Title	Type	Severity	Status	Score	Description	Mitigations

SSH Connection. (Data Flow)

Description: Dev env to server, used to copy image and update image.

Number	Title	Type	Severity	Status	Score	Description	Mitigations

Use (Data Flow)

Number	Title	Type	Severity	Status	Score	Description	Mitigations

Utilize config (Data Flow)

Number	Title	Type	Severity	Status	Score	Description	Mitigations

SSH Keys / Password (Data Flow)

Number	Title	Type	Severity	Status	Score	Description	Mitigations

Docker Image (Store)

Description: Ready made docker image

Number	Title	Type	Severity	Status	Score	Description	Mitigations
5	Sensitive Data Exposure via Docker	Information disclosure	High	Mitigated		If Docker containers are not configured correctly, this could expose sensitive data, such as environment variables or configuration files (e.g., db credentials).	Secure Docker containers by restricting access to sensitive files and using Docker secrets for storing sensitive data securely.

Containers logs (Store)

Description: Container monitoring via Falco

Number	Title	Type	Severity	Status	Score	Description	Mitigations
6	Unauthorized Access to Logs or System Files	Repudiation	Medium	Open		An attacker could delete or alter system logs to cover their tracks after performing malicious actions (e.g., modifying Docker images or website config).	Ensure log integrity by using immutable logs and monitoring systems to alert administrators on log tampering attempts.

Falco (Process)

Number	Title	Type	Severity	Status	Score	Description	Mitigations

Website configuration files (Store)

Number	Title	Type	Severity	Status	Score	Description	Mitigations
12	Compromised Website Configuration Files	Tampering	Medium	Open		Attackers may modify Nginx configuration files to redirect users to malicious sites or modify the behavior of the site.	Store configuration files securely and implement proper file permissions. Regularly monitor and audit configurations for any unauthorized changes.

Dockerfile (Store)

Number	Title	Type	Severity	Status	Score	Description	Mitigations

Docker (Process) - *Out of Scope*

Reason for out of scope: Not required

Description: Builds docker image

Number	Title	Type	Severity	Status	Score	Description	Mitigations

Docker Image (Store)

Description: Includes website configuration files

Number	Title	Type	Severity	Status	Score	Description	Mitigations
20	Exposure of Student Data	Information disclosure	Medium	Mitigated		If the website or Docker containers aren't properly secured, sensitive student data (e.g., portfolio details) could be exposed. Also they may gain access to personal data (e.g., names, email addresses, phone number etc.).	Always encrypt sensitive data both at rest (e.g., databases) and in transit (e.g., HTTPS). Implement role-based access control (RBAC) to limit access to sensitive data.

SSH credentials (Store)

Number	Title	Type	Severity	Status	Score	Description	Mitigations
26	SSH Access to Admin and User Roles	Tampering	High	Open		If SSH credentials are weakly secured or somehow compromised, an attacker can escalate privileges to gain root access or access to sensitive user data.	Use SSH key-based authentication and disable password-based authentication. Also, restrict SSH access with a firewall.

Credentials (Store)

Number	Title	Type	Severity	Status	Score	Description	Mitigations

root (Actor)

Number	Title	Type	Severity	Status	Score	Description	Mitigations

User (Actor)

Number	Title	Type	Severity	Status	Score	Description	Mitigations

Credentials (Store)

Number	Title	Type	Severity	Status	Score	Description	Mitigations

Student user (Actor)

Number	Title	Type	Severity	Status	Score	Description	Mitigations
24	Untraceable Actions by the Student	Repudiation	Low	Mitigated		If logs are not not maintained properly, a student might perform actions, such as deleting their profile or modifying their personal information, and deny doing so because there are no proper logs or tracking mechanisms in place. This lack of accountability can lead to confusion or disputes.	Implement detailed logging for every action taken on the system and ensure logs are stored securely and cannot be tampered with.

User | Root (Actor)

Number	Title	Type	Severity	Status	Score	Description	Mitigations