XSS Checklist

□ Automation Script

□ Automation Script for Blind XSS

□ Use Arjun for hidden parameters

□ Gxss for testing reflected parameters

□ Kxss for testing unsafe characters

□ Tools Xsstrike for specific parameter

□ Burpsuite plugins (Reflection + sentinal)

□ https://xssor.io/ for encoding/decoding

- [ ]

Encoding

□ url encoding for unsafe character

□ url encoding for the whole payload

□ double url encoding for unsafe character

□ double url encoding for the whole payload

□ Use combination of Lower + UpperCase

□ Insert **%00** at any point

□ use invalid tag `<any onload=alert></any>`

□ use `<base href="url/payload.js">`

□ insert %00 in the attribute name `<img src=x o%00nclick=alert()>`

□ use attribute delimeters ``<img src=`x` onclick=alert()>``

□ HTML encoding for unsafe character

□ HTML for a character of `alert()`

□ HTML for anything you want

□ Unicode

□ use extra brackets `<<script>alert();//<</script>`

□ Payload strange works by firefox `<script<{alert(1)}/></script>`

□ UTF-7 encoding `+ADw-script+AD4-alert()+ADw-/script+AD4-`

□ US-ASCII encoding `1/4script3/4`

□ UTF-16 encoding