HARDEN YOUR SITES WITH CSP
IMPLEMENT VITAL SECURITY CONTROLS TO BLOCK ADVANCED ATTACKST

TALA

CHALLENGE

Modern web apps and websites are "client-heavy" and much of the code executes via JavaScript on the client browser. Traditional security controls such as web application firewalls do not have visibility into client-side execution.
Content Security Policy (CSP), Sub-resource Integrity (SRI), HSTS, iFrame sandboxing, referrer-policy and other security policies offer very fine-grained security controls that protect the web application as it executes on client-devices. These security controls are available across mobile and PC browsers ensuring comprehensive coverage across your user base.

Properly configured policies can protect against cross-site scripting (XSS), clickjacking, JavaScript compromises, data exfiltration attacks and several others. Many industry web vulnerability scanners are also flagging lack of these security controls - a web application without these controls may not pass audit or risk management requirements.

Despite the availability of these critical security control mechanisms, as of December 2018, only a very small percentage of websites in the Alexa 1 million had implemented CSP and other controls.

Enterprises struggle to implement these important security controls and need an automated solution:

- Implementing CSP and other policies require DevOps and Infosec engineers to spend several man-weeks to study their applications and craft and fine-tune policies.
- Modern enterprise websites and web apps change often, and maintaining and updating policies becomes a significant burden on the Infosec organization.
- Incorrect policies can lead to vulnerabilities, or break legitimate functionality in the sites.
- Even if policies were implemented, enterprises find it very difficult to monitor violations and create appropriate incident

Subresource Integrity W3C

Content Security Policy Level 3 W3C

SOLUTION

Tala's enterprise website security platform provides a completely automated, end-end solution to enable important security controls such as CSP for your applications.

- **Automated, Precise Policies.** Tala auto-generates precise CSP (and other) policies based on our fine-grained behavioral model of an enterprise website, called the AIM, which identifies over 50+ behaviors for every page on your site.
  - Tala's AI driven engine automatically determines the most precise policies to protect your website based on page artifacts, script behavior and user device features.
  - Tala policies are continually updated as and when the website or web application is changed.
- **Real3time Protection and Incident Response.** Tala's policies can be installed on a web server in minutes, without requiring any code changes.
  - Tala combines the power of threat intelligence, AI and our own fine-grained behavioral model to provide precise attack analytics and incident response capabilities.

FEATURES & BENEFITS

- **Comprehensive:** Support for CSP, SRI, HSTS, referrer policy, iFrame sandboxing and more. Provides support for all CSP capabilities and directives including noncing, reporting and analytics.
- **Real-Time Protection:** Protection against XSS, clickjacking, redirection, ad injection, code injection and many other attacks.
- **Automated:** Tala policies are generated automatically and precisely with minimal manual intervention.
- **Continuous:** Tala integrates with CI/CD pipelines via APIs, and continually monitors your websites for changes.
- **Incident Response and Analytics:** Comprehensive analytics and incident response support to pin- point where and how your mission critical web assets are being attacked.
- **Quick Installation:** Tala policies install in minutes and require no changes to the application code. Tala supports all major web server technologies.

info@talasecurity.io | www.talasecurity.io