RET-PT-2026-001 · VERSÃO 1.1

Relatório de teste de intrusão

Loja Exemplo Ltda

> Encontramos 1 falha de risco alto que permitia a um cliente logado ler pedidos de outros clientes. Nenhuma falha permite movimentar dinheiro ou assumir conta.

3 ACHADOS, 0 EM ABERTO. CADA FALHA NA NOTA DE GRAVIDADE, DE 0 A 10. PONTO CHEIO: EM ABERTO. PONTO VAZADO: CORRIGIDA OU ACEITA.



PERÍODO DO TESTE	EMITIDO EM	DESTINATÁRIO	RESPONSÁVEL TÉCNICO
03/11/2026 a 07/11/2026	16/11/2026	Diretoria de Tecnologia	Gabriel Lima Ferreira

RET TECNOLOGIA EM INFORMATICA LTDA · CNPJ 61.709.429/0001-47 · Rua Pais Leme, 215, conjunto 1713, Pinheiros, São Paulo/SP

Relatório de exemplo. A empresa, os endereços e os dados são fictícios.

Sumário

01	Controle do documento
02	Resumo para quem decide
03	Autorização, escopo e limites
04	Metodologia e escala de risco
05	Como o teste se desenrolou
06	Dados pessoais no teste (LGPD)
07	Achados
08	Nova verificação das correções
09	Uso deste relatório como evidência
10	Declarações e assinatura

01 Controle do documento

VERSÕES

VERSÃO	DESCRIÇÃO	DATA	AUTOR
1.0	Relatório inicial	07/11/2026	Gabriel Lima Ferreira
1.1	Inclui o resultado da nova verificação	16/11/2026	Gabriel Lima Ferreira

CLASSIFICAÇÃO E MANUSEIO

Este documento é **confidencial**. Descreve falhas que podem ser exploradas enquanto não forem corrigidas.

- Circula só entre as pessoas que precisam dele para decidir ou corrigir.
- É entregue em PDF protegido por senha, e a senha segue por outro canal.
- Senha, token, chave e dado pessoal aparecem mascarados nas evidências.
- A RET destrói as cópias de trabalho em até 15 dias depois da entrega, como prevê o acordo de confidencialidade, e guarda só o relatório final.

EQUIPE

Gabriel Lima Ferreira, sócio-administrador e responsável técnico da RET. Formação: Especialização CompTIA PenTest+ (Total Seminars) e Hands-On Web App Pentesting (Packt).

02 Resumo para quem decide

RESULTADO

Encontramos 1 falha de risco alto que permitia a um cliente logado ler pedidos de outros clientes. Nenhuma falha permite movimentar dinheiro ou assumir conta.

COMO LER

Gravidade

Uma nota de 0 a 10 para cada falha, calculada pelo padrão internacional CVSS 4.0. Quanto maior, mais fácil de explorar e maior o estrago. De 7 para cima é alta, de 9 para cima é crítica.

Situação

Em aberto: ainda não corrigida. Corrigida: a RET repetiu o teste e a falha não aparece mais. Risco aceito: o cliente decidiu não corrigir agora.

Nome técnico

Cada falha tem um título em palavras simples e, abaixo, o nome que o desenvolvedor usa para procurar a correção.

ACHADOS POR RISCO

0	1	1	1	0
CRÍTICO	ALTO	MÉDIO	BAIXO	INFORMATIVO

Cada falha na nota de gravidade, de 0 a 10. Ponto cheio: em aberto. Ponto vazado: corrigida ou aceita.



OBJETIVO

Verificar, antes da campanha de fim de ano, se um cliente da loja consegue ver ou alterar dados e pedidos de outro cliente, e se o checkout aceita valor ou desconto adulterado.

O QUE ISSO SIGNIFICA PARA O NEGÓCIO

- Qualquer cliente logado conseguia ler nome, endereço e itens de pedidos alheios trocando um número na URL. Isso é exposição de dado pessoal de clientes da loja.
- A tela de login informava se um e-mail tinha conta, o que facilita tentativa de senha em massa contra clientes reais.

O QUE FAZER PRIMEIRO

1. Conferir no servidor, em toda rota de pedido, que o pedido pertence a quem está logado.
2. Responder do mesmo jeito no login e na recuperação de senha, exista a conta ou não.
3. Incluir, na revisão de cada rota nova, um teste automatizado que tenta ler dado de outra conta.

PARA NÃO REPETIR

- Centralizar a conferência de dono do recurso em um único ponto da API, em vez de repetir a regra em cada rota.
- Tratar em transação, com restrição no banco, toda operação que só pode acontecer uma vez por pedido.
- Repetir o teste de intrusão a cada mudança grande no checkout ou no login, e pelo menos uma vez por ano.

O QUE JÁ ESTÁ BEM RESOLVIDO

- Senhas guardadas com algoritmo adequado e sem retorno em nenhuma resposta da API.
- Sessão expira e é invalidada no servidor depois do logout.
- Valor do pedido é recalculado no servidor: alterar o preço na requisição não muda o total cobrado.

03 Autorização, escopo e limites

AUTORIZAÇÃO

O teste foi executado com autorização escrita de quem responde pelos ativos: termo de autorização nº **RET-PT-2026-001-TA**, assinado por Diretor de Tecnologia da Loja Exemplo Ltda em 30/10/2026.

O art. 154-A do Código Penal trata como crime o acesso a sistema alheio sem autorização de quem o usa. Por isso nenhum acesso aconteceu antes da assinatura nem fora do que o termo lista.

ESCOPO

ATIVO	AMBIENTE	MODALIDADE
`https://app.lojaexemplo.com.br`	Homologação, espelho da produção	Caixa-cinza, com duas contas de cliente de teste
`https://api.lojaexemplo.com.br/v1`	Homologação, espelho da produção	Caixa-cinza, com documentação da API

FORA DO ESCOPO

- Painel administrativo interno
- Aplicativo móvel
- Teste de carga e de negação de serviço
- Engenharia social

LIMITAÇÕES

- O gateway de pagamento foi testado só em modo de teste, sem transação real.

JANELA

De 03/11/2026 a 07/11/2026, horário de Brasília. Horas de teste: 25.

ALCANCE

O teste é uma avaliação pontual, feita no período e no escopo acima. O ambiente pode ter mudado depois. Nenhum teste garante que todas as falhas foram encontradas. Este relatório registra fatos e não é parecer de conformidade nem certificação.

04 Metodologia e escala de risco

MÉTODO

O trabalho segue o OWASP Web Security Testing Guide (WSTG) para aplicação web e o OWASP API Security Top 10 para APIs. A maior parte do teste é manual. Ferramenta automática e modelo de linguagem entram como apoio, para mapear a superfície e repetir requisições. Decidir o que explorar, encadear falhas e provar o impacto é trabalho do pentester, e todo achado deste relatório foi reproduzido à mão. Dado do cliente e evidência de falha não são usados para treinar modelo público.

Cada achado recebe nota pelo CVSS 4.0, com o vetor completo, para que o cálculo possa ser refeito por quem lê.

O QUE FOI TESTADO

ÁREA	O QUE FOI VERIFICADO	RESULTADO
Controle de acesso WSTG-ATHZ · API1, API5	Leitura e alteração de pedido, endereço e cartão salvo de outra conta; acesso a rota de administrador com conta comum.	**FALHA** RET-001-01
Identidade e login WSTG-IDNT, WSTG-ATHN · API2	Enumeração de contas, bloqueio por tentativa, recuperação de senha e troca de e-mail.	**FALHA** RET-001-02
Sessão WSTG-SESS	Expiração, invalidação no logout, fixação de sessão e atributos do cookie.	**SEM FALHA**
Lógica de negócio WSTG-BUSL · API6	Alteração de preço e quantidade, cupom, frete e requisições simultâneas no checkout.	**FALHA** RET-001-03
Entrada de dados WSTG-INPV · API8	Injeção em busca, filtros e campos de cadastro; script em campos exibidos a outros usuários.	**SEM FALHA**
Exposição de dados WSTG-CRYP, WSTG-ERRH · API3	Campos devolvidos a mais pela API, mensagens de erro, transporte cifrado.	**SEM FALHA**
Configuração WSTG-CONF · API8	Cabeçalhos de segurança, métodos HTTP, arquivos e rotas esquecidas.	**SEM FALHA**

"Sem falha" quer dizer que os testes feitos nessa área, no tempo e no escopo deste trabalho, não encontraram problema. Não é garantia de ausência de falha.

ESCALA DE RISCO

RISCO	CVSS 4.0	SIGNIFICADO
CRÍTICO	9.0 a 10.0	Exploração direta, com impacto grave em dado, dinheiro ou disponibilidade
ALTO	7.0 a 8.9	Exploração viável, com impacto relevante
MÉDIO	4.0 a 6.9	Exige condição específica ou tem impacto limitado
BAIXO	0.1 a 3.9	Impacto pequeno ou exploração improvável
INFORMATIVO	0.0	Observação de boa prática, sem falha explorável

05 Como o teste se desenrolou

NARRATIVA

Com uma conta comum de cliente, abrimos um pedido próprio e observamos que a API identifica o pedido só pelo número. Trocando o número, a API devolveu o pedido de outra conta de teste.

A partir daí verificamos as demais rotas que recebem identificador. Endereço e cartão salvo conferem o dono corretamente. O problema ficou restrito à rota de pedidos.

No checkout, tentamos alterar preço, quantidade negativa e desconto. O total é recalculado no servidor, mas o mesmo cupom foi aceito duas vezes quando enviado em requisições simultâneas.

06 Dados pessoais no teste (LGPD)

PAPEL DA RET

Neste trabalho a RET atua como **operadora**: acessa dado pessoal só por ordem do cliente, que é o controlador, e só para a finalidade do teste (LGPD, arts. 5º, VII, e 39).

DADOS QUE APARECERAM

- Nome, endereço de entrega e itens de pedido de duas contas de teste criadas para o trabalho

O teste rodou em homologação com dados fictícios. Nenhum dado de cliente real foi acessado.

A RET não copiou, guardou nem usou dado pessoal real para outra finalidade.

ACHADOS QUE EXPÕEM DADO PESSOAL

ID	ACHADO	RISCO
RET-001-01	Pedido de outro cliente acessível pelo ID	ALTO
RET-001-02	Mensagem de erro revela se o e-mail tem conta	MÉDIO

O QUE CABE AO CONTROLADOR

Uma falha que expõe dado pessoal não é, só por existir, um incidente. Cabe ao cliente verificar nos próprios registros se alguém a explorou antes da correção.

Se houve acesso indevido que possa trazer risco ou dano relevante aos titulares, a LGPD (art. 48) e a Resolução CD/ANPD nº 15/2024 pedem comunicação à ANPD e aos titulares em três dias úteis, contados de quando o controlador toma conhecimento. O prazo é contado em dobro para agente de pequeno porte. O registro do incidente fica guardado por pelo menos cinco anos, mesmo quando não há comunicação.

07 Achados

LISTA

ID	FALHA	GRAVIDADE	NOTA	SITUAÇÃO
RET-001-01	Um cliente conseguia abrir o pedido de outro	ALTO	7.1	Corrigido
RET-001-02	A tela de login revelava quem tem conta	MÉDIO	6.9	Risco aceito pelo cliente
RET-001-03	O mesmo cupom de desconto valia duas vezes	BAIXO	2.3	Corrigido

O prazo de cada correção é decisão do cliente e entra no plano de ação. A ordem recomendada considera a gravidade e também se o sistema está exposto à internet e se a falha pode ser explorada de forma automática, os mesmos critérios que a diretiva BOD 26-04 da agência de cibersegurança dos Estados Unidos (CISA, junho de 2026) adotou no lugar do prazo fixo por gravidade.

RET-001-01

7.1

GRAVIDADE ALTA

NOTA DE 0 A 10

Um cliente conseguia abrir o pedido de outro

Nome técnico: Pedido de outro cliente acessível pelo ID



SITUAÇÃO	**Corrigido**. Nova verificação em 14/11/2026: Corrigido. A mesma requisição passou a devolver 404.
ATIVO AFETADO	`GET /api/orders/{id}`
DESCRIÇÃO	A rota devolve o pedido pelo número, sem conferir se ele pertence ao usuário da sessão.
IMPACTO	Qualquer cliente logado lê nome, endereço e itens de pedidos de outros clientes. Como os números são sequenciais, dá para percorrer todos os pedidos da loja.
ESFORÇO DO ATACANTE	Baixo. Basta uma conta comum e trocar um número na URL.
ESFORÇO PARA CORRIGIR	Poucas horas de desenvolvimento, mais o teste automatizado. É uma estimativa: quem conhece o código confirma.
DADO PESSOAL	Sim. Ver a seção 6.

COMO REPRODUZIR

1. Entrar com a conta de teste A e abrir um pedido próprio.
2. Trocar o número do pedido na URL pelo de um pedido da conta de teste B.
3. A resposta traz o pedido de B.

```
GET /api/orders/10482 HTTP/1.1
Host: api.lojaexemplo.com.br
Authorization: Bearer eyJ…[token da conta A, mascarado]

HTTP/1.1 200 OK
{"id":10482,"customer":{"name":"C***
B***","email":"c***@exemplo.com"},"address":"Rua ***, 1**","items":[…]}
```

CORREÇÃO RECOMENDADA

> Conferir no servidor que o pedido pertence ao usuário da sessão antes de responder, e devolver 404 quando não pertencer. Criar um teste automatizado que tenta ler o pedido de outra conta.

CLASSIFICAÇÃO

CWE-639 · OWASP API1:2023

`CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:N/VC:H/VI:N/VA:N/SC:N/SI:N/SA:N`

REFERÊNCIAS

- https://cwe.mitre.org/data/definitions/639.html
- https://owasp.org/API-Security/editions/2023/en/0xa1-broken-object-level-authorization/

RET-001-02

6.9

GRAVIDADE MÉDIA

NOTA DE 0 A 10

A tela de login revelava quem tem conta

Nome técnico: Mensagem de erro revela se o e-mail tem conta



SITUAÇÃO	**Risco aceito pelo cliente**. Nova verificação em 14/11/2026: Risco aceito pelo cliente, que vai tratar na próxima versão.
ATIVO AFETADO	`POST /api/auth/login e POST /api/auth/forgot`
DESCRIÇÃO	O login responde "usuário não encontrado" para e-mail sem conta e "senha incorreta" para e-mail com conta. A recuperação de senha faz a mesma distinção.
IMPACTO	Um atacante confirma quais e-mails são clientes da loja e concentra neles a tentativa de senha e o phishing.
ESFORÇO DO ATACANTE	Baixo. Não exige conta.
ESFORÇO PARA CORRIGIR	Poucas horas de desenvolvimento. É uma estimativa: quem conhece o código confirma.
DADO PESSOAL	Sim. Ver a seção 6.

COMO REPRODUZIR

1. Enviar o login com um e-mail sem cadastro e anotar a mensagem.
2. Enviar o login com o e-mail da conta de teste A e senha errada.
3. As duas respostas são diferentes.

```
POST /api/auth/login HTTP/1.1
{"email":"naoexiste@exemplo.com","password":"x"}
→ 404 {"error":"Usuário não encontrado"}

POST /api/auth/login HTTP/1.1
{"email":"a***@exemplo.com","password":"x"}
→ 401 {"error":"Senha incorreta"}
```

CORREÇÃO RECOMENDADA

> Devolver a mesma mensagem e o mesmo código nos dois casos, com tempo de resposta parecido. Na recuperação de senha, responder sempre que o e-mail será enviado se a conta existir.

CLASSIFICAÇÃO

CWE-204 · OWASP WSTG-IDNT-04

`CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N`

REFERÊNCIAS

- https://cwe.mitre.org/data/definitions/204.html

RET-001-03

2.3

GRAVIDADE BAIXA

NOTA DE 0 A 10

O mesmo cupom de desconto valia duas vezes

Nome técnico: Cupom aplicado mais de uma vez em requisições paralelas



SITUAÇÃO	**Corrigido**. Nova verificação em 14/11/2026: Corrigido. Em 50 requisições simultâneas, só uma foi aceita.
ATIVO AFETADO	`POST /api/cart/coupon`
DESCRIÇÃO	A verificação de uso do cupom e a gravação do uso não acontecem na mesma operação. Duas requisições enviadas ao mesmo tempo passam pela verificação antes de qualquer uma gravar.
IMPACTO	Um cliente aplica duas vezes um cupom de uso único. O prejuízo por pedido é limitado ao valor do cupom.
ESFORÇO DO ATACANTE	Médio. Exige enviar requisições simultâneas com ferramenta.
ESFORÇO PARA CORRIGIR	Um dia de desenvolvimento, por mexer em transação no banco. É uma estimativa: quem conhece o código confirma.
DADO PESSOAL	Não envolve.
COMO REPRODUZIR	1. Colocar um item no carrinho da conta de teste A. 2. Enviar 10 requisições simultâneas aplicando o mesmo cupom. 3. O desconto aparece duas vezes no total.

```
POST /api/cart/coupon HTTP/1.1  (10 requisições em paralelo)
{"code":"BEMVINDO10"}
→ 2 respostas 200, 8 respostas 409
```

CORREÇÃO RECOMENDADA	Verificar e gravar o uso do cupom na mesma transação, com restrição de unicidade por pedido e cupom no banco.
CLASSIFICAÇÃO	CWE-362 · OWASP WSTG-BUSL-07 `CVSS:4.0/AV:N/AC:H/AT:P/PR:L/UI:N/VC:N/VI:L/VA:N/SC:N/SI:N/SA:N`
REFERÊNCIAS	• https://cwe.mitre.org/data/definitions/362.html

08 Nova verificação das correções

ALCANCE

A nova verificação cobre só os achados deste relatório. Funcionalidade nova fica fora e entra num novo escopo.

RESULTADO

ID	ACHADO	DATA	RESULTADO
RET-001-01	Pedido de outro cliente acessível pelo ID	14/11/2026	Corrigido. A mesma requisição passou a devolver 404.
RET-001-02	Mensagem de erro revela se o e-mail tem conta	14/11/2026	Risco aceito pelo cliente, que vai tratar na próxima versão.
RET-001-03	Cupom aplicado mais de uma vez em requisições paralelas	14/11/2026	Corrigido. Em 50 requisições simultâneas, só uma foi aceita.

09 Uso deste relatório como evidência

COMO USAR

Este relatório pode ser apresentado como evidência dos controles abaixo. A decisão sobre conformidade é do auditor ou da própria instituição.

CONTROLES

REFERÊNCIA	CONTROLE	OBSERVAÇÃO
Res. CMN nº 4.893/2021 e Res. BCB nº 85/2021, Art. 22-A	Teste de intrusão anual, independente e documentado	Aplicável só a instituição autorizada pelo Banco Central.
Mesmas resoluções, Art. 23, X	Guarda da documentação dos testes e dos planos de ação	Cinco anos, contados da data de execução do teste. A guarda é da instituição.
ISO/IEC 27001:2022, Anexo A 8.8	Gestão de vulnerabilidades técnicas	A norma não cita teste de intrusão. O teste entra como evidência.
SOC 2, critérios CC4.1 e CC7.1	Avaliação dos controles e detecção de vulnerabilidades	O CC4.1 cita teste de intrusão como exemplo de avaliação, sem obrigar. Aceite a critério do auditor.
PCI DSS v4.0.1, requisito 11.4	Teste de intrusão externo e interno	Só vale se o escopo incluir o ambiente de dados de cartão.
LGPD, art. 46	Medidas técnicas para proteger dado pessoal	O teste é uma das medidas e registra a diligência do controlador.

10 Declarações e assinatura

INDEPENDÊNCIA	A RET não participou do desenvolvimento, da operação nem da manutenção dos sistemas testados, não tem vínculo societário, de emprego ou de subordinação com a equipe responsável por eles, e executou o teste com autonomia técnica sobre método e resultado.
VERACIDADE	As evidências deste relatório foram obtidas pela RET, no período e no escopo indicados, e não foram alteradas além do mascaramento de dado sensível.
ASSINATURA	São Paulo, 16/11/2026.

Gabriel Lima Ferreira
sócio-administrador e responsável técnico
RET TECNOLOGIA EM INFORMATICA LTDA · CNPJ 61.709.429/0001-47
Rua Pais Leme, 215, conjunto 1713, Pinheiros, São Paulo/SP
contato@rettecnologia.org