Modelagem de Ameaças - UniVerse

Visão Geral

Nome do Ambiente: UniVerse

Propósito: WebAluno para faculdades

Data: 29/10/2023

Ferramentas Utilizadas: Microsoft Threat Modeling Tool

Responsáveis: Ary Farah, Adriano Vale

Contexto

Descrição do Ambiente:
UniVerse é um site com a mesma proposta de um WebAluno, onde os alunos, além de poderem conversar um com os outros, terão acesso a materiais de estudo utilizados em aula, notas, posição financeira, matérias, grade curricular e horária, calendário escolar, etc. Porém, conta com um diferencial: FaculRides. É um sistema de carona que oferece opção dos estudantes e professores que moram perto um do outro conversarem entre si e negociarem caronas, incluindo horários, preços, datas ou a quantidade de pessoas no carro.

Stakeholders:
Alunos, Professores, Funcionários.

Modelagem de Ameaças

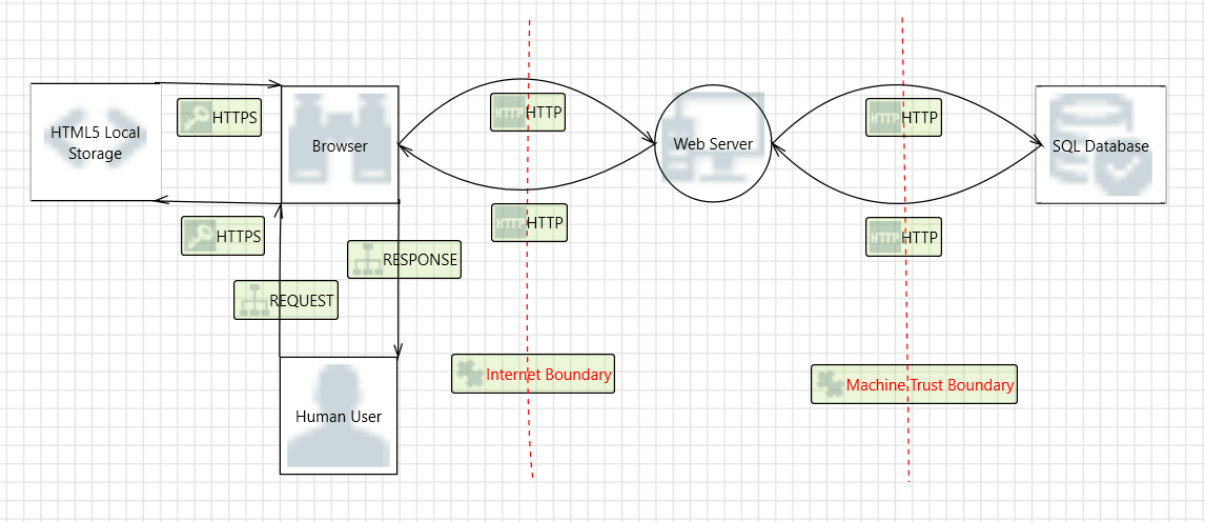
Objetivo da Modelagem:
Identificar ameaças e vulnerabilidades com o propósito de tornar o site mais seguro e sem oferecer risco de vazar informações confidenciais dos integrantes da faculdade.

Metodologia Utilizada:
STRIDE

Categorias de Ameaças a serem consideradas:

- **Ameaças Externas:** Hackers que buscam alguma vantagem, negociação em troca da não divulgação de dados confidenciais
- **Ameaças Internas:** Alunos mal-intencionados, seja por motivos concretos ou só por “diversão”.
- **Vulnerabilidades Conhecidas:** Injection, Cryptography Failures, Security Logging and Monitoring Failures.
- **Riscos de Segurança:** Vazamento de informações confidenciais e pessoais.

Arquitetura



Riscos Identificados

Ativo	S	T	R	I	D	E
Spoofing of Destination Data Store SQL Database	X					
Risks from Logging		X				
Potential SQL Injection Vulnerability for SQL Database		X				
The SQL Database Data Store Could Be Corrupted		X				
Lower Trusted Subject Updates Logs			X			
Data Logs from an Unknown Source			X			
Insufficient Auditing			X			
Potential Weak Protections for Audit Data			X			
Data Store Denies SQL Database Potentially Writing Data			X			
Authorization Bypass				X		

Ativo	S	T	R	I	D	E
Data Flow Sniffing				X		
Weak Credential Storage				X		
Weak Credential Transit				X		
Potential Excessive Resource Consumption for Web Server or SQL Database					X	
Data Flow HTTP Is Potentially Interrupted					X	
Data Store Inaccessible					X	
Spoofing the Web Server Process	X					
Spoofing of Source Data Store SQL Database	X					
Risks from Logging		X				
Cross Site Scripting		X				
Persistent Cross Site Scripting		X				
Potential Data Repudiation by Web Server			X			
Weak Access Control for a Resource				X		
Potential Process Crash or Stop for Web Server					X	
Data Flow HTTP Is Potentially Interrupted					X	
Data Store Inaccessible					X	
Web Server May be Subject to Elevation of Privilege Using Remote Code Execution						X
Elevation by Changing the						X

Ativo	S	T	R	I	D	E
Execution Flow in Web Server						
Spoofing the Web Server Process	X					
Spoofing the Browser External Entity	X					
Potential Lack of Input Validation for Web Server		X				
Cross Site Scripting		X				
Potential Data Repudiation by Web Server			X			
Data Flow Sniffing				X		
Potential Process Crash or Stop for Web Server					X	
Data Flow HTTP Is Potentially Interrupted					X	
Elevation Using Impersonation						X
Web Server May be Subject to Elevation of Privilege Using Remote Code Execution						X
Elevation by Changing the Execution Flow in Web Server						X
Spoofing of Source Data Store HTML5 Local Storage	X					
Weak Access Control for a Resource				X		
Spoofing of Destination Data Store HTML5 Local Storage	X					