IE Content-Type 無視

[IE]

http://www.atmarkit.co.jp/fcoding/articles/webapp/02/webapp02a.html

概要

・IE は“ text/plain ”と指定された Content-Type ヘッダに従わず、コンテンツ内に含まれる内容から「HTML」であると判断して、そこに含まれるスクリプトを実行する場合がある
・攻撃者によるクロスサイトスクリプティング（XSS）攻撃が可能となってしまう。
・IE が Content-Type だけでなく、ファイルタイプを決定するためにコンテンツの内容をスキャンする動作は「Content sniffing」と呼ばれる

対応

■ IE 側

・「拡張子ではなく、内容によってファイルを開くこと」を「無効にする」に設定する

■サーバ側

・レスポンスヘッダに X-Content-Type-Options: nosniff を追加する（IE8 向け）

ファイルタイプをどのように判断するか

・IE がコンテンツの処理方法を決定するための要因としては、少なくとも以下の 3 種類

1. サーバのレスポンスヘッダで指定された Content-Type
2. コンテンツ自身の中身（Content sniffing）
3.URL

" これら 3 種類の情報と、レジストリ（HKCR\Mime\Database\Content Type）に登録されている情報によってファイルタイプを決定していると考えられる """

・レジストリ（HKCR\Mime\Database\Content Type）には、IE が扱うことのできる Content-Type の一覧が格納されている。