CURSO DE TECNOLOGIA EM DEFESA CIBERNÉTICA

Projeto Serasa - Feedback para clientes

SÃO PAULO – SP

<Outubro/2023>

<Paulo Condutta Villas Boas - RM96662>

<Gabriel Mozelli Moreto – RM97522>

<Mariana Amorim – RM92078>

Fase 1 – Modelagem de Ameaças

SÃO PAULO – SP

<Outubro/2023>

SUMÁRIO

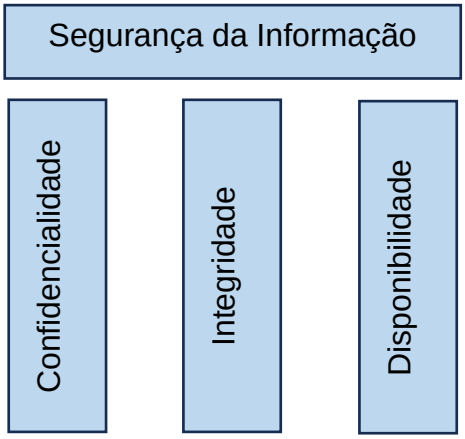
1. INTRODUÇÃO

O desafio crescente das ameaças existentes no ambiente cibernético coloca um holofote importante em aplicações web disponíveis via Internet. Uma das formas de efetuar a mitigação de eventos, adaptada principalmente pela área de gestão de riscos, é a modelagem de ameaças.

Link apresentação: https://www.youtube.com/watch?v=63c63ioudQg

2. CONCEITO

Para estabelecer uma estrutura consistente de segurança, a modelagem de ameaças desempenha um papel fundamental. Atuando sobre os pilares da segurança da informação (TRIADE), quando relacionados à modelagem de ameaças, formam uma abordagem abrangente para proteger os sistemas, informações e usuários.



Confidencialidade

A confidencialidade concentra-se em garantir que os dados e informações sejam acessíveis apenas por agentes autorizados. A modelagem de ameaças é essencial para identificar ameaças à confidencialidade, como o acesso não autorizado a dados confidenciais.

Integridade

A integridade atua na proteção dos dados mantendo sua situação e propósitos confiáveis e íntegros. A modelagem de ameaças ajuda a identificar ameaças

que podem comprometer a integridade como ataques de modificação ou corrompimento da informação.

Disponibilidade

A disponibilidade é a garantia de que os sistemas e informações estarão disponíveis para uso quando necessário. A modelagem de ameaças ajuda a identificar ameaças que podem levar à indisponibilidade, como ataques de negação de serviço (DDoS).

Ao relacionar a modelagem de ameaças aos pilares da segurança da informação, podemos desenvolver estratégias de segurança mais robustas, protegendo seus ativos e mantendo a integridade e a confiança nas informações. A segurança da informação é uma jornada contínua, e a modelagem de ameaças desempenha um papel central na manutenção da integridade e da segurança das informações em um mundo cada vez mais digital.

Adotada principalmente em um processo (até mesmo antes do início) do desenvolvimento seguro, onde desejamos trazer a segurança “mais à esquerda”, utilizar a modelagem possibilita reconhecer nossas fraquezas quando elas nem ao menos existem na realidade (estão ainda na ideia do Design).

A modelagem de ameaças faz parte do **Ciclo de Vida de Desenvolvimento de Segurança (SDLC) da Microsoft**. Ele identifica entidades do sistema, eventos e limites e, em seguida, aplica um conjunto de ameaças conhecidas. Usando-o, as equipes de segurança podem identificar ameaças potenciais. Essa característica a torna a prática de segurança mais eficaz que você pode aplicá-la. A imagem abaixo demostra parte do SDLC focada na concepção, seguranca e design incluindo atividade de Threat Model.

Figure 1. Architecture task flow when a project is new or a redesign – Ibid, p. 278

Existem diferentes tipos de modelagem disponíveis a serem utilizadas, uma das mais comuns, criada nos anos 90’s por dois pesquisadores de segurança da Microsoft

Praerit Garg e Loren Kohnfelder, o **STRIDE** é usa uma abordagem completa que pode auxiliar a identificar de forma contínua, sendo útil para detectar potencial problemas.

Propriedade	Ameaça	Definição
Autenticação	Spoofing	Personificar algo ou outra pessoa.
Integridade	Tampering	Modificar dados ou código
Não repúdio	Repudiação	Alegar não ter realizado uma ação.
Confidencialidade	Information disclosure	Expor informações a alguém não autorizado a vê-las
Disponibilidade	Denial of Service	Negar ou degradar o serviço aos usuários
Autorização	Elevation of Privilege	Obter recursos sem a autorização adequada

Tabela STRIDE com explicação de cada inicial de ameaça

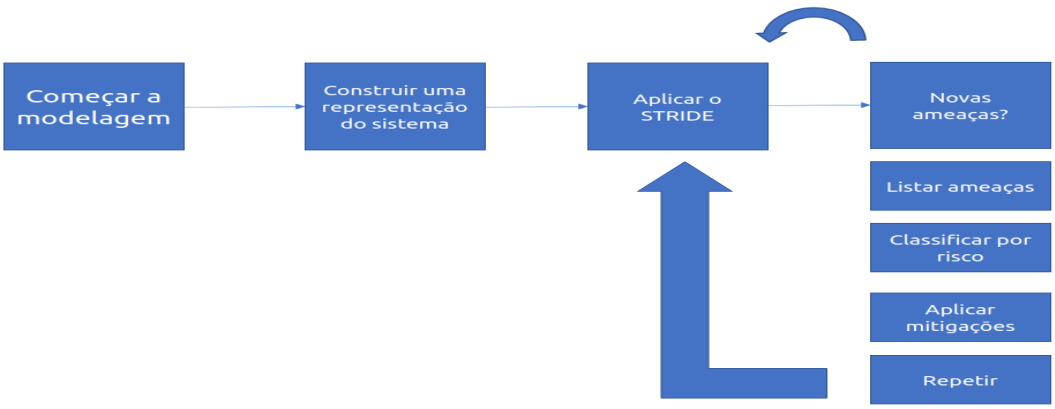
Todo desenvolvimento do trabalho será baseado nessa metodologia com auxílio da ferramenta **Microsoft Threat Modeling**.

3. OBJETIVOS

A segurança cibernética é uma preocupação essencial em ambientes web, especialmente em sistemas que lidam com informações sensíveis, como um ambiente web de feedback. Modelar ameaças é uma abordagem eficaz para identificar potenciais riscos de segurança e desenvolver estratégias de mitigação.

Alinhado aos desafios de segurança, a proposta tem que levar em consideração a **experiência do usuário (UX)** na navegação fluida e sem “bloqueios” que impactem a navegação do usuário e objetivo principal da plataforma.

Nessa fase, avaliamos o cenário atual adotado e propondo ajustes nos fluxos e proteções para atingir objetivo. Esse processo deve ser evoluído nas próximas fases além de ser contínuo e reaplicado a cada nova atualização tecnologia ou novo fluxo.

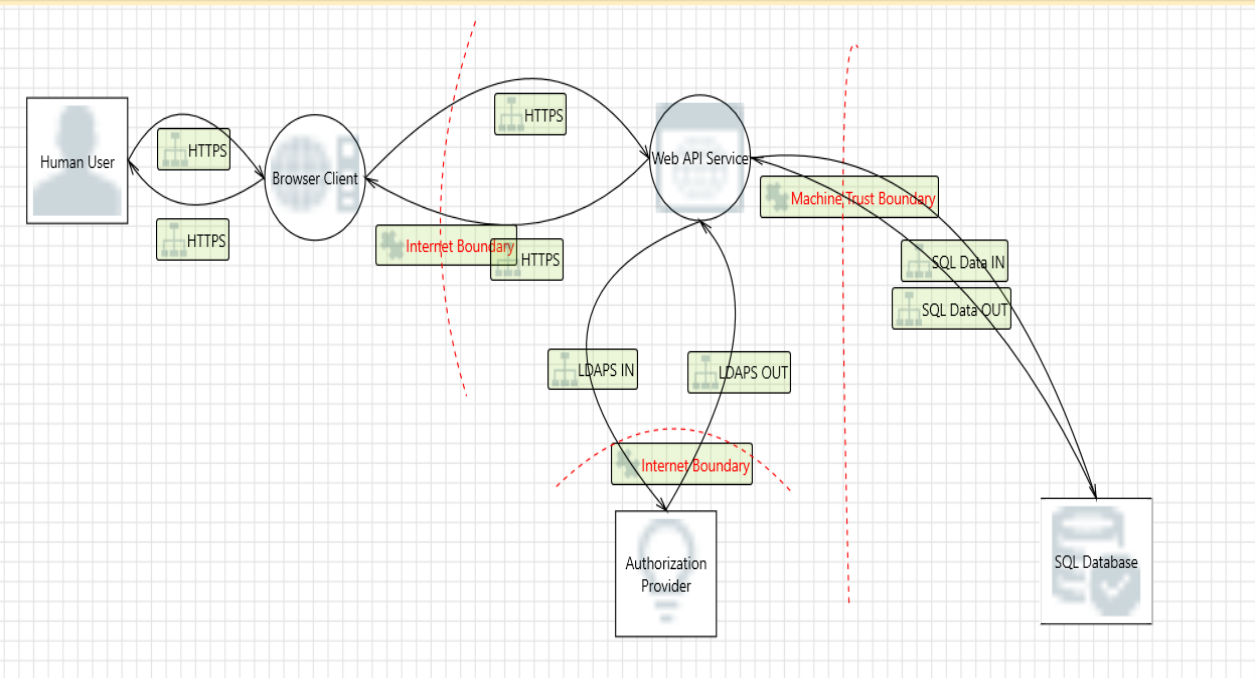


4. CENARIO ATUAL

FLUXO FUNCIONAL ATUAL

1. O usuário realiza o cadastro no sistema
2. O usuário faz o login com usuário e senha cadastrados
3. O usuário realiza o registro contendo seu feedback
4. O usuário faz o logoff

DFS ATUAL (PREVISTO)



Os diagramas de fluxo de dados (DFDs) são representa graficamente o atual cenário existente, decompondo o sistema em partes e mostrar que cada parte é não suscetível a ameaças relevantes. Esse DFD apresentado traz algumas informações sugestivas um vez que não temos informações detalhadas do atual cenário existente da aplicação na SERASA EXPIRIAN.

REPORT ATUAL

Este relatório apresenta ATUAL report da análise de modelagem de ameaças STRIDE para um sistema web de feedback.

	Ameaça	Vulnerabilidade/ Risco	Contramedida/ Mitigação
Spoofing Falsificação	Spoofing of Destination Data Store SQL Database	SQL Database may be spoofed by an attacker and this may lead to data being written to the attacker's target instead of SQL Database. Consider using a standard authentication mechanism to identify the destination data store.	Autenticação via MFA (token, mail link, sms) e monitoria
	Spoofing of Destination Data Store SQL Database	SQL Database may be spoofed by an attacker and this may lead to data being written to the attacker's target instead of SQL Database. Consider using a standard authentication mechanism to identify the destination data store.	Autenticação via MFA (token, mail link, sms) e monitoria
	Spoofing the Human User External Entity	Human User may be spoofed by an attacker and this may lead to unauthorized access to Browser Client. Consider using a standard authentication mechanism to identify the external entity.	Autenticação via MFA (token, mail link, sms) e monitoria
	Spoofing of the Authorization Provider External Destination Entity	Authorization Provider may be spoofed by an attacker and this may lead to data being sent to the attacker's target instead of Authorization Provider. Consider using a standard authentication mechanism to identify the external entity.	Autenticação via MFA (token, mail link, sms) e monitoria
Tampering Violação	Risks from Logging	Log readers can come under attack via log files. Consider ways to canonicalize data in all logs. Implement a single reader for the logs, if possible, in order to reduce attack surface area. Be sure to understand and document log file elements which come from untrusted sources.	LOG centralizados via SIEM
	Potential SQL Injection Vulnerability for SQL Database	SQL injection is an attack in which malicious code is inserted into strings that are later passed to an instance of SQL Server for parsing and execution. Any procedure that constructs SQL statements should be reviewed for injection vulnerabilities because SQL Server will execute all syntactically valid queries that it receives. Even parameterized data can be manipulated by a skilled and determined attacker.	Controle de integridade com HASH e assinaturas dos dados, assinatura digital, controles de versão e backup
	Potential SQL Injection Vulnerability for SQL Database	SQL injection is an attack in which malicious code is inserted into strings that are later passed to an instance of SQL Server for parsing and execution. Any procedure that constructs SQL statements should be reviewed for injection vulnerabilities because SQL Server will execute all syntactically valid queries that it receives. Even parameterized data can be manipulated by a skilled and determined attacker.	Controle de integridade com HASH e assinaturas dos dados, assinatura digital, controles de versão e backup
	Risks from Logging	Log readers can come under attack via log files. Consider ways to canonicalize data in all logs. Implement a single reader for the logs, if possible, in order to reduce attack surface area. Be sure to understand and document log file elements which come from untrusted sources.	LOG centralizados via SIEM
	Browser Client Process Memory Tampered	If Browser Client is given access to memory, such as shared memory or pointers, or is given the ability to control what Web API Service executes (for example, passing back a function pointer.), then Browser Client can tamper with Web API Service. Consider if the function could work with less access to memory, such as passing data rather than pointers. Copy in data provided, and then validate it.	Controle memoria Browser
	Web API Service Process Memory Tampered	If Web API Service is given access to memory, such as shared memory or pointers, or is given the ability to control what Browser Client executes (for example, passing back a function pointer.), then Web API Service can tamper with Browser Client. Consider if the function could work with less access to memory, such as passing data rather than pointers. Copy in data provided, and then validate it.	Controle memoria e integridade WebAPI
	The SQL Database Data Store Could Be Corrupted	Data flowing across SQL Data IN may be tampered with by an attacker. This may lead to corruption of SQL Database. Ensure the integrity of the data flow to the data store.	Controle de integridade com HASH e assinaturas dos dados, assinatura digital, controles de versão e backup
	The SQL Database Data Store Could Be Corrupted	Data flowing across SQL Data OUT may be tampered with by an attacker. This may lead to corruption of SQL Database. Ensure the integrity of the data flow to the data store.	Controle de integridade com HASH e assinaturas dos dados, assinatura digital, controles de versão e backup
Repudiation Repúdio	Potential Weak Protections for Audit Data	Consider what happens when the audit mechanism comes under attack, including attempts to destroy the logs, or attack log analysis programs. Ensure access to the log is through a reference monitor, which controls read and write separately. Document what filters, if any, readers can rely on, or writers should expect	Logs detalhados e centralizados em SIEM e rotatividade de LOGs
	Insufficient Auditing	Does the log capture enough data to understand what happened in the past? Do your logs capture enough data to understand an incident after the fact? Is such capture lightweight enough to be left on all the time? Do you have enough data to deal with repudiation claims? Make sure you log sufficient and appropriate data to handle a repudiation claims. You might want to talk to an audit expert as well as a privacy expert about your choice of data.	Registrar detalhadamente todas as interações dos usuários, incluindo envios de feedback, para fins de auditoria.
	Data Logs from an Unknown Source	Do you accept logs from unknown or weakly authenticated users or systems? Identify and authenticate the source of the logs before accepting them.	Logs detalhados e centralizados em SIEM
	Lower Trusted Subject Updates Logs	If you have trust levels, is anyone other outside of the highest trust level allowed to log? Letting everyone write to your logs can lead to repudiation problems. Only allow trusted code to log.	Logs detalhados e centralizados em SIEM
	Lower Trusted Subject Updates Logs	If you have trust levels, is anyone other outside of the highest trust level allowed to log? Letting everyone write to your logs can lead to repudiation problems. Only allow trusted code to log.	Logs detalhados e centralizados em SIEM

	Data Logs from an Unknown Source	Do you accept logs from unknown or weakly authenticated users or systems? Identify and authenticate the source of the logs before accepting them.	Autenticação forte pra envio de LOGS
	Insufficient Auditing	Does the log capture enough data to understand what happened in the past? Do your logs capture enough data to understand an incident after the fact? Is such capture lightweight enough to be left on all the time? Do you have enough data to deal with repudiation claims? Make sure you log sufficient and appropriate data to handle a repudiation claims. You might want to talk to an audit expert as well as a privacy expert about your choice of data.	Registrar detalhadamente todas as interações dos usuários, incluindo envios de feedback, para fins de auditoria.
	Potential Weak Protections for Audit Data	Consider what happens when the audit mechanism comes under attack, including attempts to destroy the logs, or attack log analysis programs. Ensure access to the log is through a reference monitor, which controls read and write separately. Document what filters, if any, readers can rely on, or writers should expect	Autenticação forte e rotatividade de Logs
	Potential Data Repudiation by Web API Service	Web API Service claims that it did not receive data from a source outside the trust boundary. Consider using logging or auditing to record the source, time, and summary of the received data.	Monitoramento
	Potential Data Repudiation by Browser Client	Browser Client claims that it did not receive data from a source outside the trust boundary. Consider using logging or auditing to record the source, time, and summary of the received data.	N/A
	Potential Data Repudiation by Web API Service	Web API Service claims that it did not receive data from a source outside the trust boundary. Consider using logging or auditing to record the source, time, and summary of the received data.	Monitoramento
	External Entity Authorization Provider Potentially Denies Receiving Data	Authorization Provider claims that it did not receive data from a process on the other side of the trust boundary. Consider using logging or auditing to record the source, time, and summary of the received data.	Monitoramento e Controle de chamadas
	Data Store Denies SQL Database Potentially Writing Data	SQL Database claims that it did not write data received from an entity on the other side of the trust boundary. Consider using logging or auditing to record the source, time, and summary of the received data.	Monitoramento e Controle de chamadas
	Data Store Denies SQL Database Potentially Writing Data	SQL Database claims that it did not write data received from an entity on the other side of the trust boundary. Consider using logging or auditing to record the source, time, and summary of the received data.	Monitoramento e Controle de chamadas
Information Disclosure **Divulgação de Informações**	Authorization Bypass	Can you access SQL Database and bypass the permissions for the object? For example by editing the files directly with a hex editor, or reaching it via filesharing? Ensure that your program is the only one that can access the data, and that all other subjects have to use your interface.	Implementar autenticação forte, criptografia para proteger informações sensíveis e garantir que apenas usuários autorizados tenham acesso.
	Weak Credential Storage	Credentials held at the server are often disclosed or tampered with and credentials stored on the client are often stolen. For server side, consider storing a salted hash of the credentials instead of storing the credentials themselves. If this is not possible due to business requirements, be sure to encrypt the credentials before storage, using an SDL-approved mechanism. For client side, if storing credentials is required, encrypt them and protect the data store in which they're stored	Implementar autenticação forte, criptografia para proteger informações sensíveis e garantir que apenas usuários autorizados tenham acesso.
	Weak Credential Storage	Credentials held at the server are often disclosed or tampered with and credentials stored on the client are often stolen. For server side, consider storing a salted hash of the credentials instead of storing the credentials themselves. If this is not possible due to business requirements, be sure to encrypt the credentials before storage, using an SDL-approved mechanism. For client side, if storing credentials is required, encrypt them and protect the data store in which they're stored	Implementar autenticação forte, criptografia para proteger informações sensíveis e garantir que apenas usuários autorizados tenham acesso.
	Authorization Bypass	Can you access SQL Database and bypass the permissions for the object? For example by editing the files directly with a hex editor, or reaching it via filesharing? Ensure that your program is the only one that can access the data, and that all other subjects have to use your interface.	Implementar autenticação forte, criptografia para proteger informações sensíveis e garantir que apenas usuários autorizados tenham acesso.
	Weak Authentication Scheme	Custom authentication schemes are susceptible to common weaknesses such as weak credential change management, credential equivalence, easily guessable credentials, null credentials, downgrade authentication or a weak credential change management system. Consider the impact and potential mitigations for your custom authentication scheme.	Implementar autenticação forte, criptografia para proteger informações sensíveis e garantir que apenas usuários autorizados tenham acesso.
	Weak Credential Transit	Credentials on the wire are often subject to sniffing by an attacker. Are the credentials re-usable/re-playable? Are credentials included in a message? For example, sending a zip file with the password in the email. Use strong cryptography for the transmission of credentials. Use the OS libraries if at all possible, and consider cryptographic algorithm agility, rather than hardcoding a choice.	Implementar autenticação forte, criptografia para proteger informações sensíveis e garantir que apenas usuários autorizados tenham acesso.
	Weak Credential Transit	Credentials on the wire are often subject to sniffing by an attacker. Are the credentials re-usable/re-playable? Are credentials included in a message? For example, sending a zip file with the password in the email. Use strong cryptography for the transmission of credentials. Use the OS libraries if at all possible, and consider cryptographic algorithm agility, rather than hardcoding a choice.	Implementar autenticação forte, criptografia para proteger informações sensíveis e garantir que apenas usuários autorizados tenham acesso.
Denial of Service **Negação de Serviço**	Potential Excessive Resource Consumption for Web API Service or SQL Database	Does Web API Service or SQL Database take explicit steps to control resource consumption? Resource consumption attacks can be hard to deal with, and there are times that it makes sense to let the OS do the job. Be careful that your resource requests don't deadlock, and that they do timeout.	Controles e limites de requisição/segundo
	Potential Excessive Resource Consumption for Web API Service or SQL Database	Does Web API Service or SQL Database take explicit steps to control resource consumption? Resource consumption attacks can be hard to deal with, and there are times that it makes sense to let the OS do the job. Be careful that your resource requests don't deadlock, and that they do timeout.	Controles e limites de requisição/segundo

	Data Flow HTTPS Is Potentially Interrupted	An external agent interrupts data flowing across a trust boundary in either direction.	Controles via Firewall de limites de requisição ip / requisições por segundo
	Potential Process Crash or Stop for Web API Service	Web API Service crashes, halts, stops or runs slowly; in all cases violating an availability metric.	Controles e limites de requisição/segundo
	Data Flow HTTPS Is Potentially Interrupted	An external agent interrupts data flowing across a trust boundary in either direction.	Controles e limites de requisição/segundo
	Potential Process Crash or Stop for Browser Client	Browser Client crashes, halts, stops or runs slowly; in all cases violating an availability metric.	Controles de Memoria
	Data Flow LDAPS OUT Is Potentially Interrupted	An external agent interrupts data flowing across a trust boundary in either direction.	Controles e limites de requisição/segundo
	Potential Process Crash or Stop for Web API Service	Web API Service crashes, halts, stops or runs slowly; in all cases violating an availability metric.	Servidores escaláveis em Alta Disponibilidade
	Data Flow LDAPS IN Is Potentially Interrupted	An external agent interrupts data flowing across a trust boundary in either direction.	Controles e limites de requisição/segundo
	Data Store Inaccessible	An external agent prevents access to a data store on the other side of the trust boundary.	Bancos em Alta Disponibilidade
	Data Flow SQL Data IN Is Potentially Interrupted	An external agent interrupts data flowing across a trust boundary in either direction.	Controles e limites de requisição/segundo
	Data Store Inaccessible	An external agent prevents access to a data store on the other side of the trust boundary.	Bancos em Alta Disponibilidade
	Data Flow SQL Data OUT Is Potentially Interrupted	An external agent interrupts data flowing across a trust boundary in either direction.	Controles e limites de requisição/segundo
	Potential Excessive Resource Consumption for Web API Service or SQL Database	Does Web API Service or SQL Database take explicit steps to control resource consumption? Resource consumption attacks can be hard to deal with, and there are times that it makes sense to let the OS do the job. Be careful that your resource requests don't deadlock, and that they do timeout.	Controles e limites de requisição/segundo
Elevation of Privilege **Elevação de Privilégio**	Elevation Using Impersonation	Browser Client may be able to impersonate the context of Human User in order to gain additional privilege.	Implementar o princípio do menor privilégio, onde os usuários têm apenas o acesso necessário para realizar suas tarefas e monitorar atividades suspeitas.
	Elevation Using Impersonation	Web API Service may be able to impersonate the context of Authorization Provider in order to gain additional privilege.	Implementar o princípio do menor privilégio, onde os usuários têm apenas o acesso necessário para realizar suas tarefas e monitorar atividades suspeitas.
	Elevation Using Impersonation	Web API Service may be able to impersonate the context of Browser Client in order to gain additional privilege.	Implementar o princípio do menor privilégio, onde os usuários têm apenas o acesso necessário para realizar suas tarefas e monitorar atividades suspeitas.
	Elevation Using Impersonation	Browser Client may be able to impersonate the context of Web API Service in order to gain additional privilege.	Implementar o princípio do menor privilégio, onde os usuários têm apenas o acesso necessário para realizar suas tarefas e monitorar atividades suspeitas.
	Elevation by Changing the Execution Flow in Web API Service	An attacker may pass data into Web API Service in order to change the flow of program execution within Web API Service to the attacker's choosing.	Implementar o princípio do menor privilégio, onde os usuários têm apenas o acesso necessário para realizar suas tarefas e monitorar atividades suspeitas.

	Web API Service May be Subject to Elevation of Privilege Using Remote Code Execution	Browser Client may be able to remotely execute code for Web API Service.	Implementar o princípio do menor privilégio, onde os usuários têm apenas o acesso necessário para realizar suas tarefas e monitorar atividades suspeitas.
	Browser Client May be Subject to Elevation of Privilege Using Remote Code Execution	Web API Service may be able to remotely execute code for Browser Client.	Implementar o princípio do menor privilégio, onde os usuários têm apenas o acesso necessário para realizar suas tarefas e monitorar atividades suspeitas.
	Elevation by Changing the Execution Flow in Browser Client	An attacker may pass data into Browser Client in order to change the flow of program execution within Browser Client to the attacker's choosing.	Implementar o princípio do menor privilégio, onde os usuários têm apenas o acesso necessário para realizar suas tarefas e monitorar atividades suspeitas.
	Elevation by Changing the Execution Flow in Web API Service	An attacker may pass data into Web API Service in order to change the flow of program execution within Web API Service to the attacker's choosing.	Implementar o princípio do menor privilégio, onde os usuários têm apenas o acesso necessário para realizar suas tarefas e monitorar atividades suspeitas.
	Web API Service May be Subject to Elevation of Privilege Using Remote Code Execution	Authorization Provider may be able to remotely execute code for Web API Service.	Implementar o princípio do menor privilégio, onde os usuários têm apenas o acesso necessário para realizar suas tarefas e monitorar atividades suspeitas.

Podemos avaliar de forma mais detalhada o atual cenário nos anexos abaixo o relatório apresentado pela ferramenta Microsoft Threat Modeling Tool onde exportamos as ameaças identificadas e além Report completo da ferramenta.

report-ameacas-atual .xlsx

report STRIDE.htm

Reforçamos que analise foi efetuada com informações disponíveis, em um cenário limitado, gerando assim uma ideia de como atual ambiente está desenhado.

5. PROPOSTA

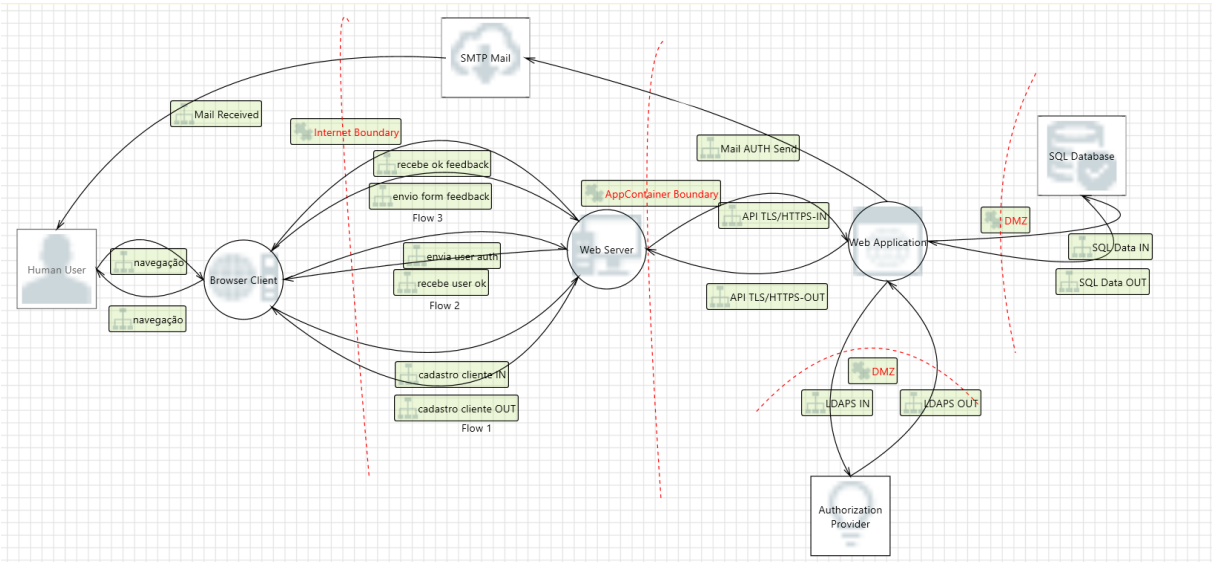
Propomos que a abordagem de proteção cibernética seja um esforço contínuo, e a análise de ameaças deve ser atualizada regularmente para acompanhar as mudanças no ambiente de ameaças e novas vulnerabilidades que possam surgir. Nessa fase, avaliamos o fluxo atual e iniciamos ajustes de fluxo funcional, fluxo da aplicação, e proteções baseadas em boas práticas que devem ser evoluídas nas próximas fases do projeto.

NOVO FLUXO FUNCIONAL PROPOSTO – FASE 1

1. O usuário realiza o cadastro no sistema
2. Sistema dispara um mail para usuário com mail já cadastrado na base
3. O usuário faz o login com usuário e senha cadastrados
4. O usuário realiza o registro contendo seu feedback
5. O usuário faz o logoff

Adicionalmente, apontamos a necessidade de criação de canal de ouvidoria para reclamações de usuários que não detém cadastro na base.

NOVO DFS PROPOSTO – FASE 1



O DFD apresentado aqui é apenas uma ideia inicial de boa prática para melhoras iniciais apresentadas na Fase 1. Ações adicionais e ajustes serão efetuadas conforme evolução tecnologia e maior detalhamento das fases seguintes.

	Ameaça	Vulnerabilidade/ Risco	Contramedida/ Mitigação
Spoofing Falsificação	Spoofing of the External Web Service External Destination Entity	External Web Service may be spoofed by an attacker and this may lead to data being sent to the attacker's target instead of External Web Service. Consider using a standard authentication mechanism to identify the external entity.	
	Spoofing of the External Web Service External Destination Entity	External Web Service may be spoofed by an attacker and this may lead to data being sent to the attacker's target instead of External Web Service. Consider using a standard authentication mechanism to identify the external entity.	
	Spoofing the Browser Client Process	Browser Client may be spoofed by an attacker and this may lead to information disclosure by External Web Service. Consider using a standard authentication mechanism to identify the destination process.	
	Spoofing of the External Web Service External Destination Entity	External Web Service may be spoofed by an attacker and this may lead to data being sent to the attacker's target instead of External Web Service. Consider using a standard authentication mechanism to identify the external entity.	
	Spoofing of Destination Data Store SMTP Mail	SMTP Mail may be spoofed by an attacker and this may lead to data being written to the attacker's target instead of SMTP Mail. Consider using a standard authentication mechanism to identify the destination data store.	
	Spoofing of Destination Data Store SQL Database	SQL Database may be spoofed by an attacker and this may lead to data being written to the attacker's target instead of SQL Database. Consider using a standard authentication mechanism to identify the destination data store.	

	Spoofing of Source Data Store SMTP Mail	SMTP Mail may be spoofed by an attacker and this may lead to incorrect data delivered to Human User. Consider using a standard authentication mechanism to identify the source data store.	
	Spoofing of Source Data Store SQL Database	SQL Database may be spoofed by an attacker and this may lead to incorrect data delivered to External Web Application. Consider using a standard authentication mechanism to identify the source data store.	
	Spoofing of Destination Data Store SMTP Mail	SMTP Mail may be spoofed by an attacker and this may lead to data being written to the attacker's target instead of SMTP Mail. Consider using a standard authentication mechanism to identify the destination data store.	
Tampering **Violação**	Authenticated Data Flow Compromised	An attacker can read or modify data transmitted over an authenticated dataflow.	
	The SQL Database Data Store Could Be Corrupted	Data flowing across SQL Data IN may be tampered with by an attacker. This may lead to corruption of SQL Database. Ensure the integrity of the data flow to the data store.	
	Possible SQL Injection Vulnerability for SQL Database	SQL injection is an attack in which malicious code is inserted into strings that are later passed to an instance of SQL Server for parsing and execution. Any procedure that constructs SQL statements should be reviewed for injection vulnerabilities because SQL Server will execute all syntactically valid queries that it receives. Even parameterized data can be manipulated by a skilled and determined attacker.	
	The SMTP Mail Data Store Could Be Corrupted	Data flowing across Mail AUTH Send may be tampered with by an attacker. This may lead to corruption of SMTP Mail. Ensure the integrity of the data flow to the data store.	
Repudiation **Repúdio**	External Entity External Web Service Potentially Denies Receiving Data	External Web Service claims that it did not receive data from a process on the other side of the trust boundary. Consider using logging or auditing to record the source, time, and summary of the received data.	
	External Entity External Web Service Potentially Denies Receiving Data	External Web Service claims that it did not receive data from a process on the other side of the trust boundary. Consider using logging or auditing to record the source, time, and summary of the received data.	
	External Entity External Web Service Potentially Denies Receiving Data	External Web Service claims that it did not receive data from a process on the other side of the trust boundary. Consider using logging or auditing to record the source, time, and summary of the received data.	
	External Entity External Web Application Potentially Denies Receiving Data	External Web Application claims that it did not receive data from a process on the other side of the trust boundary. Consider using logging or auditing to record the source, time, and summary of the received data.	
	Potential Data Repudiation by Browser Client	Browser Client claims that it did not receive data from a source outside the trust boundary. Consider using logging or auditing to record the source, time, and summary of the received data.	
	Potential Data Repudiation by Browser Client	Browser Client claims that it did not receive data from a source outside the trust boundary. Consider using logging or auditing to record the source, time, and summary of the received data.	
	External Entity External Web Service Potentially Denies Receiving Data	External Web Service claims that it did not receive data from a process on the other side of the trust boundary. Consider using logging or auditing to record the source, time, and summary of the received data.	
	Potential Data Repudiation by Browser Client	Browser Client claims that it did not receive data from a source outside the trust boundary. Consider using logging or auditing to record the source, time, and summary of the received data.	
	Data Store Denies SQL Database Potentially Writing Data	SQL Database claims that it did not write data received from an entity on the other side of the trust boundary. Consider using logging or auditing to record the source, time, and summary of the received data.	
	Data Logs from an Unknown Source	Do you accept logs from unknown or weakly authenticated users or systems? Identify and authenticate the source of the logs before accepting them.	
	Lower Trusted Subject Updates Logs	If you have trust levels, is anyone other outside of the highest trust level allowed to log? Letting everyone write to your logs can lead to repudiation problems. Only allow trusted code to log.	
	External Entity Authorization Provider Potentially Denies Receiving Data	Authorization Provider claims that it did not receive data from a process on the other side of the trust boundary. Consider using logging or auditing to record the source, time, and summary of the received data.	
	External Entity Human User Potentially Denies Receiving Data	Human User claims that it did not receive data from a process on the other side of the trust boundary. Consider using logging or auditing to record the source, time, and summary of the received data.	
	External Entity External Web Application Potentially Denies Receiving Data	External Web Application claims that it did not receive data from a process on the other side of the trust boundary. Consider using logging or auditing to record the source, time, and summary of the received data.	
	External Entity External Web Application Potentially Denies Receiving Data	External Web Application claims that it did not receive data from a process on the other side of the trust boundary. Consider using logging or auditing to record the source, time, and summary of the received data.	
	Data Store Denies SMTP Mail Potentially Writing Data	SMTP Mail claims that it did not write data received from an entity on the other side of the trust boundary. Consider using logging or auditing to record the source, time, and summary of the received data.	
	Data Logs from an Unknown Source	Do you accept logs from unknown or weakly authenticated users or systems? Identify and authenticate the source of the logs before accepting them.	
	Lower Trusted Subject Updates Logs	If you have trust levels, is anyone other outside of the highest trust level allowed to log? Letting everyone write to your logs can lead to repudiation problems. Only allow trusted code to log.	
Information Disclosure **Divulgação de Informações**	Weak Access Control for a Resource	Improper data protection of SMTP Mail can allow an attacker to read information not intended for disclosure. Review authorization settings.	
	Weak Access Control for a Resource	Improper data protection of SQL Database can allow an attacker to read information not intended for disclosure. Review authorization settings.	
Denial of Service **Negação de Serviço**	Data Flow envio form feedback Is Potentially Interrupted	Browser Client crashes, halts, stops or runs slowly; in all cases violating an availability metric.	
	Data Flow envia user auth Is Potentially Interrupted	An external agent interrupts data flowing across a trust boundary in either direction.	
	Data Flow API TLS/HTTPS-OUT Is Potentially Interrupted	An external agent prevents access to a data store on the other side of the trust boundary.	
	Data Flow API TLS/HTTPS-IN Is Potentially Interrupted	An external agent interrupts data flowing across a trust boundary in either direction.	
	Data Flow cadastro cliente OUT Is Potentially Interrupted	An external agent prevents access to a data store on the other side of the trust boundary.	

	Potential Process Crash or Stop for Browser Client	An external agent interrupts data flowing across a trust boundary in either direction.	
	Data Flow recebe user ok Is Potentially Interrupted	An external agent interrupts data flowing across a trust boundary in either direction.	
	Potential Process Crash or Stop for Browser Client	An external agent prevents access to a data store on the other side of the trust boundary.	
	Data Flow cadastro cliente IN Is Potentially Interrupted	An external agent prevents access to a data store on the other side of the trust boundary.	
	Potential Process Crash or Stop for Browser Client	An external agent interrupts data flowing across a trust boundary in either direction.	
	Data Flow recebe ok feedback Is Potentially Interrupted	An external agent interrupts data flowing across a trust boundary in either direction.	
	Data Store Inaccessible	An external agent interrupts data flowing across a trust boundary in either direction.	
	Data Flow Mail Received Is Potentially Interrupted	An external agent prevents access to a data store on the other side of the trust boundary.	
	Data Store Inaccessible	An external agent interrupts data flowing across a trust boundary in either direction.	
	Data Flow SQL Data IN Is Potentially Interrupted	Browser Client crashes, halts, stops or runs slowly; in all cases violating an availability metric.	
	Data Flow LDAPS IN Is Potentially Interrupted	An external agent interrupts data flowing across a trust boundary in either direction.	
	Data Store Inaccessible	An external agent prevents access to a data store on the other side of the trust boundary.	
	Data Store Inaccessible	An external agent interrupts data flowing across a trust boundary in either direction.	
	Data Flow Mail AUTH Send Is Potentially Interrupted	An external agent prevents access to a data store on the other side of the trust boundary.	
	Data Flow SQL Data OUT Is Potentially Interrupted	An external agent interrupts data flowing across a trust boundary in either direction.	
	Data Flow LDAPS OUT Is Potentially Interrupted	An external agent interrupts data flowing across a trust boundary in either direction.	
	Data Store Inaccessible	An external agent prevents access to a data store on the other side of the trust boundary.	
	Data Flow Mail AUTH Send Is Potentially Interrupted	An external agent prevents access to a data store on the other side of the trust boundary.	
Elevation of Privilege **Elevação de Privilégio**	Elevation by Changing the Execution Flow in Browser Client	An attacker may pass data into Browser Client in order to change the flow of program execution within Browser Client to the attacker's choosing.	
	Browser Client May be Subject to Elevation of Privilege Using Remote Code Execution	External Web Service may be able to remotely execute code for Browser Client.	
	Elevation Using Impersonation	Browser Client may be able to impersonate the context of External Web Service in order to gain additional privilege.	
	Elevation by Changing the Execution Flow in Browser Client	An attacker may pass data into Browser Client in order to change the flow of program execution within Browser Client to the attacker's choosing.	
	Browser Client May be Subject to Elevation of Privilege Using Remote Code Execution	External Web Service may be able to remotely execute code for Browser Client.	
	Elevation Using Impersonation	Browser Client may be able to impersonate the context of External Web Service in order to gain additional privilege.	
	Elevation Using Impersonation	Browser Client may be able to impersonate the context of External Web Service in order to gain additional privilege.	
	Browser Client May be Subject to Elevation of Privilege Using Remote Code Execution	External Web Service may be able to remotely execute code for Browser Client.	
	Elevation by Changing the Execution Flow in Browser Client	An attacker may pass data into Browser Client in order to change the flow of program execution within Browser Client to the attacker's choosing.	

Podemos avaliar de forma mais detalhada o cenário proposto nos anexos abaixo o relatório apresentado pela ferramenta Microsoft Threat Modeling Tool onde exportamos as ameaças identificadas e além Report completo da ferramenta.

report-proposto.xlsx

report STRIDE-PROPOSTO.h

6. REFERÊNCIAS

https://www.microsoft.com/en-us/security/blog/2007/09/11/stride-chart/

https://docs.microsoft.com/en-us/azure/architecture/secure-by-design/threat-modeling-stride

https://www.oreilly.com/library/view/threat-modeling/9781492056546/ch04.html

https://www.iriusrisk.com/

https://safecode.org/wp-content/uploads/2017/05/SAFECode_TM_Whitepaper.pdf

https://www.zendesk.com.br/blog/feedback-do-cliente/

https://www.threatmodelingmanifesto.org/

https://learn.microsoft.com/pt-br/security/engineering/threat-modeling-with-dev-ops