

20200716信息安全实训

笔记本： 我的第一个笔记本

创建时间： 2020/7/16 14:32

更新时间： 2020/7/16 17:43

作者： 820410740@qq.com

URL： <https://www.cnblogs.com/flokz/p/xxe.html>

xxe漏洞 (XML外部实体)

xml的主要作用 传输数据

XXE (外部实体注入) 是XML注入的一种, 普通的XML注入利用面比较狭窄, 如果有的话也是逻辑类漏洞。XXE扩大了攻击面。

当允许引用外部实体时, 就可能导致**任意文件读取、系统命令执行、内网端口探测、攻击内网网站**等危害。

防御方法: 禁用外部实体 (PHP: 可以将libxml_disable_entity_loader设置为TRUE来禁用外部实体)

<https://www.cnblogs.com/flokz/p/xxe.html>

https://blog.csdn.net/new_Smile/article/details/51768145

DTD的作用

XML文档是一种元标记语言, 即一种定义标记语言的语言。在XML中可以创建新的标记语言, 这些新的标记语言(也叫标记集)要通过文档类型定义(Document Type Definitions, DTD)来定义。DTD文档是这些新的标记语言的法律性文档。如果XML文档的语法符, DTD的定义和规定, 那么就称为一个合法的XML文档, 否则就是非法的XML文档。合法的XML文档在实际应用中的地位很重要, 因为只有合法的XML文档才能被应用软件有效地处理。

DTD定义了文档的逻辑结构, 规定了文档中所使用的元素、实体、元素的属性、元素与实体之间的关系。其作用主要表现在以下几个方面。

- (1) 使用DTD可以提供一种统一的格式。XML的可扩展性为文档的作者提供了很高的灵活性, 可有时候需要的是统一, 要求某一类文档具有相同的结构。
- (2) 使用DTD可以保证数据交流和共享的顺利进行。
- (3) DTD使用户能够不依赖具体的数据就知道文档的逻辑结构。在没有XML文档的时候, 也可以根据DTD为XML文档编写样式单, 编写处理程序, 这样可以有效地提高工作效率。
- (4) 使用DTD可以验证数据的有效性。DTD对文档的逻辑结构进行了约束, 这种约束可以比较宽松, 也可以十分严格。可以根据DTD检查数据, 以验证其是否符合规定和要求, 这可以保证数据的正确和有效。

DTD元素

DTD中描述的基本部件是元素和属性, 它们负责确定XML文档的逻辑结构。元素表示一个信息对象, 而属性表示这个对象的性质。所有元素中有且只有一个根元素, 其他的元素都是它的子元素, 除根元素外, 每个元素都被其他元素包含, 一个元素可以有几个不同类型的子元素。

robots协议 robots.txt

<https://www.batmanit.com/p/453.html>