

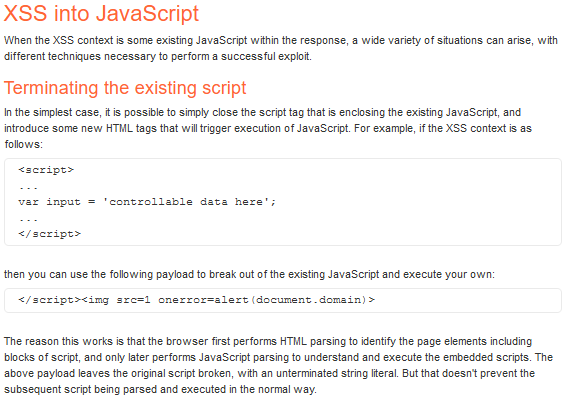
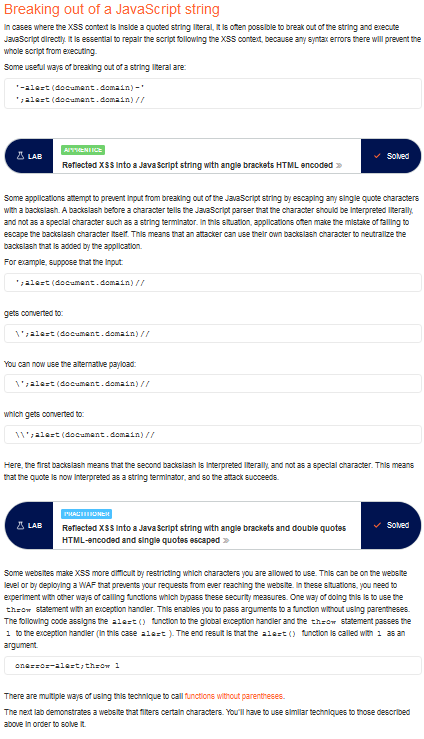
Graphical user interface, text, application, Teams

Description automatically generated

In some cases we can literally add the following as a parameter to the url to cause reflected xss:

'accesskey='x'onclick='alert(1)

This will cause the alert function to get executed when a certain set of buttons are pressed in this case alt+x or crtl+alt+x. We can literally add /? Followed by the payload to the url to basically create a parameter and set an accesskey for the entire page. In real world, look for thr structure of how parameters work and try to add this or just replace the value of an existing parameter.



Find what important chars are encoded and try to use payloads that make use of chars that aren’t being encoded.

Graphical user interface, text, application, email

Description automatically generatedwhen you see a / appearing before a special char after you submit your payload, this shows you that the app is trying to escape that character to basically make it act like a char in a string to stop us from being able to break out. Often if we see this adding a \ before the char being escaped could escape the \ being added by the application. This is basically escapes the escape char(\) being put in by the application.

Graphical user interface, text, application, email

Description automatically generated

Look for input being reflected in a script or string encapsulated in backticks ``, like shown below. This is some JQuery or other template stuff so we can just call a new function with the ${} syntax.

Text

Description automatically generated with medium confidence