JQuery XSS DOM:

JqueryXSS.html Finding

Another approach a friend of mine once used was this:

var hash = location.hash.split('#')[1];

This also has its issues, which are ironically less than the first one, even though it seems a far more naive approach.

* With the same test hash, it would at least get the "foo@o" part, which means it only fails when the hash contains a pound sign
* When there’s no hash, it doesn’t throw an error, although it returns undefined instead of the empty string.

JqueryXSS2.html Finding

.html() will just call .innerHTML after doing some checks for nodeTypes and stuff. It also uses a try/catch block where it tries to use innerHTML first and if that fails, it'll fallback gracefully to jQuery's .empty() + append()

AngularJS XSS

Angular.html and angular2.html

Pay attention to the HTML code entered in the text field. It is printed as it is, on to the HTML page. Having a bit of trouble making it work.