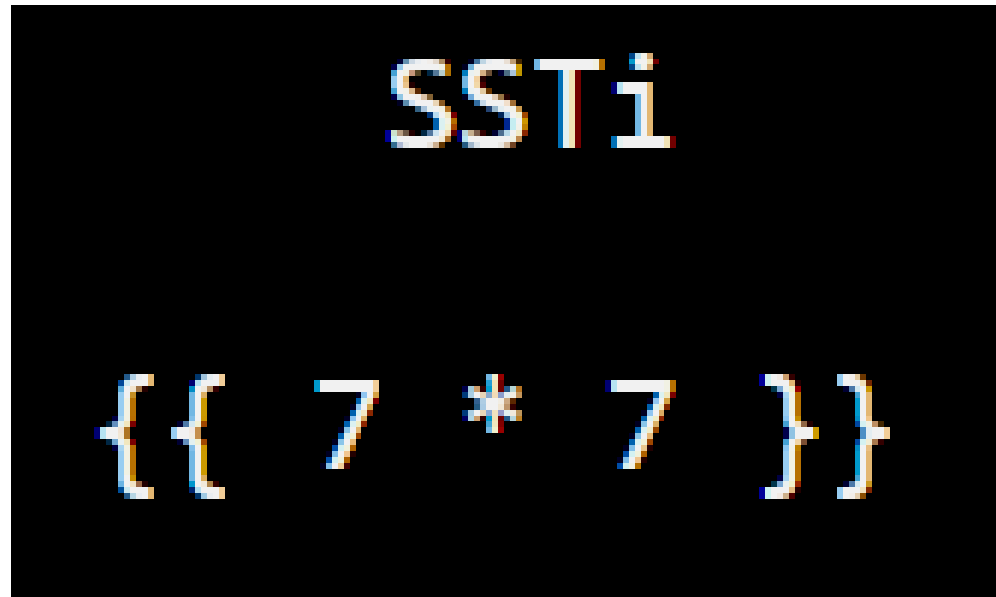
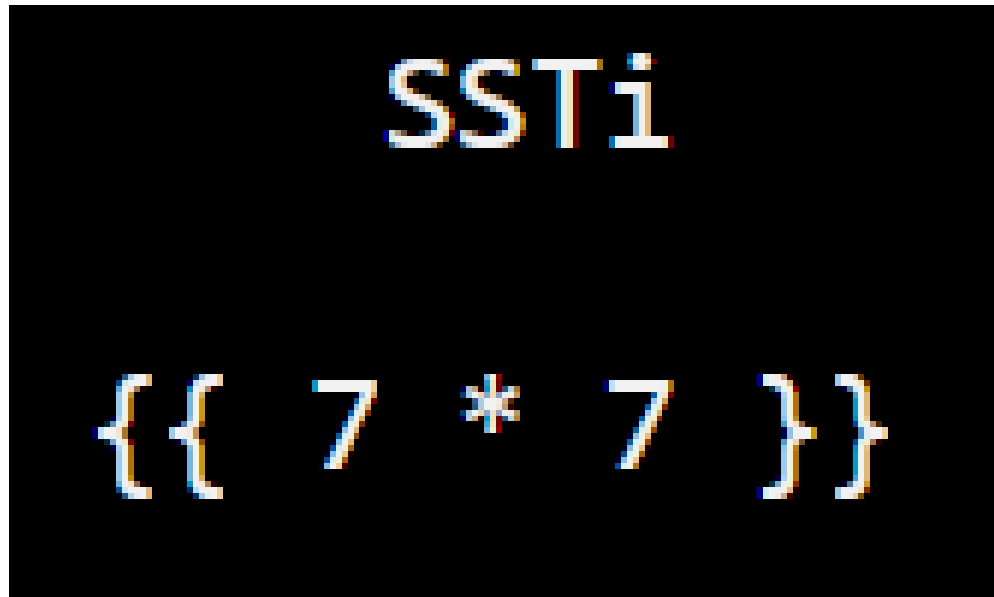


SSTI1 – SSTi Vulnerability



SSTi (server-side template injection) is a web app vulnerability where the app uses a templating engine to create web page content--

SSTI1 – SSTi Vulnerability



But if the app is coded insecurely, a user could inject malicious code into the app to interact with the templating engine to achieve remote code execution on the app

SSTI1 – SSTi Vulnerability

What do you want to announce: hackerfrogs rule!

Ok

**hackerfrogs
rule!**

A very common way to identify a potential SSTi vulnerability is when we find a webpage which echoes back user input

SSTI1 – SSTi Vulnerability

49

If we can ID such a webpage, we can confirm the vulnerability by having the app perform math operations