Student Website Threat Model

Owner: Teacher
Reviewer: Matias Kauranen
Contributors:
Date Generated: Fri Sep 12 2025

Executive Summary

High level system description

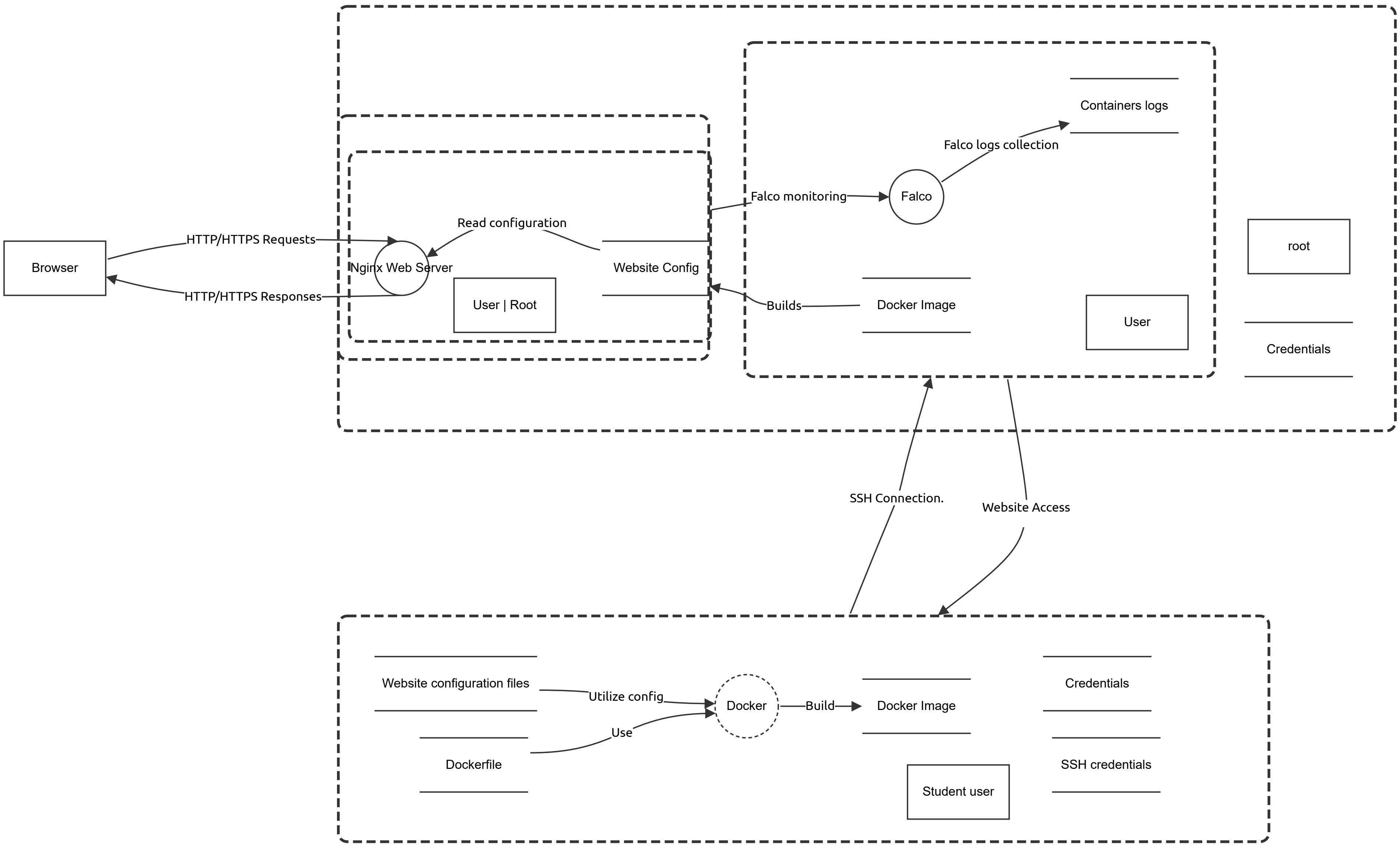
Whole system for a containerized website on cloud node.

Summary

Total Threats	10
Total Mitigated	10
Total Open	0
Open / Critical Severity	0
Open / High Severity	0
Open / Medium Severity	0
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

Nginx Web Server (Process)

Description: Engine

Number	Title	Type	Severity	Status	Score	Description	Mitigations
1	Man-in-the-Middle Attack on Web Traffic	Spoofing	High	Mitigated		Attacker intercepts unencrypted HTTP traffic and impersonates the website.	Implement HTTPS/TLS encryption for all web traffic. Configure Nginx with valid SSL certificates and redirect all HTTP to HTTPS.
7	Web Server Resource Exhaustion	Denial of service	Medium	Mitigated		HTTP flood attacks overwhelming the web server.	Implement rate limiting in Nginx, configure connection limits, use reverse proxy with DDoS protection, implement caching.

Website Config (Store)

Description: HTML and CSS for the website

Number	Title	Type	Severity	Status	Score	Description	Mitigations
10	Insecure Direct Object Reference via Website Config	Information disclosure	High	Mitigated		Attacker exploits path traversal vulnerabilities in Nginx configuration to access files outside the web root directory, potentially reading sensitive system files or configuration data that should not be publicly accessible	Configure Nginx with proper root directory restrictions, implement strict access controls on file paths, disable directory listing, use chroot jail for web server process, validate all file path requests to prevent directory traversal attacks

Read configuration (Data Flow)

Number	Title	Type	Severity	Status	Score	Description	Mitigations

Builds (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
2	Spoofing Identity	Tampering	High	Mitigated		Attacker uses compromised or weak SSH keys to impersonate legitimate user	Use strong SSH key pairs, implement SSH key rotation policy, disable password authentication.
8	SSH Brute Force Attack	Denial of service	Medium	Mitigated		Automated brute force attempts against SSH service.	Change SSH port from default 22 to 9999 (as indicated), implement fail2ban, use SSH keys only, configure connection limits.

Use (Data Flow)

Number	Title	Type	Severity	Status	Score	Description	Mitigations

Utilize config (Data Flow)

Number	Title	Type	Severity	Status	Score	Description	Mitigations

Website Access (Data Flow)

Number	Title	Type	Severity	Status	Score	Description	Mitigations

HTTP/HTTPS Requests (Data Flow)

Number	Title	Type	Severity	Status	Score	Description	Mitigations

HTTP/HTTPS Responses (Data Flow)

Number	Title	Type	Severity	Status	Score	Description	Mitigations

Falco monitoring (Data Flow)

Number	Title	Type	Severity	Status	Score	Description	Mitigations
9	Privilege Escalation via Falco	Tampering	High	Mitigated		Compromising Falco process to gain elevated privileges	Run Falco with minimal required privileges, implement proper RBAC, regular security updates, monitor Falco's own logs.

Docker Image (Store)

Description: Ready made docker image

Number	Title	Type	Severity	Status	Score	Description	Mitigations

Containers logs (Store)

Description: Container monitoring via Falco

Number	Title	Type	Severity	Status	Score	Description	Mitigations
5	Log Tampering	Tampering	Medium	Mitigated		Attacker modifies or deletes audit logs to hide malicious activities	Implement centralized logging with write-once storage, log integrity checking, separate log server with restricted access.

Falco (Process)

Number	Title	Type	Severity	Status	Score	Description	Mitigations

Website configuration files (Store)

Number	Title	Type	Severity	Status	Score	Description	Mitigations

Dockerfile (Store)

Number	Title	Type	Severity	Status	Score	Description	Mitigations
4	Dockerfile Manipulation	Tampering	High	Mitigated		Malicious modifications to dockerfile introducing vulnerabilities or backdoors	Store dockerfile in version control with commit signing, implement code review process, use immutable infrastructure practices.

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
3	Container Image Tampering	Tampering	High	Mitigated		Malicious Docker images or base images with backdoors	Use official base images only, implement image signing and verification, scan images for vulnerabilities before deployment.

SSH credentials (Store)

Number	Title	Type	Severity	Status	Score	Description	Mitigations
6	SSH Credential Exposure	Information disclosure	High	Mitigated		SSH private keys exposed through insecure storage or transmission	Encrypt private keys with strong passphrases, use SSH agent forwarding carefully, store keys in secure locations with proper file permissions.

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

User | Root (Actor)

Number	Title	Type	Severity	Status	Score	Description	Mitigations