**RE&VA**

**Introduction:**

The ticket exchange platform, designed to facilitate the exchange of tickets for various shows, URL: https://dev.ticket-barter.com/. Through manual testing using Burp Suite, five vulnerabilities were discovered, posing significant security risks to users of the platform. Then apply mitigation on the vulnerabilities to reduce the risk.

**Methodology/Tools:**

I used **Burp Suite**, a widely-used web application security testing tool, for manual testing of the ticket exchange platform.

Along with Burp Suite we also used **Nikto** tool for automated scan.

**Feroxbuster** for directory numeration.

**Nmap** scan for overview of the network and the IP.

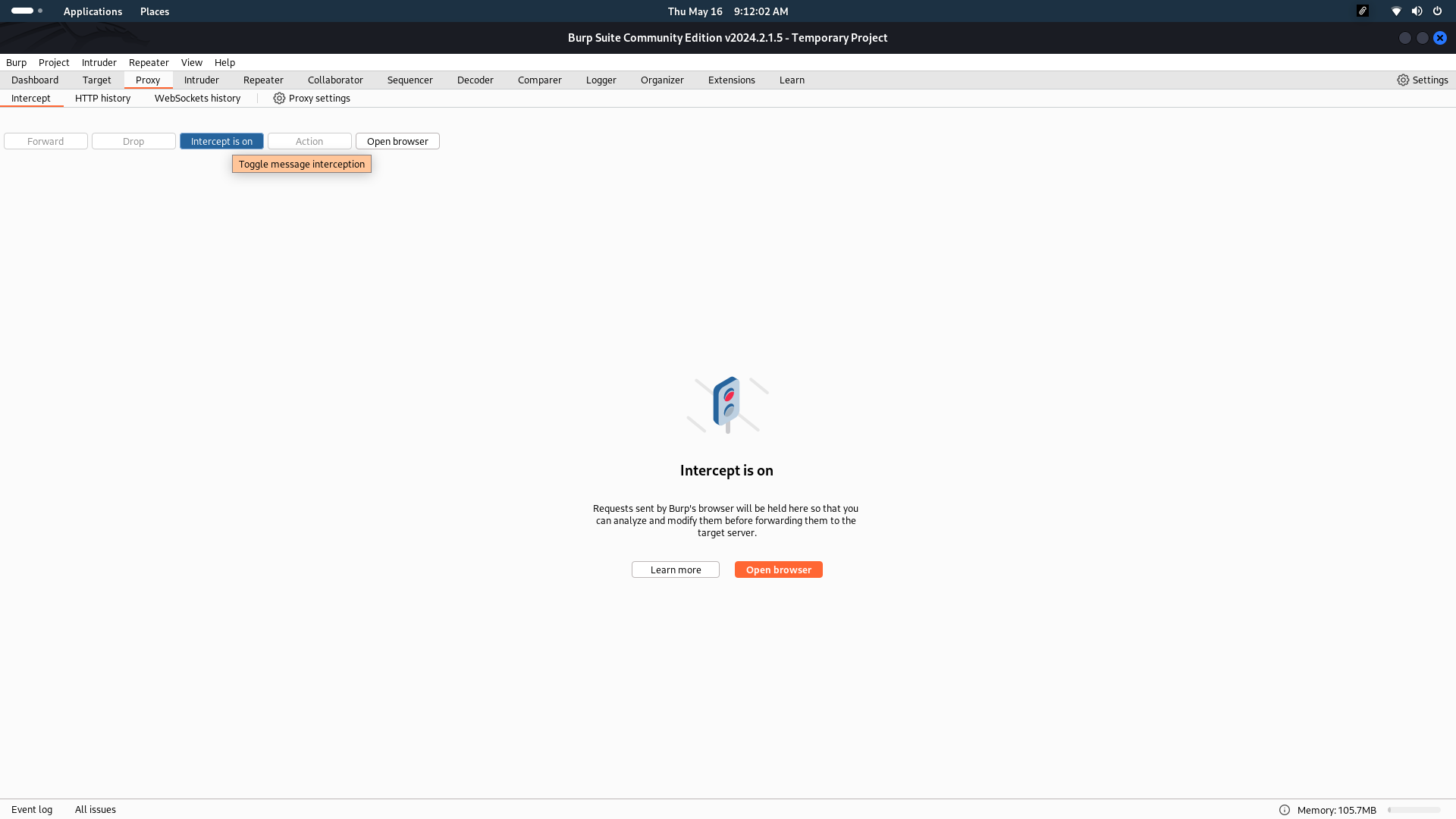
**Attack scenarios using Burp Suite:**

**Vulnerability Identification**

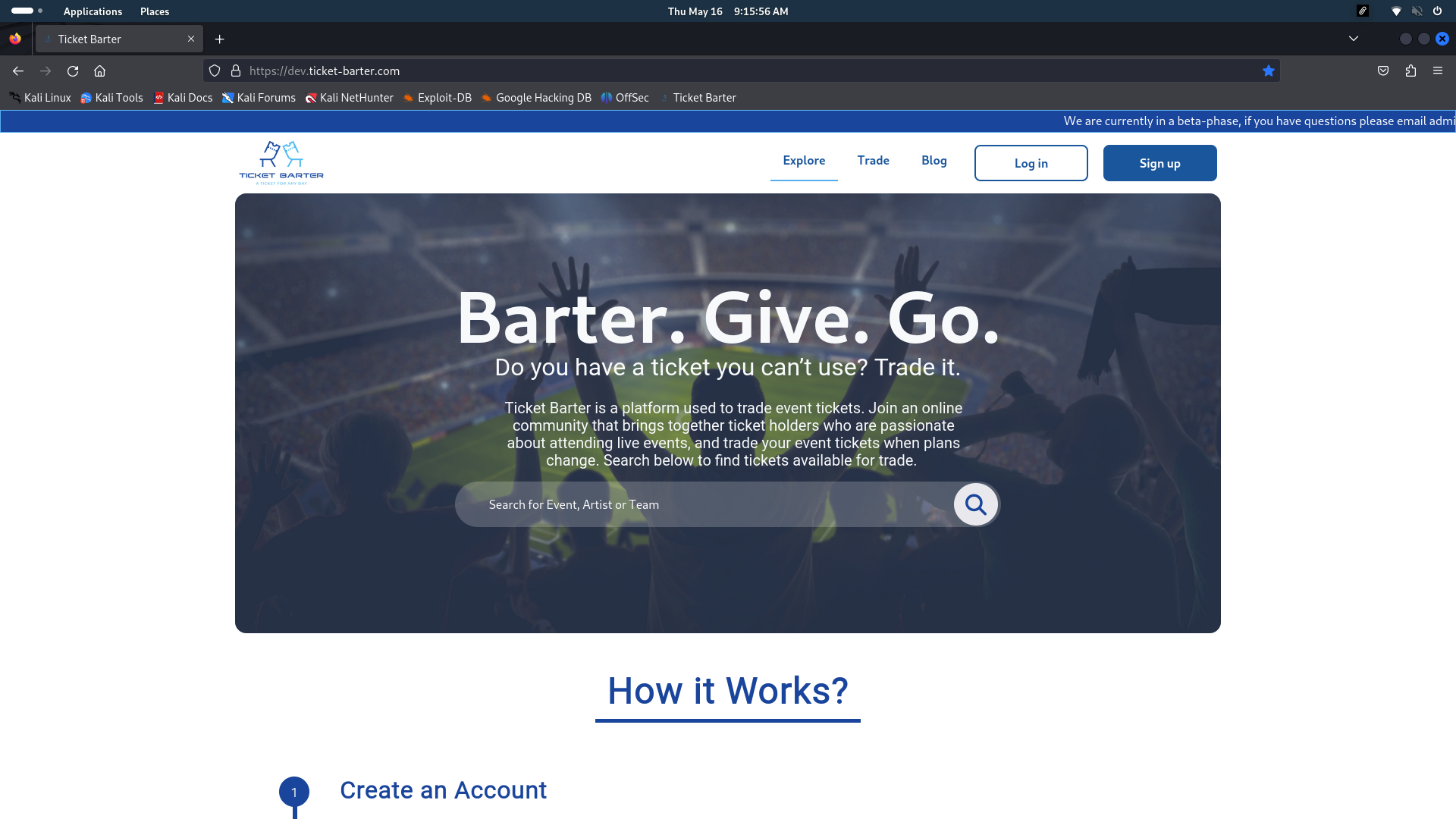
* **Missing Strict-Transport-Security Header:**

**Steps**:

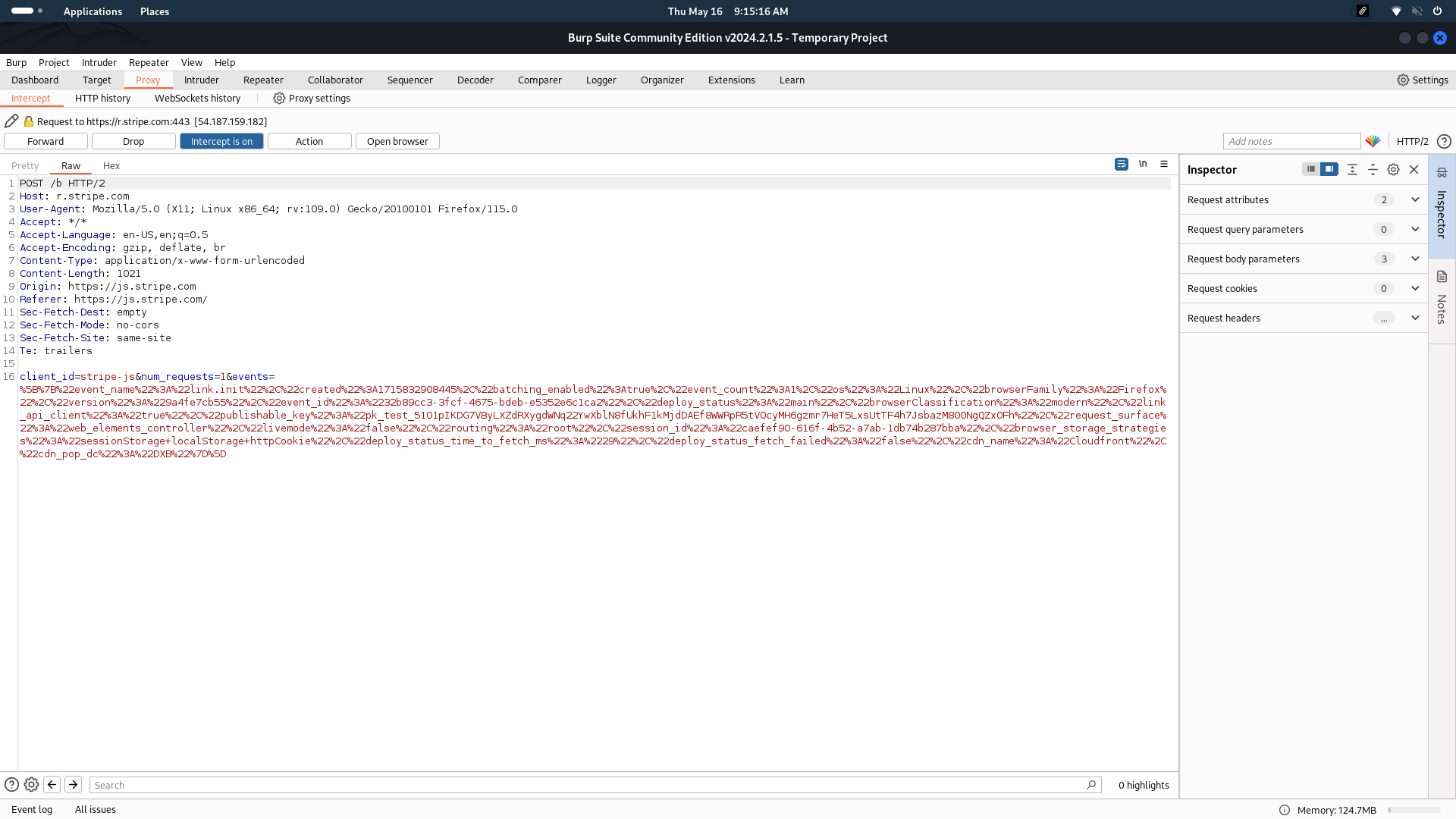
1. Open Burp Suite and navigate to the Proxy tab.
2. Start the intercept mode in Burp Suite's Proxy tool.



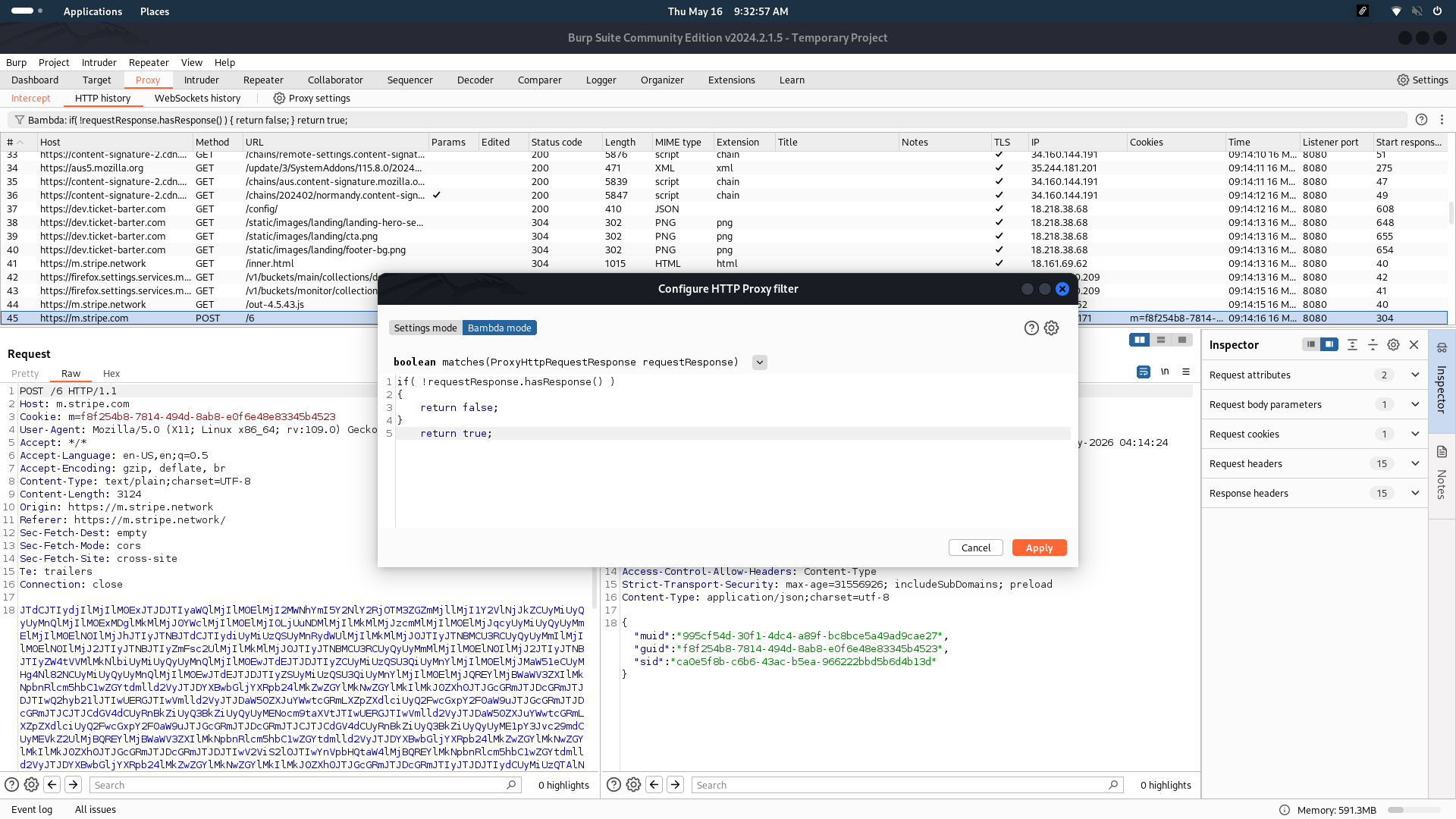
1. Browse the website (<https://dev.ticket-barter.com/>) to generate traffic.



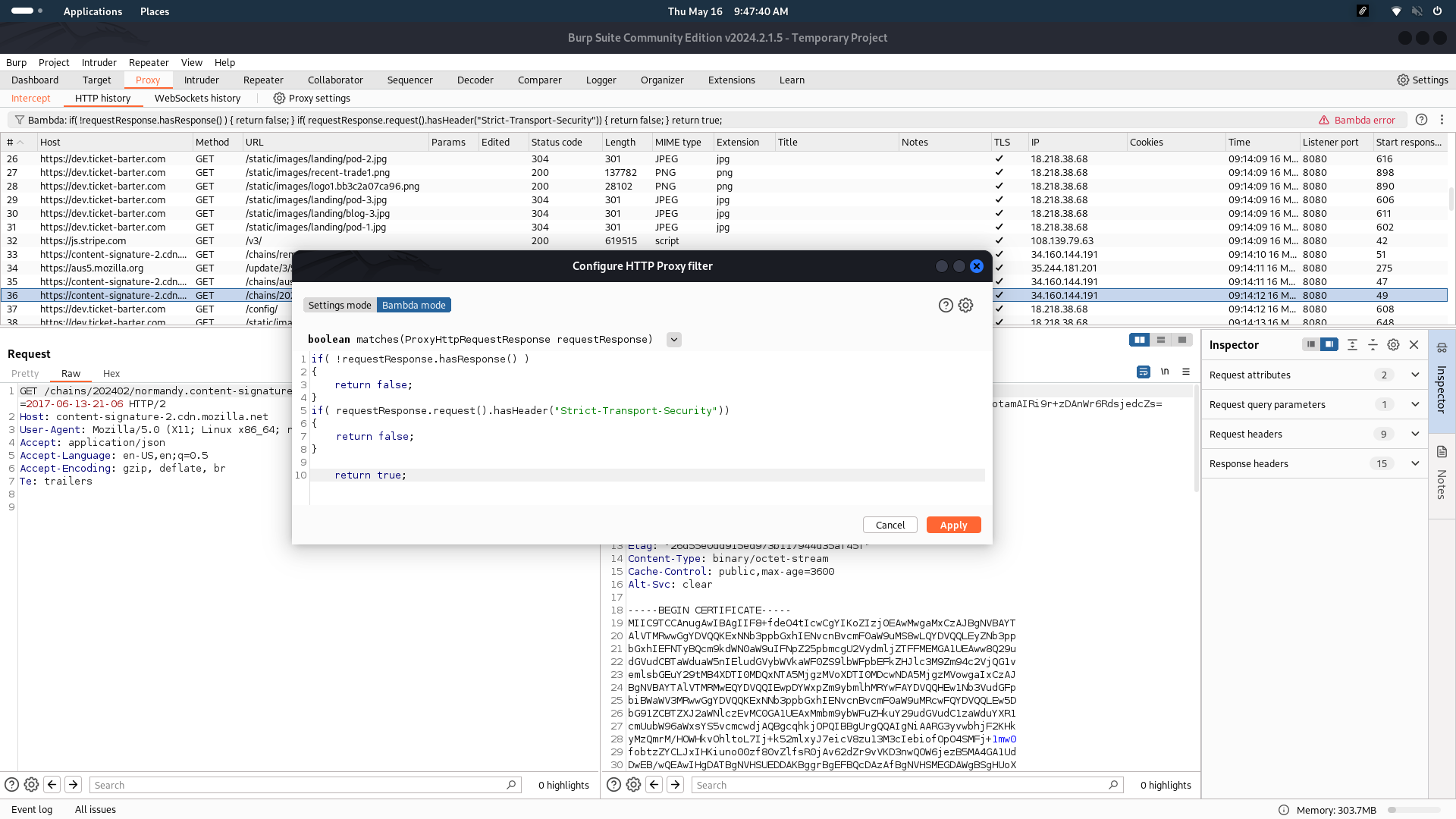
1. Review intercepted requests and responses in the Proxy history.



1. Apply a filter to show only responses.



1. Look for responses without the Strict-Transport-Security header.



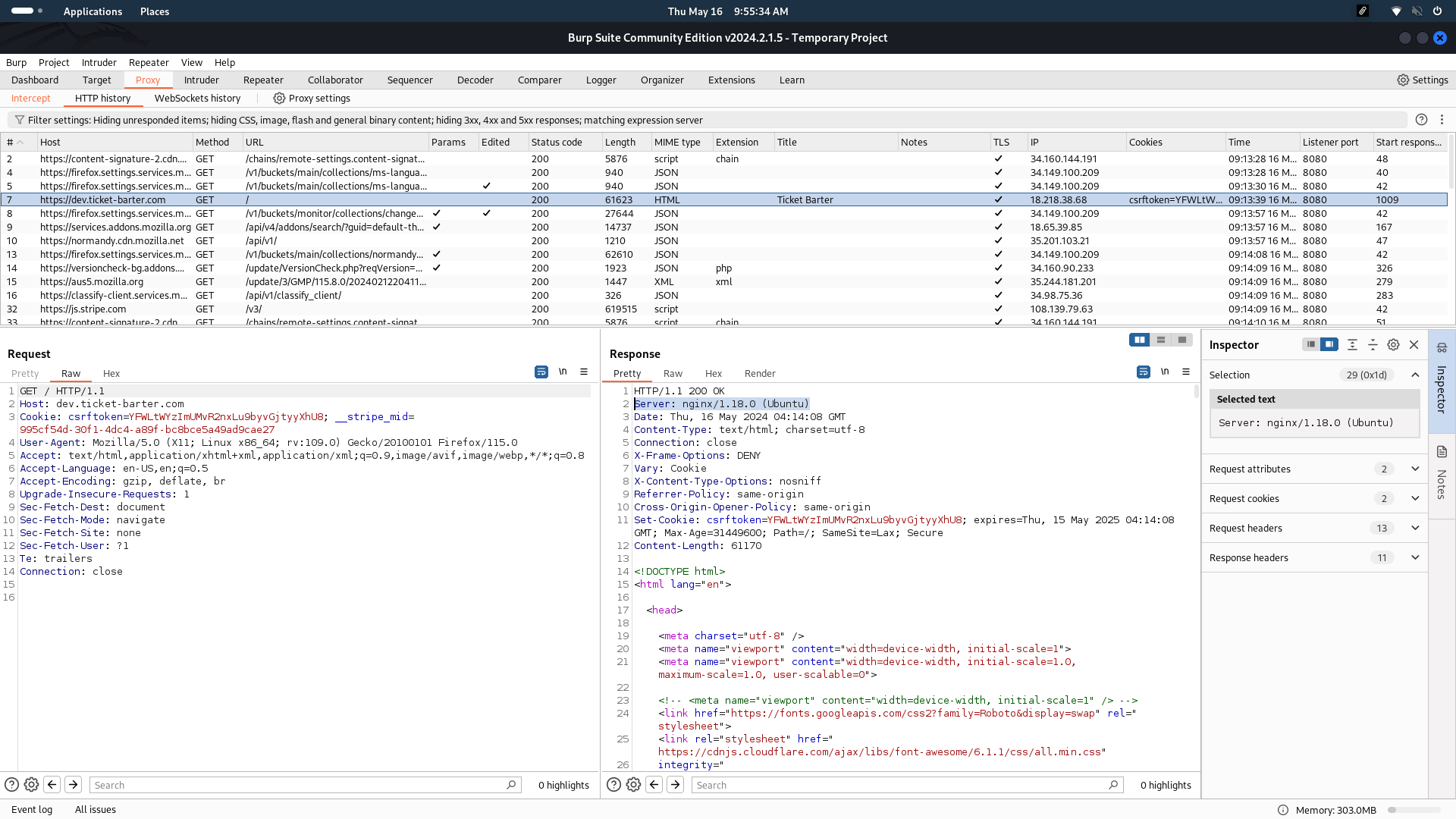
1. Review the filtered responses to identify instances where the header is missing.

Almost all the responses missing the HSTS header.

* **Outdated Server Software (nginx version 1.18.0):**

**Steps**:

Repeat steps 1-4 from the previous process to intercept traffic.

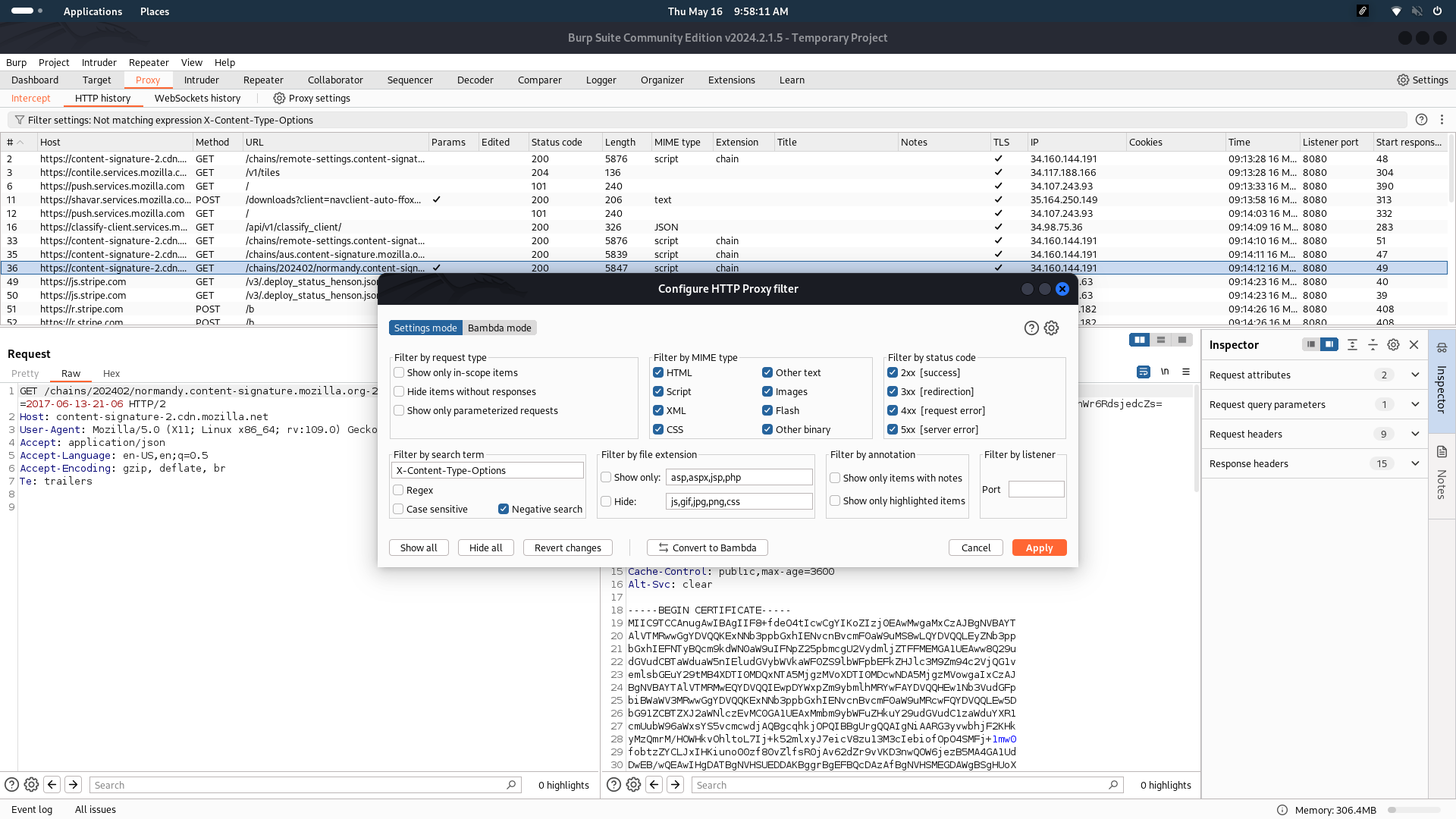
1. Review intercepted responses in the Proxy history.
2. Look for server headers containing version information.
3. Identify server headers indicating the version of nginx.
4. Determined that the version is outdated.

* **Missing X-Content-Type-Options Header:**

**Steps**:

Repeat steps 1-6 from the first process to intercept and filter responses.

1. Look for responses without the X-Content-Type-Options header.



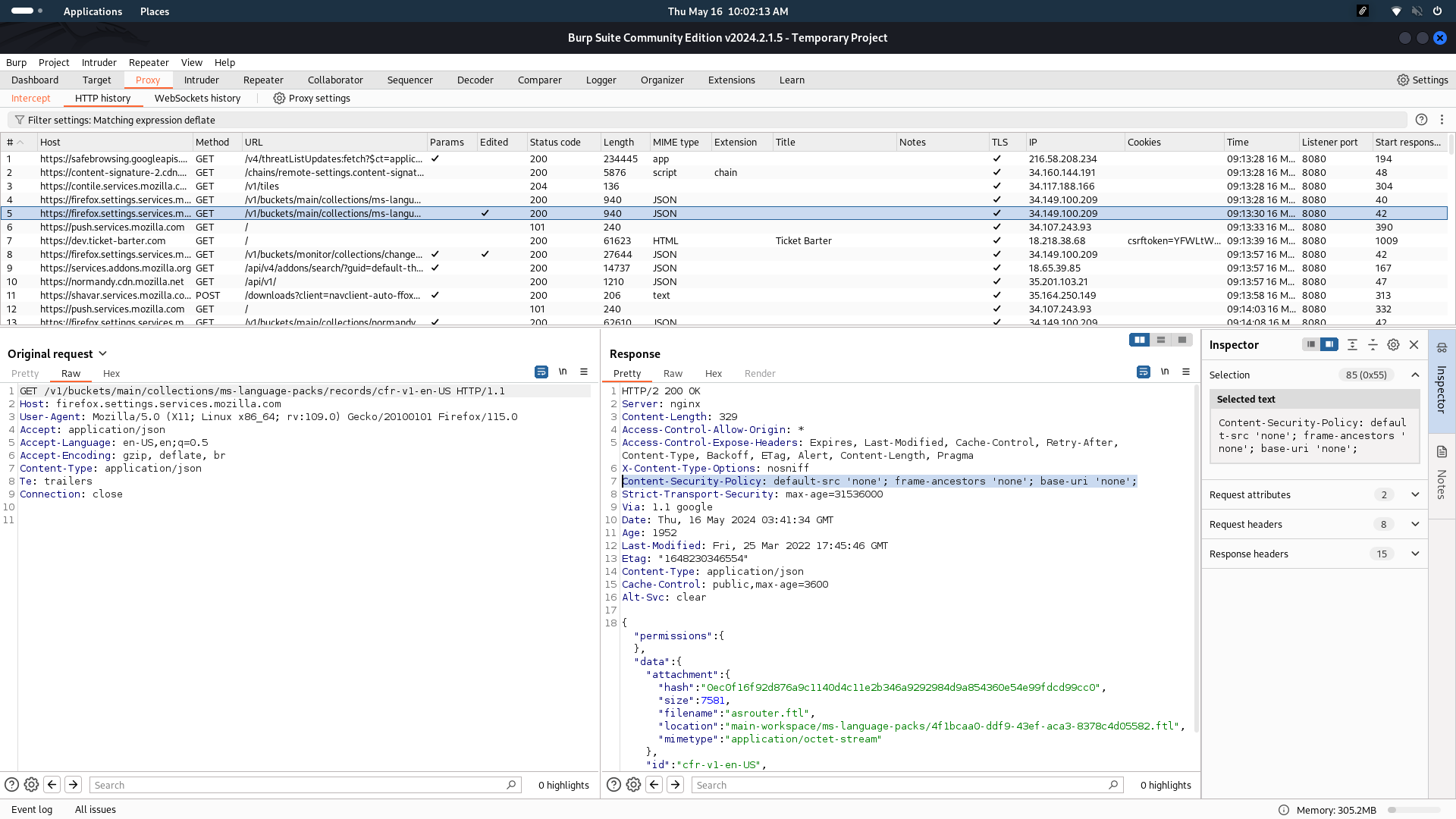
1. Review the filtered responses to identify instances where the header is missing.

* **BREACH Attack Vulnerability:**

**Steps**:

Repeat steps 1-6 from the first process to intercept and filter responses.

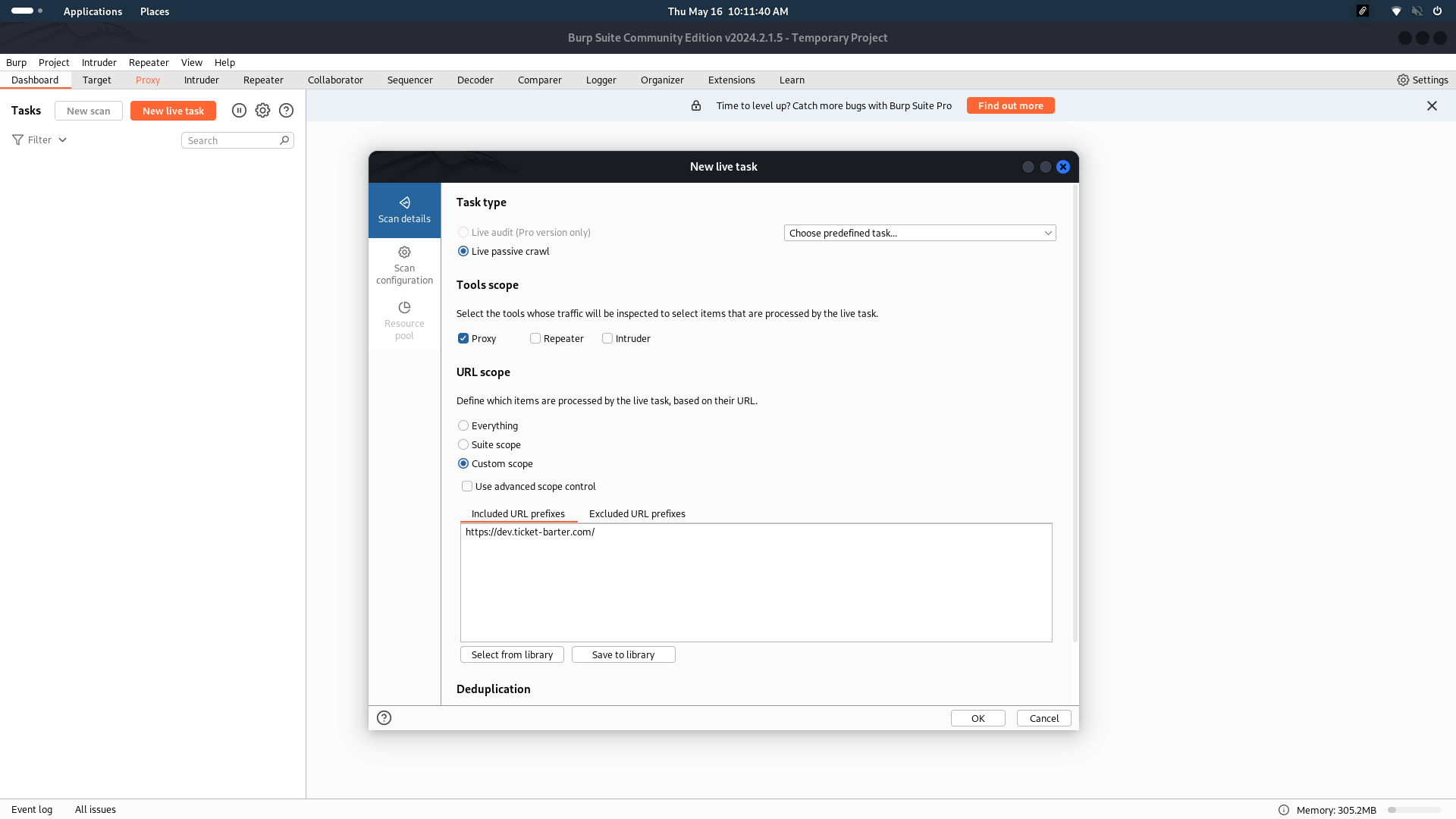
1. Look for responses with the Content-Encoding: deflate header.

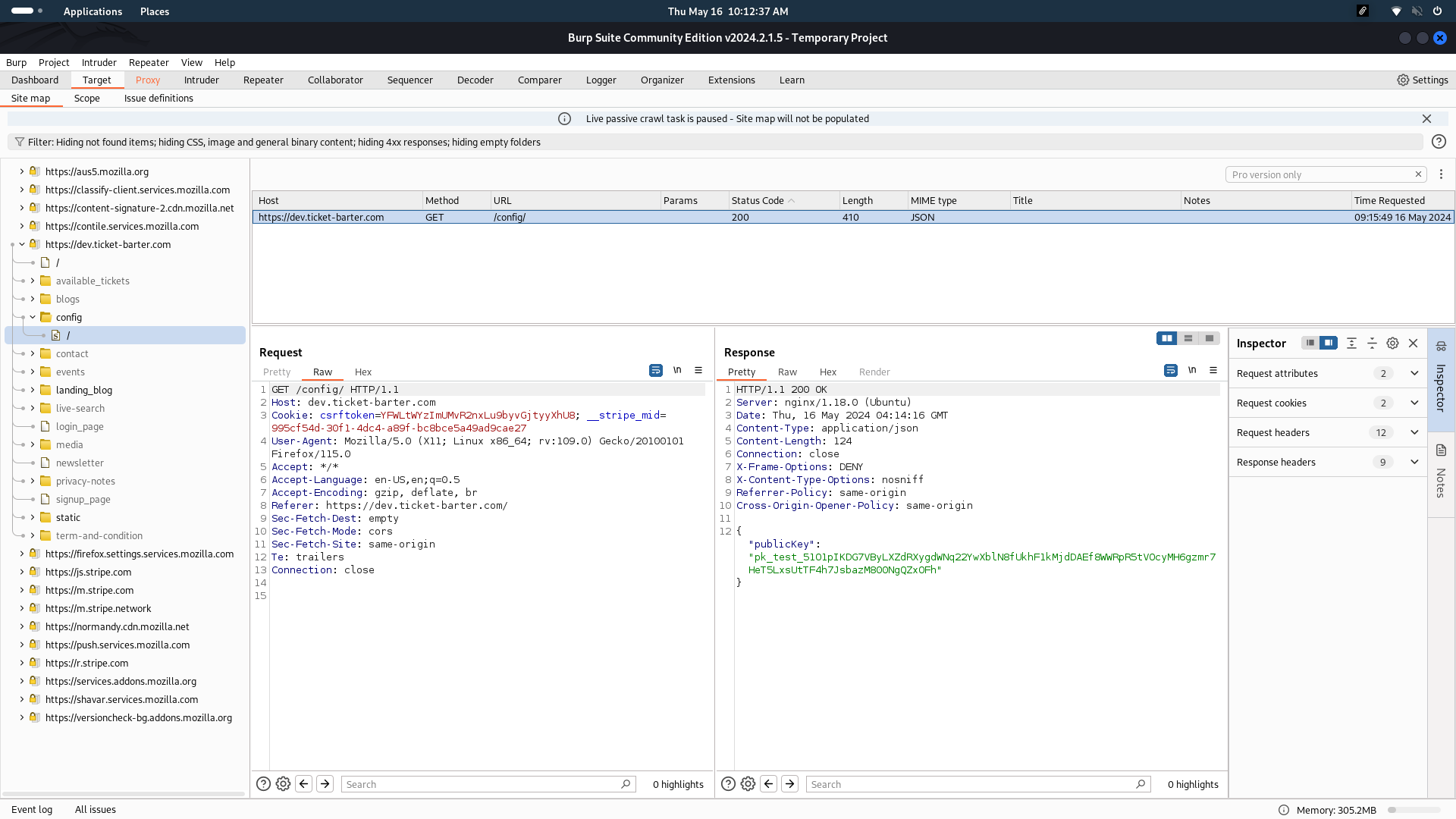


1. Analyze compressed responses for variations in size.
2. Look for patterns that may indicate potential plaintext recovery vulnerabilities.

* **Potentially Exposed Configuration Information:**

**Steps**:

1. Use Burp Suite's spider tool to crawl the website and discover directories and files.
2. Review the discovered directories and files in the Target tab.
3. Look for directories or files that may contain sensitive configuration information (e.g., /config/).



1. Manually inspect the content of the discovered directories and files for potential exposure of sensitive information.

**Attack scenarios using Nikto:**

**Introduction:**

Nikto is an automated web vulnerability scanner widely used by security professionals and system administrators to identify security risks in web servers swiftly.

With its comprehensive scanning capabilities, flexible parameters, and detailed reporting, Nikto enables users to conduct thorough security audits, penetration tests, and continuous monitoring of web server security posture.

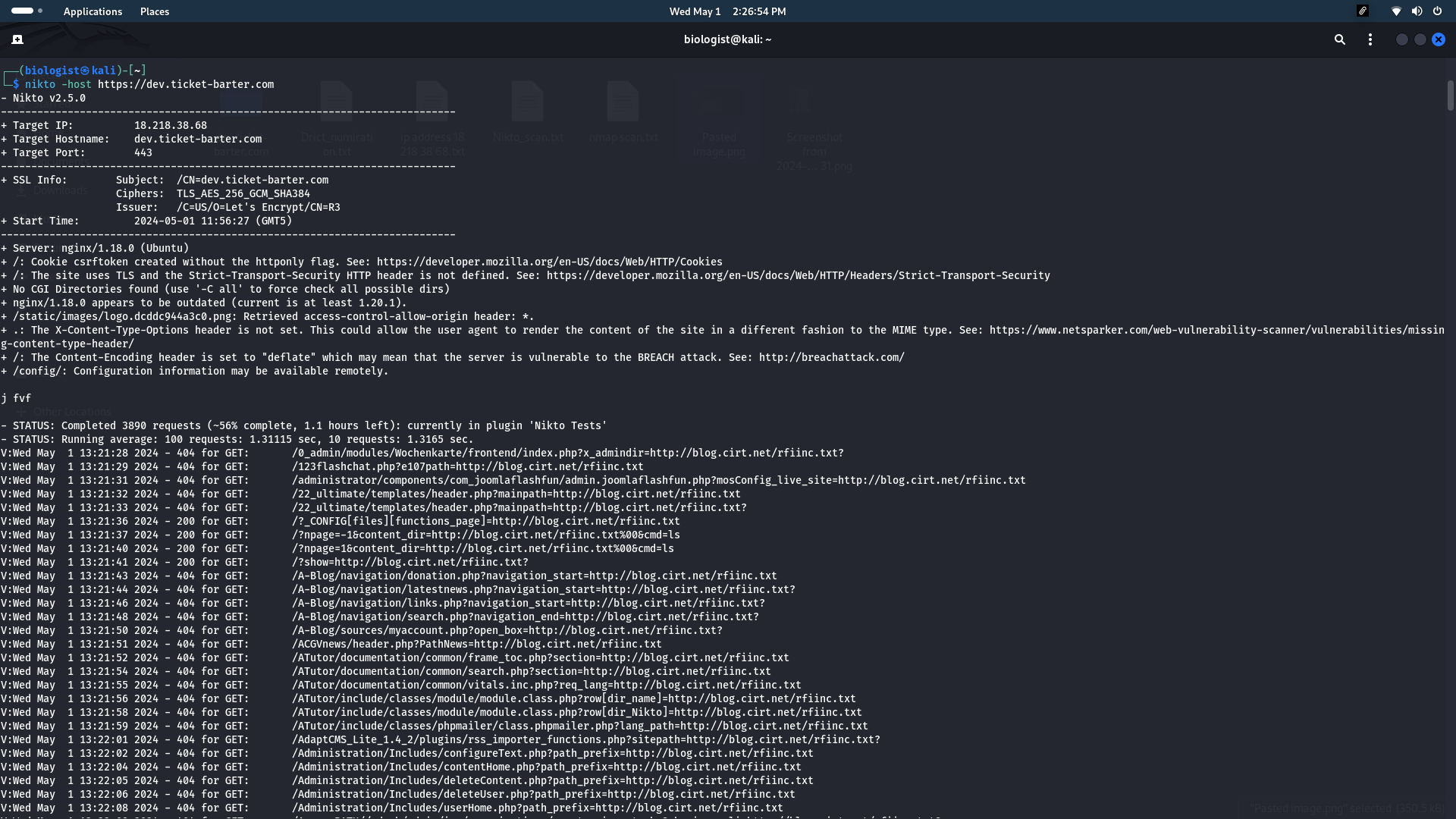
I used it to perform an automated scan on the website.

**Step 1:**

Mostly Nikto is pre-installed on kali Linux so open the terminal and run this command:

Nikto -host https://dev.ticket-barter.com

it will start scanning the website and in the end show the results. It will take sometime so leave it for a while.



**Step 2:**

After sometime it will show the results(list of existing vulnerabilities) in my case its:

* Cookie Flags Not Set (HTTPS only flag missing)
* Missing Strict-Transport-Security Header
* Outdated Server Software (nginx version 1.18.0)
* Missing X-Content-Type-Options Header
* BREACH Attack Vulnerability
* Potentially Exposed Configuration Information
* **Attack scenarios using Feroxbuster:**

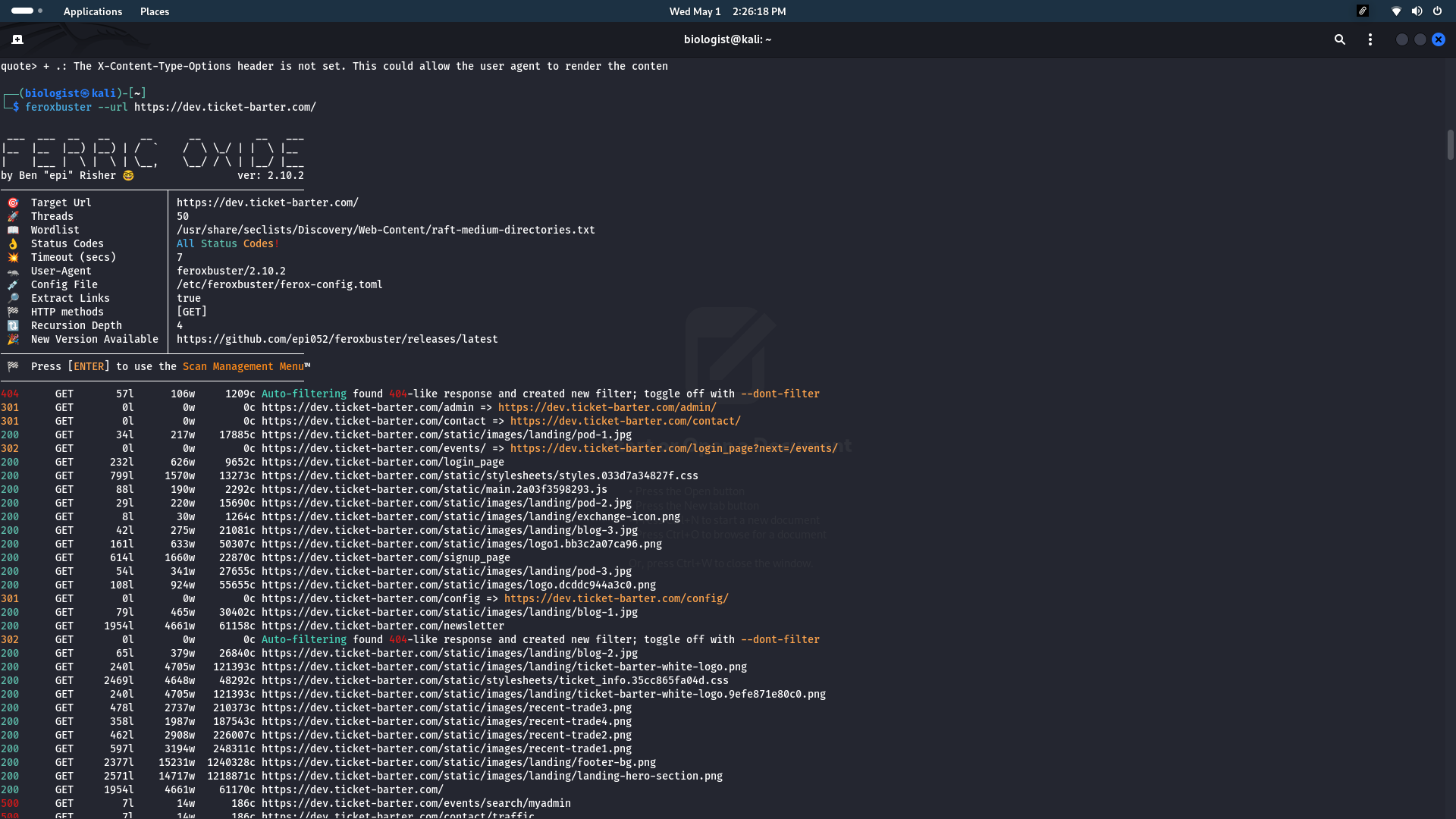
Feroxbuster is a powerful web content discovery tool designed to enumerate directories and files on web servers efficiently. It's commonly use to map out a target's web presence, uncover hidden resources, and identify potential attack vectors.

I used it for directory enumeration tin the seek of finding any fishy file in any directory

**Step 1:**

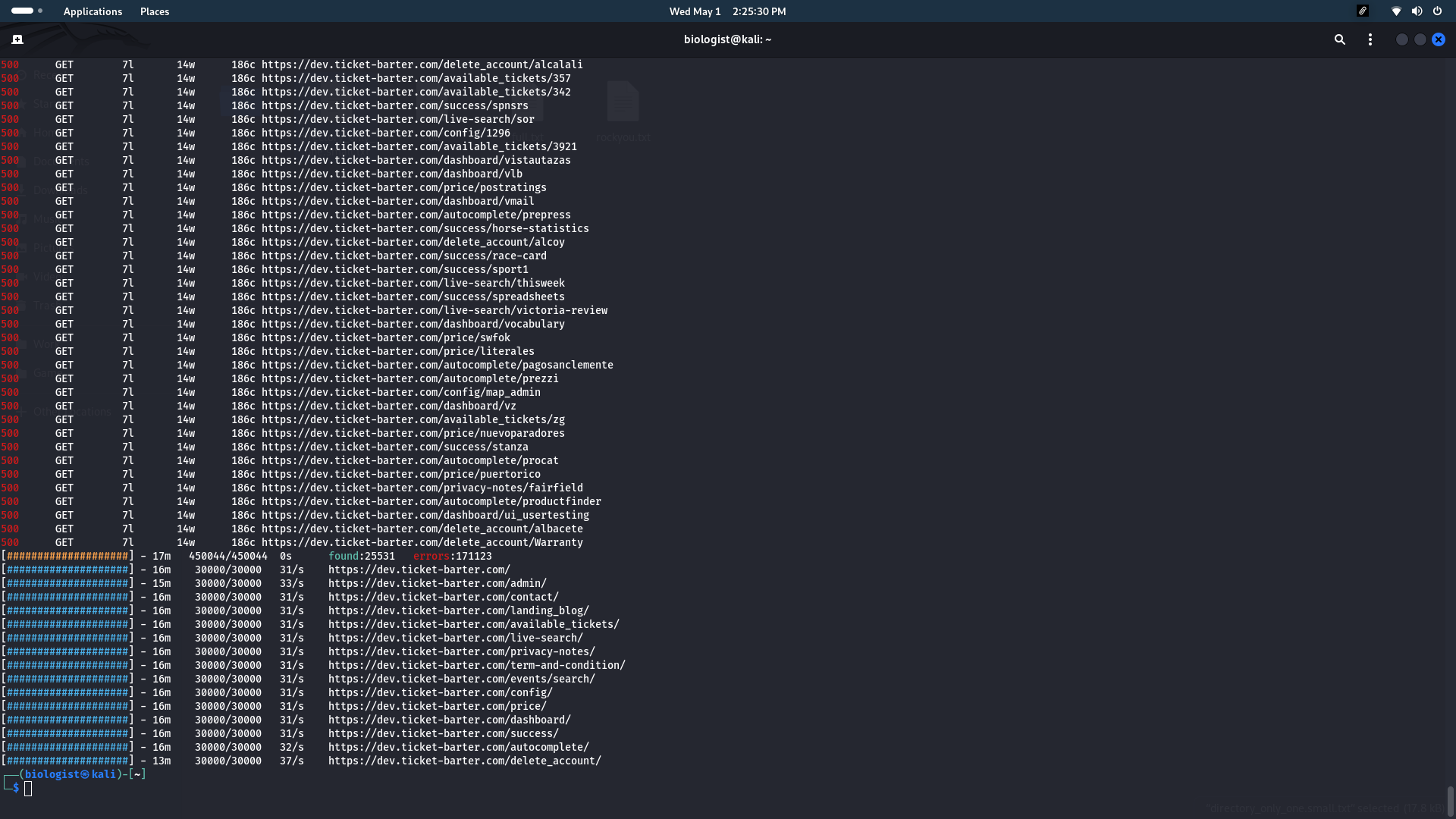
Open terminal and run this command:

feroxbuster –url [https://dev.ticket-barter.com](https://dev.ticket-barter.com/)



**Step 2:**

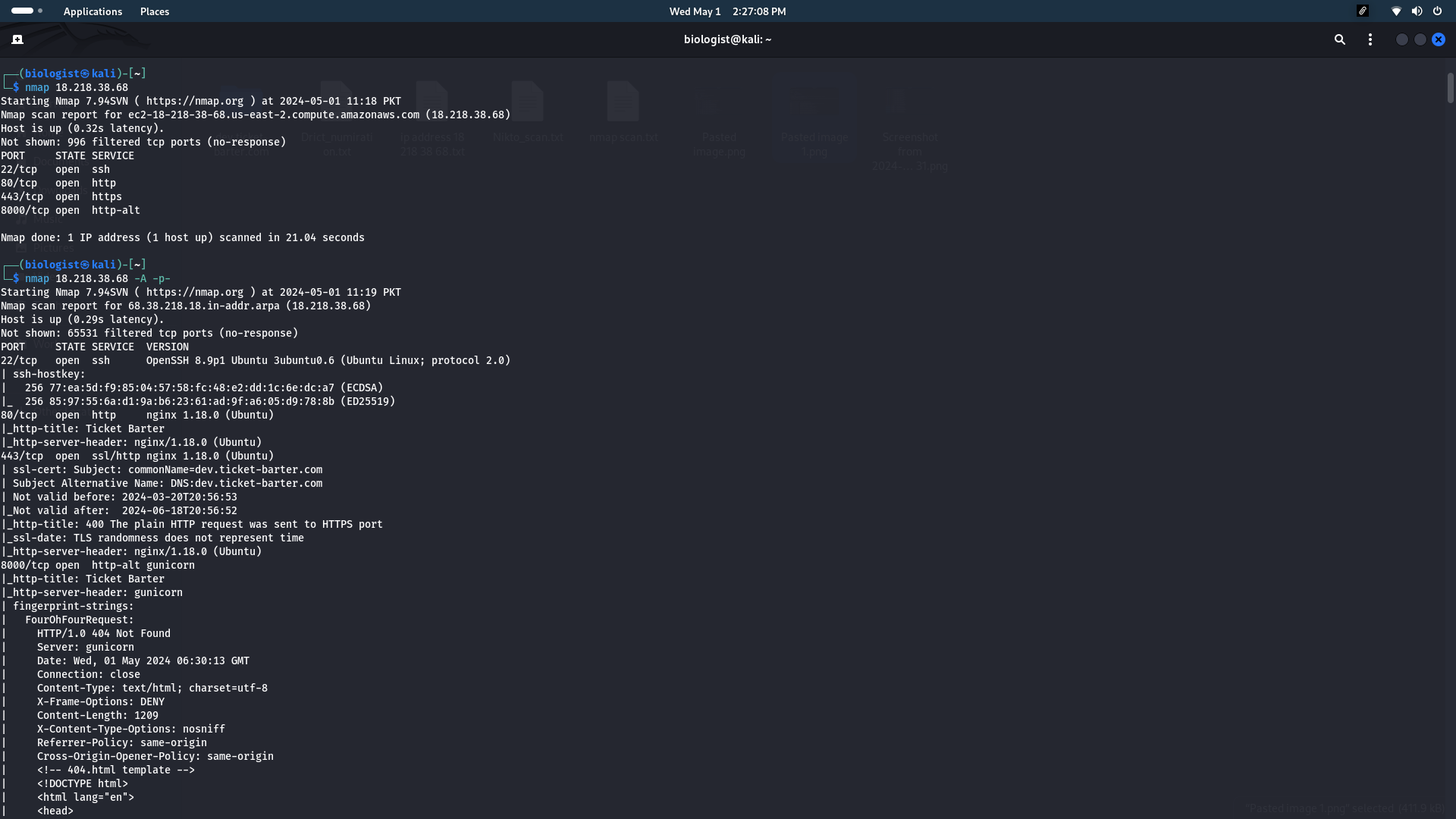
It will take sometime and then show the result all the accessible directories and files that may be hidden in browser(found that the config file is accessible):



**Quick nmap scan:**

Nmap is versatile open-source network scanning tool used for discovering devices and services on computer networks, thus creating a "map" of the network's structure. It facilitates tasks such as network inventory, service version detection, host discovery, and vulnerability scanning.

I used it for getting the basic network idea and check all the ports status and which service running on which port:

**Bas****ic scan:**

**Advanced/aggressive scan:**

