RELATÓRIO DE TESTE DE INTRUSÃO

Avaliação de Segurança de Aplicação Web

Sistema de Gestão Pública Municipal — Cliente Confidencial

Consultor	Daniel Gonçalves Rissi
Cliente / Autorizante	Confidencial (contrato assinado)
Escopo	Sistema Web de Gestão Municipal [Confidencial]
Data do Teste	Agosto de 2026
Classificação	CONFIDENCIAL

DOCUMENTO CONFIDENCIAL — Distribuição restrita ao autorizante

1. Sumário Executivo

Em agosto de 2026, foi conduzido um teste de intrusão autorizado contra um sistema de gestão municipal utilizado por órgão público, doravante denominado "Cliente". O teste foi realizado por Daniel Gonçalves Rissi com base em contrato de autorização assinado digitalmente por ambas as partes.

Foram identificadas quatro (4) vulnerabilidades de severidade CRÍTICA e quatro (4) de severidade MÉDIA, incluindo acesso não autorizado confirmado ao painel interno do sistema de gestão pública.

⚠ **AÇÃO IMEDIATA REQUERIDA: As vulnerabilidades críticas devem ser corrigidas antes de qualquer uso do sistema com dados reais de cidadãos.**

CRÍTICO	ALTO	MÉDIO	BAIXO
4	0	4	0

2. Escopo e Autorização

Alvos Autorizados	Sistema web de gestão municipal e subdomínios do autorizante
Fora do Escopo	CDN/WAF de terceiros, SaaS, hospedagem compartilhada de terceiros
Autorizante	Confidencial (contrato assinado digitalmente)
Executado por	Daniel Gonçalves Rissi
Autorização	Contrato formal assinado por ambas as partes — disponível mediante solicitação

3. Metodologia

O teste foi conduzido seguindo metodologia estruturada baseada nas diretrizes do PTES (Penetration Testing Execution Standard), OWASP Testing Guide e melhores práticas da indústria de segurança ofensiva:

- Pré-engajamento: Definição formal de escopo, regras de engajamento e coleta de autorização.
- Reconhecimento Passivo (OSINT): Coleta de informações via DNS, WHOIS, certificados SSL, registros SPF/MX e inteligência de fontes abertas.
- Reconhecimento Ativo: Varredura de portas e serviços, fingerprinting de aplicação, análise de headers HTTP e enumeração de endpoints.
- Análise de Vulnerabilidades: Testes manuais de autenticação, controle de acesso, validação de entrada e lógica de negócio.
- Exploração Controlada: Validação das vulnerabilidades com mínimo impacto e dentro dos limites do escopo autorizado.
- Coleta de Evidências: Documentação de respostas HTTP, comportamentos anômalos e confirmação de acessos não autorizados.
- Relatório: Documentação técnica com CVSS, impacto, evidências e recomendações de remediação priorizadas.

4. Vulnerabilidades Identificadas

F-01 — Serviço de Banco de Dados Exposto Publicamente (Porta 3306)

CRÍTICO **CVSS 9.8**

Severidade	CRÍTICO
CVSS Score	9.8
CWE	CWE-284 — Controle de Acesso Inadequado

Descrição

O servidor de banco de dados MySQL estava acessível diretamente a partir da internet pública na porta TCP 3306, sem qualquer restrição de firewall. A ausência de controle de acesso em nível de rede permite que qualquer endereço externo realize tentativas de autenticação diretamente no banco de dados.

Evidência Técnica

Conexão TCP estabelecida com sucesso ao servidor de banco de dados. O serviço respondeu com handshake de protocolo MySQL, confirmando acessibilidade externa. A resposta de autenticação retornou mensagem de erro contendo informações sobre o endereço de origem da conexão.

Impacto

Credenciais comprometidas resultariam em acesso irrestrito a todos os dados do sistema municipal. A versão em uso (MySQL 5.7) atingiu o fim de vida (EOL) e possui CVEs públicas sem correção disponível.

Recomendações de Remediação

- Bloquear a porta 3306 para endereços externos via firewall (iptables/UFW/nftables).
- Configurar o parâmetro bind-address para 127.0.0.1 no arquivo de configuração do MySQL.
- Utilizar túnel SSH ou VPN para acesso administrativo remoto ao banco de dados.
- Atualizar o MySQL 5.7 (EOL) para MySQL 8.x ou MariaDB 10.x com suporte ativo.

F-02 — Exposição de Endereço IP Real via Registro SPF — Bypass de WAF/CDN

CRÍTICO **CVSS 8.6**

Severidade	CRÍTICO
CVSS Score	8.6
CWE	CWE-200 — Exposição de Informações Sensíveis

Descrição

O registro SPF do domínio continha os endereços IP reais dos servidores de aplicação, possibilitando que um atacante identificasse e acessasse a infraestrutura diretamente, contornando completamente as proteções oferecidas pela CDN/WAF.

Evidência Técnica

Consulta DNS ao registro TXT do domínio revelou os endereços IPv4 reais dos servidores de origem. Confirmado acesso direto ao servidor utilizando o endereço IP obtido via OSINT passivo, com resposta HTTP 200 e identificação do hostname real de hospedagem.

Impacto

Todas as proteções de WAF, rate limiting e mitigação de DDoS providas pela CDN tornam-se ineficazes. O acesso direto ao servidor de origem expõe a aplicação a todos os vetores de ataque normalmente bloqueados pela camada de proteção.

Recomendações de Remediação

- Utilizar serviço de relay de email externo (SendGrid, Mailgun, Amazon SES) para não expor o IP do servidor no registro SPF.
- Configurar regra no servidor web para rejeitar requisições que não originem dos ranges de IP da CDN.
- Implementar restrição via configuração de servidor para validar o header Host das requisições.
- Revisar todos os registros DNS públicos para eliminar referências ao IP real do servidor.

F-03 — Registro de Conta Público sem Validação de Identidade

CRÍTICO **CVSS 9.1**

Severidade	CRÍTICO
CVSS Score	9.1
CWE	CWE-287 — Autenticação Inadequada

Descrição

O endpoint de registro de contas permitia a criação de usuários sem qualquer validação da identidade informada. Números de CPF fictícios foram aceitos sem consulta a base de dados governamental, e o processo não exigia aprovação administrativa prévia.

Evidência Técnica

Conta criada com sucesso utilizando CPF gerado aleatoriamente e endereço de email temporário. O sistema aceitou os dados, criou o registro e enviou email transacional confirmando o cadastro. O ID sequencial atribuído ao novo usuário revelou baixo número de usuários reais no sistema.

Impacto

Qualquer pessoa pode criar uma conta no sistema de gestão pública municipal sem nenhum vínculo com o órgão. Isso compromete o princípio de controle de acesso baseado em identidade verificada para plataformas que processam dados de cidadãos.

Recomendações de Remediação

- Desabilitar o registro público — contas devem ser criadas exclusivamente por administradores.
- Caso o registro seja necessário, implementar fluxo de aprovação administrativa antes da ativação.
- Validar o CPF informado via API da Receita Federal (consulta de situação cadastral).
- Restringir emails de cadastro ao domínio institucional do órgão público.

F-04 — Bypass de Verificação de Email via Fluxo Alternativo de Autenticação

CRÍTICO **CVSS 8.8**

Severidade	CRÍTICO
CVSS Score	8.8
CWE	CWE-306 — Ausência de Autenticação para Função Crítica

Descrição

O sistema implementava dois fluxos de autenticação distintos. O middleware de verificação de email era aplicado apenas ao fluxo de login por email, sendo completamente ignorado no fluxo alternativo por CPF, permitindo acesso pleno ao sistema sem confirmação de identidade.

Evidência Técnica

Conta criada com email não verificado. Tentativa de autenticação via email resultou em bloqueio com mensagem de endereço não verificado. Autenticação utilizando o CPF cadastrado, com a mesma conta sem verificação, concedeu acesso completo ao painel do sistema de gestão, confirmando o bypass do controle.

Impacto

A verificação de email, único mecanismo de confirmação de identidade implementado, pode ser completamente contornada. Acesso ao painel do sistema de gestão pública municipal foi confirmado sem qualquer validação de identidade real.

Recomendações de Remediação

- Aplicar o middleware de verificação em todas as rotas autenticadas, independentemente do método de login.
- Verificar o campo de confirmação de email ao autenticar por qualquer método antes de conceder acesso.
- Implementar autenticação em dois fatores (2FA) para sistemas de gestão pública.

- Unificar o guard de autenticação para que todos os fluxos passem pelas mesmas verificações de segurança.

F-05 — Endpoint de API Retorna Erro Interno do Servidor (HTTP 500)

MÉDIO	CVSS 5.3

Severidade	MÉDIO
CVSS Score	5.3
CWE	CWE-755 — Tratamento Inadequado de Condições Excepcionais

Descrição

O endpoint de perfil do usuário autenticado retornava resposta HTTP 500 em determinadas condições, em vez de resposta adequada. O erro não tratado pode expor informações de stack trace caso o modo de debug esteja habilitado no ambiente de produção.

Evidência Técnica

Requisição autenticada ao endpoint da API de usuário retornou HTTP 500 com mensagem genérica de erro do servidor. O comportamento foi reproduzido de forma consistente com conta autenticada no ambiente de produção.

Impacto

Configuração com modo debug habilitado expõe stack traces com caminhos internos, versões de bibliotecas e detalhes do banco de dados. Erros não tratados podem revelar a estrutura interna da aplicação.

Recomendações de Remediação

- Identificar e corrigir a exceção não tratada no controller ou model responsável pelo endpoint.
- Garantir que modo debug esteja desabilitado e ambiente configurado como produção.
- Implementar handler global de exceções para retornar respostas padronizadas e seguras.
- Adicionar monitoramento e alertas para erros HTTP 500 em produção.

F-06 — Divulgação Completa da Stack Tecnológica via Headers HTTP

MÉDIO	CVSS 5.3

Severidade	MÉDIO

CVSS Score	5.3
CWE	CWE-200 — Exposição de Informações Sensíveis

Descrição

Headers HTTP de resposta e comportamento da aplicação revelavam a stack tecnológica completa em uso, incluindo framework, biblioteca de autenticação, tecnologia de frontend, versão do banco de dados, versão do PHP e infraestrutura de hospedagem.

Evidência Técnica

Análise de headers HTTP e respostas da aplicação identificou todos os componentes da stack: framework web, biblioteca de autenticação, biblioteca de SPA, banco de dados com versão específica em EOL, servidor de hospedagem compartilhada e nomes padrão de cookies do framework.

Impacto

Informações detalhadas da stack permitem que atacantes direcionem exploits a versões específicas com vulnerabilidades conhecidas. A versão EOL do banco de dados possui CVEs sem correção disponível.

Recomendações de Remediação

- Remover ou suprimir headers que identificam tecnologias das respostas HTTP.
- Personalizar os nomes dos cookies para evitar fingerprinting do framework.
- Atualizar todos os componentes da stack para versões com suporte ativo.
- Implementar headers de segurança: X-Content-Type-Options, X-Frame-Options, Content-Security-Policy.

F-07 — Ausência de Segregação entre Serviços na Mesma Infraestrutura

MÉDIO **CVSS 4.3**

Severidade	MÉDIO
CVSS Score	4.3
CWE	CWE-653 — Compartimentação Insuficiente

Descrição

O servidor de email transacional, a aplicação web e o banco de dados coexistiam no mesmo servidor físico, em ambiente de hospedagem compartilhada, sem qualquer segregação entre os serviços.

Evidência Técnica

Email transacional enviado com IP de origem idêntico ao da aplicação web e do banco de dados. Varredura identificou serviços de email ativos no mesmo host da aplicação. Registro DNS de email apontando para o mesmo endereço IP do servidor de aplicação.

Impacto

Comprometimento de qualquer serviço resulta automaticamente no comprometimento de toda a infraestrutura. A hospedagem compartilhada amplifica o risco, pois outros clientes no mesmo servidor podem impactar o sistema.

Recomendações de Remediação

- Utilizar serviço de relay de email externo para desacoplar o envio de emails do servidor de aplicação.
- Migrar para ambiente com segregação de serviços: aplicação, banco de dados e email em instâncias separadas.
- Avaliar migração de hospedagem compartilhada para cloud ou VPS com controle total do ambiente.

F-08 — Enumeração Completa de Rotas da Aplicação sem Autenticação

MÉDIO	CVSS 4.3

Severidade	MÉDIO
CVSS Score	4.3
CWE	CWE-200 — Exposição de Informações Sensíveis

Descrição

A aplicação expunha o mapeamento completo de todas as rotas do sistema — incluindo rotas administrativas, de auditoria e de gestão de usuários — a qualquer requisição não autenticada, através da configuração da biblioteca de roteamento client-side.

Evidência Técnica

Requisição à página pública retornou 873 rotas completas da aplicação embutidas no HTML da resposta, incluindo rotas de administração, controle de acessos, auditoria de usuários, gestão de dados e módulos internos do sistema. Versões de módulos e nomenclaturas internas também foram expostos.

Impacto

Atacantes obtêm mapa completo da superfície de ataque sem necessidade de descoberta ativa. Rotas administrativas ficam conhecidas, facilitando ataques direcionados de escalação de privilégios e enumeração de dados sensíveis.

Recomendações de Remediação

- Filtrar as rotas expostas pelo router client-side para incluir apenas as acessíveis ao usuário atual.
- Implementar geração de lista de rotas baseada em permissões do usuário autenticado.

- Remover da resposta pública informações de versão, módulos e estrutura interna da aplicação.
- Revisar a configuração do servidor para não expor dados de estrutura antes da autenticação.

5. Conclusão e Próximos Passos

O sistema avaliado apresenta vulnerabilidades de severidade crítica que permitem acesso não autorizado ao painel de gestão pública municipal. O achado mais grave — bypass de verificação de identidade com acesso confirmado ao sistema — demonstra ausência de controles de autenticação adequados para uma plataforma que processa dados de cidadãos.

Recomenda-se a seguinte ordem de prioridade para remediação:

- Imediato (0–7 dias): Fechar porta 3306 para acesso externo e aplicar middleware de verificação em todos os fluxos de autenticação (F-01 e F-04).
- Curto prazo (7–30 dias): Desabilitar registro público ou implementar validação de identidade e eliminar exposição de IP via registro DNS (F-02 e F-03).
- Médio prazo (30–90 dias): Endereçar os achados de severidade média, incluindo atualização da stack tecnológica e segregação de serviços (F-05 a F-08).

Recomenda-se nova avaliação de segurança após a implementação das correções para validar a efetividade das remediações aplicadas.

Daniel Gonçalves Rissi
Consultor de Segurança Ofensiva
20/08/2026

Autorização:
Contrato assinado — disponível mediante solicitação