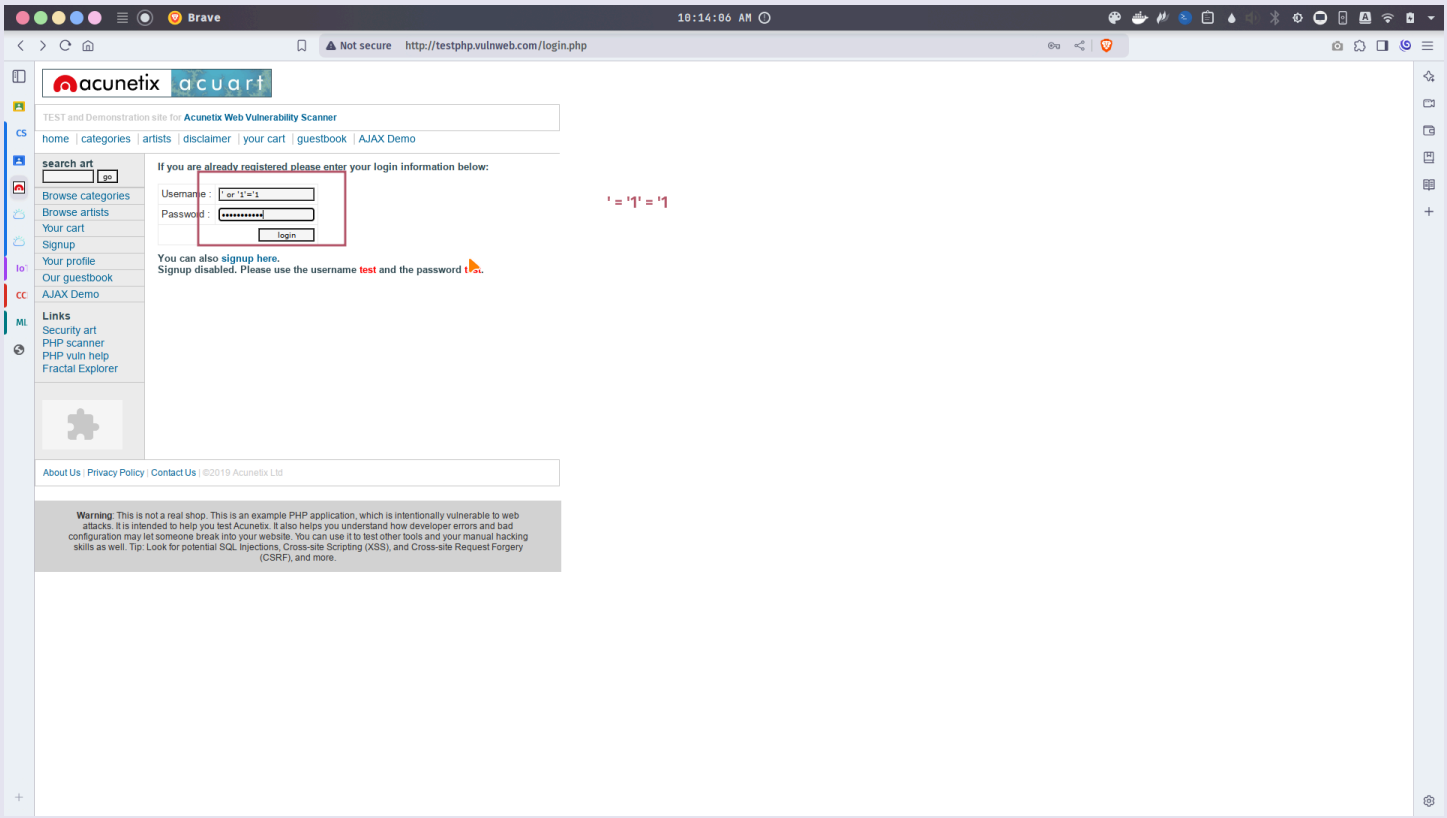
Name - Yash Lakhtariya
Enrollment number - 21162101012
Branch - CBA Batch - 71
CS Practical 2

Scenario : You are a cloud security analyst for ane-commerce website (testphp.vulnweb.com), and your task is to perform a security assessment of their online store. During the assessment, you discover a potential vulnerability in their functionality, which is susceptible to a Union-based SQL injection attack. Exploit the functionality of the e-commerce website to bypass the login page as well as retrieve sensitive information from the database.

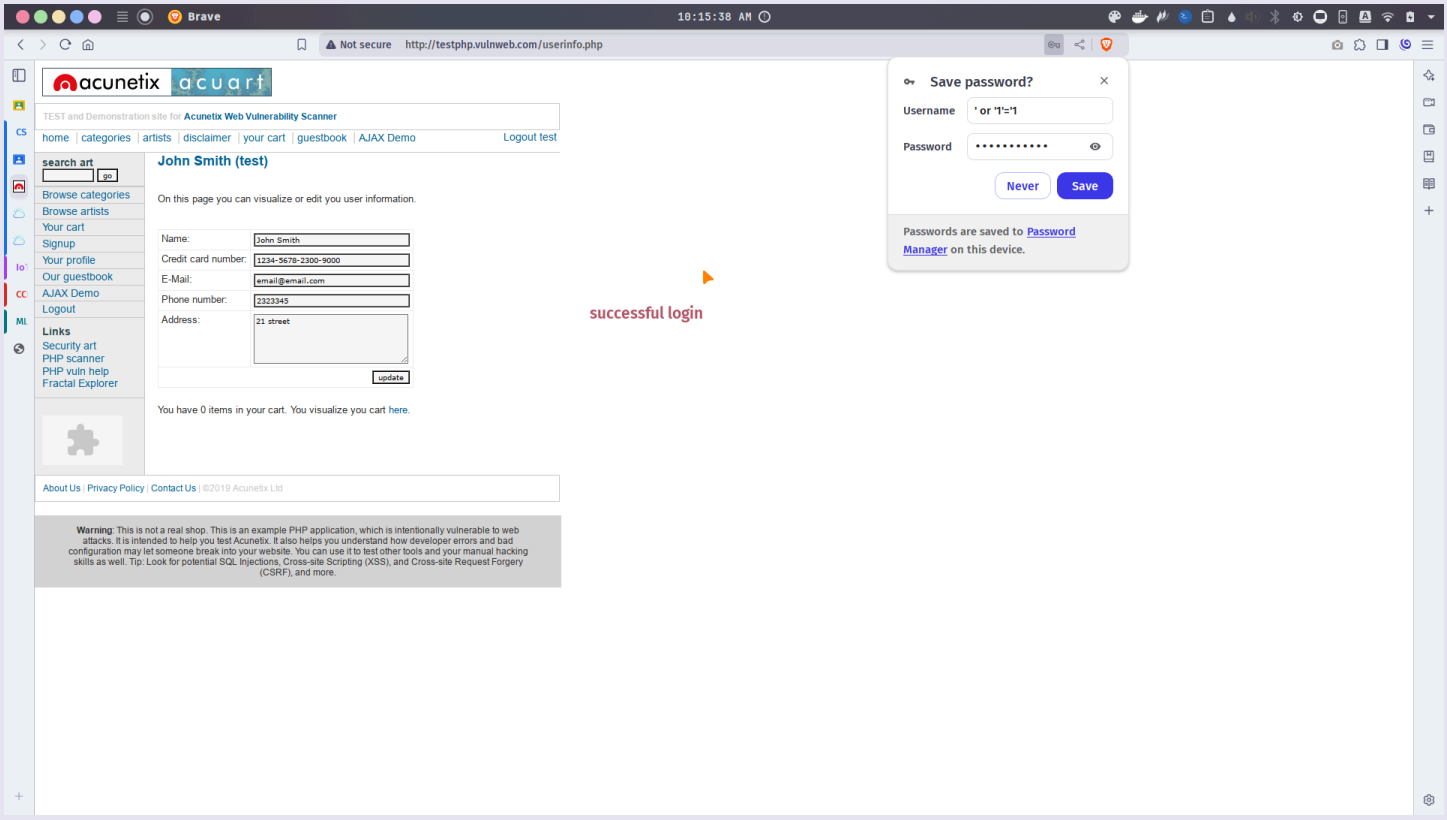
TASK:
https://demo.testfire.net/index.jsp?content=personal_deposit.htm
Identify any 3 web application vulnerabilities and website defects in the provided link

Screenshots and steps :

1. Visit Your profile tab in testphp site and login using ‘1 or ‘1’=‘1 (As it can be SQL query of username and password, true condition in or can be used to hack)

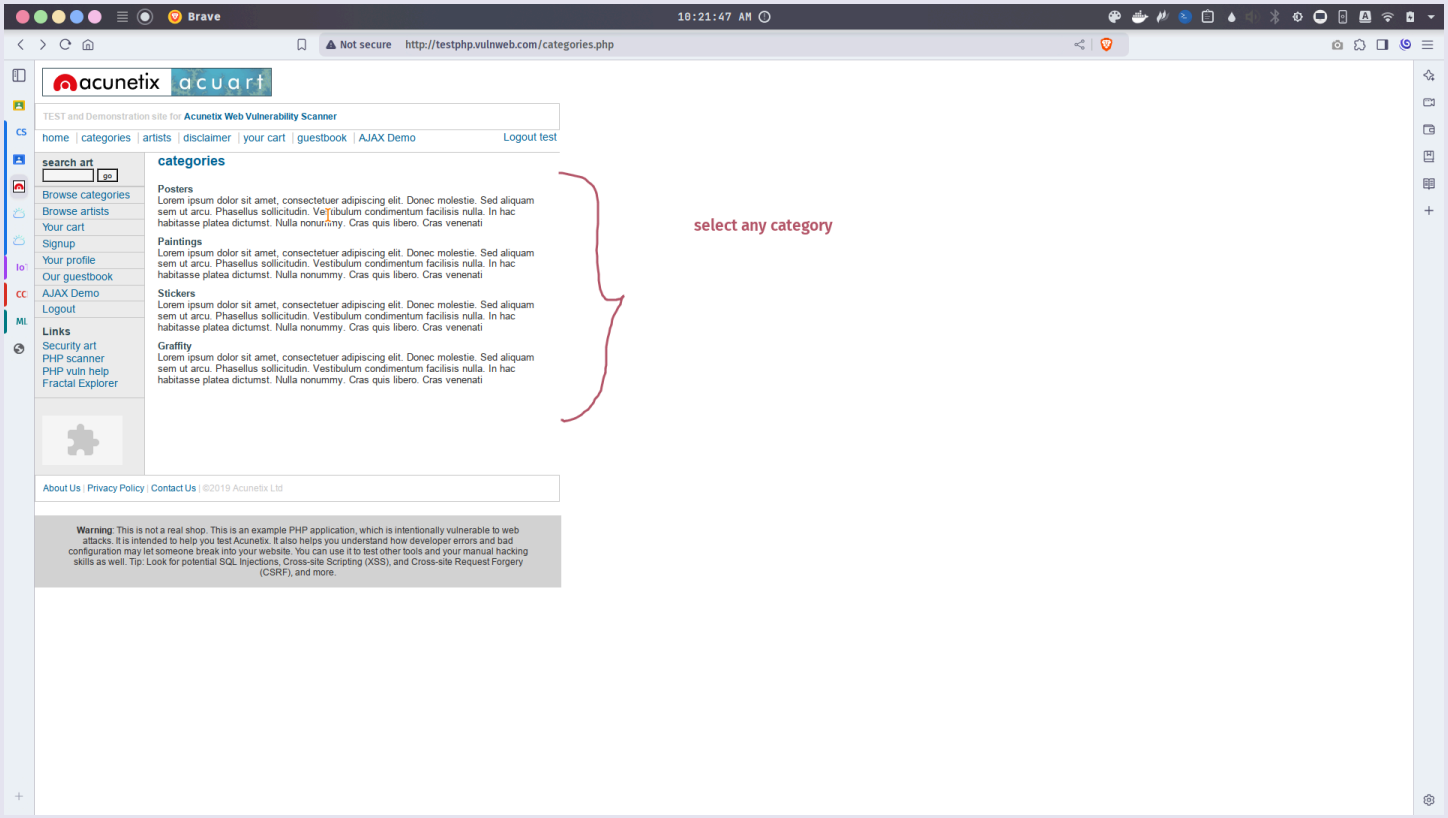


Name - Yash Lakhtariya
Enrollment number - 21162101012
Branch - CBA Batch - 71
CS Practical 2

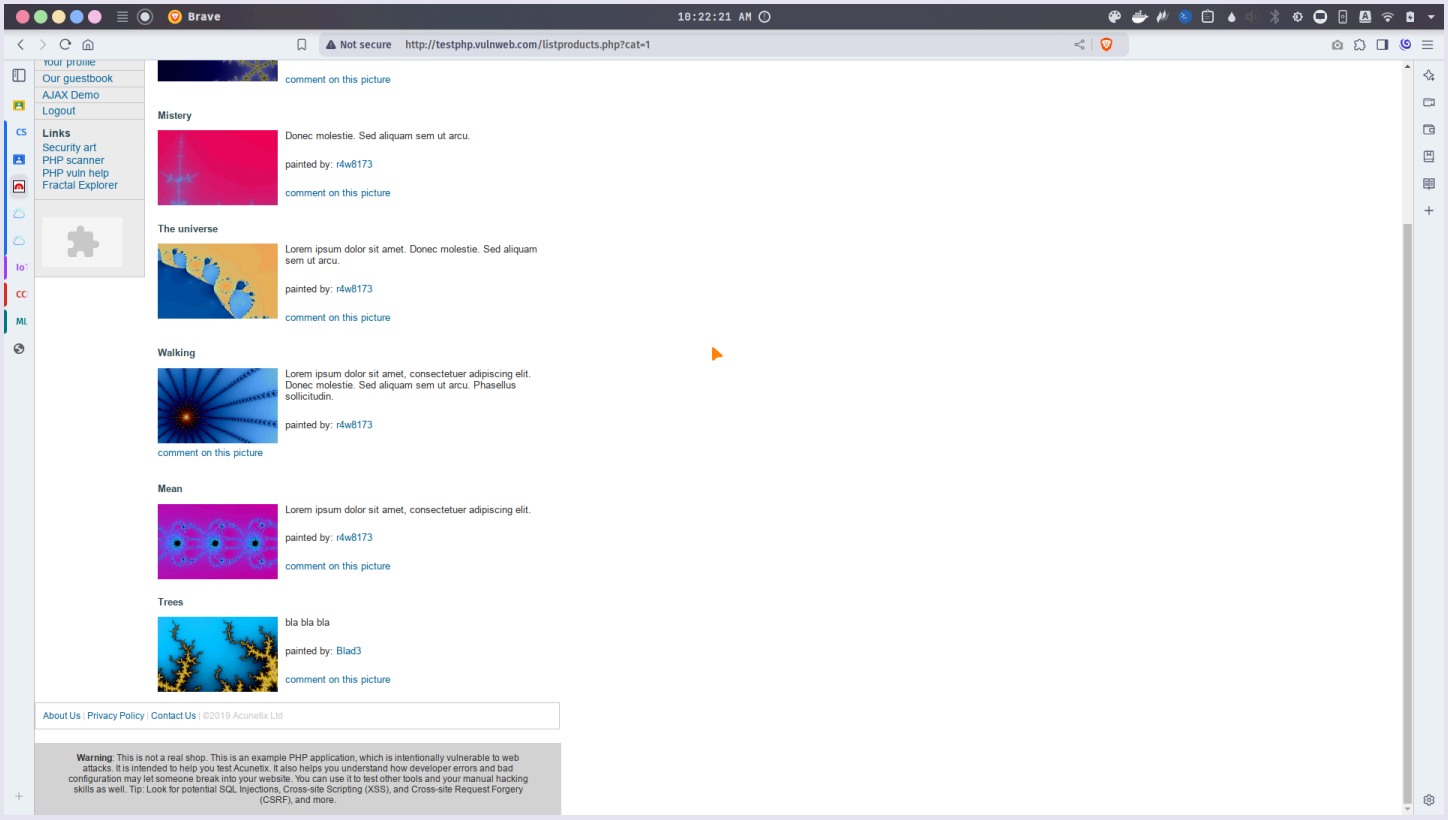


Name - Yash Lakhtariya
Enrollment number - 21162101012
Branch - CBA Batch - 71
CS Practical 2

2. Now select any category in Categories

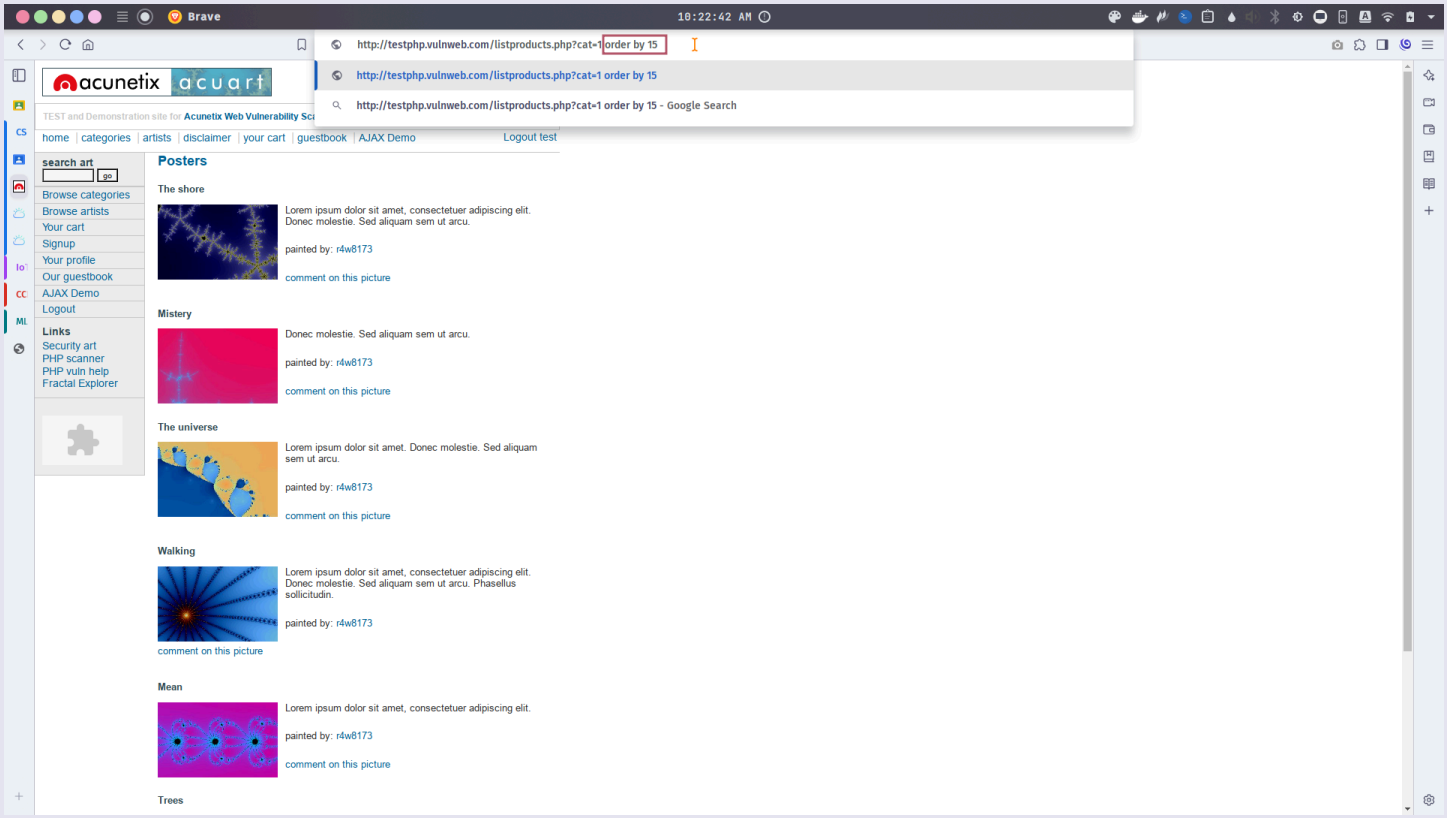


Name - Yash Lakhtariya
Enrollment number - 21162101012
Branch - CBA Batch - 71
CS Practical 2



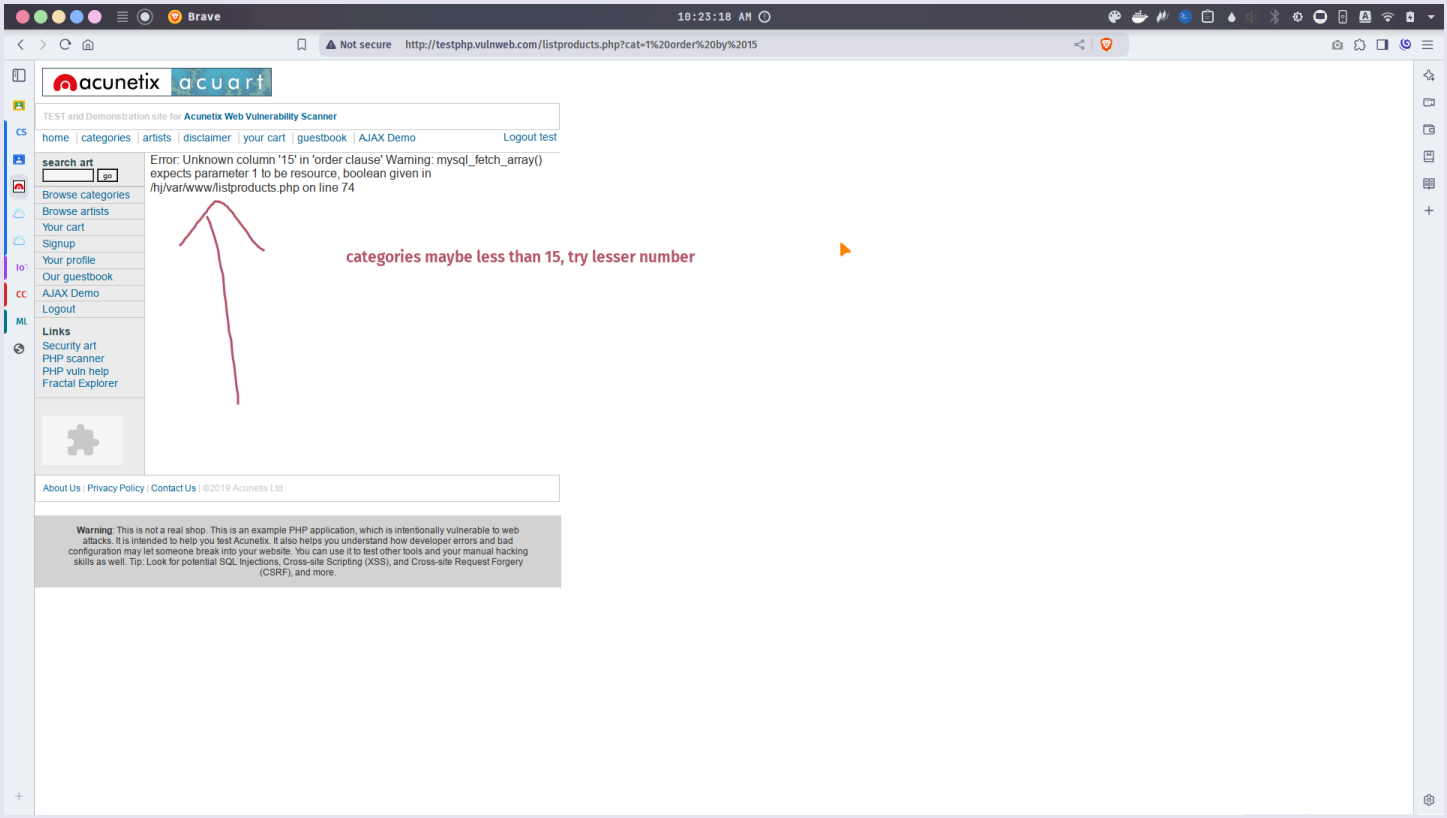
Name - Yash Lakhtariya
Enrollment number - 21162101012
Branch - CBA Batch - 71
CS Practical 2

3. Add order by 15 in URL to check how many columns it can contain

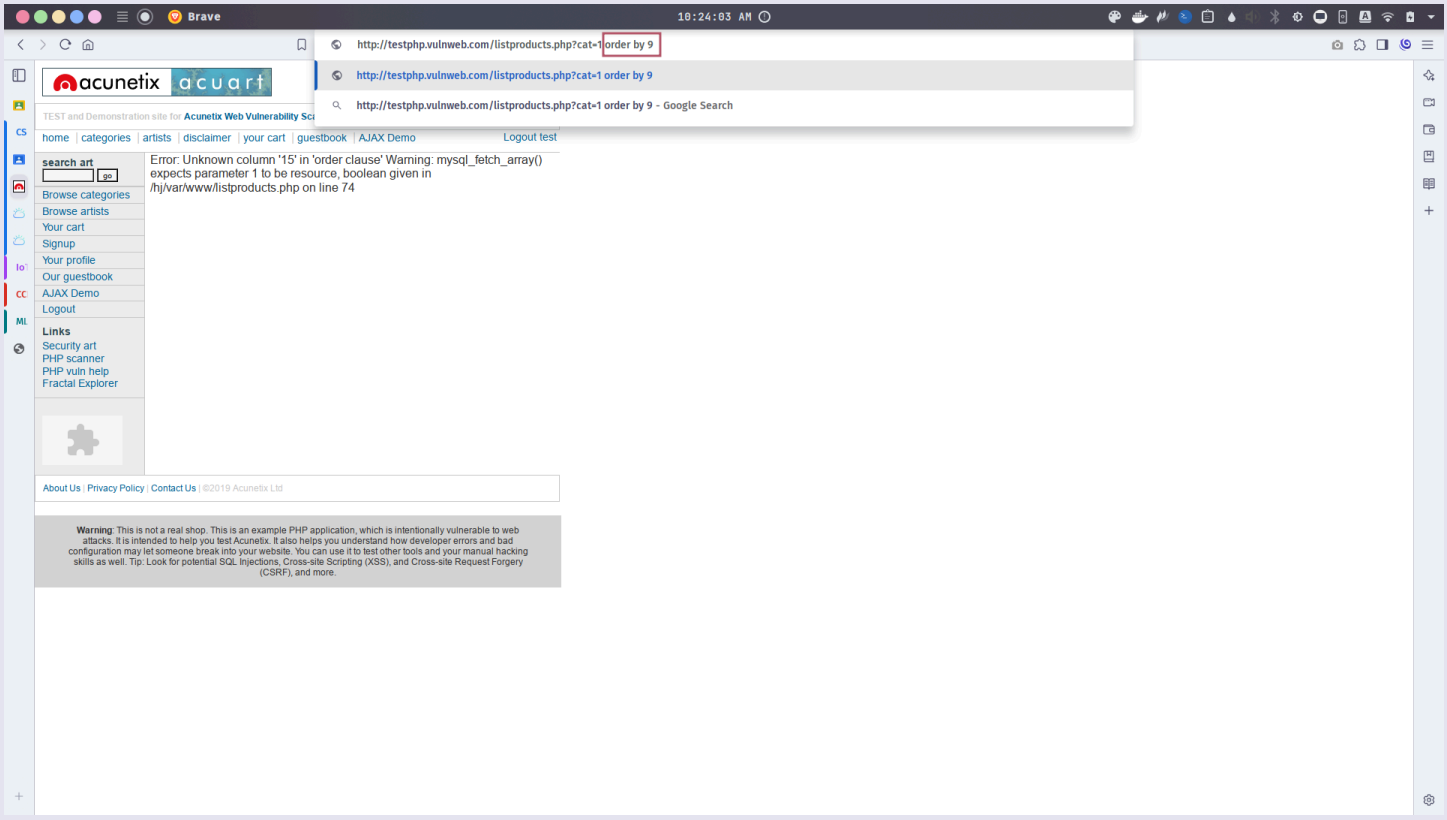


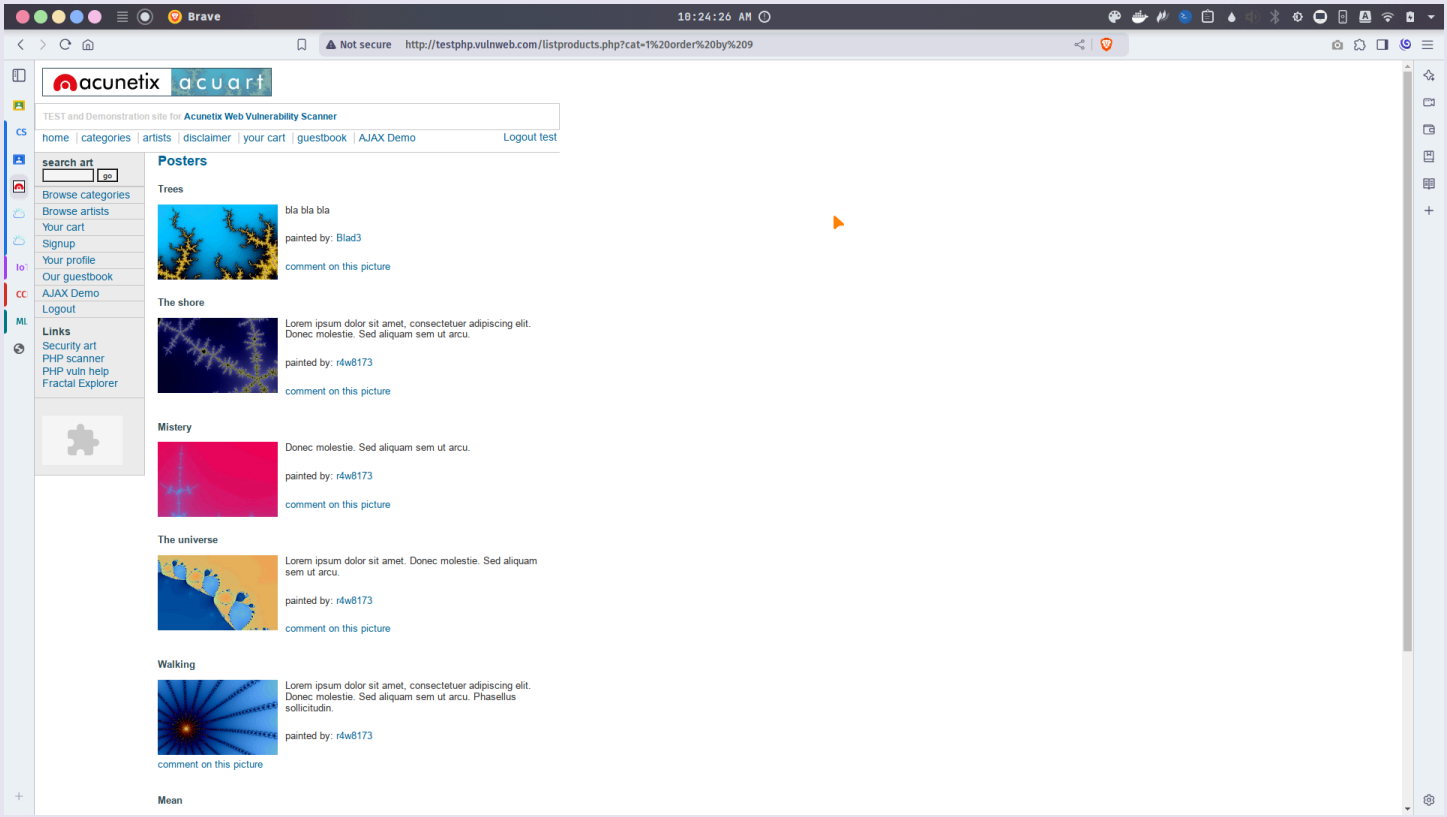
Name - Yash Lakhtariya
Enrollment number - 21162101012
Branch - CBA Batch - 71
CS Practical 2

4. As it has less listing try lesser number



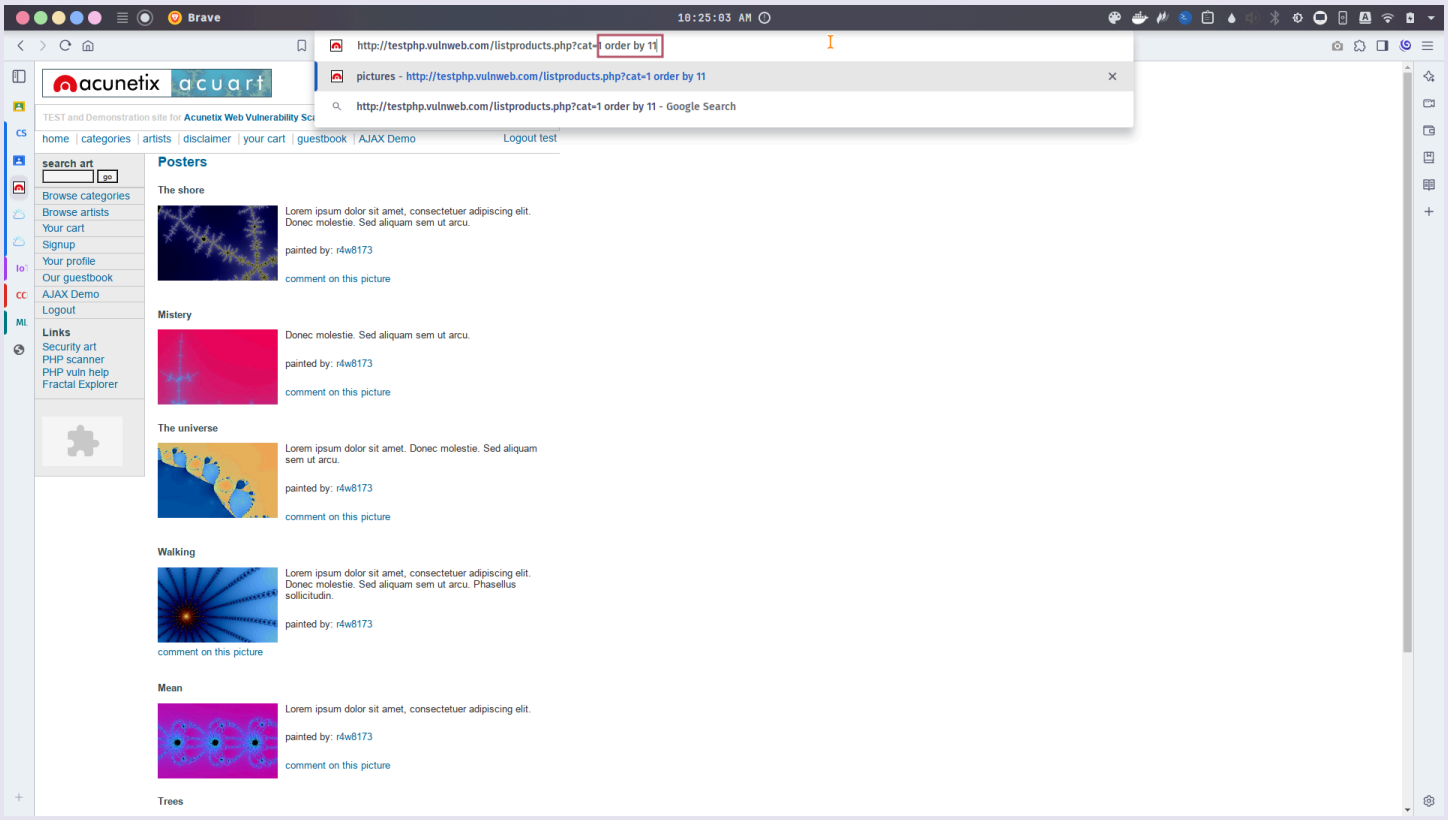
Name - Yash Lakhtariya
Enrollment number - 21162101012
Branch - CBA Batch - 71
CS Practical 2



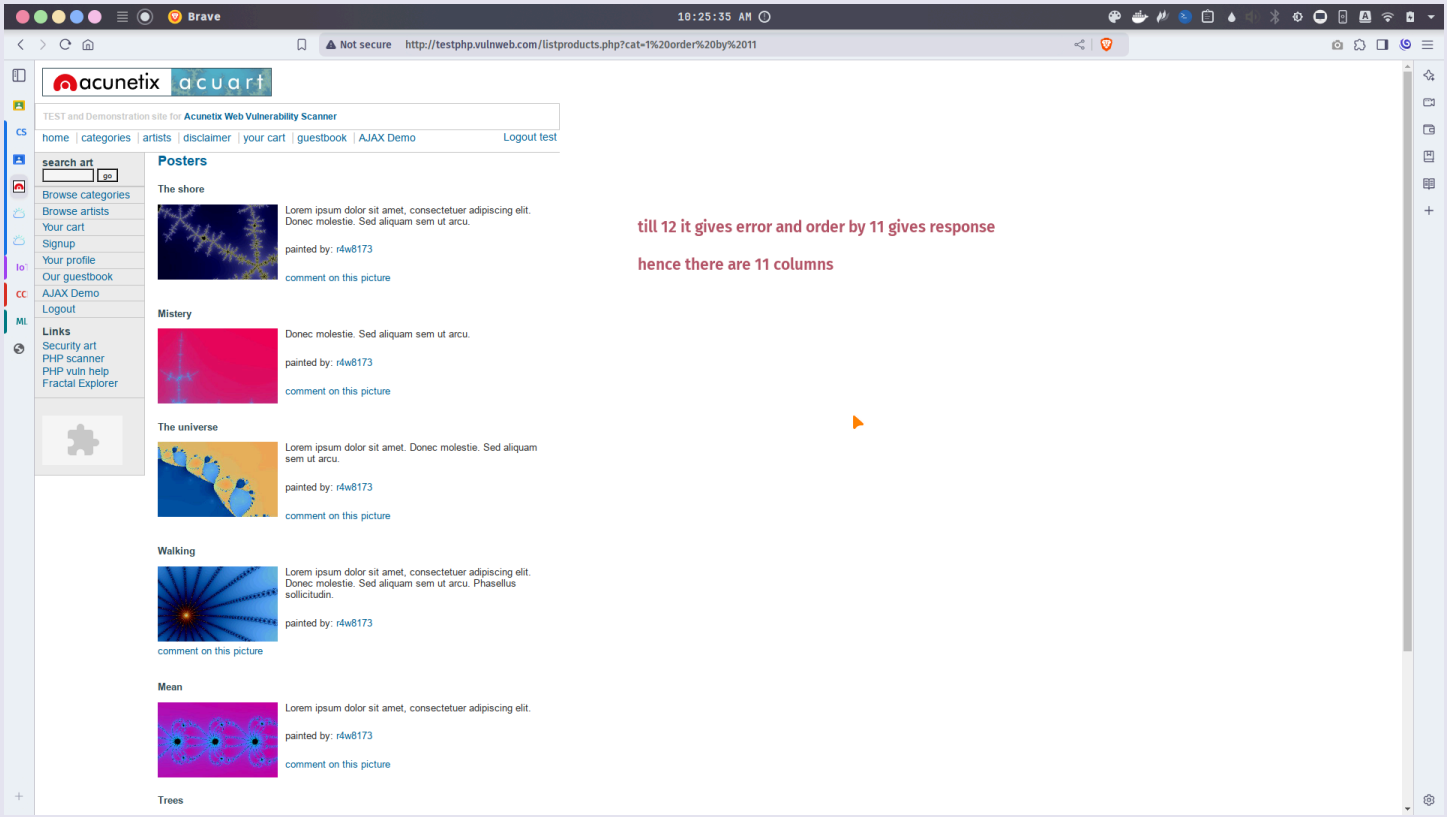


Name - Yash Lakhtariya
Enrollment number - 21162101012
Branch - CBA Batch - 71
CS Practical 2

5. It gives error till 12 and response upto 11, hence there are 11 listings in the category 1



Name - Yash Lakhtariya
Enrollment number - 21162101012
Branch - CBA Batch - 71
CS Practical 2

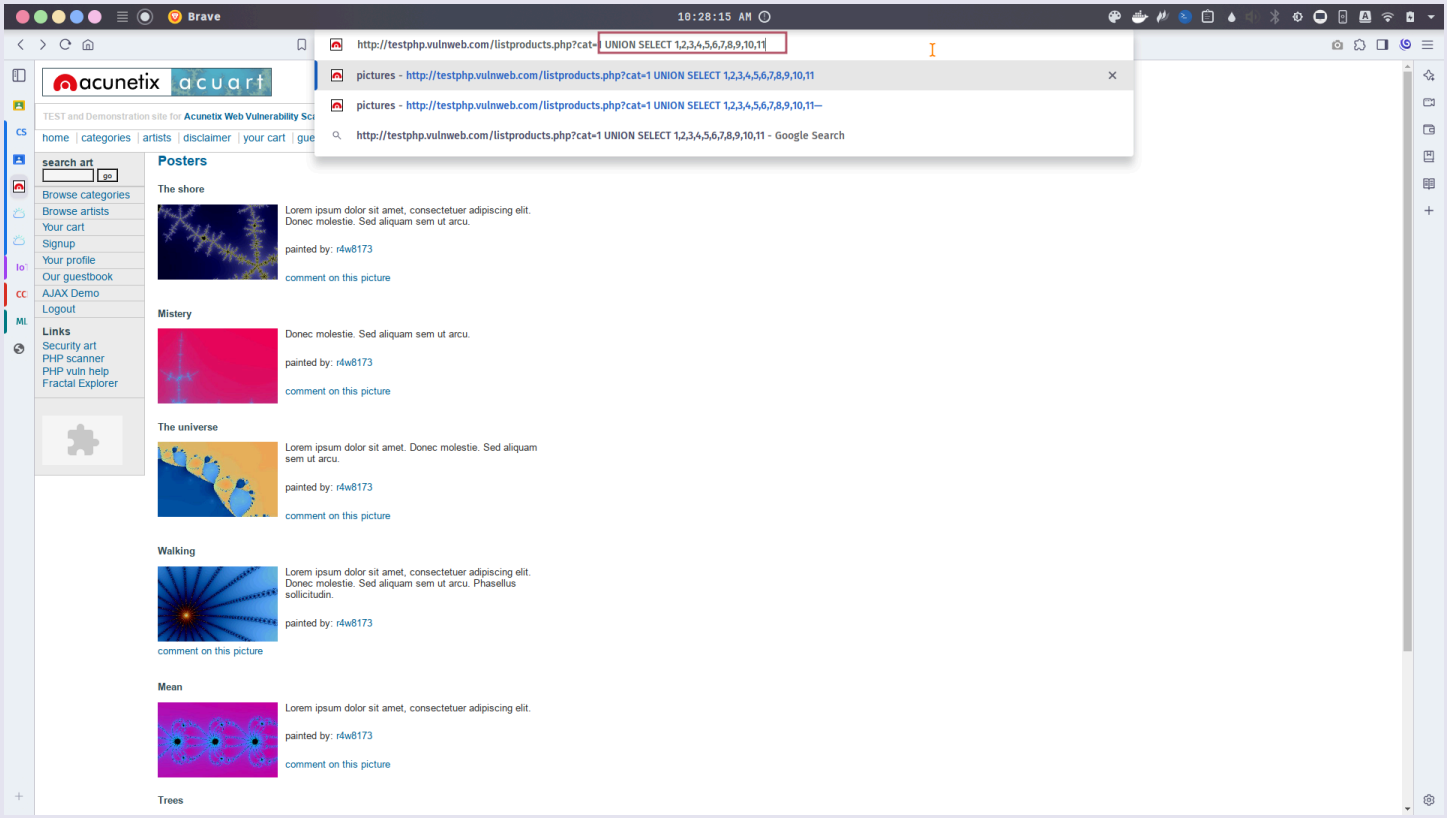


till 12 it gives error and order by 11 gives response

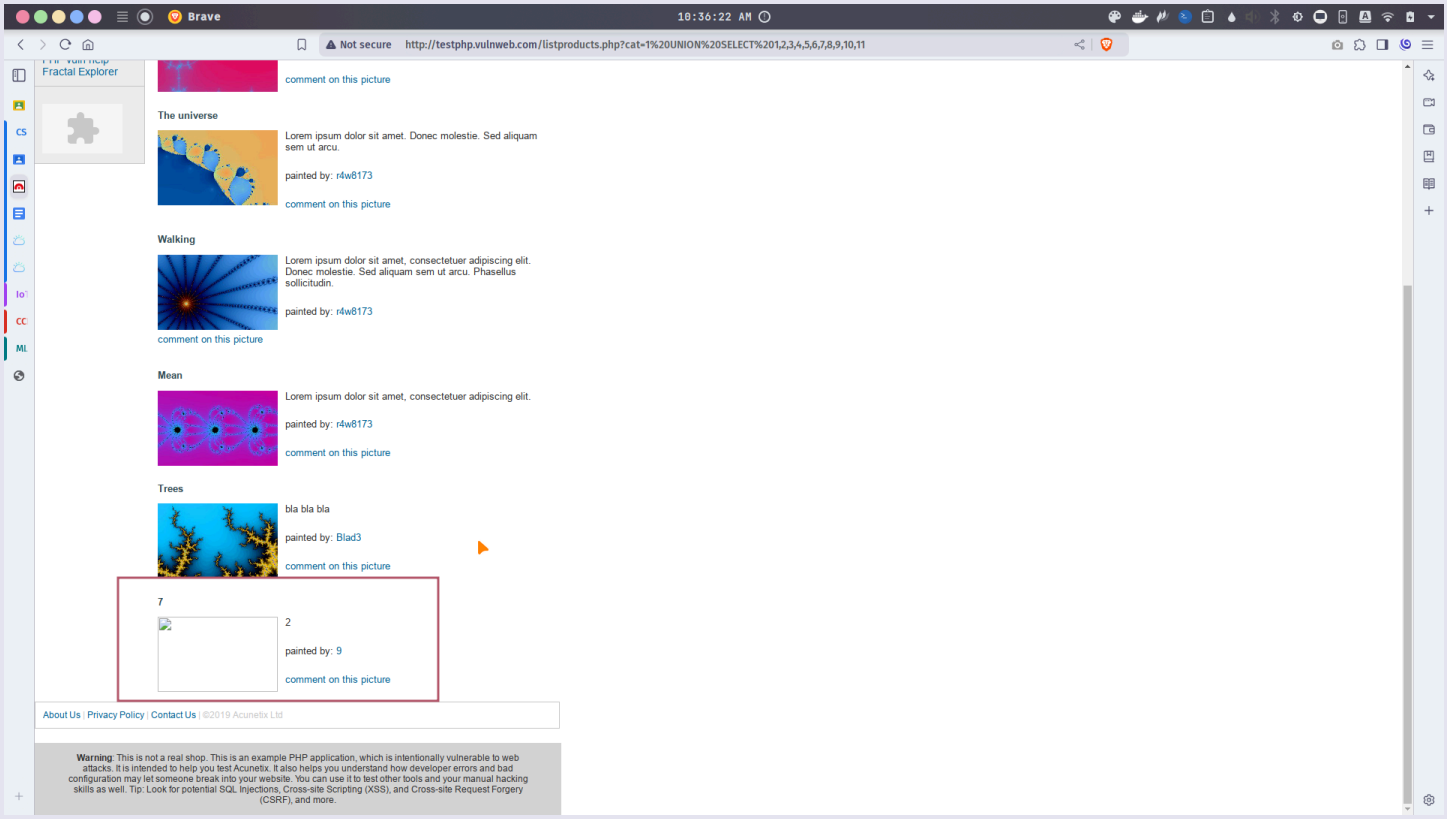
hence there are 11 columns

Name - Yash Lakhtariya
Enrollment number - 21162101012
Branch - CBA Batch - 71
CS Practical 2

6. Try union select to check the injectable columns



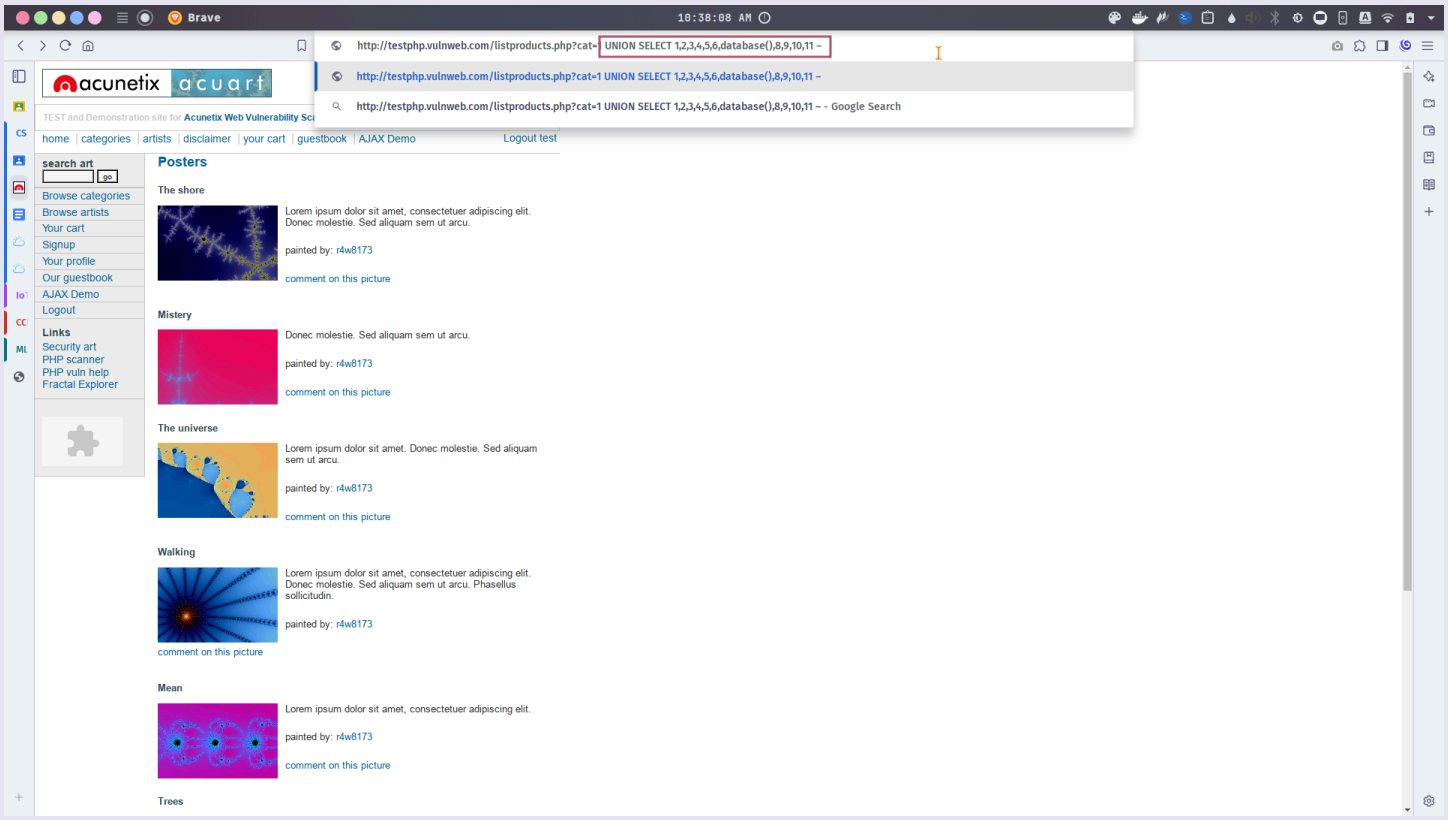
Name - Yash Lakhtariya
Enrollment number - 21162101012
Branch - CBA Batch - 71
CS Practical 2



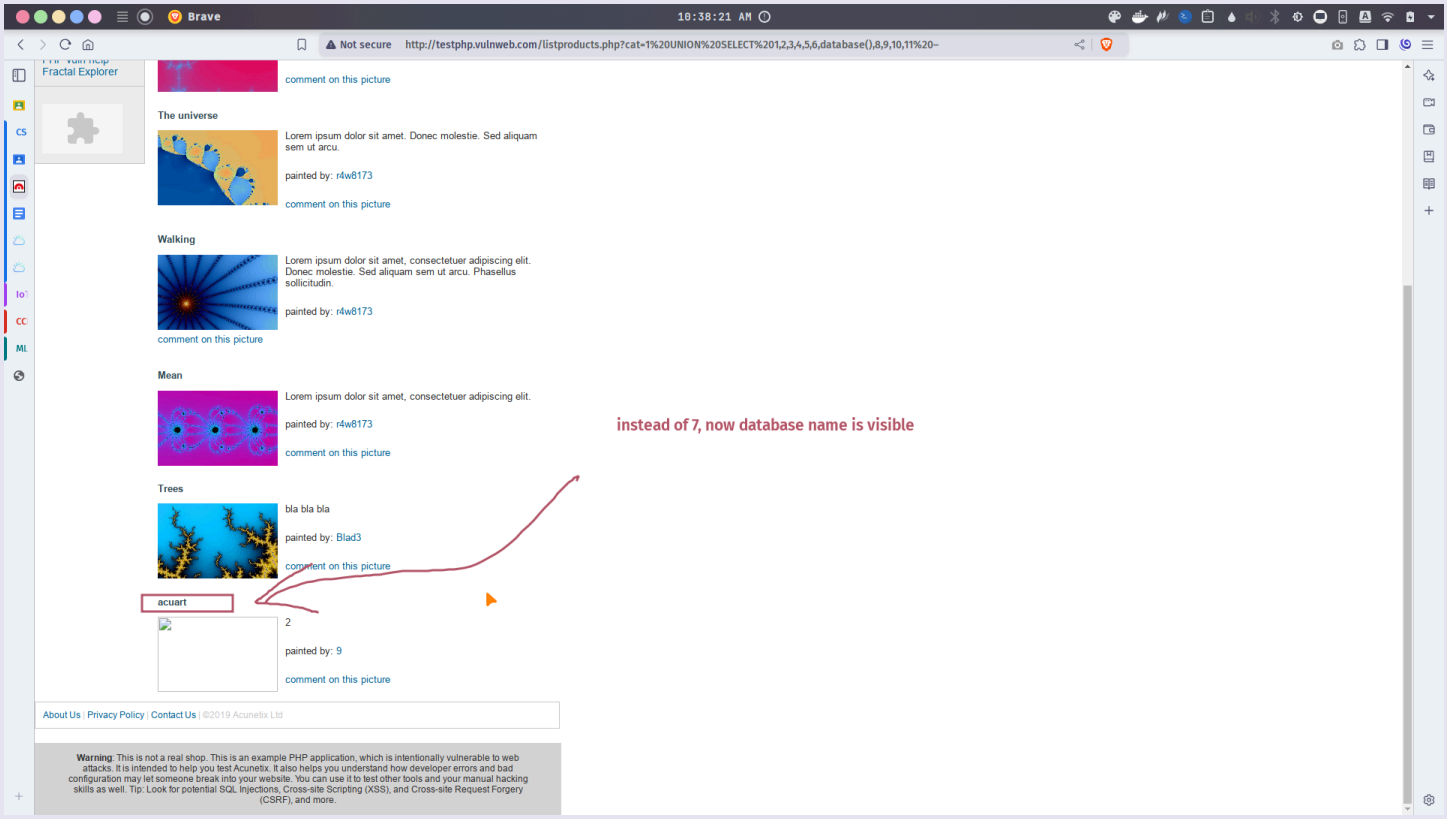
Here 2, 7 and 9 maybe injectable or editable

Name - Yash Lakhtariya
Enrollment number - 21162101012
Branch - CBA Batch - 71
CS Practical 2

7. Now, use databasename() method instead of any number say 7 here to check its db name

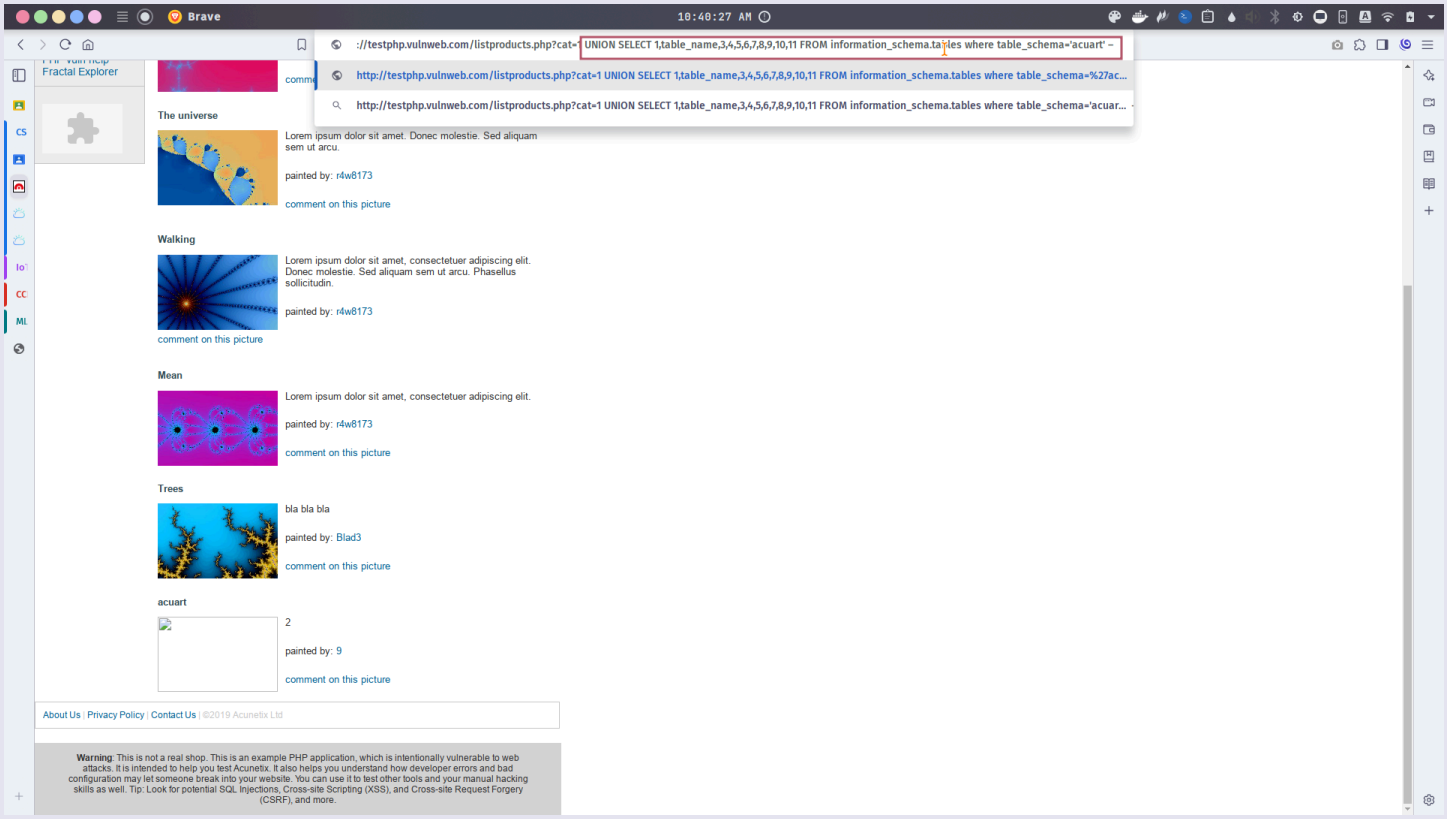


Name - Yash Lakhtariya
Enrollment number - 21162101012
Branch - CBA Batch - 71
CS Practical 2

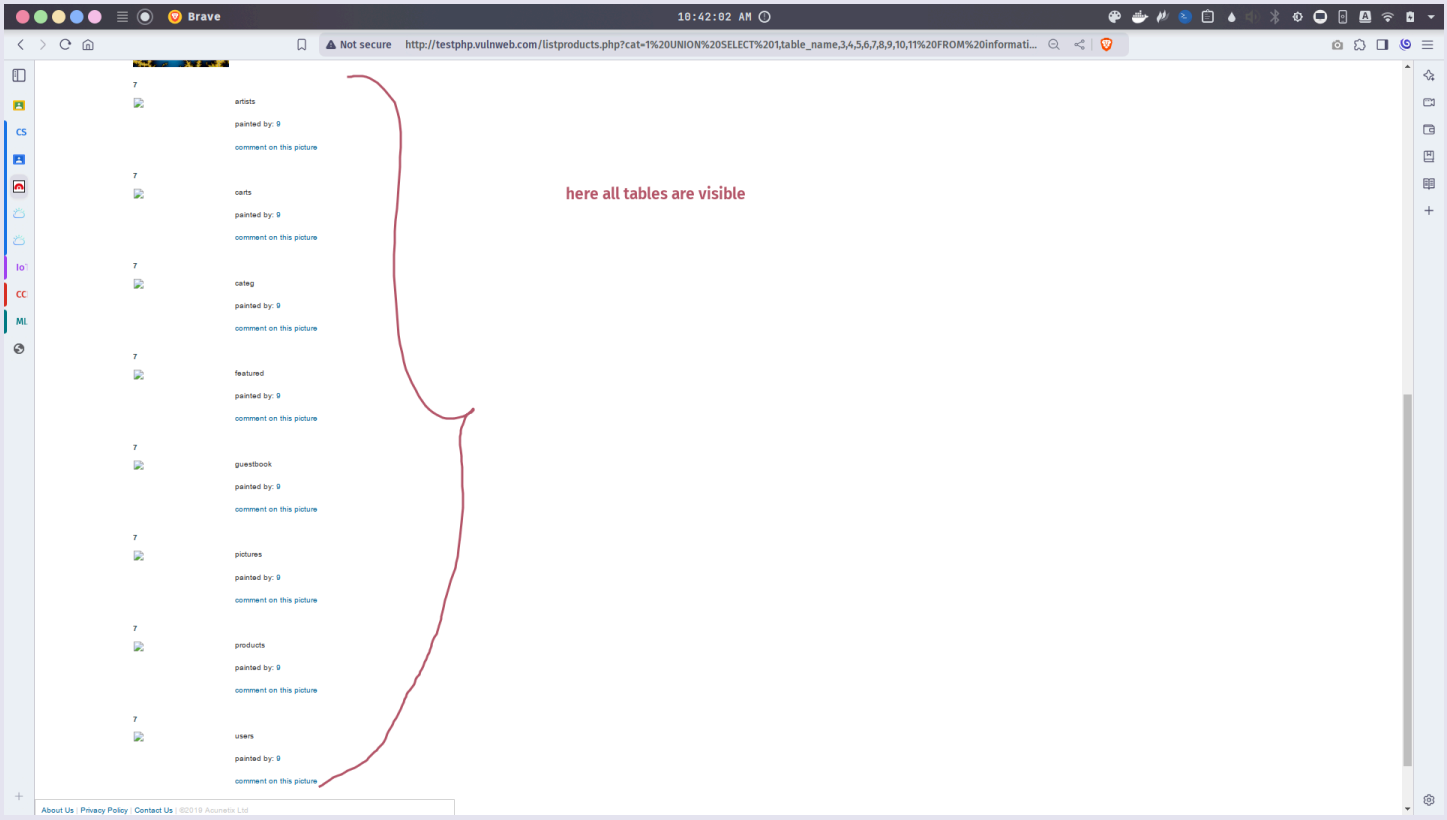


Name - Yash Lakhtariya
Enrollment number - 21162101012
Branch - CBA Batch - 71
CS Practical 2

8. Now, try to get all table names of the database

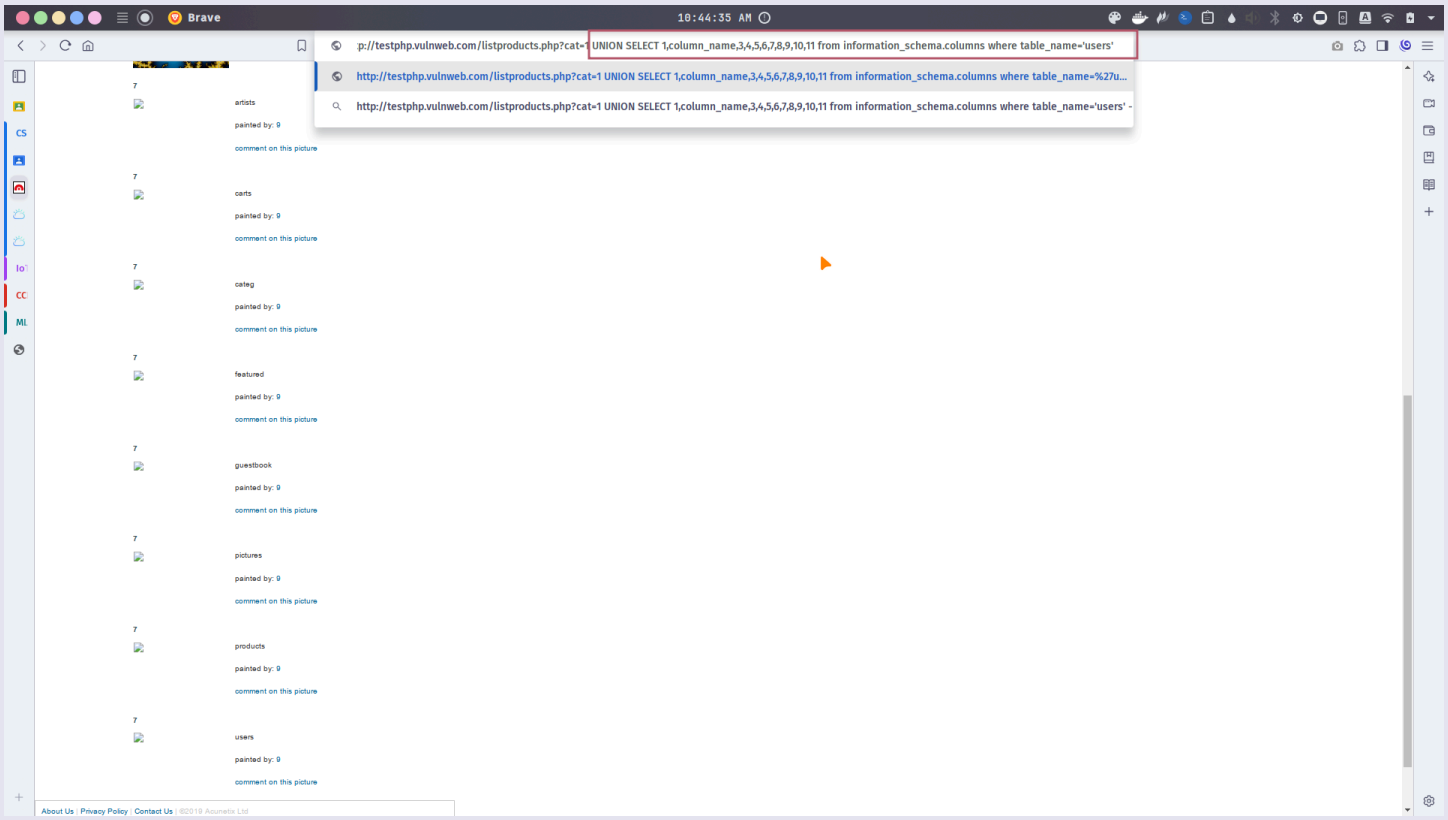


Name - Yash Lakhtariya
Enrollment number - 21162101012
Branch - CBA Batch - 71
CS Practical 2

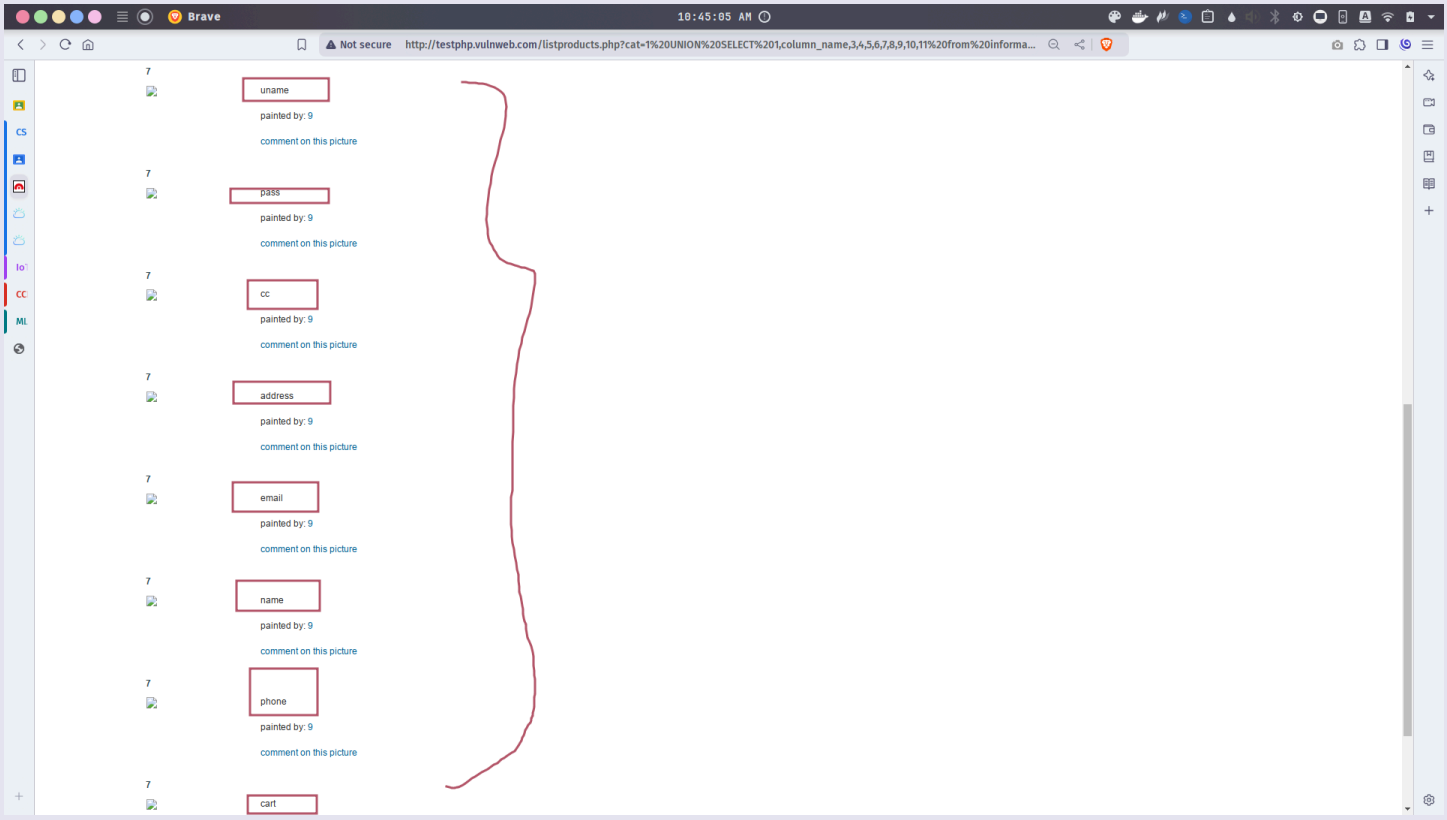


Name - Yash Lakhtariya
Enrollment number - 21162101012
Branch - CBA Batch - 71
CS Practical 2

9. Now, to check columns of users table, which can be useful to hack, try specifying users in table name

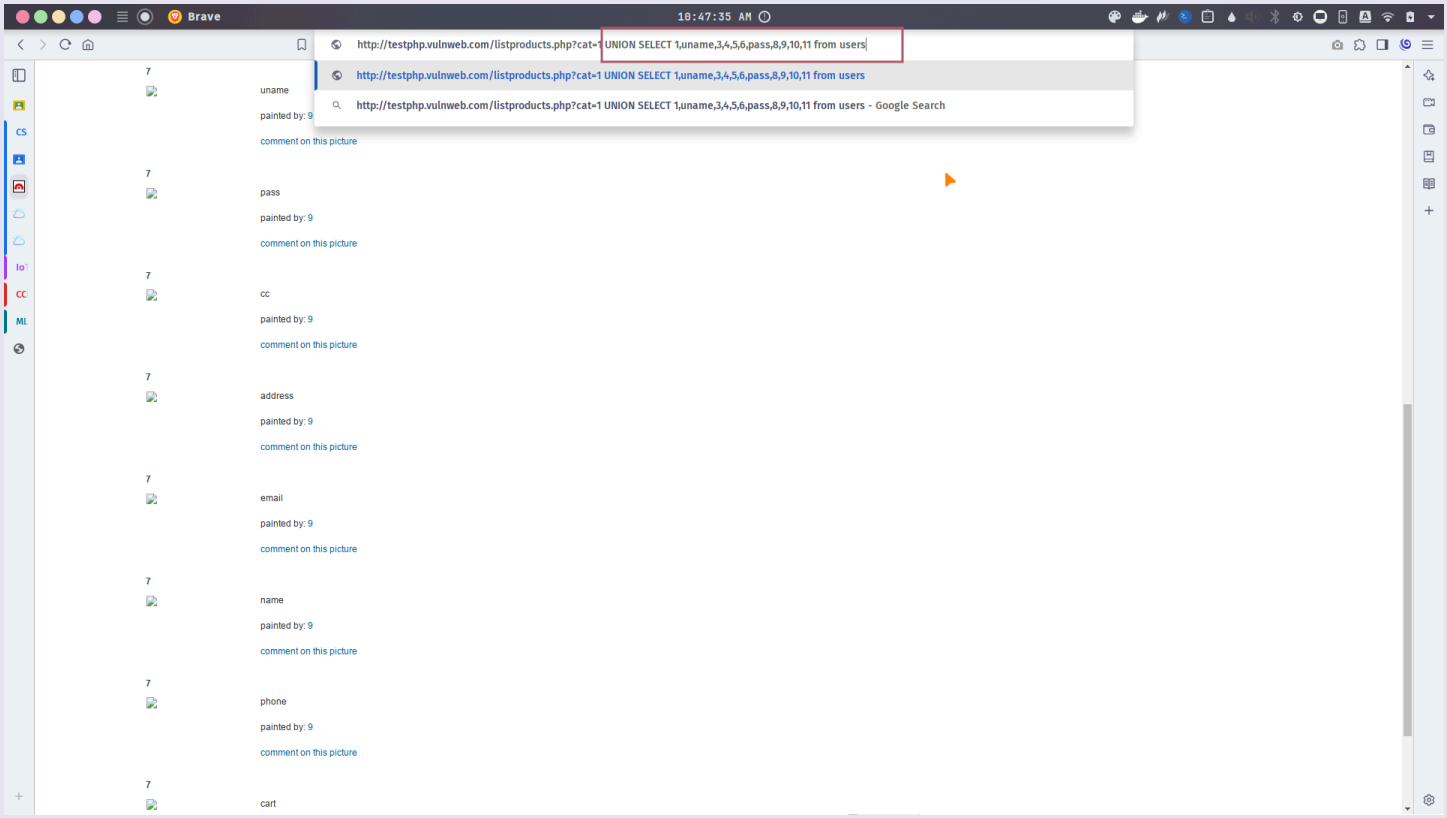


Name - Yash Lakhtariya
Enrollment number - 21162101012
Branch - CBA Batch - 71
CS Practical 2

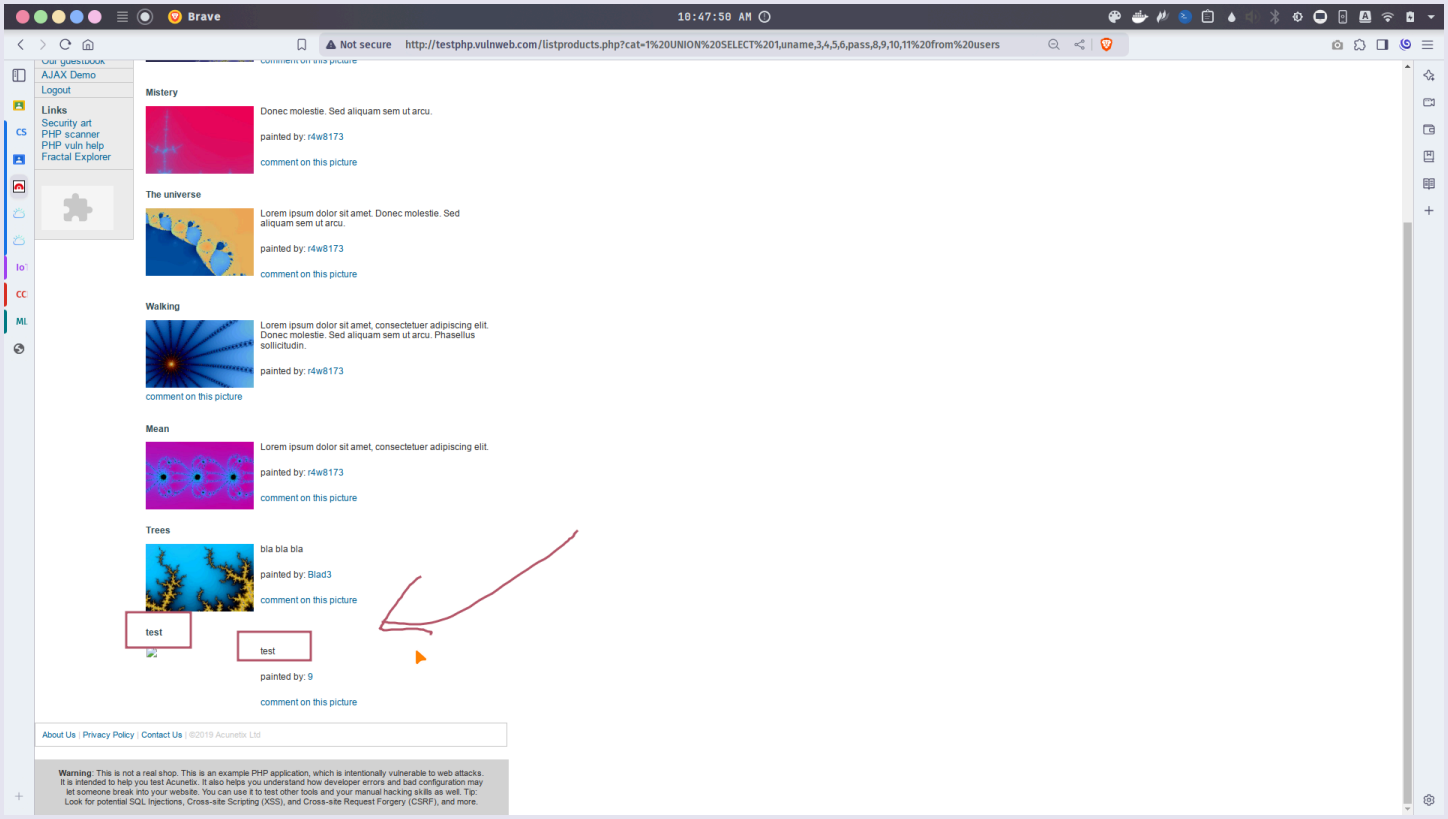


Name - Yash Lakhtariya
Enrollment number - 21162101012
Branch - CBA Batch - 71
CS Practical 2

10. Now, username and password can be get by using the column name

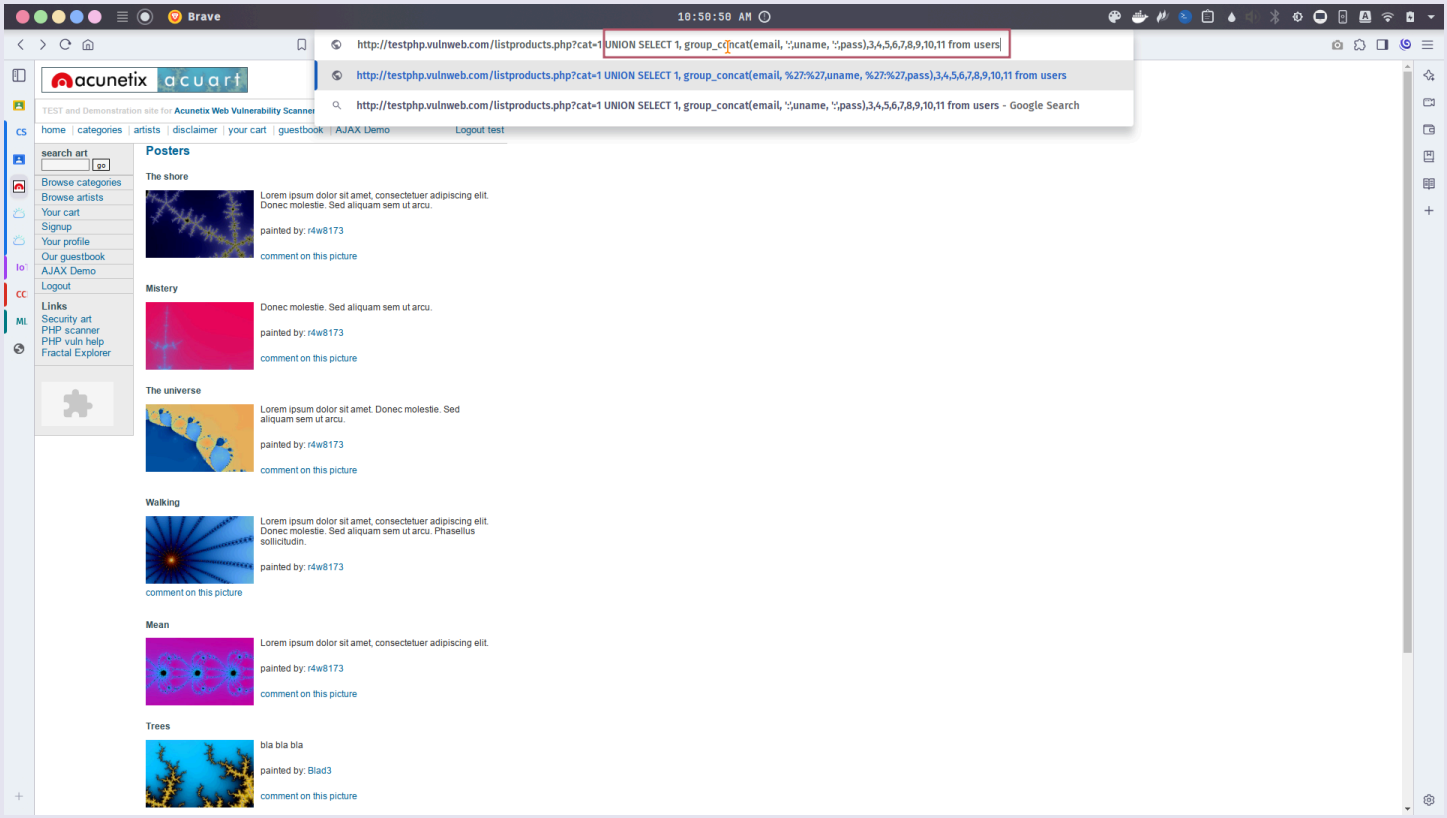


Name - Yash Lakhtariya
Enrollment number - 21162101012
Branch - CBA Batch - 71
CS Practical 2

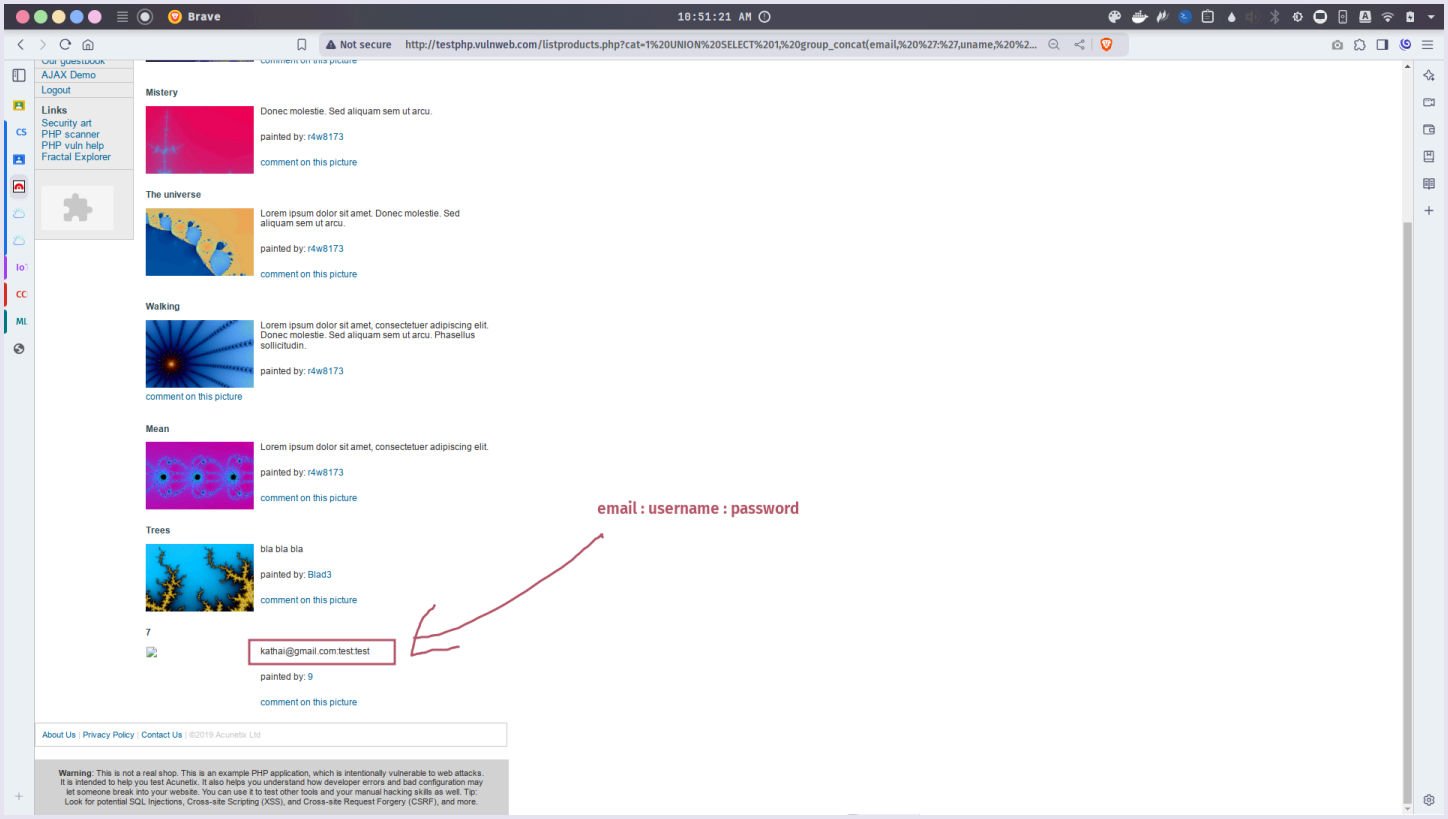


Name - Yash Lakhtariya
Enrollment number - 21162101012
Branch - CBA Batch - 71
CS Practical 2

11. Try to get email, username and password all in single injection



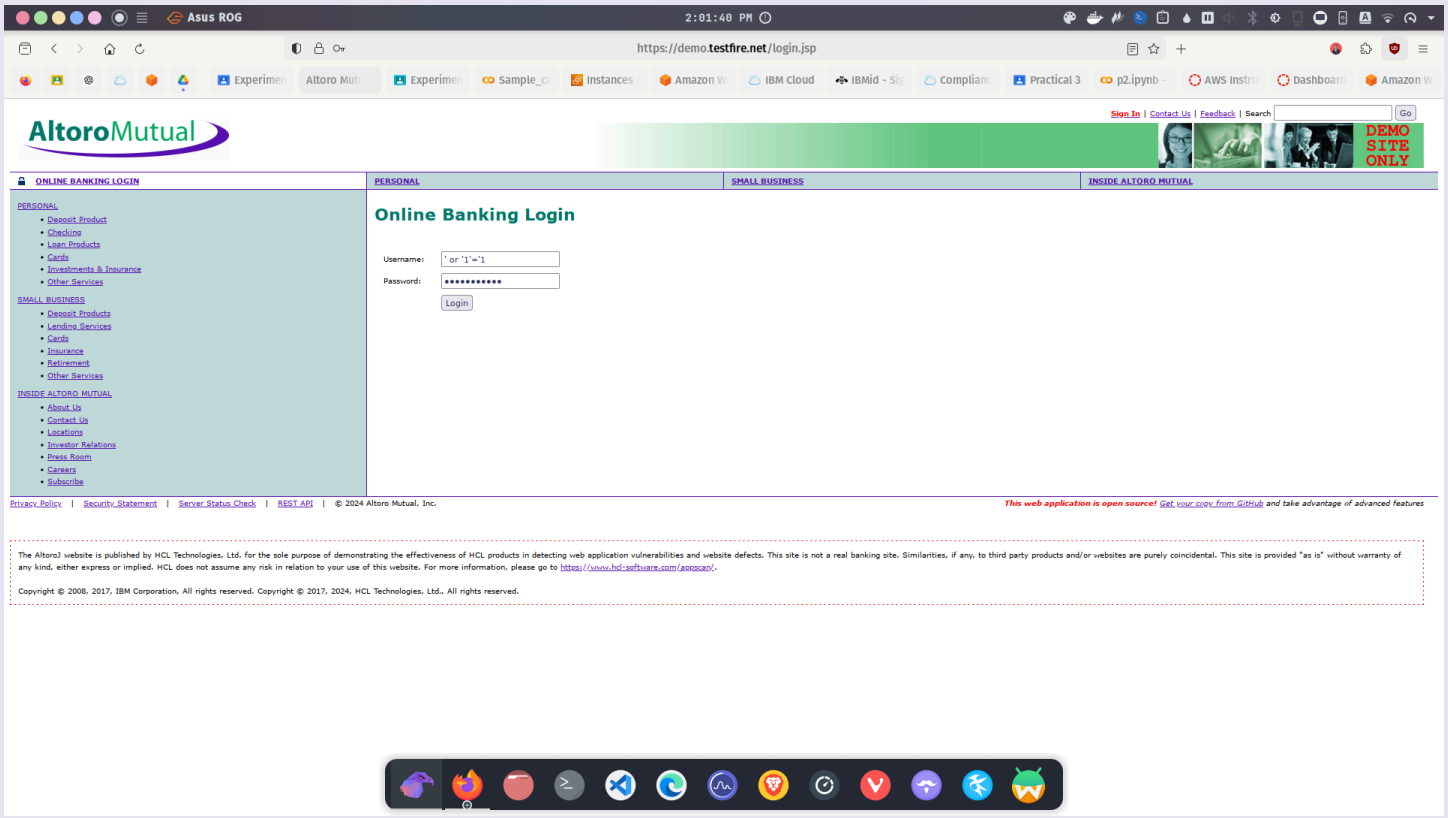
Name - Yash Lakhtariya
Enrollment number - 21162101012
Branch - CBA Batch - 71
CS Practical 2



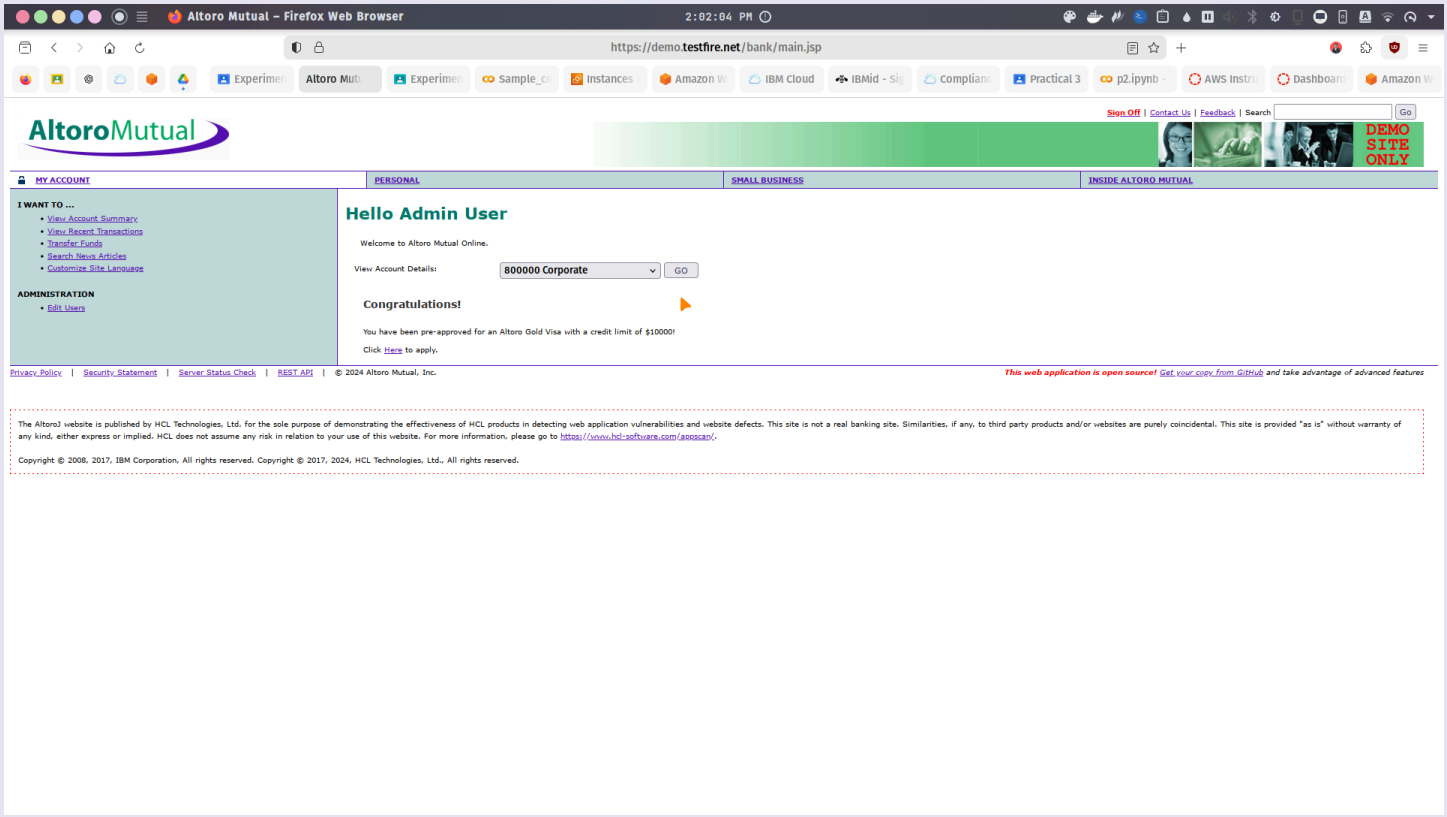
Name - Yash Lakhtariya
Enrollment number - 21162101012
Branch - CBA Batch - 71
CS Practical 2

Task :

1. SQL injection as previously done for login without username and/or password

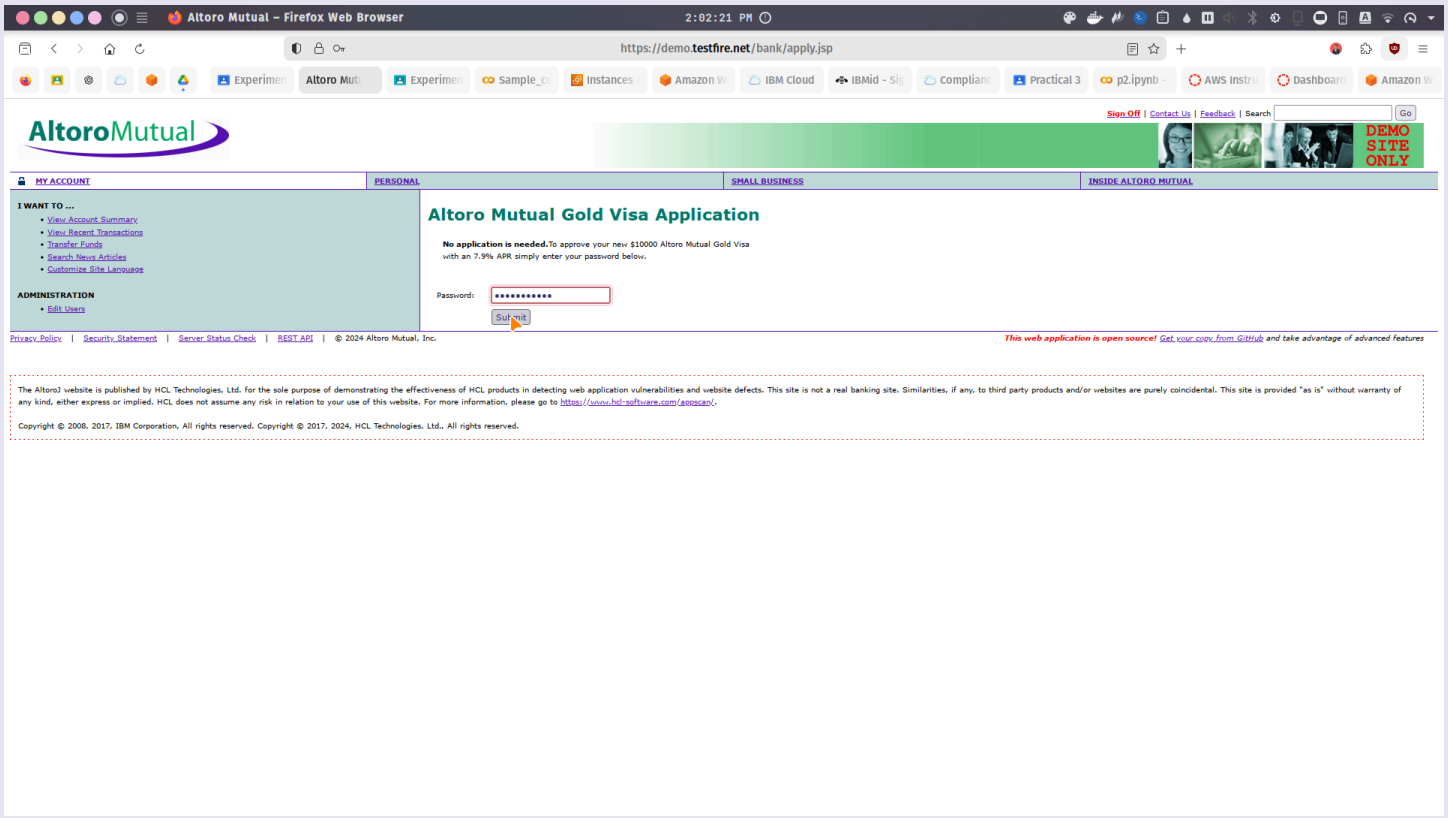


Name - Yash Lakhtariya
Enrollment number - 21162101012
Branch - CBA Batch - 71
CS Practical 2

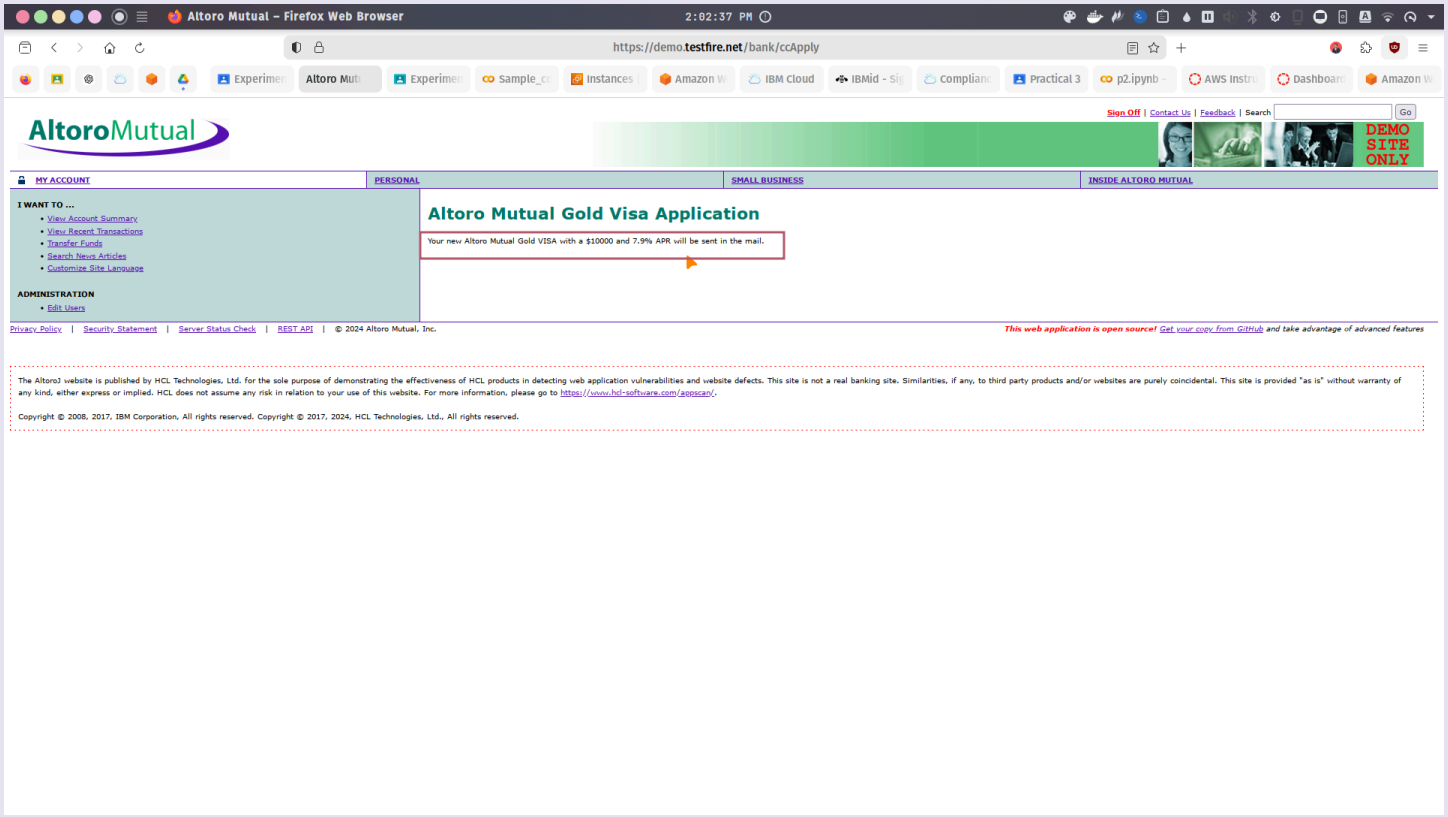


Name - Yash Lakhtariya
Enrollment number - 21162101012
Branch - CBA Batch - 71
CS Practical 2

2. Applying for $10000 worth Gold VISA without password (using SQL injection of : ‘ or ‘1’=’1

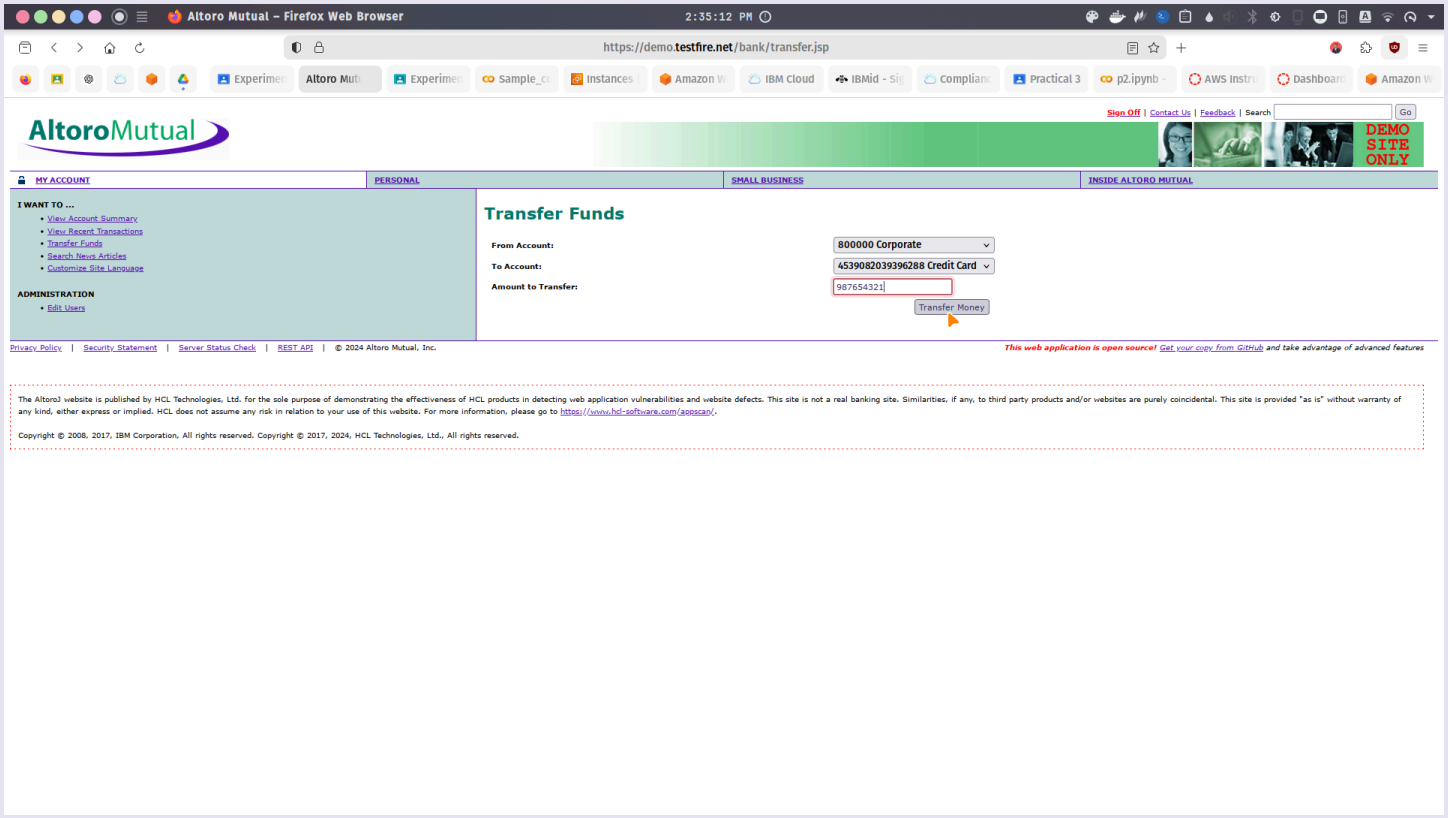


Name - Yash Lakhtariya
Enrollment number - 21162101012
Branch - CBA Batch - 71
CS Practical 2

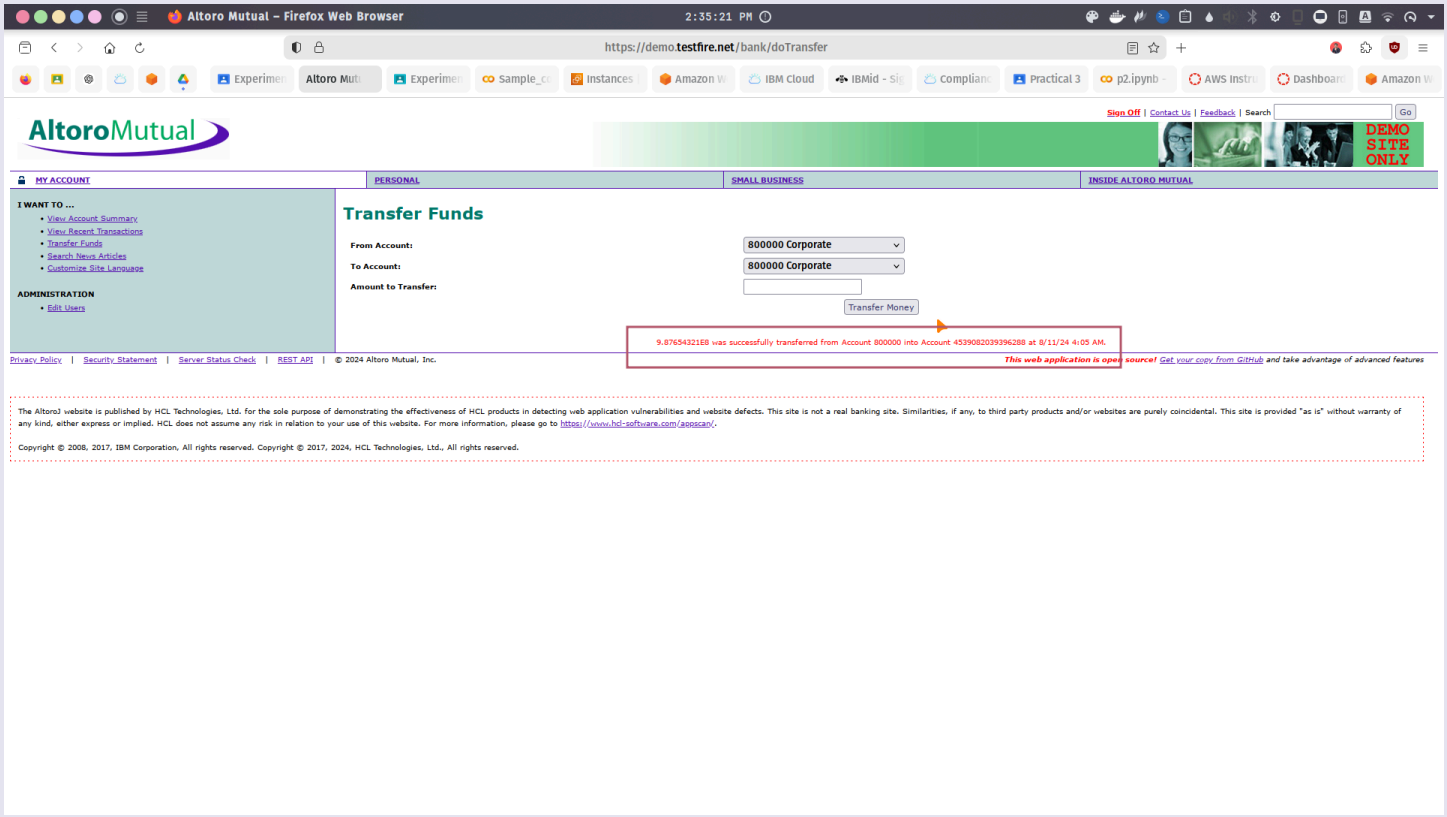


Name - Yash Lakhtariya
Enrollment number - 21162101012
Branch - CBA Batch - 71
CS Practical 2

3. Transferring money without access (using SQL injection on login account first)



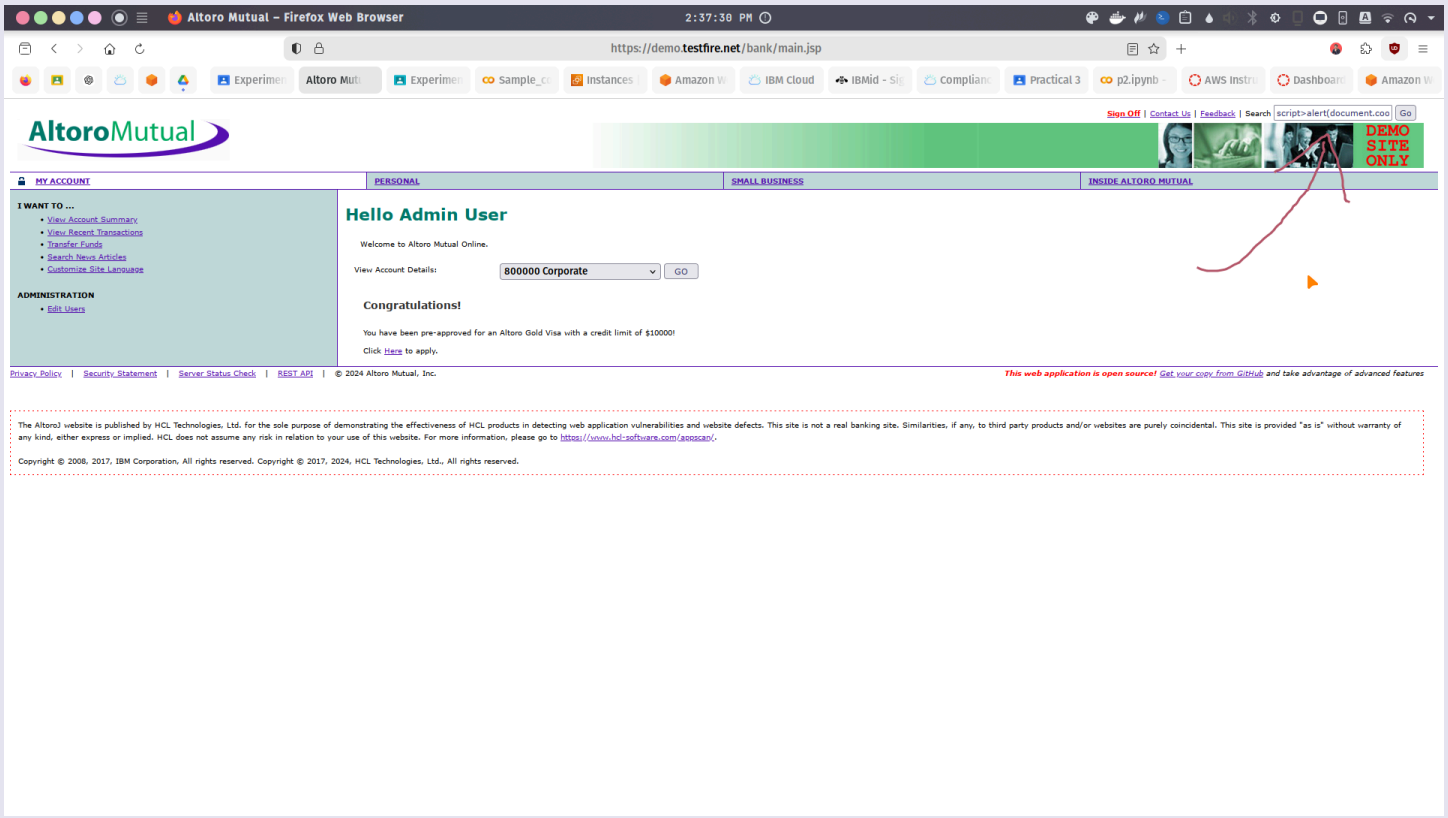
Name - Yash Lakhtariya
Enrollment number - 21162101012
Branch - CBA Batch - 71
CS Practical 2



(Note : Only above 2 SQL injections possible where login part is there after which full access is there an no need for SQL injection, further attacks can be done)

Name - Yash Lakhtariya
Enrollment number - 21162101012
Branch - CBA Batch - 71
CS Practical 2

4. Getting access to cookie for session storage for future access using javascript injection : <script>alert(document. cookie);</script>



Name - Yash Lakhtariya
Enrollment number - 21162101012
Branch - CBA Batch - 71
CS Practical 2