- Eseguire l'escape del testo JavaScript prima di inserire dati non attendibili nel codice JavaScript.
- Eseguire l'escape HTML di valori JSON prima di inserire i dati nel contenuto degli elementi HTML e leggere i dati con "JSON.parse".
- Eseguire l'escape CSS e attuare rigorose validazioni prima di inserire i dati non attendibili nei valori di proprietà di stile HTML.
- Eseguire l'escape dell'URL prima di inserire dati non attendibili nei valori dei parametri dell'URL.
- Bonificare i Markup HTML con una libreria progettata a tale scopo.
- Utilizzare il flag HTTPOnly per i cookie.
- Implementare la politica Content Security Policy.
- Utilizzare un sistema Auto-Escaping Template System.
- Utilizzare l'X-XSS-Protection Response Header.

Valutazione della priorità della minaccia (Ranking)

DREAD	Descrizione	Score
Damage Potential	Lo script malevolo può accedere a qualsiasi cookie, token di sessione o altre informazioni sensibili conservate dal browser (qui Browser Client) e utilizzati esclusivamente nel dialogo con il sito d'origine (qui Web Server). Questi script possono anche riscrivere il contenuto della pagina HTML. In definitiva il Tampering dell'url produce Information Disclosure, tra cui la compromissione del token di sessione che abilita il "Session hijacking" (che è una forma di furto di identità – spoofed identity). Nel peggiore dei casi, l'attaccante potrebbe impersonare l'amministratore del Web Server.	2
Reproducibility	L'attacco funziona sempre. Tuttavia il token di sessione (che è il dato la cui compromissione è particolarmente grave: spoofed identity) è utilizzabile finché la sessione non scade.	2
Exploitability	L'attacco non è banale: occorre una figura senior.	2
Affected Users	100% (nel caso in cui l'attaccante arrivasse a impersonare l'amministratore.)	3
Discoverability	Occorre identificare un url in cui un input utente ritorna in output senza aver subito alcuna bonifica o che può modificare il "DOM" enviroment.	1

DREAD Score: 10/15 (MEDIO)

7.2.5 Ripudio di dati da parte del 'Browser Client'

Categoria: Repudiation

Descrizione: Il 'Client Browser' sostiene di non aver inviato i dati al 'Web Server'.

Contromisure:

- È consigliabile che l'applicazione ricevente (qui 'Web Server') utilizzi file di log o di audit per registrare l'origine, l'ora e il riepilogo dei dati ricevuti, affinché il mittente di informazioni non possa negare l'invio delle stesse.
- Si raccomanda inoltre che il destinatario autentichi il mittente per assicurare che la comunicazione avvenga con il mittente corretto.