CSTI

What is it?

CSTI: Client side template injection

This type of vulnerability occurs when developers use a client side templating engine such as vue or angular. These templating engines allow us to push code to the client that contains placeholders (ex. {{NAME}}). These placeholders will then be replaced in the clients browser with their respective values.

These types of vulnerabilities are not researched well at yet and it will be up to the hunter to properly research this vulnerability when it is encountered. First of all try to get to know what templating engine is being used, then look up how that engine works and try to find out how to exploit the issue.

Attack strategy

Our attack strategy taught us that we should insert an SSTI attack vector in every possible input field. This should in theory allow us to identify CSTI vulnerabilities as well.

When we identified a resolved attack vector, it's important that we know how the templating engine works because we need to craft a good attack vector with proper impact as our basic attack vector was {{7*7}}. This attack vector would resolve to 49 which means a calculation gets executed. This would give us a pretty good idea that a CSTI vulnerability exists but ofcourse, using a website as a calculator is not really a vulnerability. We will have to increase our impact before we report this vulnerability.

The impact itself will also highly depend on what we are able to pull off. CSTI vulnerabilities lead to XSS attacks which we can exploit like any other XSS attack, however if the templating engine is only used to display non-sensitive public data, there's nothing much we can steal with our attack of value and it will be marked as a low impact issue. If, however, there exists another application on the same domain that can access the session cookies, we might be able to steal those and raise our severity.