Manipulating HTTP Request Headers with Header Tools

Introduction

Header Tools is a Firefox extension that allows users to inject and edit HTTP request headers. This can be useful for modifying requests, testing security configurations, and understanding server behavior based on headers.

Tools and Requirements

- Mozilla Firefox browser  
- Install the [Header Tools Firefox extension](https://addons.mozilla.org/en-US/firefox/addon/headertools/?utm\_source=addons.mozilla.org&utm\_medium=referral&utm\_content=search)  
- Basic understanding of HTTP request headers and web development

Scenario

As a participant in this CTF challenge, your task is to use the Header Tools Firefox extension to manipulate HTTP request headers sent to http://testphp.vulnweb.com/. Modify the headers and answer the following questions based on your findings.

Begin

1. Install the Header Tools Firefox extension from the provided link.  
2. Visit http://testphp.vulnweb.com/ and use the extension to inject and edit HTTP request headers.  
3. Utilize the extension features to answer the questions.

Questions and Answers

Flag 1: Use Header Tools to add a custom X-Test-Header with the value CTF-Challenge. What is the modified HTTP request header?

Answer:

X-Test-Header: CTF-Challenge

Flag Captured.

Flag 2: Modify the User-Agent header to Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.124 Safari/537.36. What is the updated User-Agent header value?

Answer:

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

Flag Captured.

Hint