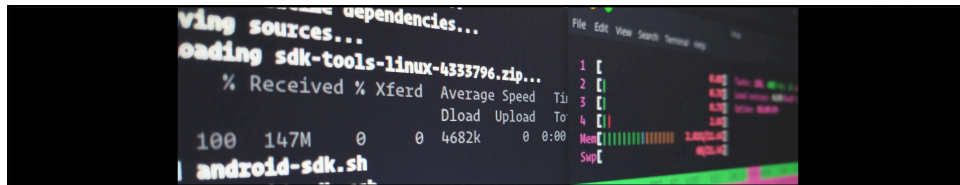


XSS in eXceSS: A "learn-XSS tool"

Martin Paul Eve

16 May 2007 (last updated 6 September 2026)



Cite as: Martin Paul Eve, "XSS in eXceSS: A "learn-XSS tool"", *eve.gd: Martin Paul Eve*, May 16, 2007, <https://doi.org/10.59348/xwgby-3hj54>.

DOI: <https://doi.org/10.59348/xwgby-3hj54>

Available at: <https://eve.gd/2007/05/16/xss-in-excess-a-learn-xss-tool/>

kishord today presents a tool, called [XSS in eXceSS](#) and hosted by [.mario](#) that will allow you test attack vectors against a page in different contexts. On top of that it also incorporates [PHP IDS](#), allowing you to skip whichever rules you choose.

From kishord's post:

It takes the input via various get parameters and leads to different areas in the HTML page. E.g. parameter `freehtml=ATTACK_VECTOR` will place the injection in to the HTML body. There are more than 25 such parameters which lead to different XSS areas.

Please read the usage notes on the [page](#).

In order to make it a learning tool, it is coupled with PHP IDS with some modifications. It lets the user choose which IDS rules to skip. Thus each XSS area now can be XSSed by challenging different filters. E.g. If you are able to attack in an area where only the `<script>` can cause an injection, (E.g. html body, ummm, well ignore other cases for now) then you have to ask the page to skip the filter that detects script tag.

Good stuff!

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.

.mario's security blog <http://mario.heideri.ch/>

kishord WAS Journal post on XSS in eXceSS tool

<<http://wasjournal.blogspot.com/2007/05/xss-in-excess.html>>