Student Website Threat Model

Owner: Teacher
Reviewer: Tommy Meriläinen
Contributors:
Date Generated: Thu Sep 12 2024

Executive Summary

High level system description

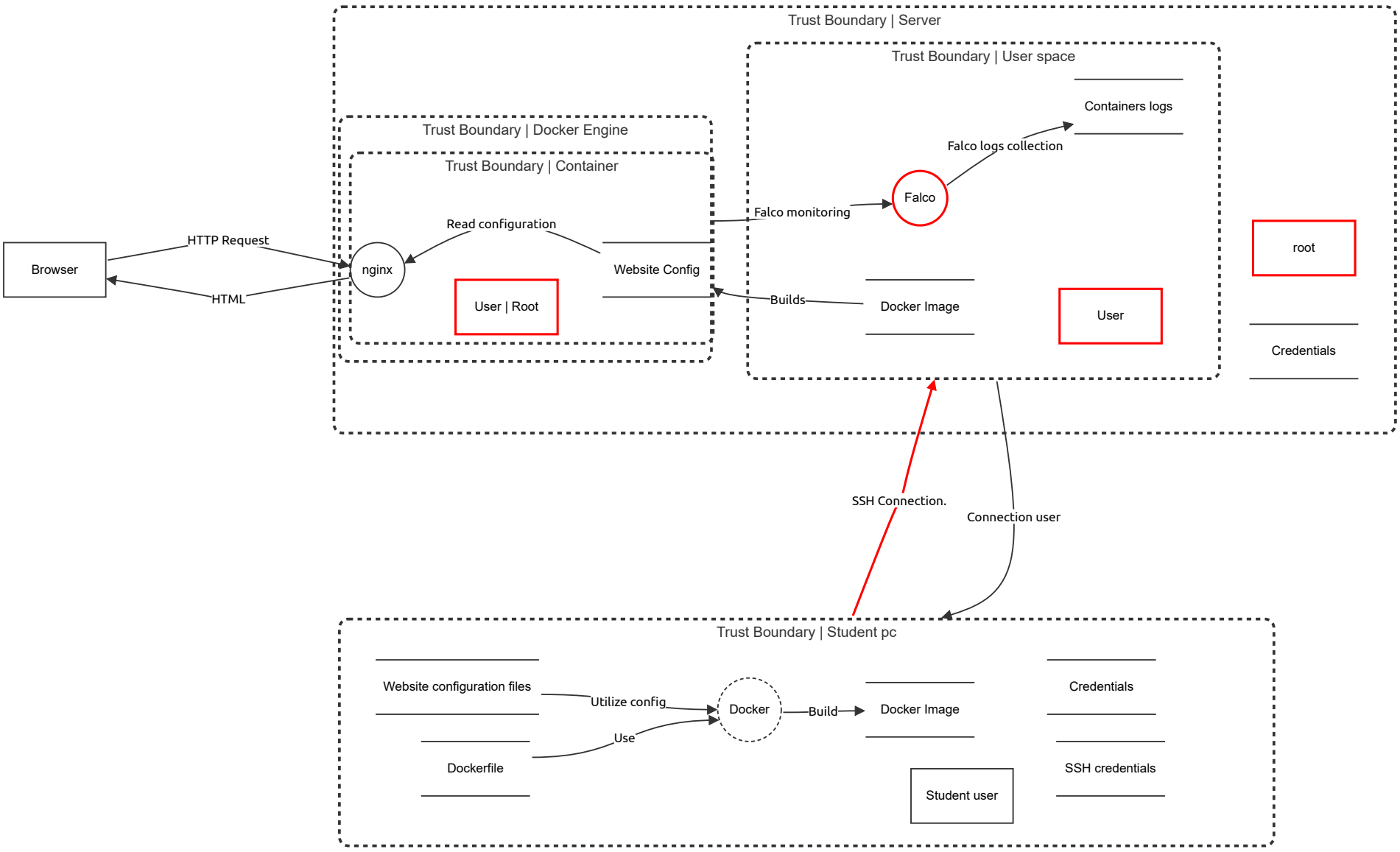
Whole system for a containerized website on cloud node.

Summary

Total Threats	11
Total Mitigated	6
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
1	Browser threat	Spoofing	High	Mitigated		Attacker can inject malicious scripts into the browser that can alter the behaviour of the website	Put browser in a Trust Boundary

nginx (Process)

Engine

Number	Title	Type	Priority	Status	Score	Description	Mitigations

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

HTML (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

HTTP Request (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
11	SSH connections from student pc to user space	Denial of service	Medium	Open		Repeated login attempts can lock the account	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

Connection user (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
9	Container logs in user space	Information disclosure	Medium	Mitigated		Logs can be exposed with no proper security	Use encryption for both, log storage and transmission

Falco (Process)

Number	Title	Type	Priority	Status	Score	Description	Mitigations
12	Falco not having own trust boundary	Spoofing	Medium	Open		If attacker gets access to user space he might be able to modify the stuff that's in falco.	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

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
2	SSH credentials on student pc	Tampering	High	Mitigated		Having ssh credentials on user pc can give the attacker an opportunity to alter the ssh key and get unauthorized backdoor to the server	chmod 600 the credentials so the file owner can only modify and read the file

Credentials (Store)

Number	Title	Type	Priority	Status	Score	Description	Mitigations
6	Credentials on server side	Denial of service	Medium	Mitigated		If attacker gets access to credentials from server, attacker can delete data or send malicious requests	Use proper databases with proper security systems with MFA

root (Actor)

Number	Title	Type	Priority	Status	Score	Description	Mitigations
13	root privileges inside server	Spoofing	Medium	Open		Attacker can gain access to root privileges	Provide remediation for this threat or a reason if status is N/A

User (Actor)

Number	Title	Type	Priority	Status	Score	Description	Mitigations
10	User in user space	Spoofing	Medium	Open		User information can be attacked	Provide remediation for this threat or a reason if status is N/A

Credentials (Store)

Number	Title	Type	Priority	Status	Score	Description	Mitigations
4	Credentials on student pc	Repudiation	Medium	Mitigated		Attacker can log in to student pc and pretend to be the student therefore student is to be blamed	Use MFA

Student user (Actor)

Number	Title	Type	Priority	Status	Score	Description	Mitigations
7	Student user in student pc	Spoofing	Medium	Mitigated		Student can fall for phishing attacks that can lead to stealing the credentials	MFA and education about not falling to phishing scams

User | Root (Actor)

Number	Title	Type	Priority	Status	Score	Description	Mitigations
14	root in container	Spoofing	Medium	Open		Attacker can alter container files if gets access to user root	Provide remediation for this threat or a reason if status is N/A