Student Website Threat Model

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

Executive Summary

High level system description

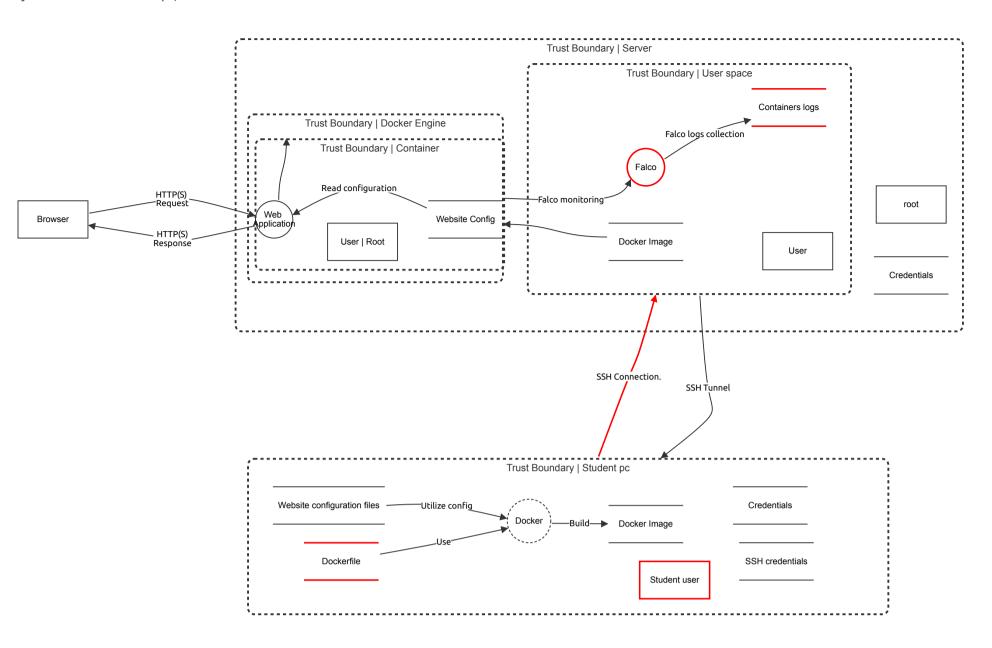
Whole system for a containerized website on cloud node.

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
Number	Title	туре	Priority	Status	Score	Description	Micigacions

Web Application (Process)

Engine

Number	Title	Туре	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	Туре	Priority	Status	Score	Description	Mitigations	

Read configuration (Data Flow)

Number	Title	Туре	Priority	Status	Score	Description	Mitigations

HTTP(S) Response (Data Flow)

Number	Title	Туре	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	Туре	Priority	Status	Score	Description	Mitigations
Falco monit	oring (Da	ta Flow)					
racco illollic	ornig (Da	ta riow)					
Number	Title	Туре	Priority	Status	Score	Description	Mitigations
Ealea loge e	allaction	(Data Flor					
Falco logs c	ottection	(Data Fio	w)				
Number	Title	Туре	Priority	Status	Score	Description	Mitigations
Build (Data	Flow						
Build (Data	rtow)						
Number	Title	Туре	Priority	Status	Score	Description	Mitigations
CCU Cooos	tics /D-t	n Flaus					
SSH Connec	cion. (Dat	a rlow)					
Dev env to server, used	I to copy image and	update image.					
			ity Status Score	Description			Mitigations
Number Title	Туре	Prior		Description Sensitive information	on like SSH crodooti		Mitigations Provide remediation for this threat
	Type ection Informa	Prior ation Medi		Sensitive information		als, could be exposed.	Mitigations Provide remediation for this threat or a reason if status is N/A
Number Title 6 SSH Conne	Type ection Informa	Prior ation Medi		Sensitive information		als, could be exposed.	Provide remediation for this threat
Number Title 6 SSH Conner Disclosure	Type ection Informatisclos	Prior ation Medi		Sensitive information		als, could be exposed.	Provide remediation for this threat
Number Title 6 SSH Conne	Type ection Informatisclos	Prior ation Medi		Sensitive information		als, could be exposed.	Provide remediation for this threat
Number Title 6 SSH Conner Disclosure	Type ection Informatisclos	Prior ation Medi		Sensitive information		als, could be exposed.	Provide remediation for this threat
Number Title 6 SSH Conner Disclosure	Type ection Informatisclos	Prior ation Medi		Sensitive information		als, could be exposed.	Provide remediation for this threat
Number Title 6 SSH Conner Disclosure	Type ection Informatisclose low)	Prior ation Medi ure	um Open	Sensitive informati This makes it possib	ole to listen in on con	als, could be exposed. Ifidential information.	Provide remediation for this threat or a reason if status is N/A
Number Title 6 SSH Conner Disclosure Number	Type ection Informatisclos low) Title	Prior ation Medicure Type	um Open	Sensitive informati This makes it possib	ole to listen in on con	als, could be exposed. Ifidential information.	Provide remediation for this threat or a reason if status is N/A
Number Title 6 SSH Conner Disclosure	Type ection Informatisclos low) Title	Prior ation Medicure Type	um Open	Sensitive informati This makes it possib	ole to listen in on con	als, could be exposed. Ifidential information.	Provide remediation for this threat or a reason if status is N/A
Number Title 6 SSH Conner Disclosure Number	Type ection Informatisclos low) Title	Prior ation Medicure Type	um Open	Sensitive informati This makes it possib	ole to listen in on con	als, could be exposed. Ifidential information.	Provide remediation for this threat or a reason if status is N/A
Number Title 6 SSH Conner Disclosure Number	Type ection Informatisclos low) Title	Prior ation Medicure Type	um Open	Sensitive informati This makes it possib	ole to listen in on con	als, could be exposed. Ifidential information.	Provide remediation for this threat or a reason if status is N/A
Number Title 6 SSH Conner Disclosure Use (Data F Number	Type ection Informatisclos low) Title	Prior ation Medicure Type	um Open Priority	Sensitive information This makes it possible Status	Score	als, could be exposed. Ifidential information. Description	Provide remediation for this threat or a reason if status is N/A Mitigations
Number Title 6 SSH Conner Disclosure Number Utilize conf	Title Type Informatisclos Title Title	Type Type	um Open Priority	Sensitive information This makes it possible Status	Score	als, could be exposed. Ifidential information. Description	Provide remediation for this threat or a reason if status is N/A Mitigations
Number Title 6 SSH Conner Disclosure Use (Data F Number	Title Type Informatisclos Title Title	Type Type	um Open Priority	Sensitive information This makes it possible Status	Score	als, could be exposed. Ifidential information. Description	Provide remediation for this threat or a reason if status is N/A Mitigations
Number Title 6 SSH Conner Disclosure Number Utilize conf	Title Type Informatisclos Title Title	Type Type	um Open Priority	Sensitive information This makes it possible Status	Score	als, could be exposed. Ifidential information. Description	Provide remediation for this threat or a reason if status is N/A Mitigations
Number Title 6 SSH Conner Disclosure Number Utilize conf	Title Type Informatisclos Title Title	Type Type	um Open Priority	Sensitive information This makes it possible Status	Score	als, could be exposed. Ifidential information. Description	Provide remediation for this threat or a reason if status is N/A Mitigations

Data Flow (Data Flow)

Number	Title	Туре	Priority	Status	Score	Description	Mitigations	

Data Flow (Data Flow)

Number	Title	Туре	Priority	Status	Score	Description	Mitigations

Docker Image (Store)

Ready made docker image

Number	Title	Туре	Priority	Status	Score	Description	Mitigations

Containers logs (Store)

Container monitoring via Falco

Number	Title	Туре	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	Туре	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	Туре	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)

21	Dockerfile Tampering	Tampering	Medium C	open The dockerfile could be tampered with to allow security vulnerabilites in the final Docker image.		security	Provide remediation for this threat or a reason if status is N/A		
Docker (Process) - Out of Scope									
Builds docker image									
Number	Titl	e Ty _l	pe	Priority	Status	Score	Description	Mitigations	
Dock	er Image (Store)							
Includes v	website configuratio	n files							
Number	Titl	e Ty _l	pe	Priority	Status	Score	Description	Mitigations	
SSH	redential	s (Store)							
Number	Titl	e Ty _l	ne.	Priority	Status	Score	Description	Mitigations	
Number	1160	- 191	, pe	Thomey	Julius	3.010	Descripcion	Meigacions	
Crede	entials (St	ore)							
	•	,							
Number	Titl	e Ty _l	pe	Priority	Status	Score	Description	Mitigations	
root ((Actor)								
Number	Titl	e Ty _l	pe	Priority	Status	Score	Description	Mitigations	
llsar	(Actor)								
0361	(76601)								
Number	Titl	e Ty _l	pe	Priority	Status	Score	Description	Mitigations	
Credentials (Store)									

Description

 ${\bf Mitigations}$

Title

Туре

Priority

Status

Score

Number

Number	Title	Туре	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	Туре	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	Туре	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).