**CTF: Analysing and Exploiting HTTP Headers with Chrome Extension**

**1. Introduction**

HTTP headers are a fundamental part of web communication, containing essential metadata and instructions for both the server and the client. This CTF challenge will guide you through using a Chrome extension to analyse and manipulate HTTP headers to identify and exploit vulnerabilities.

**Tools and Requirements**

Web Browser: Google Chrome

Chrome Extension: "ModHeader" or any similar HTTP header modification extension

Target Website: <http://zero.webappsecurity.com>

Extension Link:

<https://chromewebstore.google.com/detail/http-headers/fabjnpecogealbfoebkcjfbmdhnnfhbj>

**Setup and Configuration**

1. Install ModHeader:

* Go to the Chrome Web Store and install the "ModHeader" extension.

2. Configure ModHeader:

* Open ModHeader from the Chrome extensions menu.
* Familiarise yourself with adding, modifying, and removing HTTP headers.

**Challenge Instructions**

1. Analyse HTTP Headers:

* Open Chrome and navigate to the target website: http://zero.webappsecurity.com.
* Use Chrome Developer Tools (F12) to inspect HTTP requests and responses.
* Identify common HTTP headers such as User-Agent, Referrer, Cookie, and Authorization.

2. Modify and Resend HTTP Headers:

* Use ModHeader to modify headers for requests to the target website.
* For example, change the `User-Agent` to impersonate a different browser or device.
* Resend requests and observe how the server responds to modified headers.

**Tasks and Questions**

Question: What is the status of the response connection <http://zero.webappsecurity.com/login.html>?

Answer: Keep-Alive / Keep Alive

Question: What is the minimum and maximum time of response alive ?

Answer: 5 and 100

**Hint and Tips**

Hint: Use the Network tab in Chrome Developer Tools to see detailed information about HTTP headers.

Tip: Modifying headers can sometimes reveal hidden functionality or vulnerabilities in how the server processes requests.

**Conclusion**

This CTF challenge is designed to teach you how to use Chrome extensions like ModHeader to analyse and manipulate HTTP headers, intercept HTTP traffic, and identify and exploit web vulnerabilities on `http://zero.webappsecurity.com`. By following these steps, you will gain practical experience in web security testing and vulnerability exploitation.

Detailed Steps for Each Task

1. Task 1: Inspect HTTP Headers

- Open Chrome and navigate to `http://zero.webappsecurity.com/login.html`.

- Press `F12` to open Developer Tools.

- Go to the "Network" tab and refresh the page.

- Click on the login request and examine the headers under the "Headers" section.

2. Task 2: Modify User-Agent Header

- Open ModHeader and add a new header with:

- Header Name: User-Agent

- Header Value: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.124 Safari/537.36`

- Navigate to http://zero.webappsecurity.com and observe any differences in how the site responds or renders.