Ano letivo 2024/2025

- Diogo Teixeira(A044483@umaia.pt)
- Joao Rebelo (A044484@umaia.pt)
- José Cardoso (A045146@umaia.pt)

Conteúdo

1. Introdução

A API do VirusTotal é uma excelente escolha para explorar os conceitos de APIs REST, múltiplos métodos HTTP, formatos de mensagem e autenticação.

Ela oferece uma interface robusta para interagir com uma vasta base de dados de informações sobre malwares e URLs maliciosos, permitindo que os desenvolvedores integrem as suas aplicações com um poderoso motor de análise de ameaças.

2. Arquitetura REST e Métodos HTTP

A API do VirusTotal segue a arquitetura REST, o que significa que utiliza recursos identificados por URL's e interage com os mesmos através de métodos HTTP. Os principais métodos HTTP utilizados pela API incluem:

- **GET**: Utilizado para recuperar informações sobre um recurso específico, como o relatório de análise de um arquivo ou URL.
- **POST**: Utilizado para enviar dados para a API, como um arquivo para análise ou uma URL para verificação.
- **DELETE**: Em alguns casos, pode ser utilizado para excluir recursos, como um comentário a um relatório.

3. Formatos de Mensagem

A API do VirusTotal suporta tanto o formato JSON quanto o XML para a representação dos dados. A escolha do formato é geralmente feita através de um parâmetro na URL da requisição.

3.1 Autenticação

A API do VirusTotal utiliza um sistema de chaves API para autenticar as requisições. A chave API é única para cada utilizador e deve ser incluída em cada requisição como um parâmetro.

3.2 Objetivos da API

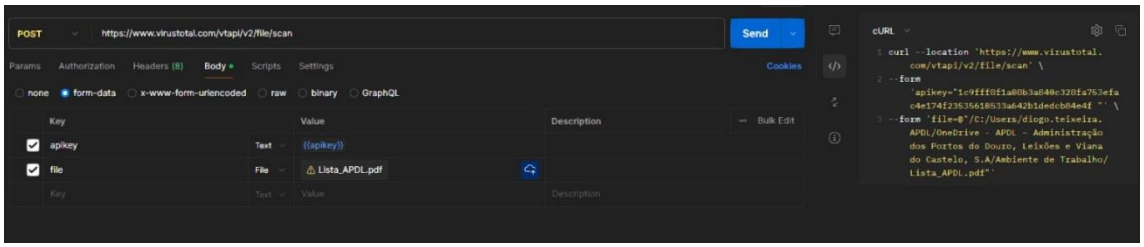
A API do VirusTotal tem como objetivo principal fornecer aos desenvolvedores uma interface para aceder e utilizar os serviços de análise de malwares e URL's.

O que é possível fazer?

- Enviar arquivos e URL's para análise.
- Obter relatórios detalhados sobre a reputação de arquivos e URL's.
- Pesquisar por hash de arquivos.
- Criar e gerir comentários em relatórios.
- Obter estatísticas sobre as análises realizadas.

4. Modo de Funcionamento e Exemplos Funcionais

Exemplo 1: Enviando um arquivo para análise (método POST)



Exemplo 2: Obter o relatório de análise de uma URL (método GET)

5. Funcionalidades da API

Além das funcionalidades mencionadas anteriormente, a API do VirusTotal oferece diversas outras opções, como:

- **Análise de URL's:** Permite verificar a reputação de URL's e identificar possíveis ameaças.
- **Análise de arquivos:** Permite enviar arquivos para análise e obter um relatório detalhado sobre as deteções de antivírus.

- **Pesquisa por hash:** Permite pesquisar por hash de arquivos para verificar se eles já foram analisados anteriormente.
- **Criar e gerir comentários:** Permite adicionar comentários aos relatórios de análise.
- **Obter estatísticas:** Permite obter estatísticas sobre as análises realizadas.

6. Avaliação e Análise Crítica

A API do VirusTotal é uma ferramenta poderosa e versátil, com uma documentação clara e completa. No entanto, alguns pontos podem ser levados em consideração:

- **Limitação de requisições:** A API possui limites de requisições por minuto e por dia , (4 por minuto) e (500 por dia).
- **Dependência de terceiros:** A precisão das análises depende da qualidade dos motores de antivírus utilizados pelo VirusTotal.
- **Custo:** Para um uso intensivo da API, pode ser necessário adquirir planos pagos.

7. Construir a Apresentação

Com base nessas informações, pode criar uma apresentação completa sobre a API do VirusTotal, incluindo:

- **Slides introdutórios:** Apresentar o VirusTotal, os objetivos e os benefícios da API.
- **Arquitetura REST:** Explicar os conceitos de REST e como a API do VirusTotal se enquadra no modelo.
- **Métodos HTTP e formatos de mensagem:** Detalhar os métodos HTTP utilizados e as opções de formato de mensagem.
- **Autenticação:** Explicar o processo de autenticação e a importância da chave API.
- **Exemplos práticos:** Demonstrar o funcionamento da API com exemplos de código em diferentes linguagens de programação.
- **Casos de uso:** Apresentar exemplos de como a API pode ser utilizada em diferentes cenários.
- **Considerações finais:** Discutir os pontos fortes e fracos da API, bem como as melhores práticas para utilizá-la.

Recursos Adicionais:

- Documentação oficial: https://docs.virustotal.com/reference/overview
- Biblioteca *Python* para interagir com a API: https://pypi.org/project/virustotal-python/

Ao seguir essas diretrizes, você poderá criar uma apresentação completa e informativa sobre a API do VirusTotal, demonstrando seu conhecimento e habilidades em desenvolvimento de aplicações web.

Explicação:

- **Autenticação:** A API do VirusTotal utiliza um sistema de chaves API para autenticar as requisições. A sua chave API é única e deve ser incluída em cada requisição como um parâmetro.
- **Método HTTP:** Utilizamos o método GET para enviar a requisição. Outros métodos como POST podem ser usados para enviar arquivos maiores.
- **Resposta:** A resposta da API é geralmente em formato JSON e contém diversos campos, incluindo informações sobre a reputação da URL, deteções por diferentes antivírus, e links para relatórios mais detalhados.

8. Relações "1 para Muitos" e "Muitos para Muitos"

A API VirusTotal possui diversas relações entre seus recursos.

- Um ficheiro pode ter muitos resultados de análise: Um único ficheiro pode ser analisado por diversos antivírus, resultando numa lista de deteções. Esta é uma relação “1 para muitos”.
- Um URL pode estar relacionado a muitos domínios: Um URL pode redirecionar para outros domínios, criando uma relação "1 para muitos".
- Um domínio pode estar relacionado a muitos ficheiros: Um domínio pode hospedar vários ficheiros maliciosos, estabelecendo uma relação "muitos para muitos".

8.1 Visualizando as Relações

Para visualizar essas relações de forma mais clara, pode utilizar a ferramenta VirusTotal Graph. Esta ferramenta permite criar gráficos que mostram as conexões entre diferentes entidades, como ficheiros, URL's, domínios e endereços IP.

Outros Pontos Importantes:

- **Limites de Requisições:** A API do VirusTotal possui limites de requisições para evitar abusos. É importante consultar a documentação oficial para verificar os limites atuais.
- **Tipos de Análise:** A API suporta a análise de diversos tipos de ficheiros, incluindo executáveis, documentos, arquivos compactados e URL's.
- **Recursos Adicionais:** Além da análise de arquivos e URL's, a API oferece outros recursos, como a pesquisa por hash, a obtenção de informações sobre amostras e a criação de relatórios personalizados.

Documentação Oficial:

Para obter informações mais detalhadas sobre a API do VirusTotal, pode consultar no link abaixo:

https://docs.virustotal.com/reference/overview

Utilizando a API em Outros Projetos:

A API do VirusTotal pode ser integrada a diversos tipos de projetos, como sistemas de deteção de intrusão, ferramentas de análise forense e plataformas de segurança de e-mail.

9. Conclusão

A API do VirusTotal é uma ferramenta valiosa para desenvolvedores que desejam adicionar funcionalidades de análise de malware e URL às suas aplicações.

Ao entender os conceitos de autenticação e as relações entre os recursos da API, poderá criar soluções personalizadas e eficazes para proteger seus utilizadores contra ameaças online.