Changes in Internet Explorer 8.0 that may cause browser incompatibility problems with web applications

Cross-Site Scripting Filter

XSS attacks have emerged as a leading exploit against Web servers and Web applications. Internet Explorer 8 has an XSS filter that is able to dynamically detect type-1 XSS (reflection) attacks. This helps protect users and systems from attacks that can lead to information disclosure, cookie stealing, account/identity theft or other attempts to masquerade as the user without permission.

DEP/NX Security Restrictions

DEP/NX helps to foil attacks by preventing code from running in memory that is marked non-executable. DEP/NX, combined with other technologies like Address Space Layout Randomization (ASLR), make it harder for attackers to exploit certain types of memory-related vulnerabilities like buffer overruns. In turn, this may cause some applications to crash unexpectedly.

File Name Restriction

Internet Explorer 8 form submission has been changed so that a file upload control (input type=file) only submits the file path to the server. Previously, the full path was sent to the server. This change may cause application compatibility issues with applications that assume a specific location for a particular file.

Codepage Sniffing

Internet Explorer 8 prevents certain codepages from participating in its Codepage Sniffing heuristic. Any pages that rely on this heuristic to be recognized as 7-bit Unicode Transformation Format (UTF-7) will no longer be detected.

AJAX Navigation

Internet Explorer 8 (IE8) includes an Asynchronous JavaScript and XML (AJAX) navigation feature that allows sites to maintain and track changes in AJAX states by treating them as navigation. This can be problematic for sites that were using the "location.hash" feature to send data between cross-domain components.

Application Protocol Detection

The Application Protocol Handler Dialog security feature protects users from accidentally executing an application with dangerous content. This feature may inadvertently cause some applications to hang or not respond as expected.

MIME Type Detection Restrictions

Internet Explorer 8 (IE8) uses web-based MIME information to determine how to handle files sent by a Web server. The MIME Handling Restrictions feature reports an unsafe content handler when the reported MIME file type does not match the observed MIME file type, and the content handler for the observed MIME file type is unsafe.

Web Proxy Error Handling Changes

Internet Explorer 8 blocks application content returned by a proxy from a failed CONNECT command, or displays the content in a context based on the hostname of the proxy rather than in the context of the origin server. This may cause an application to hang or not behave as expected.

Signed Certificate Filtering

Microsoft's Internet Explorer 8 (IE8) uses Certificate Filtering to select the appropriate certificate for client authentication. This feature has been improved from the version in IE7 to remove certificates that are likely to be rejected by the server. This may cause some intranet or in-house developed applications to fail.

Source: ChangeBase