


Compilado (Resultados, Issues e Melhorias)

Informações Gerais [↗](#)

Item	Descrição
Projeto	Serverest
Período de Execução	5 de mai. de 2025 – 9 de mai. de 2025
URL / Acesso	 ServeRest
Sistema Operacional	Windows 10
Responsável	Karen K.



Resumo Executivo





Durante o período de testes no módulo de Produtos da API ServeRest, foram avaliados fluxos principais, regras críticas de negócio e segurança. Foram identificadas falhas graves relacionadas à autenticação e manipulação de produtos, com risco potencial para segurança e integridade de dados.

Resultados [↗](#)

- **Total de Cenários Planejados:** 32
- **Cenários Executados:** 17
- **Cobertura de Testes:** 53%
- **Critérios de Priorização:**
 - Fluxos principais (happy path)
 - Regras críticas de negócio (e-mail, senha, duplicidade)
 - Testes negativos de segurança (ex: ausência de token, token expirado)
 - PUTs com ID inexistente







Issues Relevantes Encontradas [↗](#)

ID Issue	Título da Issue	Descrição	Severidade	Status	Evidência (Print/Link/Log)	Notas Técnicas / Observações
I001	Token expirado	Token expirado foi aceito em	Crítica			O token expirou conforme o

	permite acesso	rota protegida, permitindo acesso indevido				JWT, mas a rota GET /rota protegida retornou 200 OK
I002	Produto não criado com token válido	Mesmo com token válido, POST /produtos retornou 401 Unauthorized	Alta	EM ANÁLISE		Suspeita de token mal formatado ou erro no cabeçalho Authorization
I003	Senha com mais de 10 caracteres é aceita em alguns casos	Em alguns testes, senhas com 11 caracteres estão sendo aceitas (201 Created), violando a regra de no máximo 10. O comportamento varia conforme o valor do campo administrador.	Alta	ABERTA		Pode indicar falha na ordem ou condição da validação do payload. Sugere-se revisar a regra de negócios aplicada no back-end.
I004	Criar usuário com domínio de e-mail inválido (Gmail/Hotmail)	Mesmo com domínio restrito, POST /usuarios permitiu criação do usuário	Alta	ABERTA		Falha na validação de domínio de e-mail conforme regra de negócio.
I005	Criar usuário com senha menor que 5 caracteres	Senhas com menos de 5 caracteres estão sendo aceitas (201 Created), violando a regra de no máximo 5. O	Alta	ABERTA		Pode indicar falha na ordem ou condição da validação do payload. Sugere-se revisar a regra de

		comportamento varia conforme o valor do campo administrador.				negócios aplicada no back-end.
--	--	--	--	--	--	--------------------------------

Evidências Positivas [🔗](#)

Título	Status	Evidência (Print/Link/Log)
Criar usuário com dados válidos	CONCLUÍDO	
Criar usuário com e-mail duplicado	CONCLUÍDO	
Atualizar usuário com ID inexistente	CONCLUÍDO	
Atualizar usuário com e-mail já utilizado	CONCLUÍDO	
Login com usuário inexistente	CONCLUÍDO	
Login com senha inválida	CONCLUÍDO	

Melhorias e Recomendações [🔗](#)

- Corrigir falha na autenticação de produtos:** validar consistência na geração e uso do token de login.
- Ajustar tratamento de token expirado:** endpoint protegido aceita token inválido, gerando risco crítico de segurança.
- Implementar mensagens de erro mais específicas:** melhorar feedback em casos de erro 401, 400 e 422.
- Revisar documentação Swagger:** há ambiguidade entre o comportamento esperado e o descrito (ex: PUT criando recursos).
- Priorizar automação dos fluxos críticos e negativos:** ganho de produtividade e rastreabilidade.

Limitações ou Restrições Identificadas [🔗](#)

Observações Finais [🔗](#)

Durante a execução dos testes relacionados aos endpoints da API de Produtos, foram identificadas respostas inesperadas de 401 Unauthorized, mesmo em cenários autenticados. Considera-se a possibilidade de que a passagem do token de autenticação não tenha sido realizada corretamente, o que compromete a validação precisa de algumas regras de negócio esperadas.

Devido à limitação de tempo para reexecução e ajustes, os cenários foram documentados conforme o comportamento obtido. Recomenda-se revisão e revalidação futura com a garantia de autenticação adequada.