Title: Analysis of Content Security Policy (CSP) Directives in Top Web Domains

Authors: Karl Mark, Seoyeon Choi

Institution: University of Albany

Introduction

Our project's aim was to analyze the distribution and configuration of Content Security Policies (CSPs) across various websites. We recognized the growing importance of CSPs in protecting against common security vulnerabilities like Cross-Site Scripting (XSS) and data injection attacks. By examining CSP implementations, we intended to understand the common practices and pinpoint prevalent misconfigurations that could undermine security efforts.

Methodology

Our methodology unfolded in four key steps:

1. Data Collection Setup: Utilizing a list of top-ranked domains (`ranked_domains.csv`), we targeted a diverse set of websites. We designed `Cspscrapper.py`, a sophisticated scraping tool capable of simulating human browsing patterns to evade anti-scraping technologies, ensuring ethical data collection.

2. Data Harvesting: The scraper was deployed to systematically gather CSP headers from the HTTP responses of the targeted websites. This process was meticulously monitored to maintain a low footprint and adhere to ethical scraping guidelines.

3. Data Analysis: With the collected data, we employed `CSPeval.py`, an analysis tool we developed to parse CSP headers. This tool assessed each directive's presence, configuration, and alignment with security best practices.

Results:

The analysis unveiled a spectrum of CSP implementations. Notably, directives like `frame-ancestors` and `script-src` were prevalent, reflecting a concerted effort to mitigate certain types of attacks. Yet, the presence of both overly permissive and overly restrictive policies signaled a lack of consistency and potential vulnerabilities.

Challenges and Limitations:

We encountered challenges primarily around anti-scraping measures, which limited our data collection breadth. Moreover, the ever-changing nature of web security policies posed a limitation to the longevity of our findings, as CSPs are frequently updated to counter emerging threats.

Conclusion:

Our exploration highlighted a varied landscape in CSP implementation, with a significant number of sites displaying configurations that could either compromise security or hinder

website functionality. These findings suggest a need for heightened awareness and regular reviews of CSP configurations.

Recommendations

We advocate for regular CSP audits using automated tools to ensure security directives are neither too lenient nor too restrictive. A balance should be sought to maximize security without impacting user experience. Our study underscores the necessity for ongoing education and adjustment of CSPs to adapt to the dynamic web security environment.

Graph Interpretations:

Included in the report are four graphs, each providing insights into different aspects of CSP configurations:

- Common CSP Misconfigurations: Shows the number of websites with specific misconfigurations, emphasizing the need for tighter security policies.
- Presence of Hash and Nonce Values in CSP Policies: Indicates low adoption of these practices, suggesting an area for enhanced security.
- Trends in Leniency and Strictness of CSP Directives: Compares the number of websites with lenient and strict CSP directives, revealing a trend towards leniency that may introduce security risks.
- Distribution of CSP Directives: Shows how frequently various CSP directives are used, indicating which security measures are prioritized by web developers.