XML eXternal Entity Injection

Text

Description automatically generated with medium confidence

Background info on XML entities:

This section will explain some key features of XML which we need to know to master the XXE injection.

Graphical user interface, text, application, email

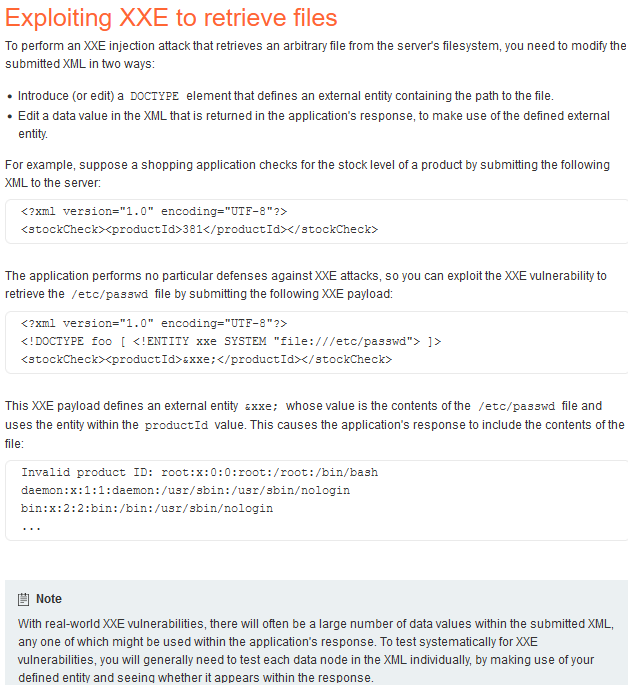
Description automatically generatedGraphical user interface, text, application, email

Description automatically generated

How/ where XXE arises and types of exploits

Graphical user interface, text, application, email

Description automatically generated



The basic idea is to modify or add the doctype declaration to any XML contained within the request. Then modify the request to use that entity you declared. Example:

Text

Description automatically generated

Text

Description automatically generated with medium confidence

Graphical user interface, text, application

Description automatically generated

Graphical user interface, text, application, email

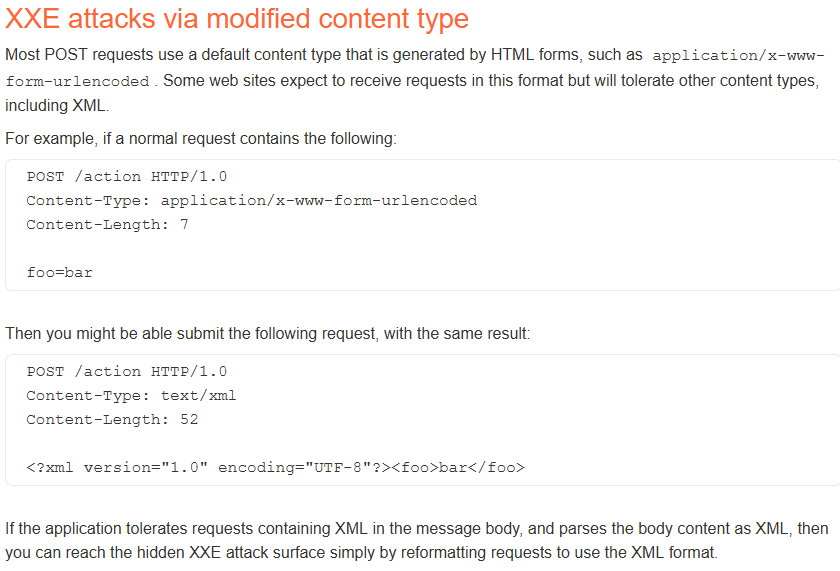
Description automatically generated--------------------------------------------------------------------------------

Often times we can upload .svg or .docx files to get processed like and XML document. Just start with a .txt file insert the malicious XML code inside and convert it to file of choice. Even if the app limits the content that can be submitted we can often bypass these restrictions. Uploading a .svg file with the following contents could trigger XXE vulnerability:

<?xml version="1.0" encoding="UTF-8"?>

<!DOCTYPE foo [ <!ENTITY xxe SYSTEM "file:///etc/hostname"> ]>

<svg width="128px" height="128px" xmlns="http://www.w3.org/2000/svg" xmlns:xlink="http://www.w3.org/1999/xlink" version="1.1"><text font-size="16" x="0" y="16">&xxe;</text></svg>



Graphical user interface, text, application, email

Description automatically generated