HTML5 e la sicurezza degli script

La bozza delle specifiche HTML5 relativa alle modifiche apportate all'elemento `script` in HTML5 evidenzia come anche per questo elemento si sia proceduto nel senso di una maggiore permissività e soprattutto come non si sia ancora una volta affrontato il problema della sicurezza e della funzionalità del codice caricato tramite questo elemento. Vediamo in dettaglio queste problematiche.

Script pericolosi?

Non esistono script pericolosi di per sè, ma esistono comportamenti potenzialmente pericolosi di per sè. La stragrande maggioranza delle violazioni di siti web comporta l'inserimento di codice JavaScript nocivo nelle pagine. I browser non sanno cosa sia questo codice, perchè non dispongono di un'euristica che invece gli antivirus hanno (come Kaspersky).

Il W3C non si è mai interessato di definire cosa può fare o non fare uno script in merito alla sicurezza di un sito e dei suoi visitatori. Sono stati gli implementatori di browser a porre dei limiti all'esecuzione degli script.

Tuttavia, esistono dei pattern nocivi ricorrenti:

1. inserimento di `iframe` nascosti
2. lunghe sequenze di `escape`

Questi pattern sono consentiti e vengono normalmente interpretati dai browser. Nel caso degli `iframe`, il problema è dovuto al fatto che questo tipo di elementi non ha le stesse restrizioni degli elementi `object`. Nel caso del codice con `escape`, tale pratica è consentita dal linguaggio JavaScript.

ECMAScript non cerca di porre rimedio al problema, per esempio introducendo un limite massimo di caratteri per una sequenza di `escape`. Francamente, nel mio lavoro non ho mai dovuto usare tali sequenze, quindi

è chiaro che si tratta di una pratica malevola. HTML5, dal canto suo, non pone restrizioni nè all'uso di elementi `script` nè all'uso di elementi `iframe`.

Per esempio, basterebbe istruire i browser ad ignorare uno script posto direttamente all'interno dell'elemento `html` o al di fuori del corpo della pagina. Mi sembra contraddittorio il fatto che si introduca l'attributo `async` per l'esecuzione differenziata e asincrona degli script e non si dica nulla sul codice eseguito all'interno dell'elemento `body`.

Meglio ancora sarebbe limitare il comportamento più nocivo, ossia il fatto di caricare URL esterni. Ma di tutto questo nè i browser nè gli implementatori nè il W3C sembrano volersi occupare.

Conclusioni

Sembra che HTML5 si concentri più su problemi teorici che non su quello che veramente interessa agli sviluppatori e ai proprietari di siti. Se avete avuto il vostro sito violato e riempito di script malevoli, sono sicuro che concorderete con me sulla necessità di affrontare il discorso della sicurezza degli script con maggiore decisione. Ma spesso si ha la sensazione che i problemi maggiori vengano trascurati in nome di qualcosa che, francamente, è poco utile.