Student Website Threat Model

Owner: Teacher
Reviewer: Walid El Idrissi
Contributors:
Date Generated: Sat Oct 12 2024

Executive Summary

High level system description

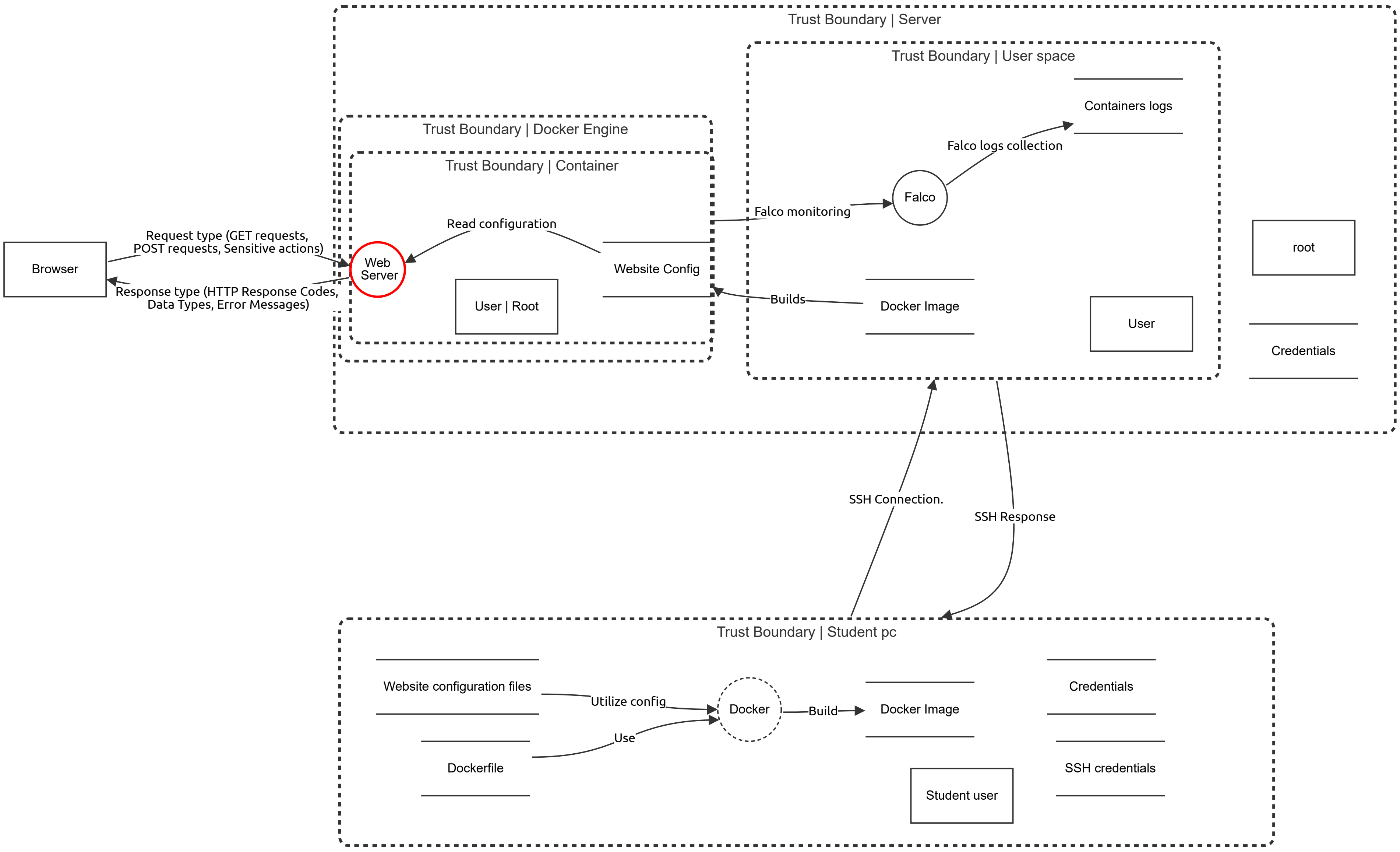
Whole system for a containerized website on cloud node.

Summary

Total Threats	10
Total Mitigated	9
Not Mitigated	1
Open / High Priority	1
Open / Medium Priority	0
Open / Low Priority	0
Open / Unknown Priority	0

System STRIDE

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



System STRIDE

Browser (Actor)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Web Server (Process)

Engine

Number	Title	Type	Priority	Status	Score	Description	Mitigations
6	DOS threat	Denial of service	High	Mitigated		The website is vulnerable to application-layer attacks that could slow down or crash the server.	Employ web application firewalls (WAF) to detect and block such attacks.
7	Information Disclosure threat	Information disclosure	High	Mitigated		Sensitive data (e.g., student personal information) is exposed through insecure data transmission (HTTP instead of HTTPS).	Enforce HTTPS for all data transmissions to protect data in transit.
8	Elevation of Privilege threat	Elevation of privilege	High	Open		A regular user gains unauthorized admin access to the website.	Provide remediation for this threat or a reason if status is N/A
9	Elevation of Privilege threat	Elevation of privilege	Medium	Mitigated		An attacker exploits a vulnerability in the application to gain higher privileges.	Regularly update and patch the software to fix known vulnerabilities.

Website Config (Store)

HTML and CSS for the website

Number	Title	Type	Priority	Status	Score	Description	Mitigations
3	Tampering threat	Tampering	High	Mitigated		Attackers alter the website's HTML/CSS to inject malicious content.	Use Content Security Policy (CSP) to prevent script injections.
4	Information Disclosure threat	Information disclosure	High	Mitigated		Error messages leak sensitive information about the server or application.	Customize error messages to avoid revealing system information.
5	Tampering threat	Tampering	High	Mitigated		An attacker modifies student data in the portfolio.	Implement data validation and access controls.

Read configuration (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Response type (HTTP Response Codes, Data Types, Error Messages) (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Request type (GET requests, POST requests, Sensitive actions) (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Builds (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Falco monitoring (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Falco logs collection (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Build (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

SSH Connection. (Data Flow)

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

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Use (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Utilize config (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

SSH Response (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Docker Image (Store)

Ready made docker image

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Containers logs (Store)

Container monitoring via Falco

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Falco (Process)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Website configuration files (Store)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Dockerfile (Store)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Docker (Process) *- Out of Scope*

Builds docker image

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Docker Image (Store)

Includes website configuration files

Number	Title	Type	Priority	Status	Score	Description	Mitigations

SSH credentials (Store)

Number	Title	Type	Priority	Status	Score	Description	Mitigations
10	Information Disclosure threat	Information disclosure	High	Mitigated		SSH credentials stored insecurely could be leaked, allowing attackers access to the server	Store SSH credentials in a secure vault or encrypted storage.

Credentials (Store)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

root (Actor)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

User (Actor)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Credentials (Store)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Student user (Actor)

Number	Title	Type	Priority	Status	Score	Description	Mitigations
1	Spoofing threat	Spoofing	High	Mitigated		An attacker can spoof a student's identity by gaining access to their credentials.	Enable two-factor authentication for logins.
2	Repudiation threat	Repudiation	High	Mitigated		Students deny submitting assignments after they are submitted.	Maintain a log of user actions, including timestamps.

User | Root (Actor)

Number	Title	Type	Priority	Status	Score	Description	Mitigations