Resources that you are loading how much do you trust? Are they really reliable or not? You can say that ohh I trust this domain but the content which are coming from the domain what if that domain goes on a toss, if there is a hack on the domain which you trusted basically right.

So consider we have some application which is a.com and I am loading some resources may be from some cdn or it can be some b.com, what I have mentioned when I loading from this resources I clearly mentioned that I trust this, basically I am saying this is my trusted resource using cors or some csp but the problem is I trust the company b.com as an whole but what about the resource inside that, what if the employee cheated ? what will happen? Or some of the resources of b.com got hacked or someone interrupted in between.

So how you can ensure that such thing cannot happen? For example we are using bootstrap cdn link in our webpage then how it ensure lets see.

<link href="https://cdn.jsdelivr.net/npm/bootstrap@5.3.3/dist/css/bootstrap.min.css" rel="stylesheet"

integrity="sha384-QWTKZyjpPEjISv5WaRU9OFeRpok6YctnYmDr5pNlyT2bRjXh0JMhjY6hW+ALEwIH" crossorigin="anonymous">

so, in above link there is one attribute called integrity and it has some sha, what does this sha says that? The sha says that there is some base 64 encoded code is generated this is a source of truth if you load this script again and you try to encrypt it again with this particular sha that you have using a crypto algorithm, if you create a crypto hash of this content using sha algorithm you will get the same hash and browser does exactly same.

So, there are certain steps which are involved –

* Browser download the resource
* Generate cryptographic Hash using sha384, 256, 512
* Generate hash using component + algorithm + crypto function
* Compares the generated hash with integrity attribute

Benefits –

* 3rd party resource is compromised
* Any content update inside resources (e.g version upgrade)