

Título: Exposição de Token JWT da API do TheMovieDB no Front-End Público

Site: [Movies Catalog](https://movies-catalog-opal.vercel.app)

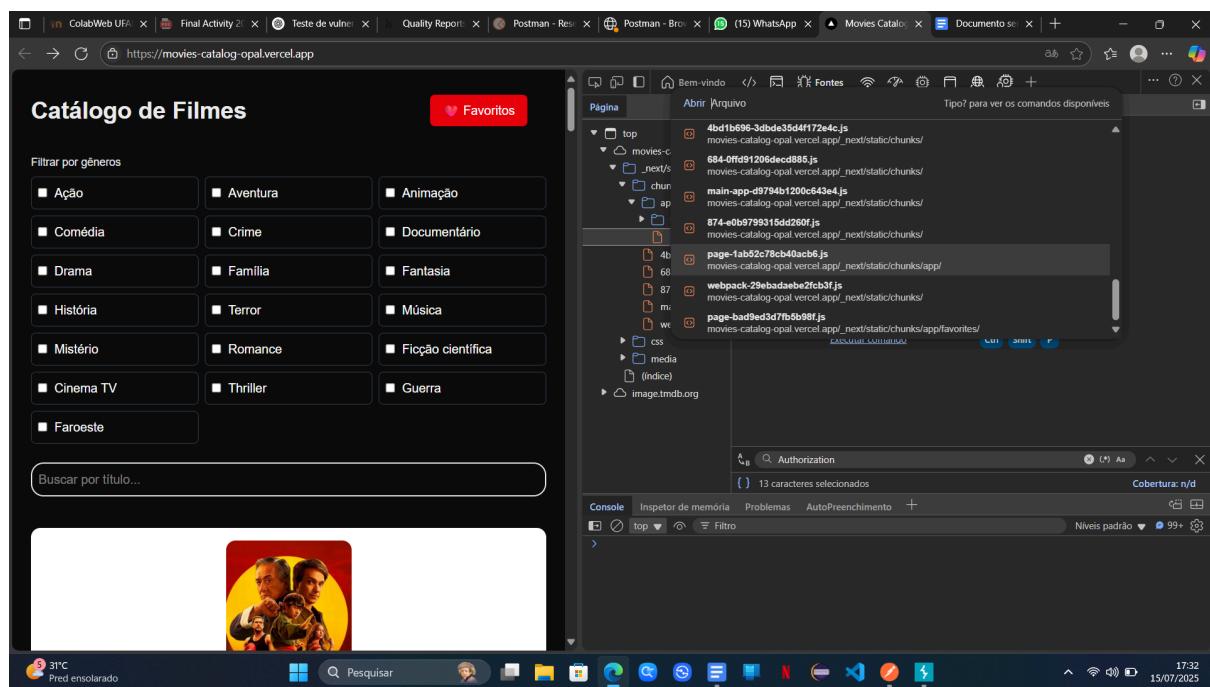
Resumo:

A aplicação <https://movies-catalog-opal.vercel.app> incorpora diretamente um token JWT da API do TheMovieDB no código JavaScript acessível ao público. Isso permite que qualquer usuário reutilize esse token para fazer requisições autenticadas como se fosse a aplicação, violando os princípios de segurança de APIs públicas.

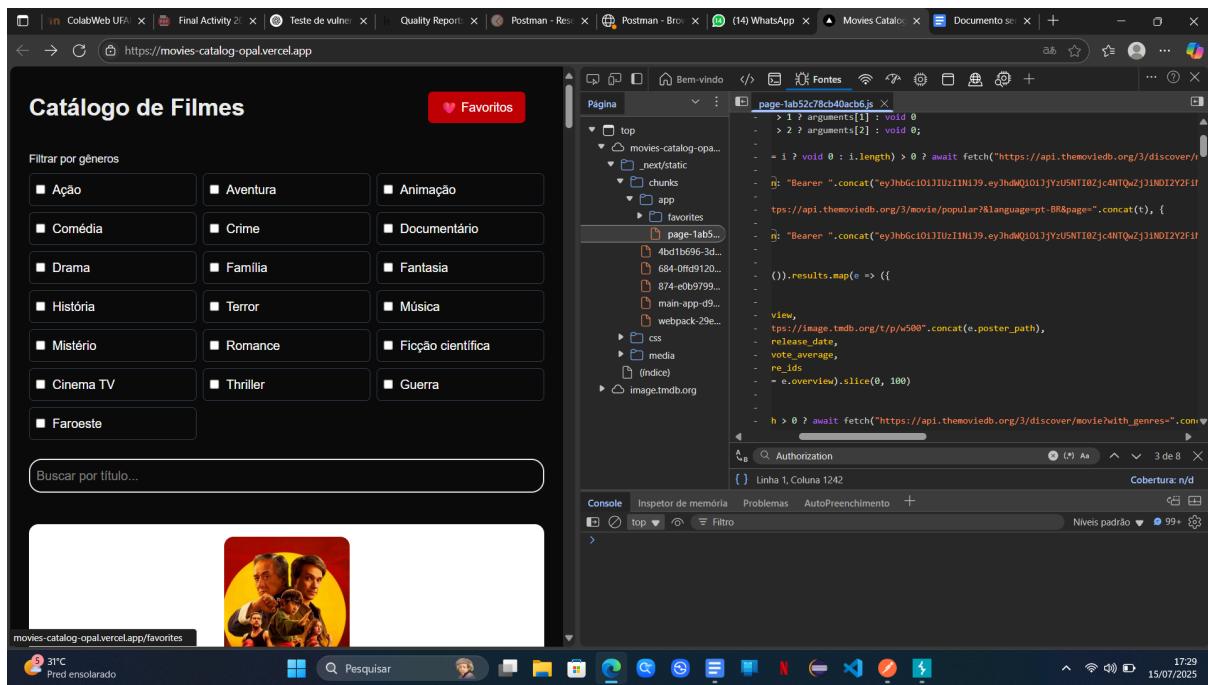
PASSO-A-PASSO:

1-Acesse o site <https://movies-catalog-opal.vercel.app>

2-Abra o DevTools com F12, vá em **Sources**, e abra [page-1ab52c78cb40acb6.js](#)



3-Procure pelo termo **Authorization**



4-Copie o token JWT presente nas chamadas `fetch()`

5-No Postman, envie a seguinte requisição:

```

{
  "adult": false,
  "backdrop_path": "/nkyBbFSooRPTJvqjz0te0l1F733.jpg",
  "genre_ids": [
    28,
    12,
    18
  ],
  "id": 1011477,
  "original_language": "en",
  "original_title": "Karate Kid: Legends",
  "overview": "Ap\u00f3s uma trag\u00e9dia familiar, o prodigo do kung fu Li Fong \u00e9 for\u00e7ado a deixar sua casa em Pequim e se mudar para Nova York com sua m\u00e3e. Li luta para deixar o passado para tr\u00e1s enquanto tenta se entrosar com seus novos colegas de classe, e, embora n\u00e3o queira brigar, os problemas parecem encontr\u00e1-lo por toda parte. Quando um novo am\u00f3go precisa de sua ajuda, Li se joga em uma competi\u00e7\u00e3o de karat\u00e9 — mas suas habilidades sozinhas n\u00e3o s\u00fao suficientes. O professor de kung fu de Li, Sr. Han, recruta o lend\u00e1rio Karat\u00e9 Kid original, Daniel LaRusso, para ajud\u00e1-lo, e Li aprende uma nova forma de lutar, combinando seus dois estilos em um confronto ep\u00f3ico de artes m\u00e1cias.",
  "popularity": 696.6227,
  "poster_path": "/gnsSOV8w1KL8dFEGKR00iIKTS.jpg",
  "release_date": "2025-05-08",
  "title": "Karate Kid: Lendas",
  "video": false
}

```

6 - A resposta ser\u00e1 200 OK com a lista de filmes — validando o uso direto do token p\u00fAblico sem prote\u00e7\u00e3o.

Gravidade sugerida: Alta

Categoria OWASP: API2 / API9

Título: Ausência de Limite de Requisições na API (Lack of Rate Limiting)

Gravidade: Alta (uso indevido, custo à API de terceiros, rate limit, abuso)

Categoria OWASP:

- API9: Improper Assets Management
- API2: Broken Authentication (se reutilizável indevidamente)

Descrição:

A aplicação Movies Catalog embute diretamente no frontend um token JWT da API do TheMovieDB. Isso permite que qualquer usuário reutilize esse token e envie requisições autenticadas em nome da aplicação, comprometendo a conta da API, podendo atingir limites ou realizar abusos.

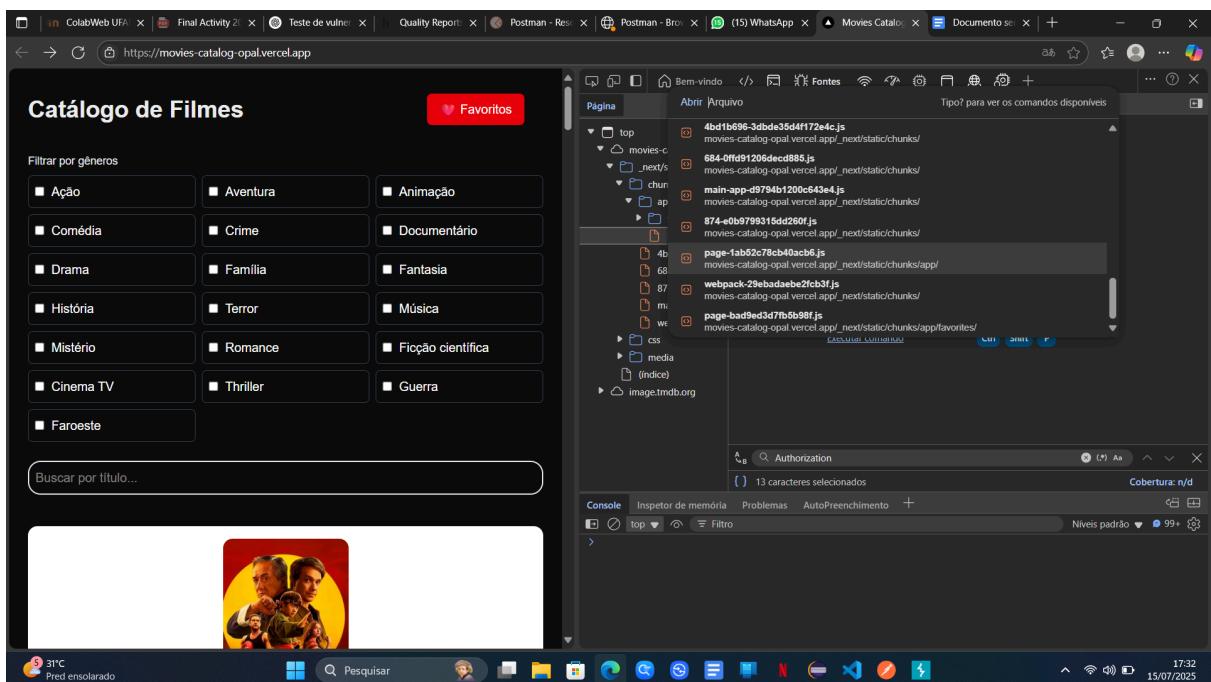
API afetada: [TheMovieDB \(TMDB\)](https://www.themoviedb.org)

Tipo de vulnerabilidade:

- Exposição de credenciais (API9 – Improper Assets Management)
- Falta de controle de requisições (API4 – Lack of Rate Limiting)

1. Obtenção do Token

- Acesse o site: <https://movies-catalog-opal.vercel.app>
- Pressione F12 → aba Sources



- Localize o script `page-xxx.js`

- Busque por "Authorization" e copie o token JWT exposto:

Token encontrado:

eyJhbGciOiJIUzI1NiJ9.eyJhdWQiOiJjYzU5NTI0Zjc4NTQwZjJiNDI2Y2FiNTA0NmJkYmVlMiIsIm5iZiI6MTc0NjY0ODAzNi43NjksInN1YiI6IjY4MWJiYmU0MTk2MDB1Zjc yYTAxZTU5MCIsInNjb3BlcyI6WyJhcGlfcmVhZCJdLCJ2ZXJzaW9uIjoxfQ.Vbf5hzWVsReuUz3YrgZyXFAnxbCKPFpyP4-qhG1EhHE

2. Teste direto via Postman

The screenshot shows the Postman interface with a collection named 'Luis's Workspace' selected. A specific request titled 'TP final | popular movies' is highlighted. The URL is `https://api.themoviedb.org/3/movie/popular?language=pt-BR&page=1`. In the Headers tab, 'Accept' and 'Content-Type' are set to 'application/json'. The Body tab displays a JSON response with the following content:

```

{
  "page": 1,
  "results": [
    {
      "adult": false,
      "backdrop_path": "/nkyBbFSpkRPTjVqjj0teD1lF733.jpg",
      "genre_ids": [
        28,
        12,
        18
      ],
      "id": 1011477,
      "original_language": "en",
      "original_title": "Karate Kid: Legends",
      "overview": "Após uma tragédia familiar, o prodigo do kung fu Li Fong é forçado a deixar sua casa em Pequim e se mudar para Nova York com sua mãe. Li luta para deixar o passado para trás enquanto tenta se entumar com seus novos colegas de classe, e, embora não queira brigar, os problemas parecem encontrá-lo por toda parte. Quando um novo amigo precisa de sua ajuda, Li entra em uma competição de karatê - mas suas habilidades sozinhas não são suficientes. O professor de kung fu de Li, Sr. Han, recruta o lendário Karatê Kid original, Daniel LaRusso, e Li aprende uma nova forma de lutar."
    }
  ]
}

```

3. Simulação de abuso com Runner (ataque DoS leve)

Luis's Workspace

Collections

Environments

Flows

APIs

Specs

History

Search collections

Run Sequence

Deselect All Select All Reset

Functional Performance

Choose how to run your collection

Run manually

Run this collection in the Collection Runner.

Schedule runs

Periodically run collection at a specified time on the Postman Cloud.

Automate runs via CLI

Configure CLI command to run on your build pipeline.

Iterations 50

Delay 0 ms

Test data file Only JSON and CSV files are accepted.

Select File

Advanced settings

Run TP final!

TP final - Run results

Ran today at 06:47:21 PM - View all runs

Source	Environment	Iterations	Duration	All tests	Avg. Resp. Time
Runner	none	50	11s 426ms	0	155 ms

All Tests Passed (0) Failed (0) Skipped (0) View Summary

Iteration 47

GET popular movies https://api.themoviedb.org/3/movie/popular?language=pt-BR&page=1 200 • 138 ms • 6.416 KB

No tests found

Iteration 48

GET popular movies https://api.themoviedb.org/3/movie/popular?language=pt-BR&page=1 200 • 133 ms • 6.416 KB

No tests found

Iteration 49

GET popular movies https://api.themoviedb.org/3/movie/popular?language=pt-BR&page=1 200 • 237 ms • 6.416 KB

No tests found

Iteration 50

GET popular movies https://api.themoviedb.org/3/movie/popular?language=pt-BR&page=1 200 • 133 ms • 6.416 KB

No tests found

Run Again + New Run Automate Run Share

TP final - Run results

Ran today at 06:47:21 PM - View all runs

Source	Environment	Iterations	Duration	All tests	Avg. Resp. Time
Runner	none	50	11s 426ms	0	155 ms

All Tests Passed (0) Failed (0) Skipped (0) View Summary

Iteration 47

GET popular movies https://api.themoviedb.org/3/movie/popular?language=pt-BR&page=1 200 • 138 ms • 6.416 KB

No tests found

Iteration 48

GET popular movies https://api.themoviedb.org/3/movie/popular?language=pt-BR&page=1 200 • 133 ms • 6.416 KB

No tests found

Iteration 49

GET popular movies https://api.themoviedb.org/3/movie/popular?language=pt-BR&page=1 200 • 237 ms • 6.416 KB

No tests found

Iteration 50

GET popular movies https://api.themoviedb.org/3/movie/popular?language=pt-BR&page=1 200 • 133 ms • 6.416 KB

No tests found

Run Again + New Run Automate Run Share

Resultado:

- 100% das respostas foram 200 OK
- Nenhum 429 Too Many Requests
- Tempo médio: ~150ms por requisição

Conclusão

1. **Exposição de Token no Front-End** – A presença do token JWT diretamente no código JavaScript permite que qualquer usuário reutilize esse token, o que viola a confidencialidade da autenticação. Essa prática configura a vulnerabilidade API2 – Broken Authentication.
2. **Má Gestão de Ativos Sensíveis** – O token está disponível publicamente sem controle, indicando falta de segregação entre componentes seguros e inseguros, caracterizando API9 – Improper Assets Management.
3. **Ausência de Rate Limiting** – Durante o teste com múltiplas requisições, nenhum erro de limite foi retornado (ex: 429), o que expõe a API a possíveis abusos, como ataques de negação de serviço leves (DoS). Isso também se relaciona com a API4 – Lack of Resources & Rate Limiting.
4. **Risco para o Terceiro (TMDb)** – Como o token pertence a uma conta da API do TheMovieDB, o uso indevido pode gerar custos, bloqueios ou suspensão da conta, afetando o proprietário da chave.
5. **Impacto Geral** – A combinação dessas falhas compromete a segurança, confiabilidade e controle de acesso da aplicação, evidenciando a necessidade de melhores práticas na proteção de APIs públicas.