External Entity Injection (XXE) Prevention in PHP

a) This is an attack against a web application that parses XML* input. This input can reference an external entity, attempting to exploit a vulnerability in the parser. An ‘external entity’ in this context refers to a storage unit, such as a hard drive. An XML parser can be duped into sending data to an unauthorized external entity, which can pass sensitive data directly to an attacker.

b) *XML or Extensible Markup Language is a markup language intended to be both human-readable and machine-readable. Due to its complexity and security vulnerabilities, it is now being phased out of use in many web applications.

c) **JavaScript Object Notation (JSON) is a type of simple, human-readable notation often used to transmit data over the internet. Although it was originally created for JavaScript, JSON is language-agnostic and can be interpreted by many different programming languages.

Prevention:

a. The best ways to prevent XEE attacks are to have web applications accept a less complex type of data, such as JSON.

b. Disable the use of external entities in an XML application.

In project’s code:

1- Make sure you write this function in your code before XML parsing:
`libxml_disable_entity_loader(true)`

2- Don’t use LIBXML_NOENT flag during XML parsing
Example:

```
$dom->loadXML($xml, LIBXML_NOENT);
```

must be

```
$dom->loadXML($xml);
```

LIBXML_NOENT flag can be found/used in a lot of functions such as:
simplexml_load_string(), simplexml_load_file(), loadXML()

So make sure you remove it from them, in your code.

3- Make sure your PHP version is up to date so the XML Parser version is up to date, otherwise your web app would be vulnerable to XML DoS attacks.

All Above Explained ideas will be Scanned in the Toolkit.

To watch about how an attack can be performed
https://www.youtube.com/watch?v=DREgLWZqMWg

To learn more, go here:

https://www.youtube.com/watch?v=g2ey7ry8_CQ
https://stackoverflow.com/questions/38807506/what-does-libxml-noent-do-and-why-isnt-it-called-libxml-ent
https://gist.github.com/lukaskuzmiak/c8306a5af855c6faaaee
https://cheatsheetseries.owasp.org/cheatsheets/XML_External_Entity_Prevention_Cheat_Sheet.html
https://owasp.org/www-project-top-ten/OWASP_Top_Ten_2017/Top_10-2017_A4-XML_External_Entities_(XXE)