Relatório de Modelagem de Ameaças

Criado em 25/07/2025 20:48:09

Nome do modelo de ameaça:

Proprietário:

Revisor:

Colaboradores:

Descrição:

Suposições:

Dependências externas:

Resumo do modelo de ameaça:

Não iniciado	2
Não aplicável	0
Precisa de investigação	0
Mitigação implementada	13
Total	15
Total migrado	0

Diagrama: Diagrama 1

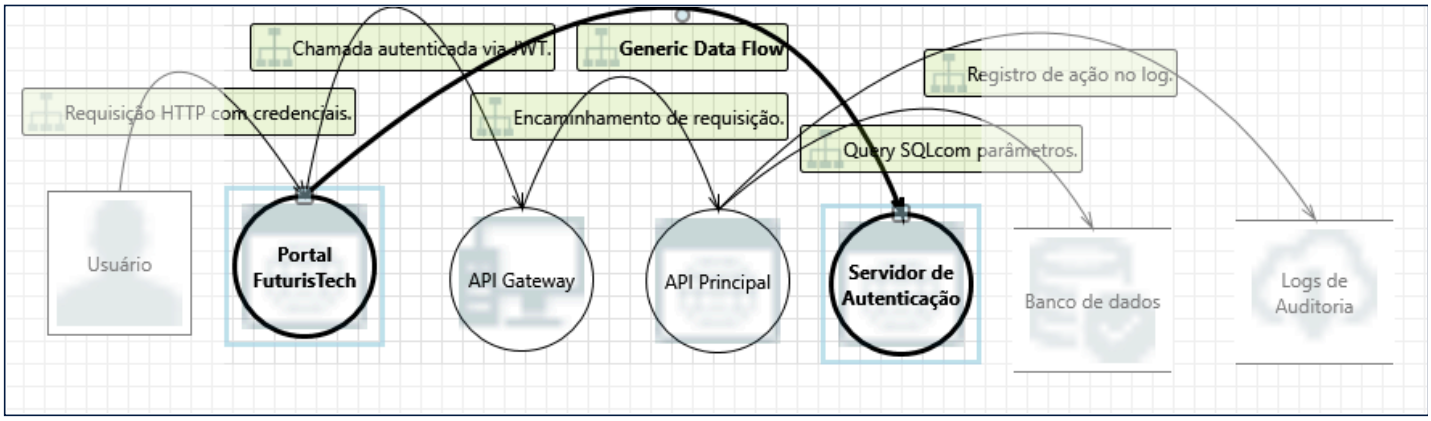
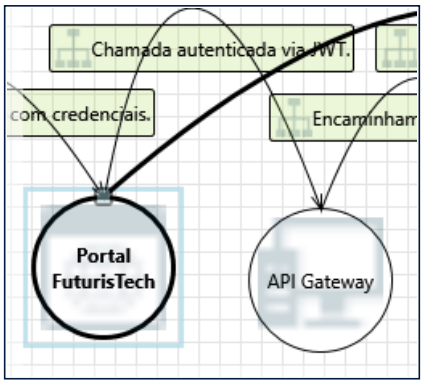


Diagrama 1 Resumo do diagrama:

Não iniciado	2
Não aplicável	0
Precisa de investigação	0
Mitigação implementada	13
Total	15
Total migrado	0

Interação: Chamada autenticada via JWT.



1. Cross Site Scripting [Estado: Não Iniciado] [Prioridade: Média]

Categoria: Adulteração

Descrição: O servidor web 'API Gateway' pode estar sujeito a um ataque de script entre sites porque não limpa entradas não confiáveis.

Justificação: Um aplicativo valida e sanitiza todas as entradas perdidas pelos usuários, utilizando codificação de caracteres para evitar a execução de scripts maliciosos.

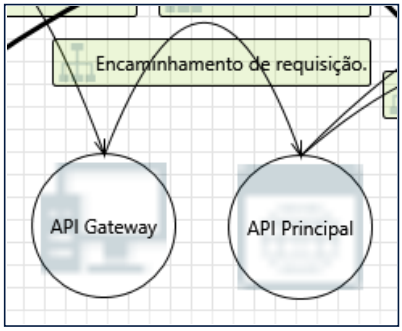
2. Elevação usando representação [Estado: Mitigação implementada] [Prioridade: Alta]

Categoria: Elevação de Privilégio

Descrição: O API Gateway pode representar o contexto do Portal FuturisTech para obter privilégios adicionais.

Justificação: O sistema utiliza RBAC (controle de acesso baseado em diversão) e ABAC (baseado em atributos) com verificação de escopos nos tokens JWT para evitar acessos indevidos.

Interação: Encaminhamento de requisição.



3. Memória do processo do API Gateway violada [Estado: Mitigação implementada] [Prioridade: Alta]

Categoria: Adulteração

Descrição: Se o API Gateway tiver acesso à memória, como memória compartilhada ou ponteiros, ou tiver a capacidade de controlar o que o API Principal executa (por exemplo, passando de volta um ponteiro de função), o API Gateway poderá interferir no API Principal. Considere se a função poderia funcionar com menos acesso à memória, como passando dados em vez de ponteiros. Copie os dados fornecidos e valide-os.

Justificação: API Gateway roda em ambiente isolado (container seguro) sem acesso direto à memória do sistema ou dados críticos.

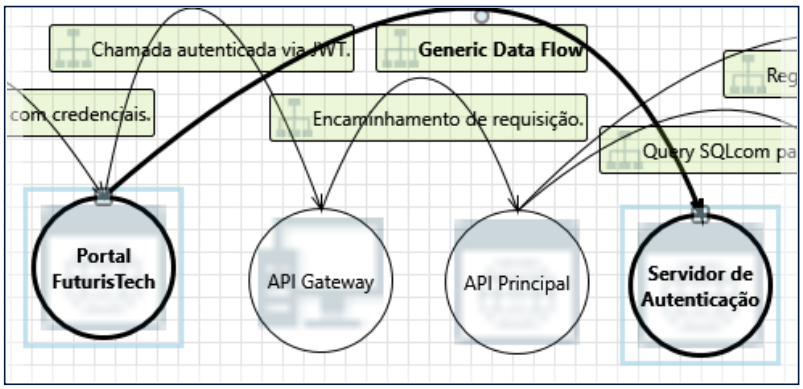
4. Elevação usando representação [Estado: Mitigação implementada] [Prioridade: Alta]

Categoria: Elevação de Privilégio

Descrição: O API Principal pode representar o contexto do API Gateway para obter privilégios adicionais.

Justificação: Uma API valida os escopos e papéis é apresentada nos tokens JWT antes de permitir qualquer operação sensível.

Interação: Fluxo de Dados Genéricos



5. Portal FuturisTech Processo de memória adulterado [Estado: Mitigação implementada] [Prioridade: Média]

Categoria: Adulteração

Descrição: Se o Portal FuturisTech tiver acesso à memória, como memória compartilhada ou ponteiros, ou tiver a capacidade de controlar o que o Servidor de Autenticação executa (por exemplo, passando de volta um ponteiro de função), o Portal FuturisTech poderá interferir no Servidor de Autenticação. Considere se a função poderia funcionar com menos acesso à memória, como passando dados em vez de ponteiros. Copie os dados fornecidos e valide-os.

Justificação: O portal aplica validações e autenticação forte para impedir modificações não autorizadas nas interfaces e nos dados.

6. Cross Site Scripting [Estado: Mitigação implementada] [Prioridade: Alta]

Categoria: Adulteração

Descrição: O servidor web 'Servidor de Autenticação' pode estar sujeito a um ataque de script entre sites porque não limpa entradas não confiáveis.

Justificação: Filtros XSS são ativos, com escape de caracteres perigosos e uso de Política de Segurança de Conteúdo (CSP) para impedir a execução de scripts externos.

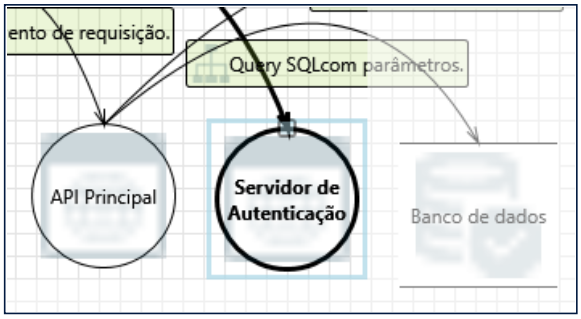
7. Elevação usando representação [Estado: Mitigação implementada] [Prioridade: Alta]

Categoria: Elevação de Privilégio

Descrição: O Servidor de Autenticação pode representar o contexto do Portal FuturisTech para obter privilégios adicionais.

Justificação: O MFA éá habilitado e a autenticaçãoção federada é feita com validação de escopos e identidade no servidor Auth.

Interação: Consulta parâmetros SQLcom.



8. Falsificação do banco de dados de destino [Estado: Mitigação implementada] [Prioridade: Média]

Categoria: Falsificação

Descrição: O banco de dados pode ser falsificado por um invasor, o que pode fazer com que os dados sejam gravados no banco de dados alvo do invasor em vez do banco de dados. Considere usar um mecanismo de autenticação padrão para identificar o repositório de dados de destino.

Justificação: Todas as conexões com o banco de dados são protegidas com TLS, desativar autenticaçãoção forte e são restritos à rede interna.

9. Vulnerabilidade potencial de injeção de SQL para Banco de dados [Estado: Não iniciado] [Prioridade: Alta]

Categoria: Adulteração

Descrição: Injeção de SQL é um ataque no qual código malicioso é inserido em strings que posteriormente são passadas para uma instância do SQL Server para análise e execução. Qualquer procedimento que construa instruções SQL deve ser revisado em busca de vulnerabilidades de injeção, pois o SQL Server executará todas as consultas sintaticamente válidas que receber. Até mesmo dados parametrizados podem ser manipulados por um invasor habilidoso e determinado.

Justificação: Mitigada com uso de ORM seguro.

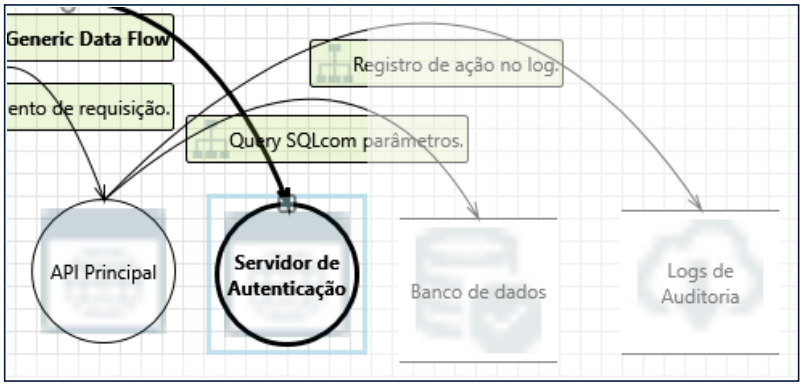
10. Potencial consumo excessivo de recursos para API Principal ou Banco de dados [Estado: Mitigação implementada] [Prioridade: Média]

Categoria: Negação de serviço

Descrição: A API Principal ou o Banco de Dados tomam medidas explícitas para controlar o consumo de recursos? Ataques de consumo de recursos podem ser difíceis de lidar, e há momentos em que faz sentido deixar o sistema operacional fazer o trabalho. Tome cuidado para que suas solicitações de recursos não entrem em deadlock e atinjam o tempo limite.

Justificação: O API Gateway aplica limitação de requisições (rate limiting) por IP e token, protegendo contra sobrecarga

Interação: Registro de ação no log.



11. Falsificação de logs de armazenamento de dados de destino de Auditoria [Estado: Mitigação implementada] [Prioridade: Média]

Categoria: Falsificação

Descrição: Os Logs de Auditoria podem ser falsificados por um invasor, o que pode fazer com que os dados sejam gravados no alvo do invasor em vez dos Logs de Auditoria. Considere usar um mecanismo de autenticação padrão para identificar o repositório de dados de destino.

Justificação: Os logs são armazenados em sistema seguro, com controle de acesso e verificação de integridade (hash ou assinatura digital).

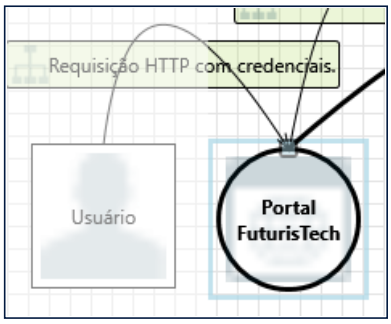
12. Potencial consumo excessivo de recursos para API Principal ou Logs de Auditoria [Estado: Mitigação implementada] [Prioridade: Média]

Categoria: Negação de serviço

Descrição: A API Principal ou o Logs de Auditoria tomam medidas explícitas para controlar o consumo de recursos? Ataques de consumo de recursos podem ser difíceis de lidar, e há momentos em que faz sentido deixar o sistema operacional fazer o trabalho. Tome cuidado para que suas solicitações de recursos não entrem em deadlock e atinjam o tempo limite.

Justificação: s logs são armazenados em sistema seguro, com controle de acesso e verificação de integridade (hash ou assinatura digital).

Interação: Requisição HTTP com credenciais.



13. Elevação usando representação [Estado: Mitigação implementada] [Prioridade: Alta]

Categoria: Elevação de Privilégio
Descrição: O Portal FuturisTech pode representar o contexto do Usuário para obter privilégios adicionais.
Justificação: As sessões temporárias e os tokens têm escopos definidos, evitando a apropriação de identidade.

14. Cross Site Scripting [Estado: Mitigação implementada] [Prioridade: Média]

Categoria: Adulteração
Descrição: O servidor web 'Portal FuturisTech' pode estar sujeito a um ataque de script entre sites porque não limpa entradas não confiáveis.
Justificação: Entradas de usuários são tratados com sanitização no backend e frontend, e CSP limita scripts externos.

15. Falsificação da entidade externa do usuário [Estado: Mitigação implementada] [Prioridade: Média]

Categoria: Falsificação
Descrição: O usuário pode ser falsificado por um invasor, o que pode levar ao acesso não autorizado ao Portal FuturisTech. Considere usar um mecanismo de autenticação padrão para identificar a entidade externa.
Justificação: Os logs são protegidos contra alteração ou exclusão, com verificação de integridade e armazenamento seguro