

One vector to rule them all

One vector to rule them all - Gareth Heyes, thespanner.co.uk.

- Published: date not stated
- Original: <<http://www.thespanner.co.uk/2010/09/15/one-vector-to-rule-them-all/>>
- Current location: <<https://thespanner.co.uk/2010/09/15/one-vector-to-rule-them-all>>
- Preserved from: <https://thespanner.co.uk/2010/09/15/one-vector-to-rule-them-all> (stored) on 2026-08-17
- 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.

I set myself a fun challenge to create a vector that would execute in many contexts. The idea being that it should work regardless where it's placed. For example:-

```
"xss"  
'xss'  
<tag alt="xss">
```

As an added challenge I tried to execute only the one payload and where possible to use a single eval. I had to use multiple evals as the contexts increased because for stuff like background= etc there was no way I could figure reusing the existing one :(So I had around 19 then got bored.

One vector to xss them all, one vector to find them, One vector to bring them all and in the darkness bind them.

```
javascript:/*-->]]>%>?></script></title></textarea></noscript></style></xmp>">[img=1,name=/alert(1)/.source]<img -/style=
```

Updated added new vectors and removed any that weren't required. Thanks to @LeverOne!!

2nd Update...Fixed comments, added name to `[]` rule so it executes without `window.name` for dom rules. Thanks again for some fixes by @LeverOne