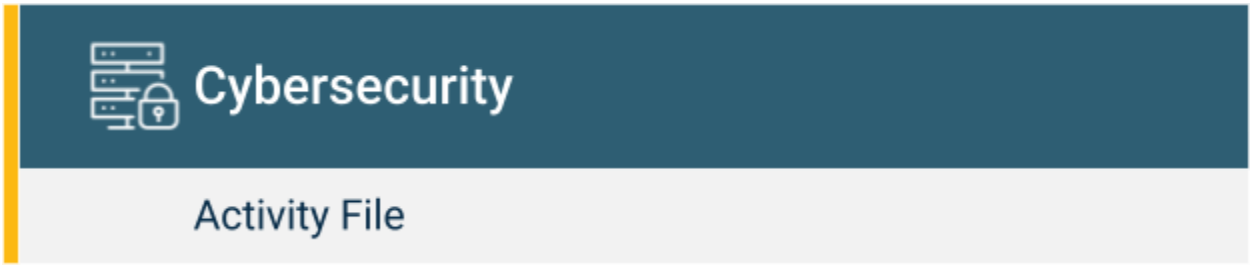


Activity File: Inspect with Developer Tools

For this activity, you will continue your role as a web app security engineer.

- You are tasked with examining the request and response headers of one of your vendor's websites to assess its HTTP security.

- For this activity, you'll use Chrome Developer Tools to examine the initial request and response set from www.crowdstrike.com.

Lab Setup

Before you start, make sure you have Google Chrome and a few other activity files installed. If your instructor has not walked you through running the setup script, please do the following:

- Run the following command in your virtual machine and enter sysadmin's password when prompted: `wget https://gist.githubusercontent.com/eddimus/231c53698940dd4962835d55a602946f/raw/9368686da1731ec7ee380d94fd578762265c4035/14-1_setup.sh && sudo chmod +x 14-1_setup.sh && sudo ./14-1_setup.sh`

    - After it's done running, feel free to delete the `14-1_setup.sh` file.

Instructions

1. Open Developer Tools by going to Chrome's settings, then **More Tools**, then **Developer Tools**.

    - Click on the **Network** tab so that your browser is ready to process HTTP requests and responses.
2. Go to www.crowdstrike.com.

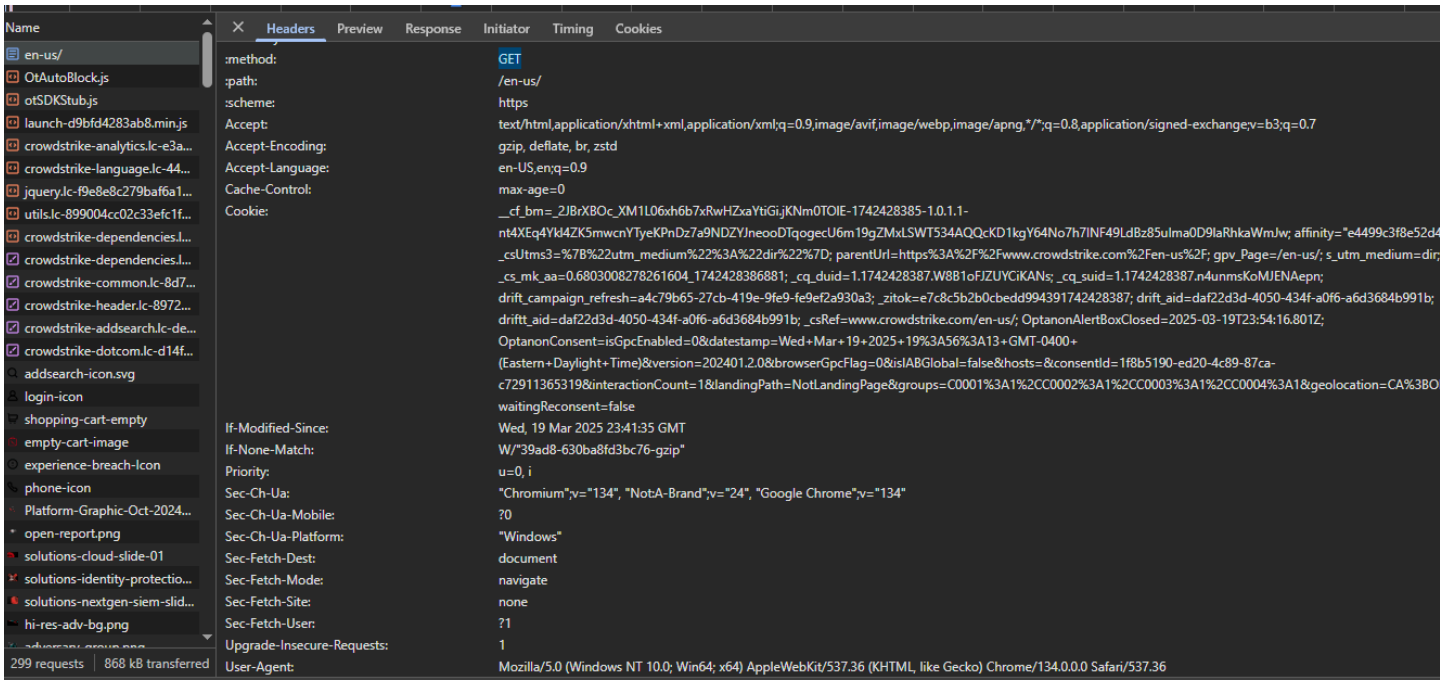
    - In the **Name** column on the left-hand side of the Developer Tools console, scroll to the first response and select it. It should be named www.crowdstrike.com.

      Note that if you do not see this, you can use your personal computer's Chrome

browser to inspect this site's responses.

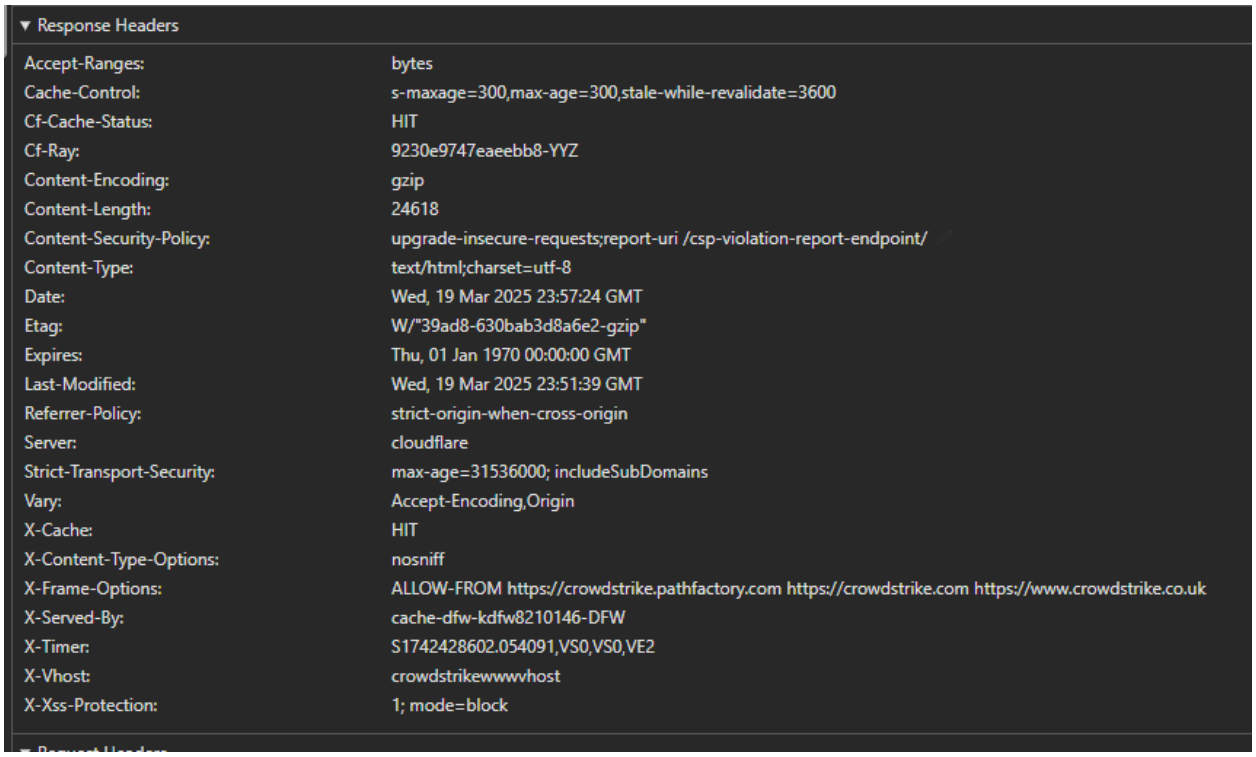
3. Answer the following questions:

    - Scroll to the bottom of the **Headers** tab to view the **Request Headers** section.



        - **Question 1:** Are there any noticeable security request headers that we've discussed? If so, what do they mean? We see a GET method that means the client is requesting resources from the server. I see the /en-us/ is the subpath we are in on the website.

- Scroll up to view the **Response Headers** section.



- **Question 2:** What response headers do you recognize from today's class? What do they mean?
  I recognize the date, the server and the options headers. The server shows we are on cloudstrike's own server and the options header shows it will allow the three options listed in the body.
- **Question 3:** Are there any notable security response headers that we've discussed? If so, what do they mean?
  We have a status code of 200 ok, meaning the response was successful. We are using https which is the secure version for http. The Strict-Transport-Security header indicates we must use https to use the webpage. X-Xss-Protection blocks the page if it has been compromised.