XML, XXE

Challenges

XML External Entity (root me) : https://www.root-me.org/en/Challenges/Web-Server/XML-External-Entity
- http://repository.root-me.org/Exploitation%20-%20Web/EN%20-%20XML%20External%20Entity%20Attacks%20(XXE)%20-%20owasp.pdf
- http://repository.root-me.org/Exploitation%20-%20Web/EN%20-%20What%20You%20Didn't%20Know%20About%20XML%20External%20Entities%20Attacks.pdf
- this is the xml rss format
- https://www.w3schools.com/xml/xml_rss.asp
- a good writeup : https://taind.wordpress.com/2017/12/25/root-me-xml-external-entity/

<!ENTITY xxe SYSTEM "php://filter/convert.base64-encode/resource=index.php"

Notes

https://github.com/swisskyrepo/PayloadsAllTheThings/tree/master/XXE%20Injection
https://portswigger.net/web-security/xxe

What is XML?
XML stands for "extensible markup language". XML is a language designed for storing and transporting data. Like HTML, XML uses a tree-like structure of tags and data. Unlike HTML, XML does not use predefined tags, and so tags can be given names that describe the data. Earlier in the web's history, XML was in vogue as a data transport format (the "X" in "AJAX" stands for "XML"). But its popularity has now declined in favor of the JSON format.

What are XML entities?

XML entities are a way of representing an item of data within an XML document, instead of using the data itself. Various entities are built in to the specification of the XML language. For example, the entities < and > represent the characters < and >. These are metacharacters used to denote XML tags, and so must generally be represented using their entities when they appear within data.

What is document type definition?

The XML document type definition (DTD) contains declarations that can define the structure of an XML document, the types of data values it can contain, and other items. The DTD is declared within the optional DOCTYPE element at the start of the XML document. The DTD can be fully self-contained within the document itself (known as an "internal DTD") or can be loaded from elsewhere (known as an "external DTD") or can be hybrid of the two.

What are XML custom entities?

XML allows custom entities to be defined within the DTD. For example:
<!DOCTYPE foo [<!ENTITY myentity "my entity value" >]>
This definition means that any usage of the entity reference &myentity; within the XML document will be replaced with the defined value: "my entity value".

What are XML external entities?

XML external entities are a type of custom entity whose definition is located outside of the DTD where they are declared.
The declaration of an external entity uses the SYSTEM keyword and must specify a URL from which the value of the entity should be loaded. For example:
<!DOCTYPE foo [<!ENTITY ext SYSTEM "http://normal-website.com" >]>
The URL can use the file:// protocol, and so external entities can be loaded from file. For example:
<!DOCTYPE foo [<!ENTITY ext SYSTEM "file:///path/to/file" >]>
XML external entities provide the primary means by which XML external entity attacks arise.