CONFIDENCIAL · RELATÓRIO TÉCNICO

Teste de Intrusão Aplicação web e API

Exemplo Pagamentos Ltda. (empresa fictícia)

CLIENTE	Exemplo Pagamentos Ltda.
ESCOPO	app.exemplo-pagamentos.test (aplicação web) e api.exemplo-pagamentos.test (API REST)
ABORDAGEM	Gray box: duas contas de teste (cliente e operador), sem código-fonte
PERÍODO	10 a 17 de março de 2026 · reteste em 31 de março de 2026
VERSÃO	1.1 (após reteste)
RESPONSÁVEL	Matheus Brunheroto · intoIT · contato@intoitsec.com

> Este documento é um **exemplo ilustrativo**. Empresa, sistemas, endereços e achados são fictícios e foram criados apenas para mostrar a estrutura e o nível de detalhe dos relatórios da intoIT. Os relatórios reais são entregues sob acordo de confidencialidade e nunca são publicados.

Sumário executivo

A intoIT realizou um teste de intrusão na aplicação web e na API da Exemplo Pagamentos entre 10 e 17 de março de 2026, com acesso a contas de teste (gray box). O objetivo foi identificar falhas que um atacante externo, com ou sem conta, poderia explorar para acessar dados de clientes ou movimentar valores.

Resultado em uma linha: um atacante com qualquer conta de cliente conseguia ler pedidos e dados cadastrais de todos os demais clientes (F-01), e a combinação de senha redefinível por token previsível (F-02) com ausência de limite de tentativas no login (F-03) permitia tomar contas sem interação da vítima.

1	2	3	2	8
CRÍTICA	ALTAS	MÉDIAS	BAIXAS	TOTAL

O que mais importa

- **Corrigir F-01 primeiro.** Exposição direta de dados pessoais e financeiros de clientes; impacto regulatório (LGPD) além do técnico. Correção simples: verificar o dono do recurso no servidor.
- **F-02 e F-03 juntas formam uma cadeia** de tomada de conta. Tratar as duas na mesma sprint.
- Os demais achados são higiene: cabeçalhos, mensagens de erro e configuração. Baixo esforço, fecham portas usadas em ataques oportunistas.

Pontos positivos

- Nenhuma injeção de SQL ou de comando encontrada nos 42 endpoints testados.
- Pagamentos usam idempotência e validação de valores no servidor; não foi possível alterar valores de cobrança.
- Senhas armazenadas com bcrypt (confirmado pelo time) e autenticação em duas etapas disponível para operadores.

Situação após o reteste (31/03)

Sete dos oito achados foram corrigidos e revalidados. F-08 (cookies sem SameSite) permanece aberto por decisão do cliente, com prazo interno de abril. O risco residual é baixo.

Lista de achados

Severidade segundo CVSS 3.1 ajustada ao contexto do negócio (ver seção 04). Estado conforme o reteste de 31/03/2026.

ID	ACHADO	SEVERIDADE	CVSS	ESTADO
F-01	Referência insegura a objeto (IDOR) na API de pedidos expõe pedidos e dados de outros clientes	CRÍTICA	8.5	Corrigido
F-02	Token de redefinição de senha previsível (timestamp) e sem expiração	ALTA	8.1	Corrigido
F-03	Login sem limite de tentativas nem bloqueio progressivo	ALTA	7.5	Corrigido
F-04	Upload de comprovante aceita SVG com script (XSS armazenado no painel do operador)	MÉDIA	6.1	Corrigido
F-05	Cabeçalhos de segurança ausentes (CSP, HSTS, X-Content-Type-Options)	MÉDIA	5.3	Corrigido
F-06	Enumeração de usuários pela mensagem do "esqueci minha senha"	MÉDIA	5.3	Corrigido
F-07	Versão do servidor e do framework expostas em cabeçalhos e páginas de erro	BAIXA	3.7	Corrigido
F-08	Cookie de sessão sem atributo SameSite	BAIXA	3.1	Aberto

Como ler cada achado

Cada item da lista tem, na seção seguinte, a mesma estrutura: descrição, evidência reproduzível (requisição e resposta, com dados mascarados), impacto para o negócio, correção recomendada, referências e o resultado do reteste. A página 4 mostra o achado F-01 completo como exemplo; os demais seguem o mesmo formato.

F-01 · IDOR na API de pedidos CRÍTICA

CVSS 3.1	8.5 · AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:L/A:N
ALVO	`GET /v1/orders/{id}` em api.exemplo-pagamentos.test
CATEGORIA	OWASP Top 10 2021 A01 · Broken Access Control · CWE-639

Descrição

O endpoint de consulta de pedido valida apenas se o token de sessão é válido, não se o pedido pertence ao cliente autenticado. Os identificadores são sequenciais, então basta variar o número para percorrer todos os pedidos da base.

Evidência

Autenticado como a conta de teste `cliente-a` (pedidos 4180 a 4183), a requisição abaixo retorna o pedido 4179, que pertence a outro cliente:

```
GET /v1/orders/4179 HTTP/1.1
Host: api.exemplo-pagamentos.test
Authorization: Bearer eyJhbGciOi…(token de cliente-a)

HTTP/1.1 200 OK
{"id":4179,"customer":{"name":"M*** S****","cpf":"***.482.***-**","email":"m***@****.com"},
 "amount":1290.00,"card_last4":"4421","status":"paid","address":{"city":"Curitiba", …}}
```

Um script simples enumerou 500 pedidos em 40 segundos sem nenhum bloqueio. A listagem foi interrompida após a confirmação; nenhum dado foi armazenado.

Impacto

Qualquer pessoa com uma conta gratuita lê nome, CPF parcial, e-mail, endereço, valor e últimos dígitos do cartão de todos os clientes. Além do dano direto, é incidente de segurança com dados pessoais sob a LGPD, com obrigação de notificação.

Correção

- No servidor, carregar o pedido sempre filtrando pelo cliente da sessão (`WHERE id = ? AND customer_id = ?`) e responder 404 quando não houver correspondência.
- Aplicar a mesma verificação em todos os endpoints que recebem um id de recurso (pedidos, comprovantes, endereços); o teste encontrou o mesmo padrão em `/v1/receipts/{id}`, corrigido junto.

Reteste (31/03/2026)

Corrigido. O endpoint responde 404 para pedidos de outros clientes; a enumeração de 500 ids não retornou nenhum registro alheio.

Metodologia, escopo e critérios

Regras do engajamento

- Autorização por escrito assinada em 05/03/2026, com os alvos listados.
- Janela de testes: dias úteis, 9h às 19h, com contato técnico de plantão.
- Fora do escopo: negação de serviço, engenharia social, ambientes de terceiros (gateway do adquirente, provedor de e-mail).
- Achados críticos comunicados assim que confirmados (F-01 foi reportado em 11/03).

Fases

- Reconhecimento: mapa da aplicação, endpoints, tecnologias, superfície exposta.
- Análise manual guiada pelo OWASP WSTG e OWASP API Security Top 10: autenticação,

Ferramentas

Burp Suite Professional, ffuf, nuclei, sqlmap, scripts próprios. Ferramentas automatizadas só apoiam o reconhecimento; todo achado listado foi reproduzido manualmente.

Classificação de severidade

SEVERIDADE	CVSS	LEITURA
CRÍTICA	9.0 a 10	Exposição ampla de dados ou controle do sistema; corrigir imediatamente
ALTA	7.0 a 8.9	Tomada de conta ou dado sensível; corrigir na sprint atual
MÉDIA	4.0 a 6.9	Requer condições ou interação; planejar
BAIXA	0.1 a 3.9	Higiene e defesa em profundidade

A severidade parte da faixa do CVSS e pode subir um nível pelo contexto do negócio: F-01 (CVSS 8.5) ficou Crítica por expor dados pessoais de todos os clientes.

Limitações

Teste pontual, no estado do sistema entre 10 e 17/03/2026. Mudanças posteriores não estão cobertas. Um pentest reduz o risco; não garante ausência de falhas.