Student Website Threat Model

Owner: Teacher
Reviewer: Linus Fulton
Contributors:
Date Generated: Fri Sep 13 2024

Executive Summary

High level system description

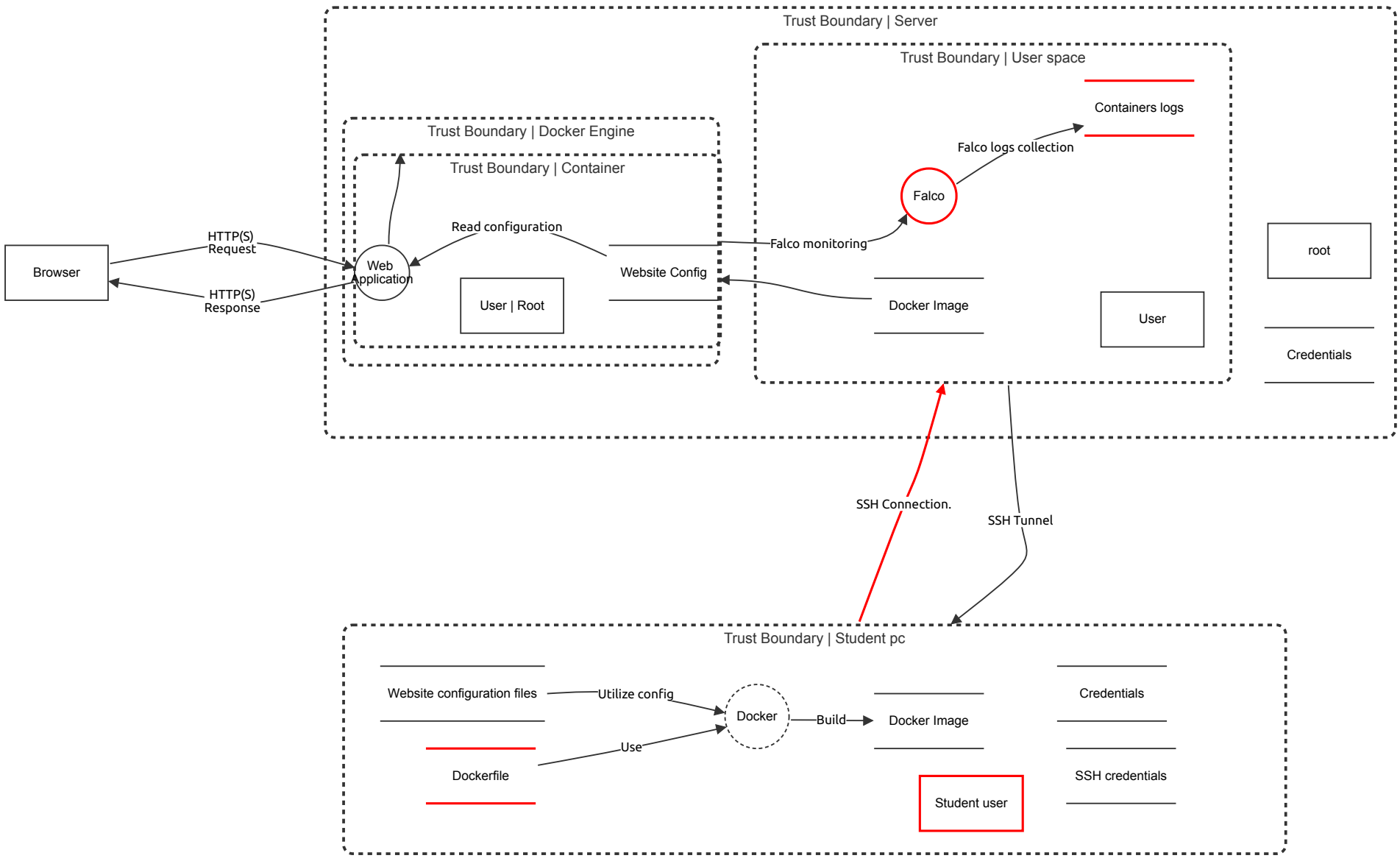
Whole system for a containerized website on cloud node.

Summary

Total Threats	10
Total Mitigated	5
Not Mitigated	5
Open / High Priority	0
Open / Medium Priority	5
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 Application (Process)

Engine

Number	Title	Type	Priority	Status	Score	Description	Mitigations
7	Web Application DoS Attack	Denial of service	Medium	Mitigated		An attacker can overload the web server and make it impossible for regular users to access it.	Implement resource limits or DDoS protection.

Website Config (Store)

HTML and CSS for the website

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Read configuration (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

HTTP(S) Response (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations
14	HTTP Connection	Information disclosure	Medium	Mitigated		Connecting via unsecured channels such as HTTP allows attackers to read information sent over the network.	Make sure to always connect over HTTPS.

HTTP(S) Request (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
6	SSH Connection Disclosure	Information disclosure	Medium	Open		Sensitive information, like SSH credentials, could be exposed. This makes it possible to listen in on confidential information.	Provide remediation for this threat or a reason if status is N/A

Use (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Utilize config (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

SSH Tunnel (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Data Flow (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Data Flow (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
5	Falco Logs Tampering	Tampering	Medium	Open		An attacker can tamper with log files to hide their intrusion.	Provide remediation for this threat or a reason if status is N/A

Falco (Process)

Number	Title	Type	Priority	Status	Score	Description	Mitigations
3	Spoofing Falco	Spoofing	Medium	Open		An attacker can spoof Falco to gain access to the system.	Provide remediation for this threat or a reason if status is N/A

Website configuration files (Store)

Number	Title	Type	Priority	Status	Score	Description	Mitigations
4	Website Config File Tampering	Tampering	Medium	Mitigated		An attacker can tamper with important configuration files.	Features such as digital signatures can be implemented.

Dockerfile (Store)

Number	Title	Type	Priority	Status	Score	Description	Mitigations
21	Dockerfile Tampering	Tampering	Medium	Open		The dockerfile could be tampered with to allow security vulnerabilites in the final Docker image.	Provide remediation for this threat or a reason if status is N/A

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

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
19	Credential Disclosure	Information disclosure	Medium	Mitigated		Storing passwords in plainetext makes it much easier for attackers to steal login data.	Properly hash and salt your passwords.

Student user (Actor)

Number	Title	Type	Priority	Status	Score	Description	Mitigations
23	Student Spoofing	Spoofing	Medium	Open		Having access to the physical users machine allows the attacker to exploit many different vulnerabilites.	Provide remediation for this threat or a reason if status is N/A

User | Root (Actor)

Number	Title	Type	Priority	Status	Score	Description	Mitigations
1	User/Root Spoofing	Spoofing	Medium	Mitigated		An attacker can impersonate the user to access the docker container.	Use MFA (such as an app, or e-mail/SMS).