Atividade Heards e Requisições

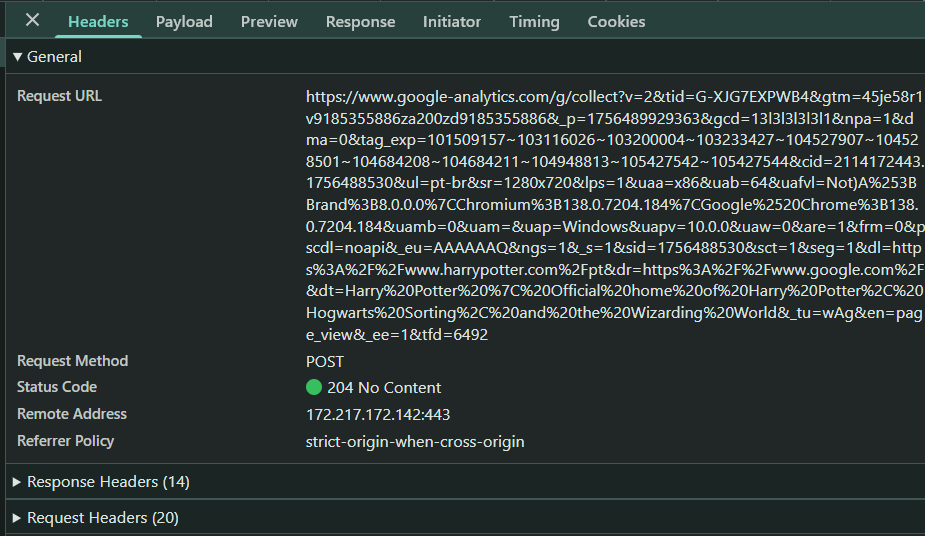
**Nome**: Layslla Eduarda Oreti

**Turma**: 2DS-TB

**Professora**: Mariany Lima

Site escolhido para a atividade: <https://www.harrypotter.com/pt> (Harry Potter - Oficial Home)

**Headers Gerais**

****

**Request URL:** Endereço web onde o pedido é enviado para a comunicação entra o cliente (navegador) e o servidor, guiando a requisição onde ele foi solicitado.

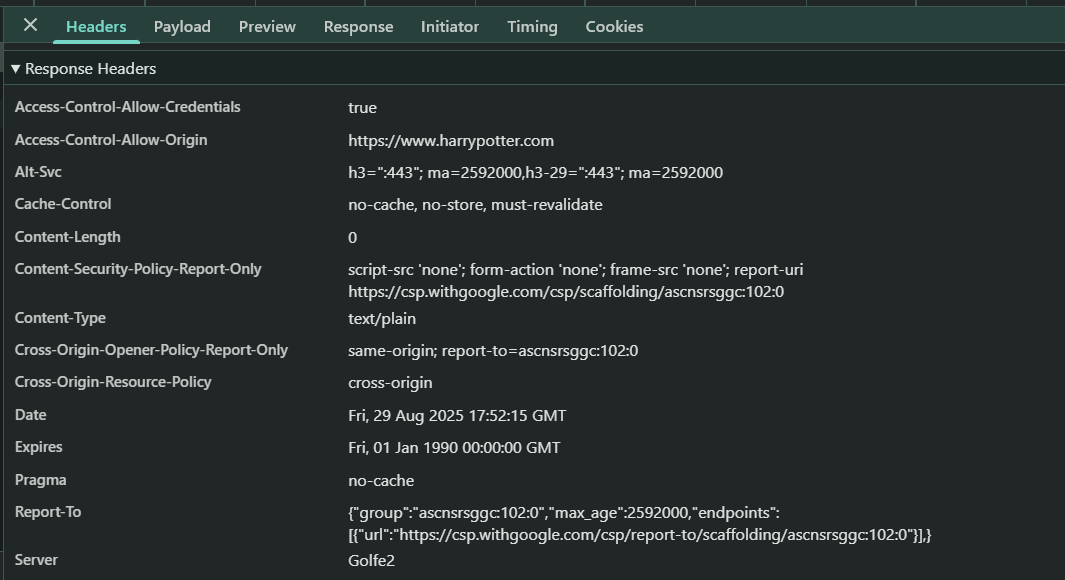
**Request Method:** Ele irá definir a ação do cliente, como navegador dentro da aplicação web, no exemplo mostrado, o método é o POST, o envio de dados ao servidor, alterando o estado atual.

**Status Code:** É a resposta enviada ao cliente para a solicitação HTTP, nesse exemplo foi o 204, informando que a requisição foi bem-sucedida e processada pelo servidor.

**Remote Address:** É o endereço IP do navegador (cliente) que está realizando a solicitação, sendo representado de forma numérica.

**Referrer Policy:** Irá determinar comoa minha URL se comportará enquanto o cliente navega dentro da minha aplicação, conforme ele interage com os componentes e links ele enviar o formato da URL.

**Response Headers**



**Expires**: Especifica a data e a hora após as quais a resposta é considerada obsoleta e não deve ser mais veiculada pelo cache do navegador sem realizar a revalidação. Nesse caso, é o dia 01 de janeiro de 1990, as 00:00.

**Cross-Origin-Resource-Policy-Report-Only:** Ele é uma header de segurança, controla como a aba interage com as outras páginas que estão abertas no navegador. Nesse exemplo, “**same-origin**” quer dizer que os conteúdos da mesma origem podem compartilhar o mesmo contexto da navegação. O “**Report-Only**” mostra que a política não está sendo aplicada de verdade, só gerando relatórios para o endpoint configurado. Por último, o “**report-to= ascnsrsggc**” indica onde os relatórios de violação devem ser enviado (um endpoint configurado pelo servidor), nesse caso, representado por números.

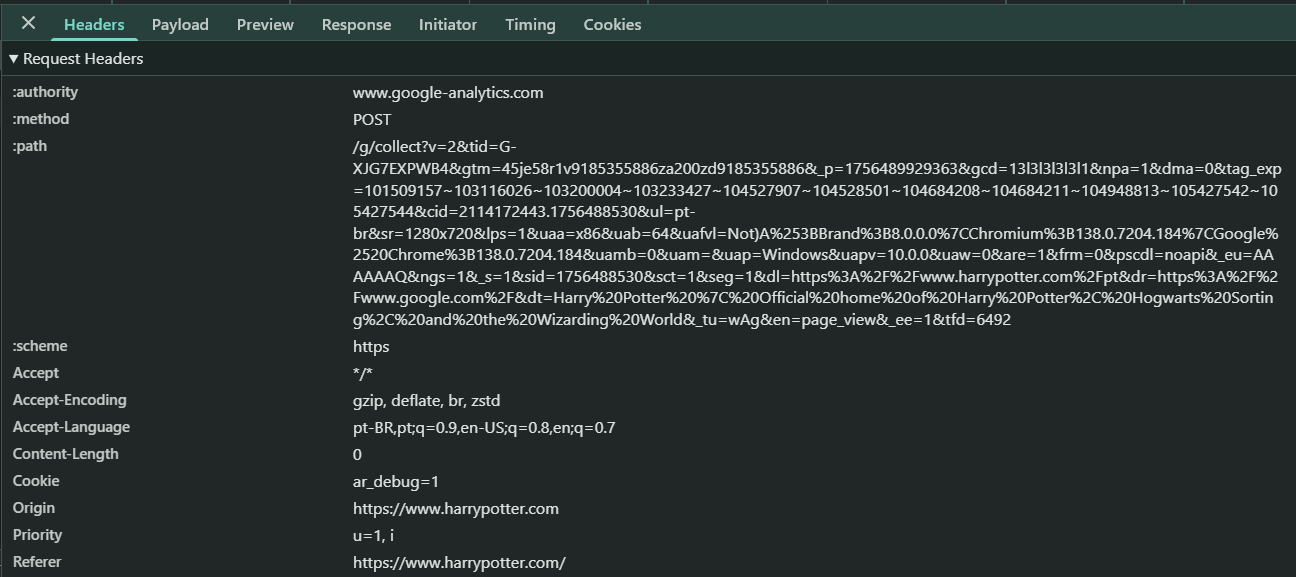
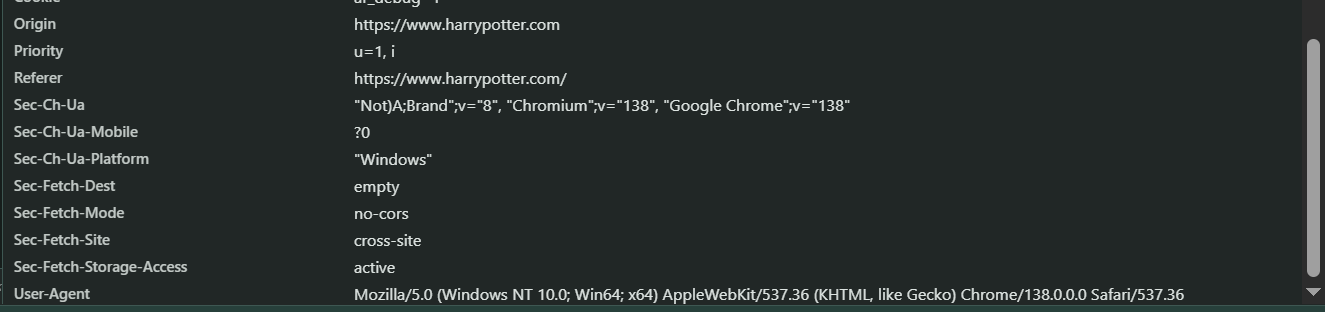
**Acess-Control-Allow-Origin:** Significa que só o domínio (<https://www.harrypotter.com/pt>) mostrado tem a permissão de acessar os recursos desse servidor via navegador, como por exemplo, se você tentar a API de outro site, o navegador bloqueará imediatamente a resposta.

**Report-To:** Ele define para onde o navegador deve enviar relatórios de violações de política de segurança. No exemplo mostrado, o **“group” (ascnsrsggc:102:0)** é o identificador do grupo de relatórios, o **“max\_age” (2592000)** é o tempo, contado em segundos, que o navegador deve manter esse endpoint de relatórios ativo, nesse caso, são 30 dias, e por último os **“endpoints”**, que é a lista de URLs para onde os relatórios serão encaminhados.

Em geral, essa configuração serve para que caso forem encontrados problemas de segurança, dentro de 30 dias, os relatórios serão mandados no formato JSON para o endpoint especificado.

**Alt-Svc:** Alternative Services, ou Alt-Svc, é usado para relatar ao navegador que a aplicação pode ser servido por outras portas ou protocolos. Em partes, o **h3=”:443”** quer dizer que o servidor suporta HTTP/3 na porta 443 (porta padrão do HTTPS). **O h3-29=”:443”** é o draft 29 do HTTP/3, que é uma versão específica de teste do protocolo), eles são executados para existir a compatibilidade com navegadores que estão em versões antigas (anteriores ao HTTP/3). Por último, o **ma=2592000** significa o tempo máximo (em segundos) que o cliente pode usar essa configuração.

**Request Headers**



**Sec-Ch-Ua-Mobile:** Ele faz parte dos Client Hints (headers opcionais que o navegador envia para o servidor, que trás informações sobre o dispositivo e o contexto do cliente). No caso do exemplo mostrado, ele indica se o usuário está em um dispositivo móvel ou não, nessa situação, a resposta (?0) significa que não é um dispositivo móvel.

**Sec-Fetch-Dest:** Diz ao navegador qual é o destino do recurso que está sendo carregado, com os possíveis valores: script, style, image, iframe, etc. Nesse caso, o “empty” significa que o destino da solicitação é uma string vazia.

**Priority: u=1, i:** Essa solicitação indica as preferências de priorização para um recurso solicitado. Em partes, o **u=1** significa o nível de urgência da solicitação, onde o valor varia de 0 a 7, onde 0 representa a maior urgência e 7, a menor. Em último, o **i** é um parâmetro booleano e indica se a resposta pode ser processada incrementalmente, que significa que se ele for verdadeiro **(i sem um valor, i=true)** o cliente pode começar a processar e renderizar a resposta conforme ela chega em partes, em vez de esperar que a resposta inteira seja recebida.

**Sec-Fetch-Site: cross-site:** Isso indica a relação entre o site que está fazendo a requisição e o servidor que irá receber. Nesse caso, está como **“cross-site”** pois a url (<https://www.harrypotter.com/pt>) está mandado os dados para o google-analytics, e isso é usado por políticas de segurança, como CORS.

**:authority:** [www.google-analytics.com](http://www.google-analytics.com): Ele é classificado como um **pseudo-header** do HTTP/2/HTTP/3 e substitui o header host do HTTP/1. Ele indica qual servidor deve atender a requisição e é essencial pois as versões dos protocolos são multiplexadas (várias requisições podem trafegar de forma simultânea pelo mesmo canal), e o **:authority** garante que cada uma chegue ao local/host correto, evitando uma possível confusão entre as múltiplas requisições existentes no mesmo fluxo.