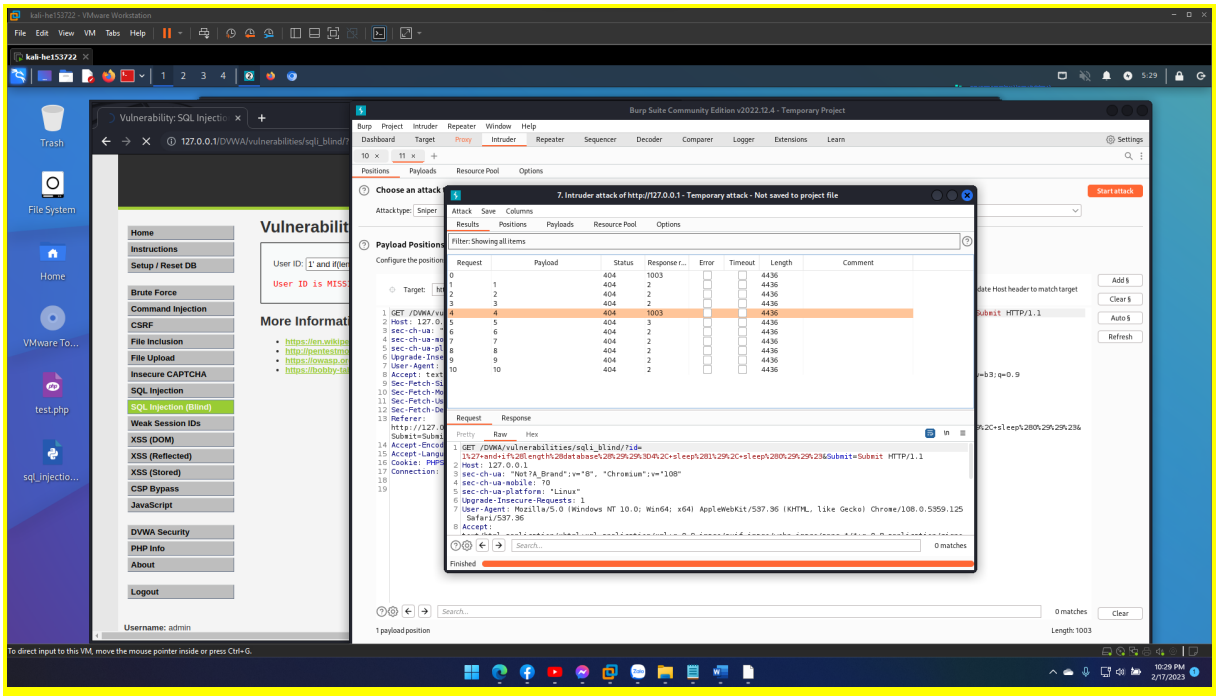
# Lab 11: Time-Based Blind SQL Injection

**Get database's info:**

**o Get length of database's name: 4**

**1' and if(length(database())=4, sleep(1), sleep(0))#**

The injected code consists of the AND operator followed by a conditional statement that checks the length of the current database name using the LENGTH() function. If the length is equal to 4, the injected code will execute the SLEEP(1) function, causing a delay of 1 second. If the length is not equal to 4, the injected code will execute the SLEEP(0) function, which causes no delay.

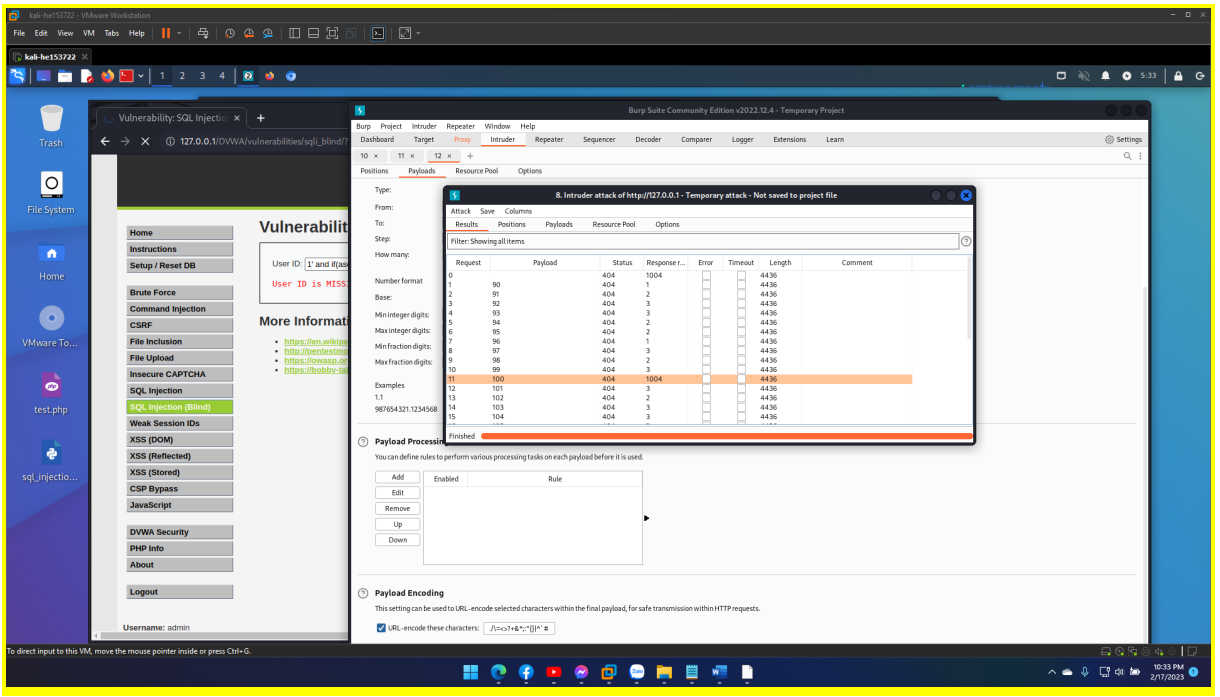


**o Get name of database by bruteforcing each character:**

**dvwa**

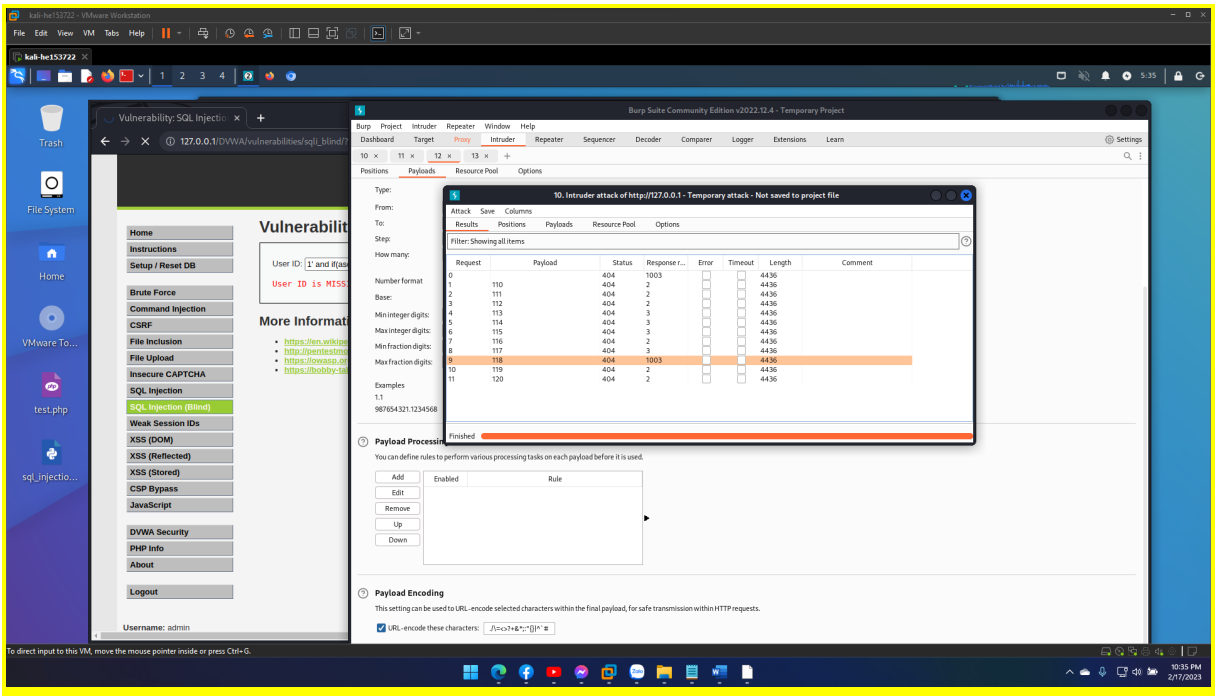
**1' and if(ascii(substr(database(),1,1))=100, sleep(1), sleep(0))#**

The injected code consists of the AND operator followed by a conditional statement that checks the ASCII value of the first character of the current database name using the ASCII() function and the SUBSTR() function. If the ASCII value of the first character is equal to 100 (which corresponds to the letter "d" in ASCII), the injected code will execute the SLEEP(1) function, causing a delay of 1 second. If the ASCII value is not equal to 100, the injected code will execute the SLEEP(0) function, which causes no delay.



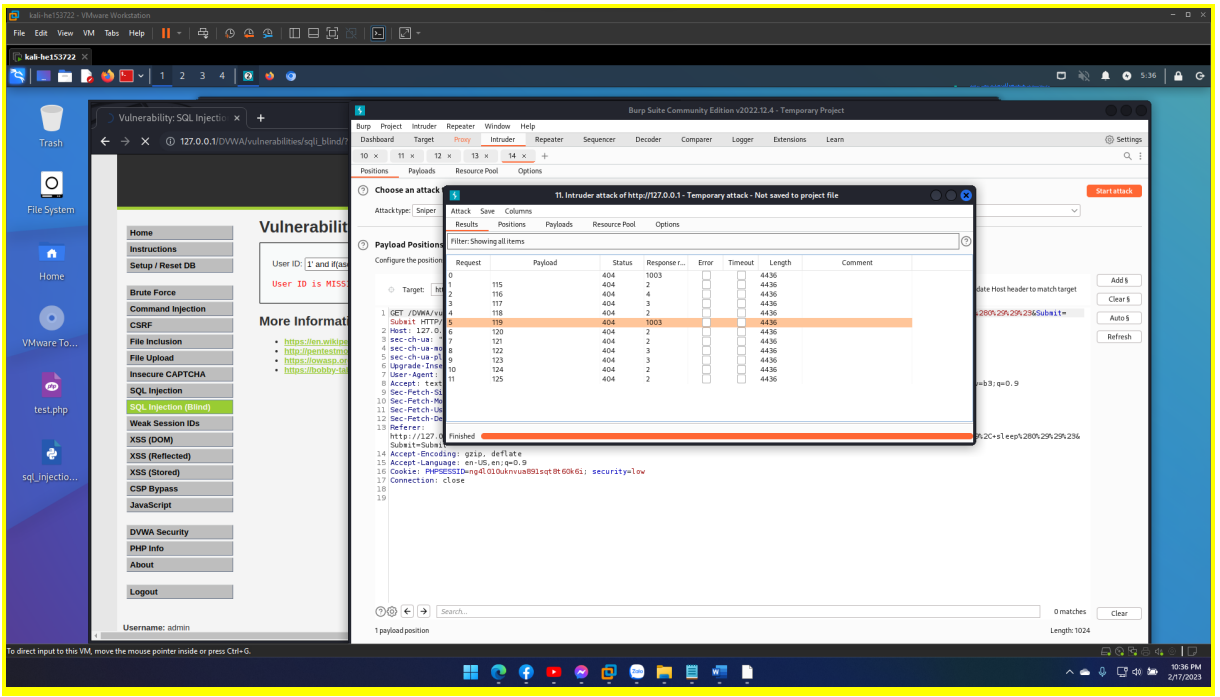
**1' and if(ascii(substr(database(),2,1))=118, sleep(1), sleep(0))#.**

The injected code consists of the AND operator followed by a conditional statement that checks the ASCII value of the second character of the current database name using the ASCII() function and the SUBSTR() function. If the ASCII value of the second character is equal to 118 (which corresponds to the letter "v" in ASCII), the injected code will execute the SLEEP(1) function, causing a delay of 1 second. If the ASCII value is not equal to 118, the injected code will execute the SLEEP(0) function, which causes no delay.



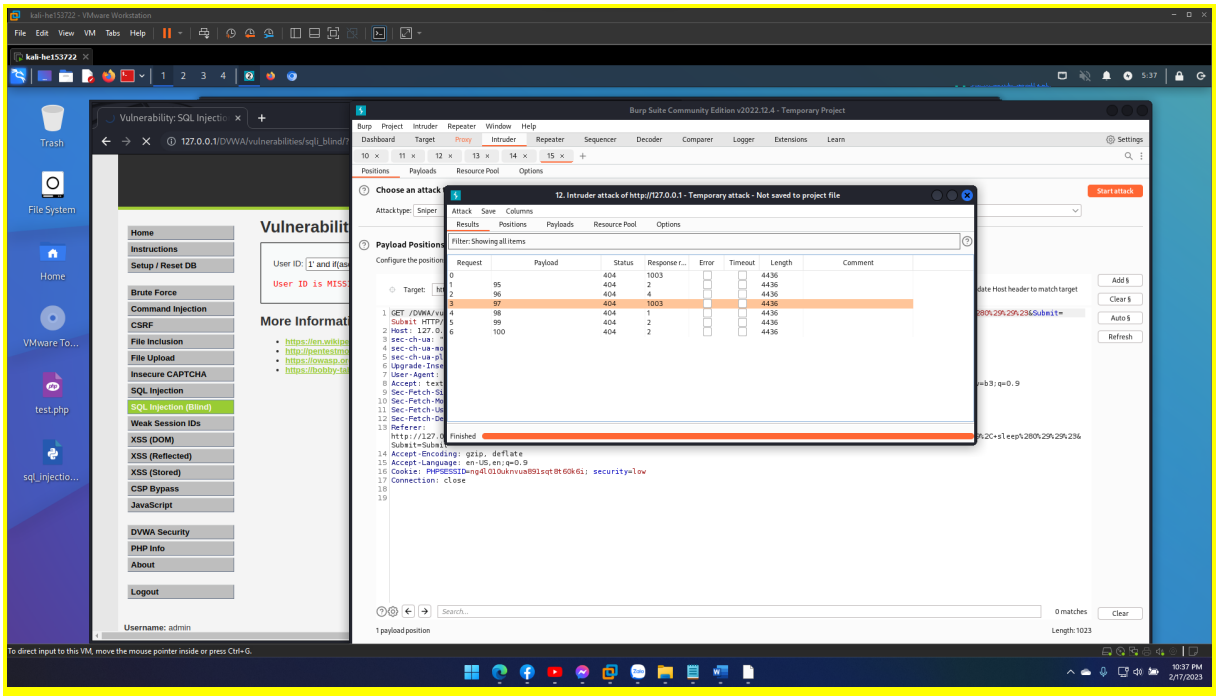

**1' and if(ascii(substr(database(),3,1))=119, sleep(1), sleep(0))#**

The injected code consists of the AND operator followed by a conditional statement that checks the ASCII value of the third character of the current database name using the ASCII() function and the SUBSTR() function. If the ASCII value of the third character is equal to 119 (which corresponds to the letter "w" in ASCII), the injected code will execute the SLEEP(1) function, causing a delay of 1 second. If the ASCII value is not equal to 119, the injected code will execute the SLEEP(0) function, which causes no delay.




**1' and if(ascii(substr(database(),4,1))=97, sleep(1), sleep(0))#**

The injected code consists of the AND operator followed by a conditional statement that checks the ASCII value of the fourth character of the current database name using the ASCII() function and the SUBSTR() function. If the ASCII value of the fourth character is equal to 97 (which corresponds to the letter "a" in ASCII), the injected code will execute the SLEEP(1) function, causing a delay of 1 second. If the ASCII value is not equal to 97, the injected code will execute the SLEEP(0) function, which causes no delay.

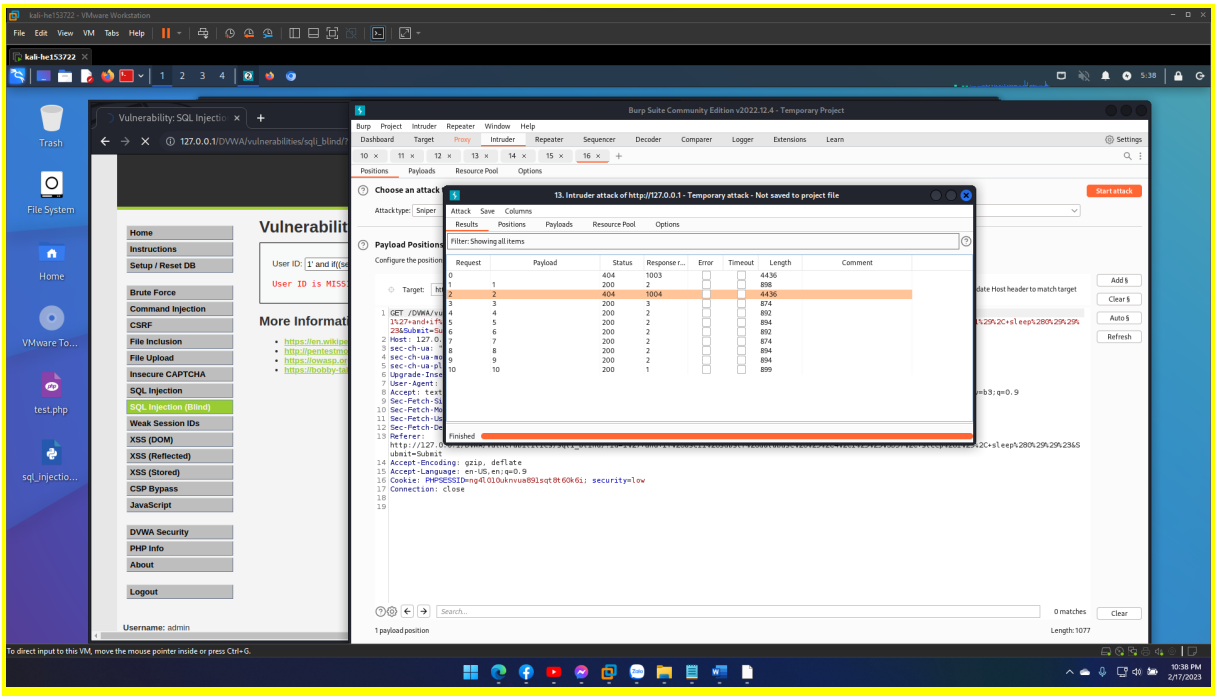


- **Get tables' info:**

**o Get number of tables in database: 2**

**1' and if((select count(table_name) from information_schema.tables where table_schema=database())=2, sleep(1), sleep(0))#**

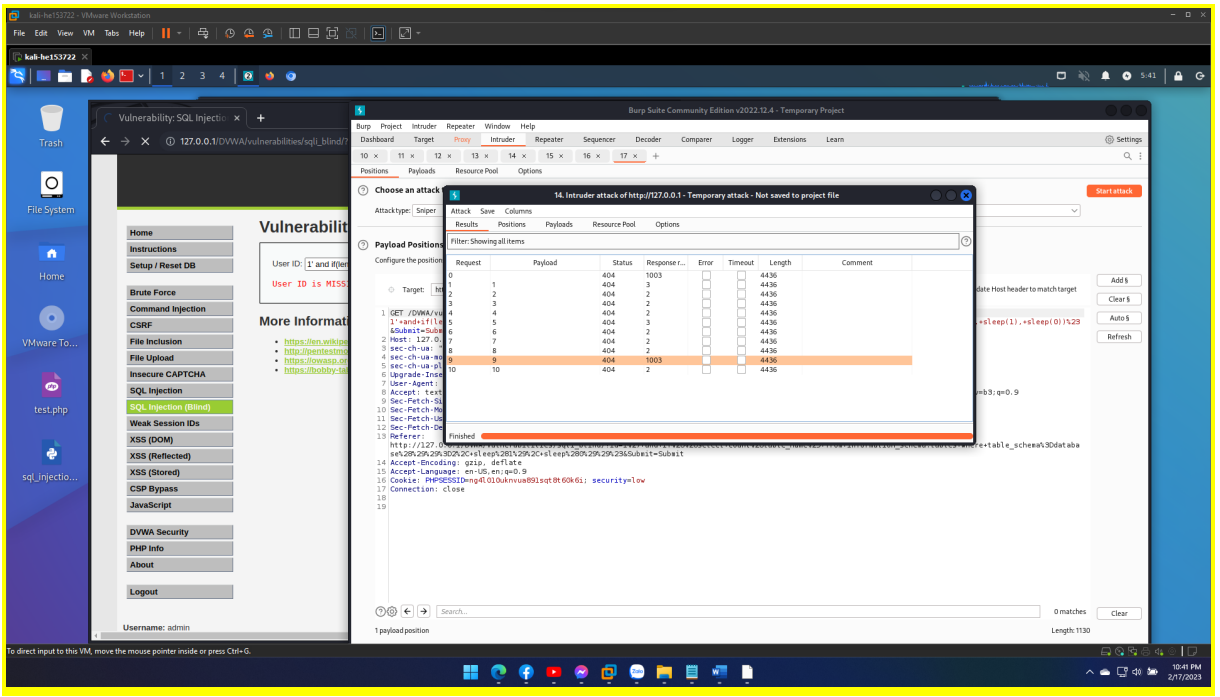
The injected code consists of the AND operator followed by a subquery that counts the number of tables in the current database using the COUNT() function and the information_schema.tables table. The subquery filters the tables by their schema using the table_schema column, which is compared to the name of the current database obtained by the DATABASE() function. If the count of tables in the current database is equal to 2, the injected code will execute the SLEEP(1) function, causing a delay of 1 second. If the count is not equal to 2, the injected code will execute the SLEEP(0) function, which causes no delay.



**o Get length of each tables' name : 9 and 5**

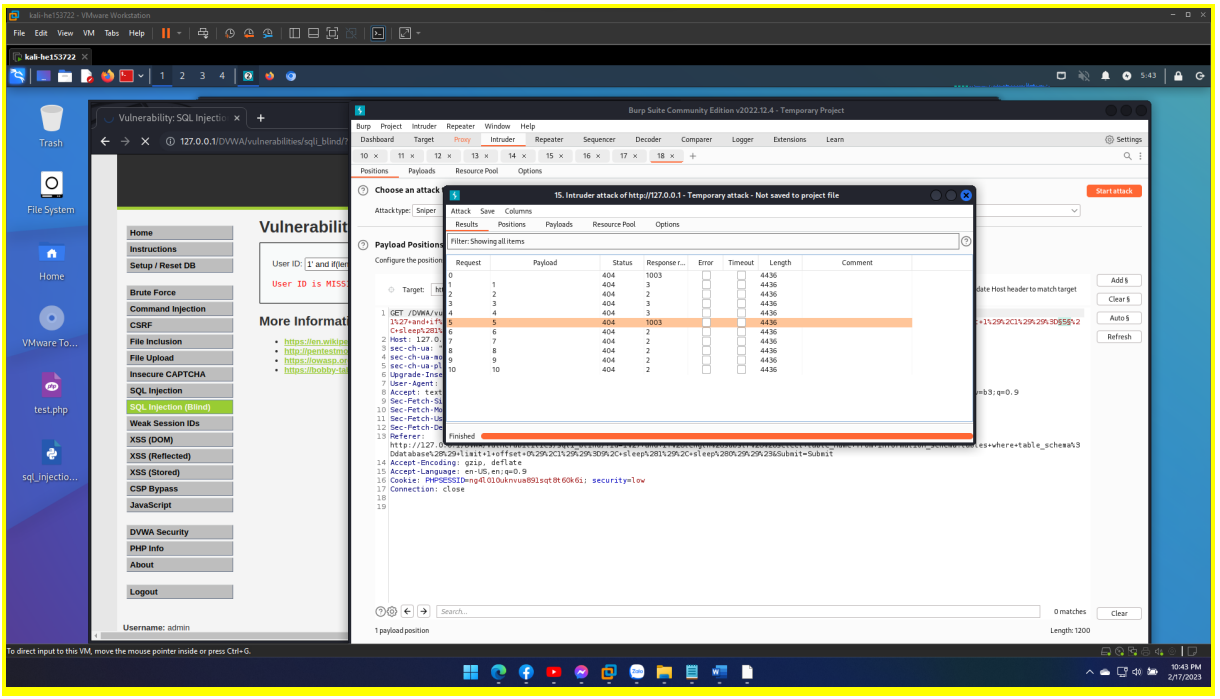
**1' and if(length(substr((select table_name from information_schema.tables where table_schema=database() limit 1 offset 0),1))=9, sleep(1), sleep(0))#**

The injected code consists of the AND operator followed by a subquery that selects the first table name in the current database using the information_schema.tables table. The subquery filters the tables by their schema using the table_schema column, which is compared to the name of the current database obtained by the DATABASE() function. The LIMIT and OFFSET clauses are used to select the first row from the result set. The SUBSTR() and LENGTH() functions are used to get the length of the first character of the selected table name, and the IF() function is used to check if the length is equal to 9. If the length of the first character of the table name is equal to 9, the injected code will execute the SLEEP(1) function, causing a delay of 1 second. If the length is not equal to 9, the injected code will execute the SLEEP(0) function, which causes no delay.



**1' and if(length(substr((select table_name from information_schema.tables where table_schema=database() limit 1 offset 1),1))=5, sleep(1), sleep(0))#**

The injected code consists of the AND operator followed by a subquery that selects the second table name in the current database using the information_schema.tables table. The subquery filters the tables by their schema using the table_schema column, which is compared to the name of the current database obtained by the DATABASE() function. The LIMIT and OFFSET clauses are used to select the second row from the result set. The SUBSTR() and LENGTH() functions are used to get the length of the first character of the selected table name, and the IF() function is used to check if the length is equal to 5. If the length of the first character of the table name is equal to 5, the injected code will execute the SLEEP(1) function, causing a delay of 1 second. If the length is not equal to 5, the injected code will execute the SLEEP(0) function, which causes no delay.



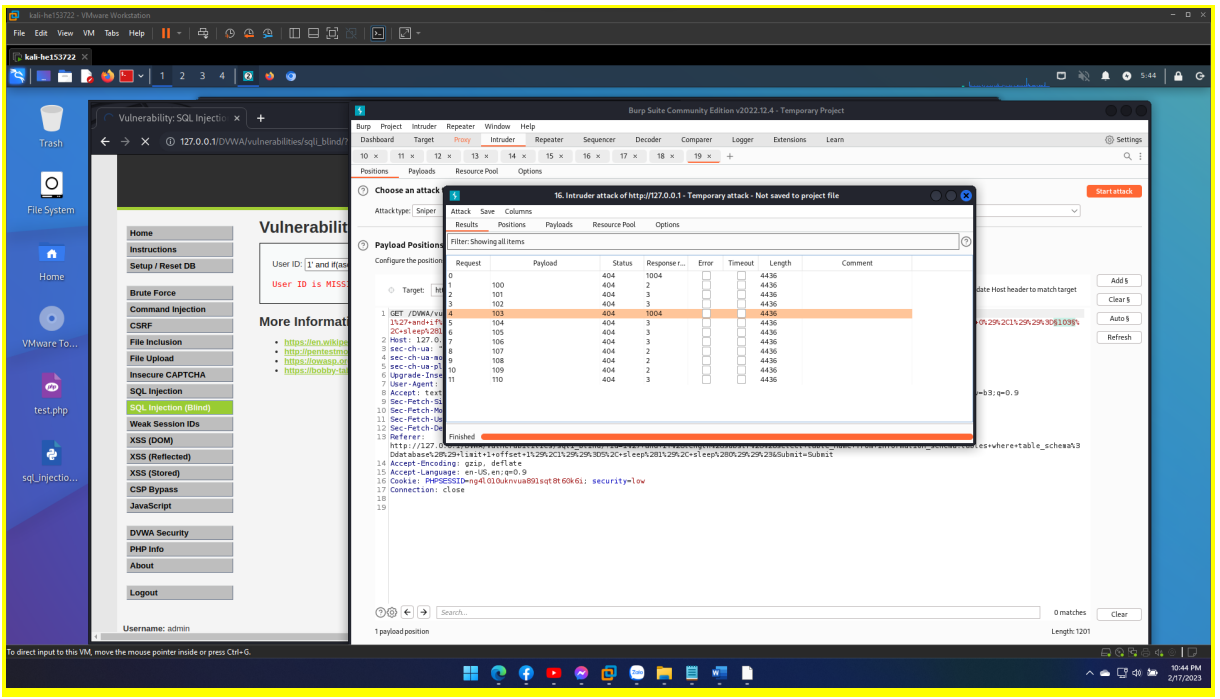
**o Get name of each table by bruteforcing each character :**

**guestbook and users**

**1' and if(ascii(substr((select table_name from information_schema.tables where table_schema=database() limit 1 offset 0),1))=103, sleep(1), sleep(0))#**

The injected code consists of the AND operator followed by a subquery that selects the first table name in the current database using the information_schema.tables table. The subquery filters the tables by their schema using the table_schema column, which is compared to the name of the current database obtained by the DATABASE() function. The LIMIT and OFFSET clauses are used to select the first row from the result set. The SUBSTR() function is used to get the first character of the selected table name, and the ASCII() function is used to get the ASCII code of that character. The IF() function is used to check if the ASCII code is equal to 103. If the ASCII code of the first character of the table name is equal to 103, the injected code will execute the SLEEP(1) function, causing a delay of 1 second. If the ASCII code is not

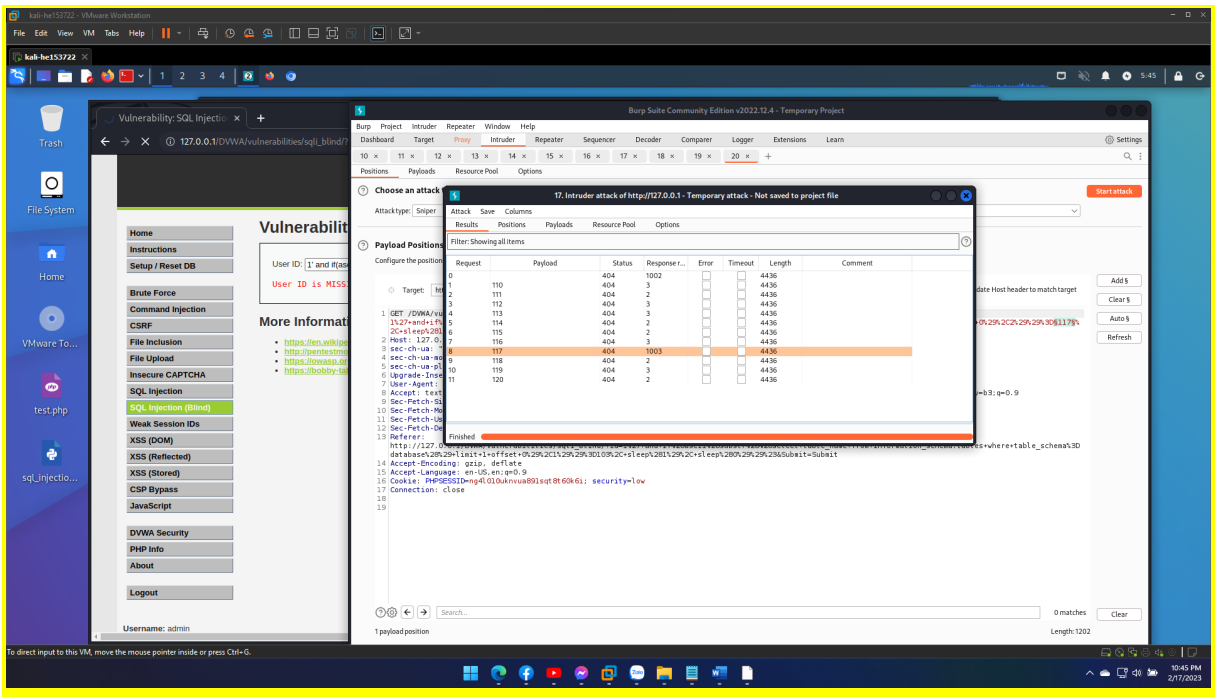
equal to 103, the injected code will execute the SLEEP(0) function, which causes no delay.



**1' and if(ascii(substr((select table_name from information_schema.tables where table_schema=database() limit 1 offset 0),2))=117, sleep(1), sleep(0))#**

The injected code consists of the AND operator followed by a subquery that selects the first table name in the current database using the information_schema.tables table. The subquery filters the tables by their schema using the table_schema column, which is compared to the name of the current database obtained by the DATABASE() function. The LIMIT and OFFSET clauses are used to select the first row from the result set. The SUBSTR() function is used to get the second character of the selected table name, and the ASCII() function is used to get the ASCII code of that character. The IF() function is used to check if the ASCII code is equal to 117. If the ASCII code of the second character of the table name is equal to 117, the injected code will execute the SLEEP(1) function, causing a delay of 1 second. If the ASCII code is not

equal to 117, the injected code will execute the SLEEP(0) function, which causes no delay.

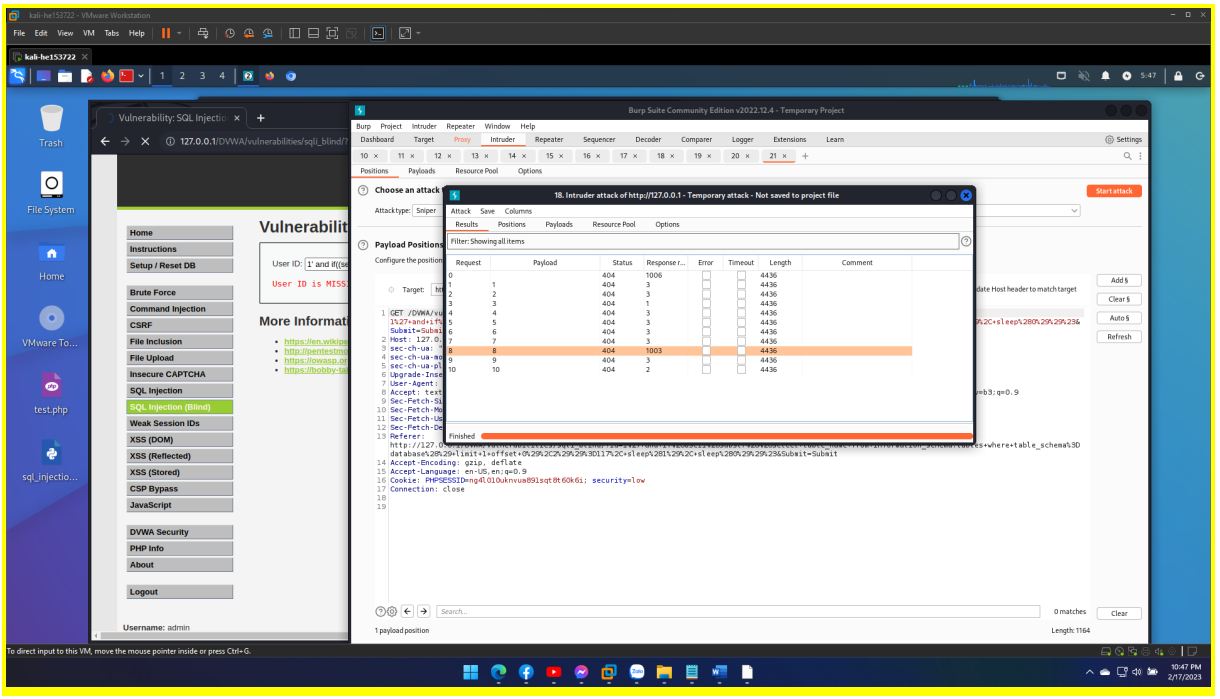


- **Get columns' info:**

**o Get number of columns in 'users' table : 8**

**1' and if((select count(column_name) from information_schema.columns where table_name='users')=8, sleep(1), sleep(0))#**

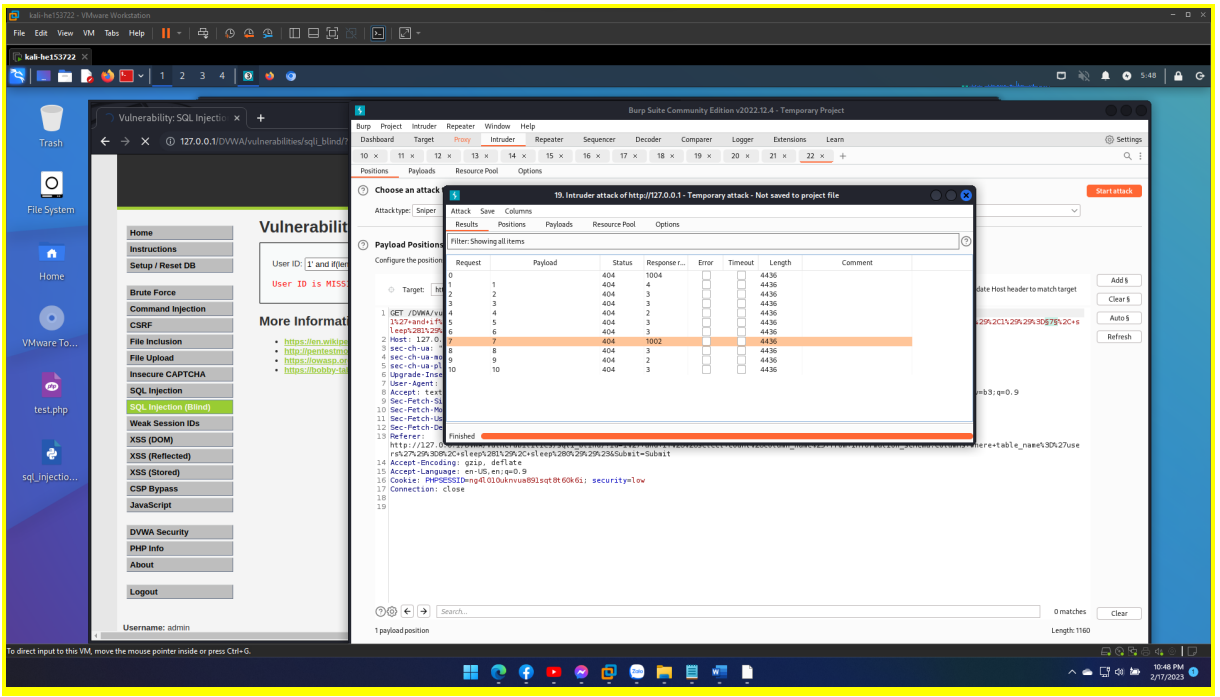
The injected code consists of the AND operator followed by a subquery that counts the number of columns in a table named users. The subquery uses the information_schema.columns table to get the column names of the users table, which is filtered by the table_name column. The IF() function is used to check if the number of columns is equal to 8. If the number of columns in the users table is equal to 8, the injected code will execute the SLEEP(1) function, causing a delay of 1 second. If the number of columns is not equal to 8, the injected code will execute the SLEEP(0) function, which causes no delay.




**o Get length of each column name : 7, 10, 9, 4, 8, 6, 10, 12**

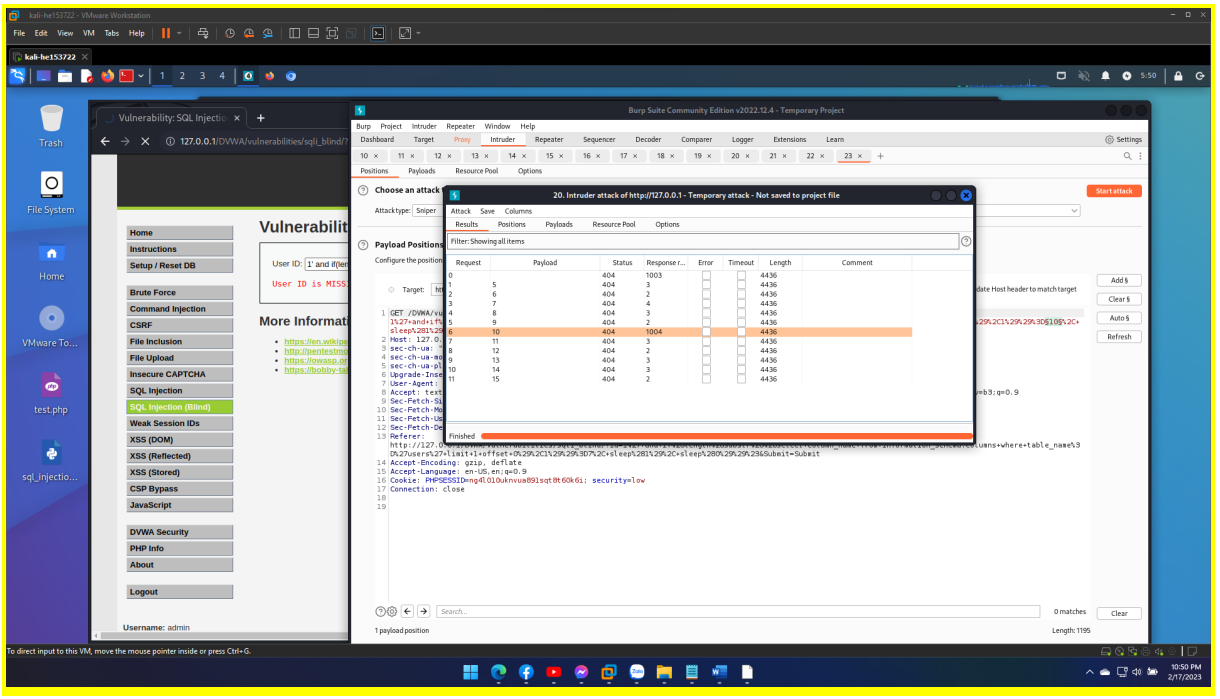
**1' and if(length(substr((select column_name from information_schema.columns where table_name='users' limit 1 offset 0),1))=7, sleep(1), sleep(0))#**

The injected code consists of the AND operator followed by a subquery that selects the first column name in the users table using the information_schema.columns table. The subquery filters the columns by their table name using the table_name column and the LIMIT and OFFSET clauses are used to select the first row from the result set. The SUBSTR() function is used to get the first character of the selected column name, and the LENGTH() function is used to get the length of the selected substring. The IF() function is used to check if the length of the selected substring is equal to 7. If the length is equal to 7, the injected code will execute the SLEEP(1) function, causing a delay of 1 second. If the length is not equal to 7, the injected code will execute the SLEEP(0) function, which causes no delay.



**1' and if(length(substr((select column_name from information_schema.columns where table_name='users' limit 1 offset 1),1))=10, sleep(1), sleep(0))#**

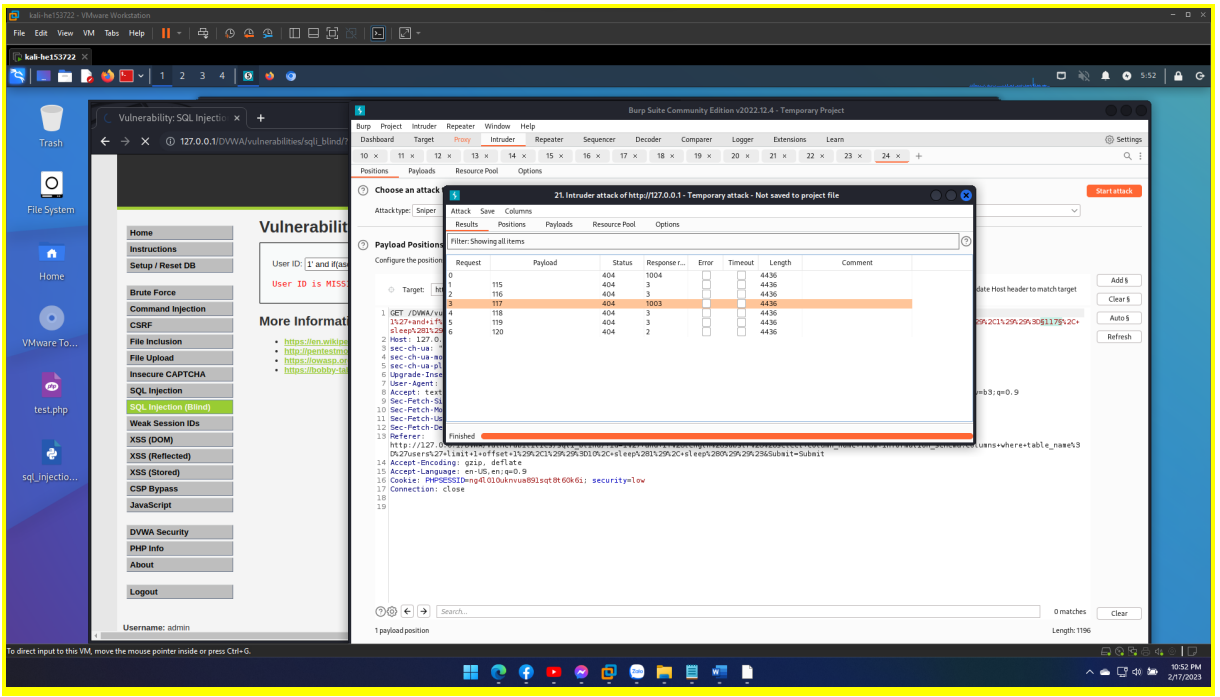
The injected code consists of the AND operator followed by a subquery that selects the second column name in the users table using the information_schema.columns table. The subquery filters the columns by their table name using the table_name column and the LIMIT and OFFSET clauses are used to select the second row from the result set. The SUBSTR() function is used to get the first character of the selected column name, and the LENGTH() function is used to get the length of the selected substring. The IF() function is used to check if the length of the selected substring is equal to 10. If the length is equal to 10, the injected code will execute the SLEEP(1) function, causing a delay of 1 second. If the length is not equal to 10, the injected code will execute the SLEEP(0) function, which causes no delay.



**o Get name of each column by bruteforcing each character : user_id, first_name, last_name, user, password, avatar, last_login, failed_login**

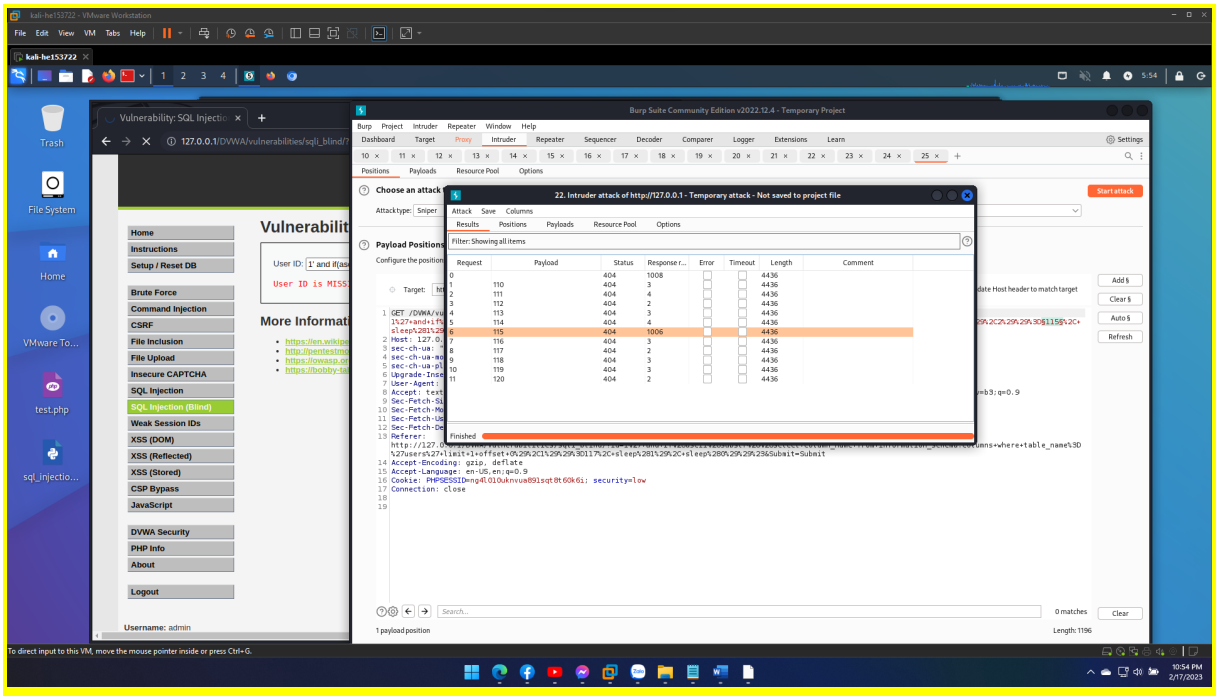
**1' and if(ascii(substr((select column_name from information_schema.columns where table_name='users' limit 1 offset 0),1))=117, sleep(1), sleep(0))#**

The injected code consists of the AND operator followed by a subquery that selects the first column name in the users table using the information_schema.columns table. The subquery filters the columns by their table name using the table_name column and the LIMIT and OFFSET clauses are used to select the first row from the result set. The SUBSTR() function is used to get the first character of the selected column name, and the ASCII() function is used to get the ASCII value of that character. The IF() function is used to check if the ASCII value of the selected character is equal to 117, which is the ASCII value of u. If the condition is true, the injected code will execute the SLEEP(1) function, causing a delay of 1 second. If the condition is false, the injected code will execute the SLEEP(0) function, which causes no delay.




**1' and if(ascii(substr((select column_name from information_schema.columns where table_name='users' limit 1 offset 0),2))=115, sleep(1), sleep(0))#**

The injected code consists of the AND operator followed by a subquery that selects the second column name in the users table using the information_schema.columns table. The subquery filters the columns by their table name using the table_name column and the LIMIT and OFFSET clauses are used to select the first row from the result set. The SUBSTR() function is used to get the second character of the selected column name, and the ASCII() function is used to get the ASCII value of that character. The IF() function is used to check if the ASCII value of the selected character is equal to 115, which is the ASCII value of u. If the condition is true, the injected code will execute the SLEEP(1) function, causing a delay of 1 second. If the condition is false, the injected code will execute the SLEEP(0) function, which causes no delay.

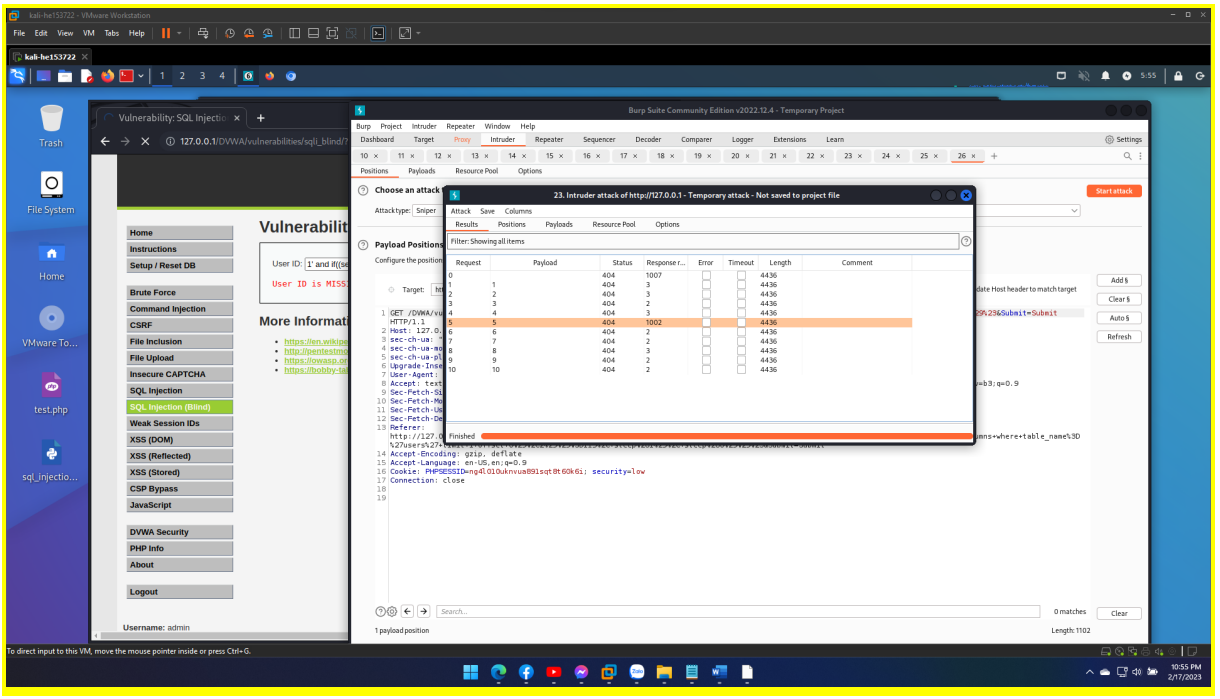



- **Get username, password:**

**o Get number of records in table : 5**

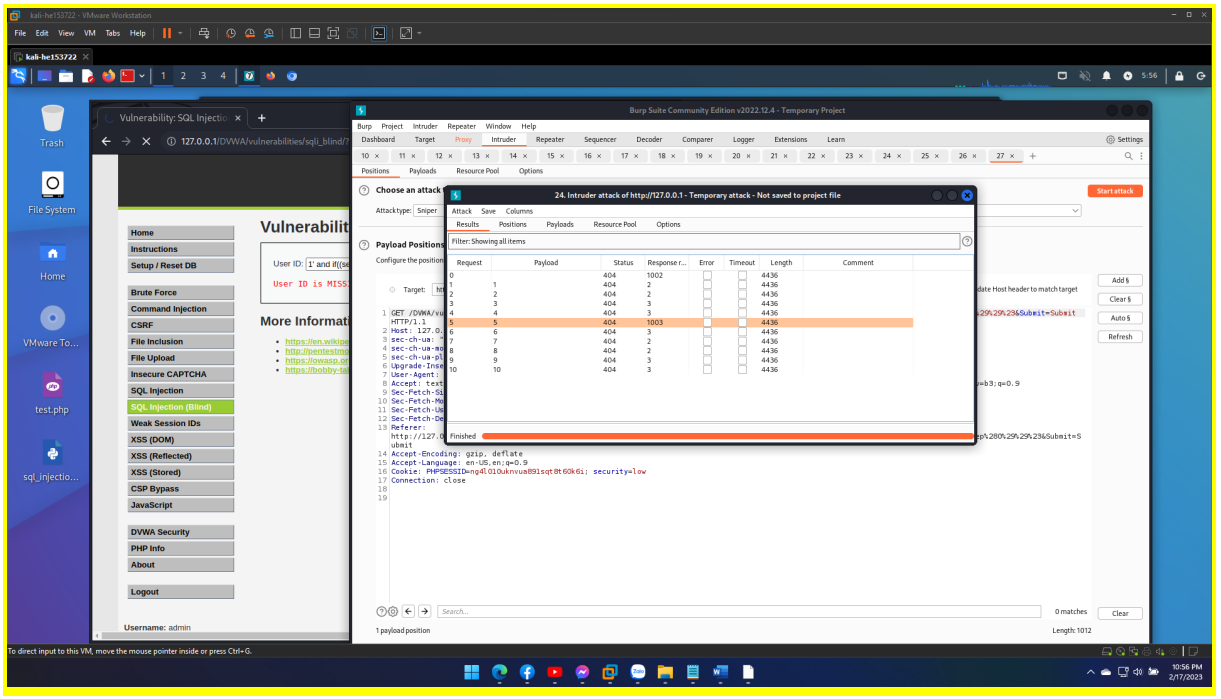
**1' and if((select count(user) from users)=5, sleep(1), sleep(0))#**

The injected code consists of the COUNT() function is used to count the number of records in the users table where the user column is not null. The IF() function is used to check if the count is equal to 5. If the condition is true, the injected code will execute the SLEEP(1) function, causing a delay of 1 second. If the condition is false, the injected code will execute the SLEEP(0) function, which causes no delay.




**1' and if((select count(password) from users)=5, sleep(1), sleep(0))#**

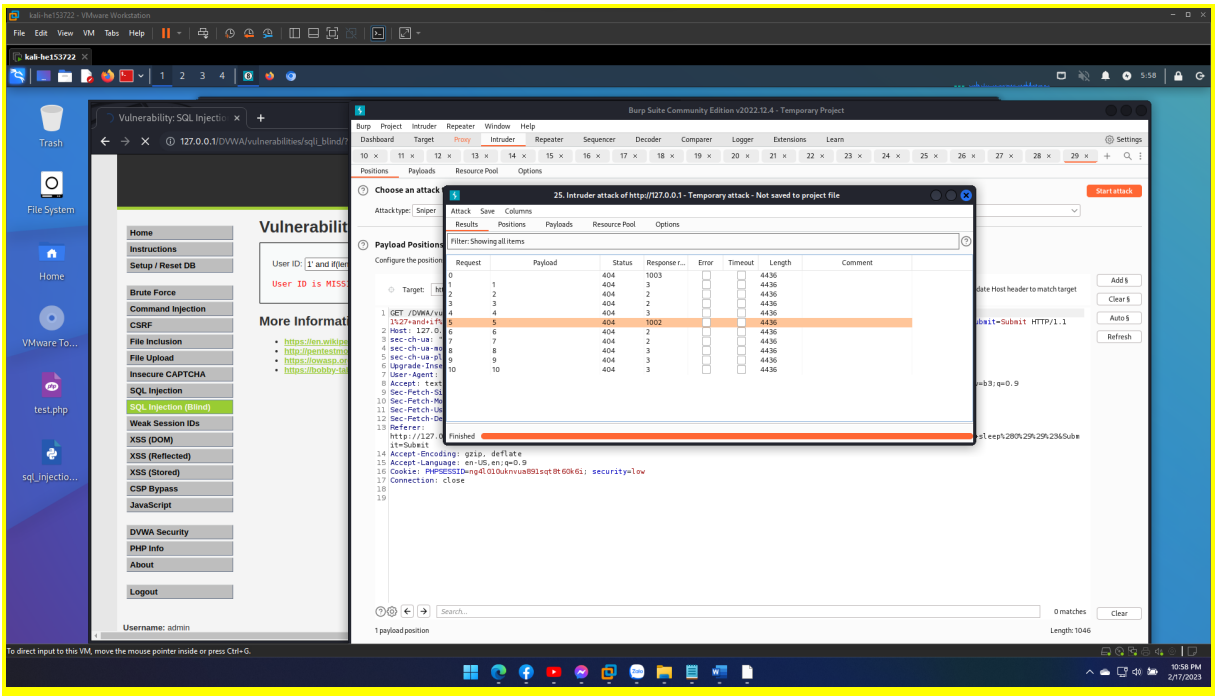
The injected code consists of the COUNT() function is used to count the number of records in the users table where the password column is not null. The IF() function is used to check if the count is equal to 5. If the condition is true, the injected code will execute the SLEEP(1) function, causing a delay of 1 second. If the condition is false, the injected code will execute the SLEEP(0) function, which causes no delay.




**o Get length of each record's data : user: 5, 7, 4, 5, 6 and password: 32**

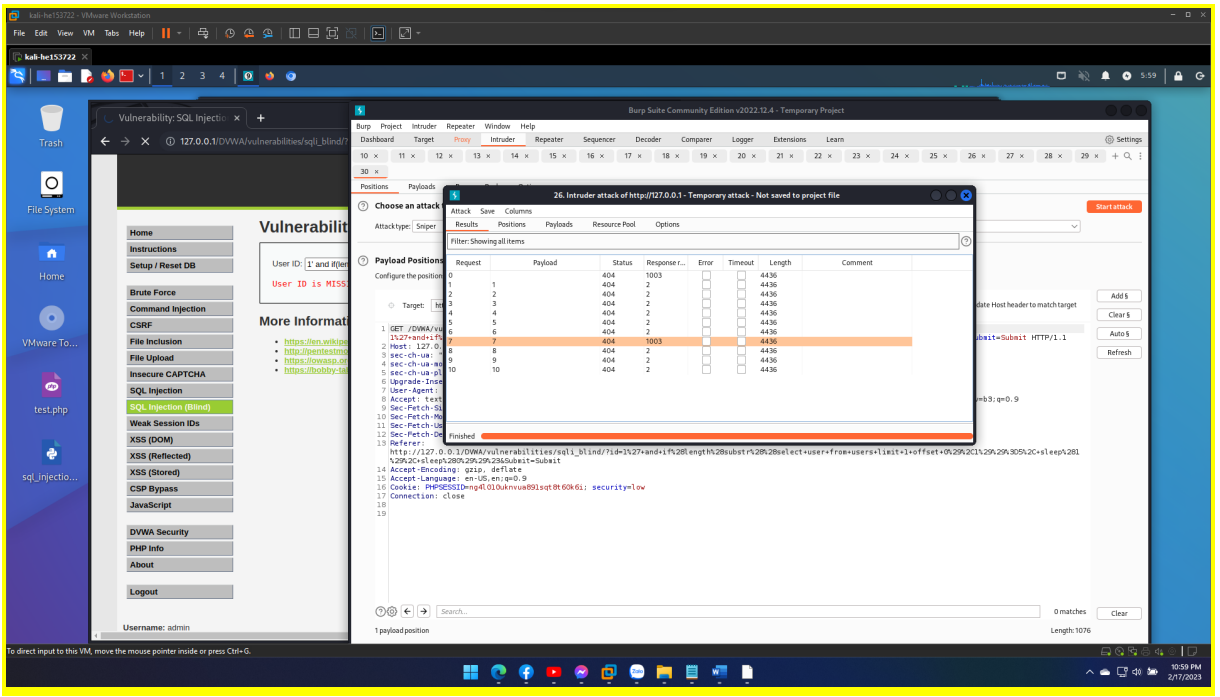
**1' and if(length(substr((select user from users limit 1 offset 0),1))=5, sleep(1), sleep(0))#**

The injected code uses the SELECT statement to query the users table for the first record using the LIMIT and OFFSET clauses. The SUBSTR() function is used to extract the value of the user column. The LENGTH() function is used to get the length of the extracted value, and the IF() function is used to check if the length is equal to 5. If the condition is true, the injected code will execute the SLEEP(1) function, causing a delay of 1 second. If the condition is false, the injected code will execute the SLEEP(0) function, which causes no delay.



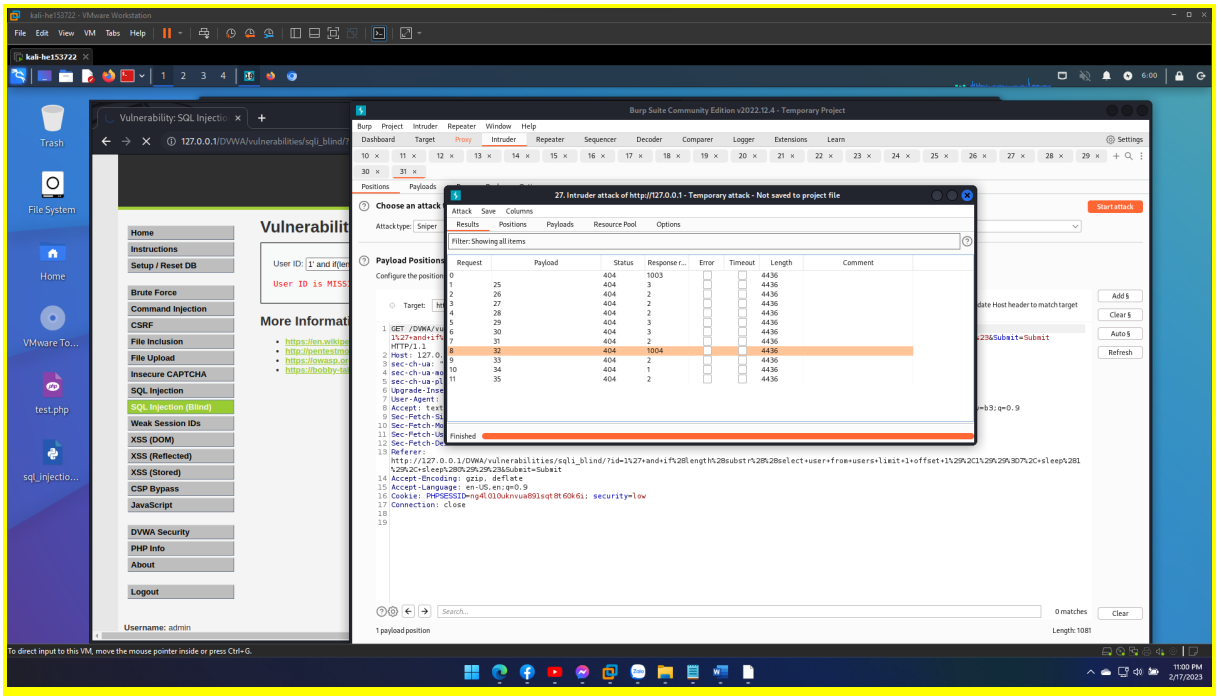

**1' and if(length(substr((select user from users limit 1 offset 1),1))=7, sleep(1), sleep(0))#**

The injected code uses the SELECT statement to query the users table for the second record using the LIMIT and OFFSET clauses. The SUBSTR() function is used to extract the value of the user column. The LENGTH() function is used to get the length of the extracted value, and the IF() function is used to check if the length is equal to 7. If the condition is true, the injected code will execute the SLEEP(1) function, causing a delay of 1 second. If the condition is false, the injected code will execute the SLEEP(0) function, which causes no delay.



**1' and if(length(substr((select password from users limit 1 offset 1),1))=32, sleep(1), sleep(0))#**

The injected code to checking the length of the password of the second user in the users table. It's checking if the length is 32 characters long. This could indicate that the password is stored as a hash. If the condition is true, the injected code will execute the SLEEP(1) function, causing a delay of 1 second. If the condition is false, the injected code will execute the SLEEP(0) function, which causes no delay.



**o Bruteforcing each character of record's data :**

**User: admin, gordonb, 1337, pablo, smithy**

**Password: 5f4dcc3b5aa765d61d8327deb882cf99**

**e99a18c428cb38d5f260853678922e03**

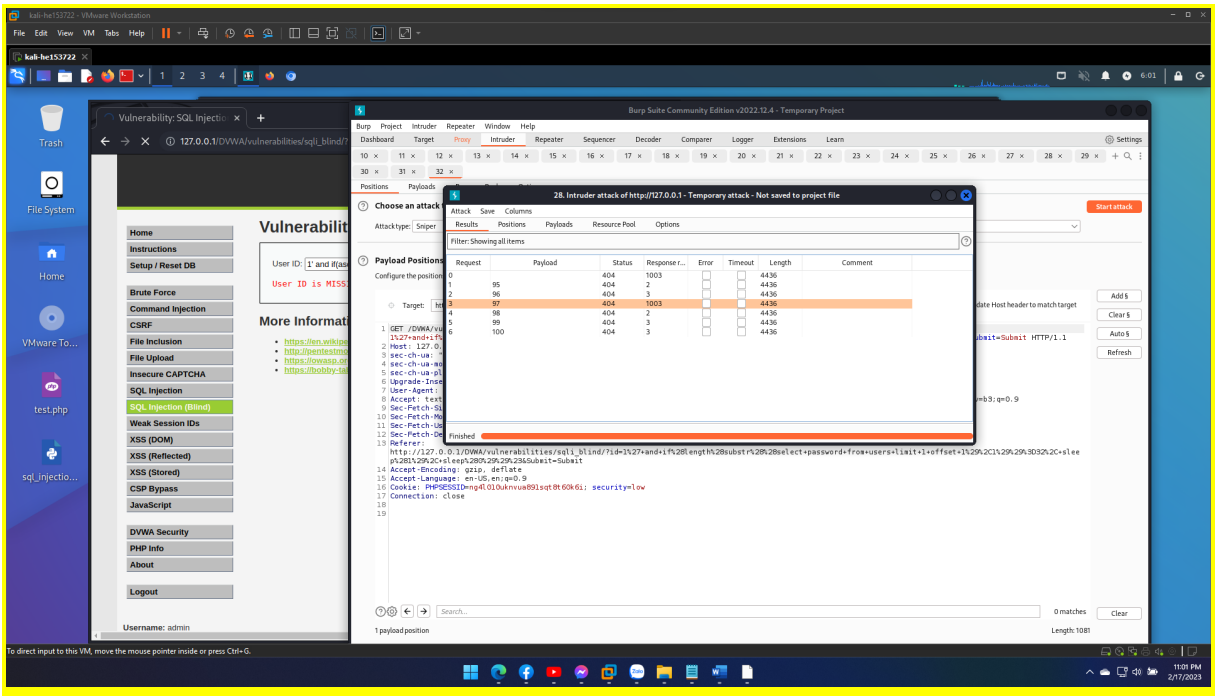
**8d3533d75ae2c3966d7e0d4fcc69216b**

**0d107d09f5bbe40cade3de5c71e9e9b7**

**5f4dcc3b5aa765d61d8327deb882cf99**

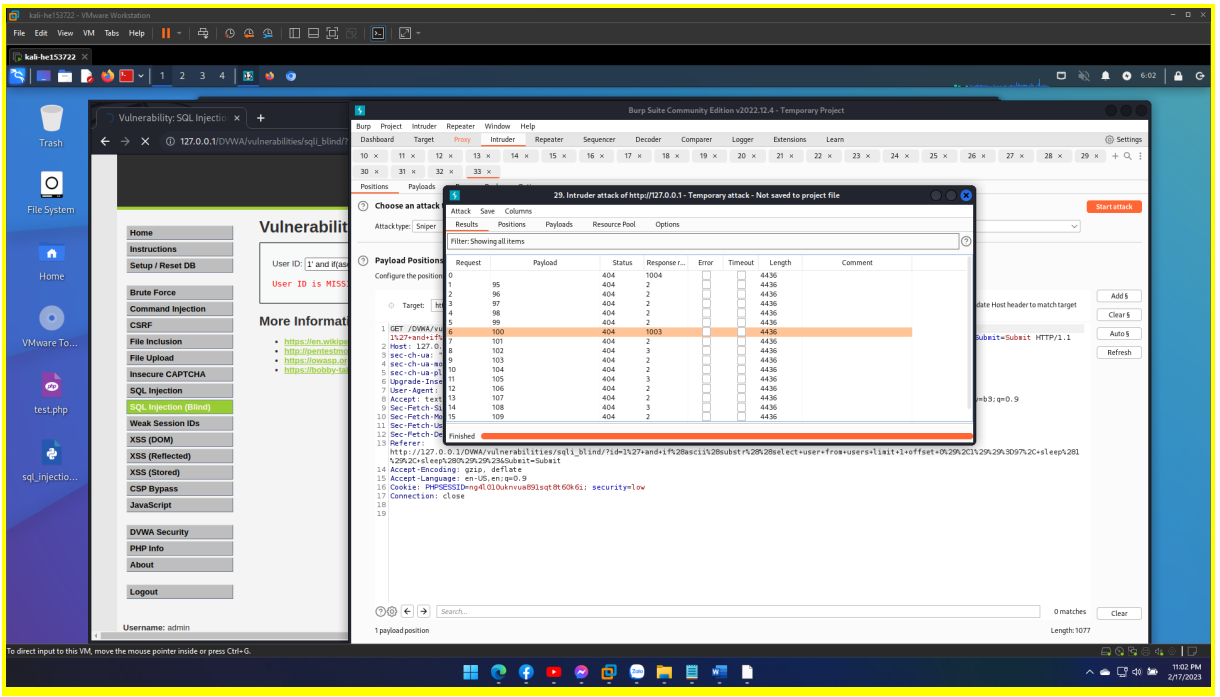
**1' and if(ascii(substr((select user from users limit 1 offset 0),1))=97, sleep(1), sleep(0))#**

The injected code to checking the first character of the username of the first user in the users table. It's checking if the ASCII code of the first character is 97, which is the ASCII code for the letter "a". If the condition is true, the injected code will execute the SLEEP(1) function, causing a delay of 1 second. If the condition is false, the injected code will execute the SLEEP(0) function, which causes no delay.



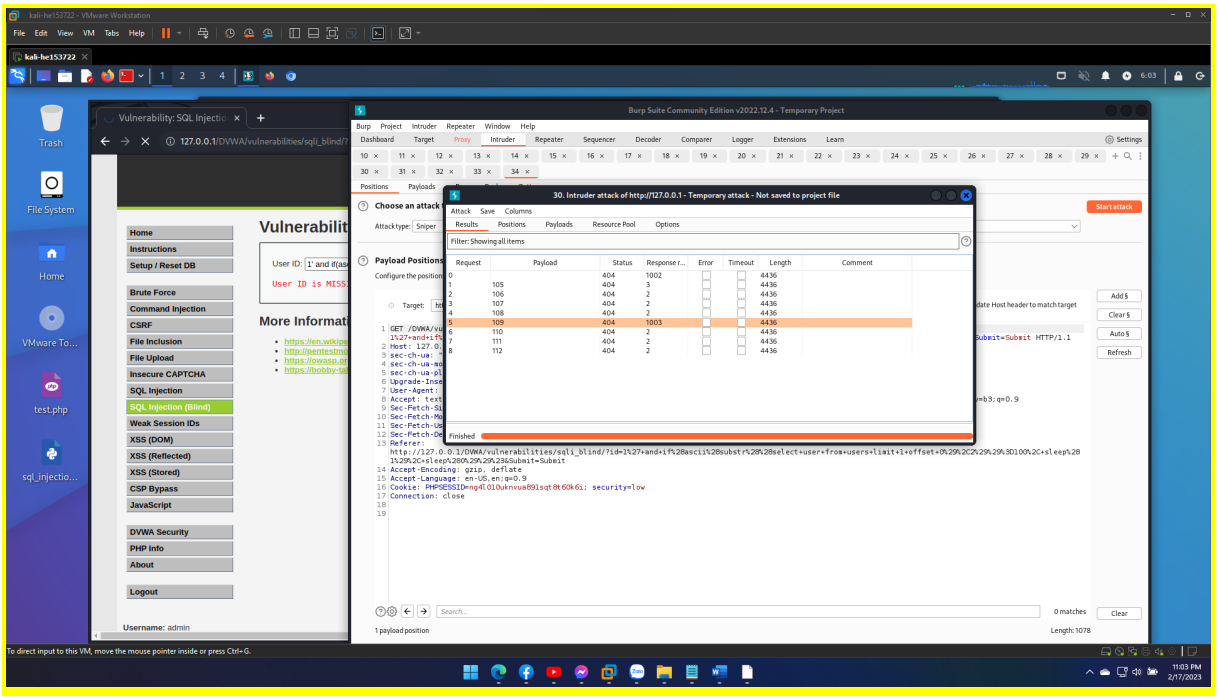
**1' and if(ascii(substr((select user from users limit 1 offset 0),2))=100, sleep(1), sleep(0))#**

The injected code to checking the second character of the username of the first user in the users table. It's checking if the ASCII code of the first character is 100, which is the ASCII code for the letter "d". If the condition is true, the injected code will execute the SLEEP(1) function, causing a delay of 1 second. If the condition is false, the injected code will execute the SLEEP(0) function, which causes no delay.



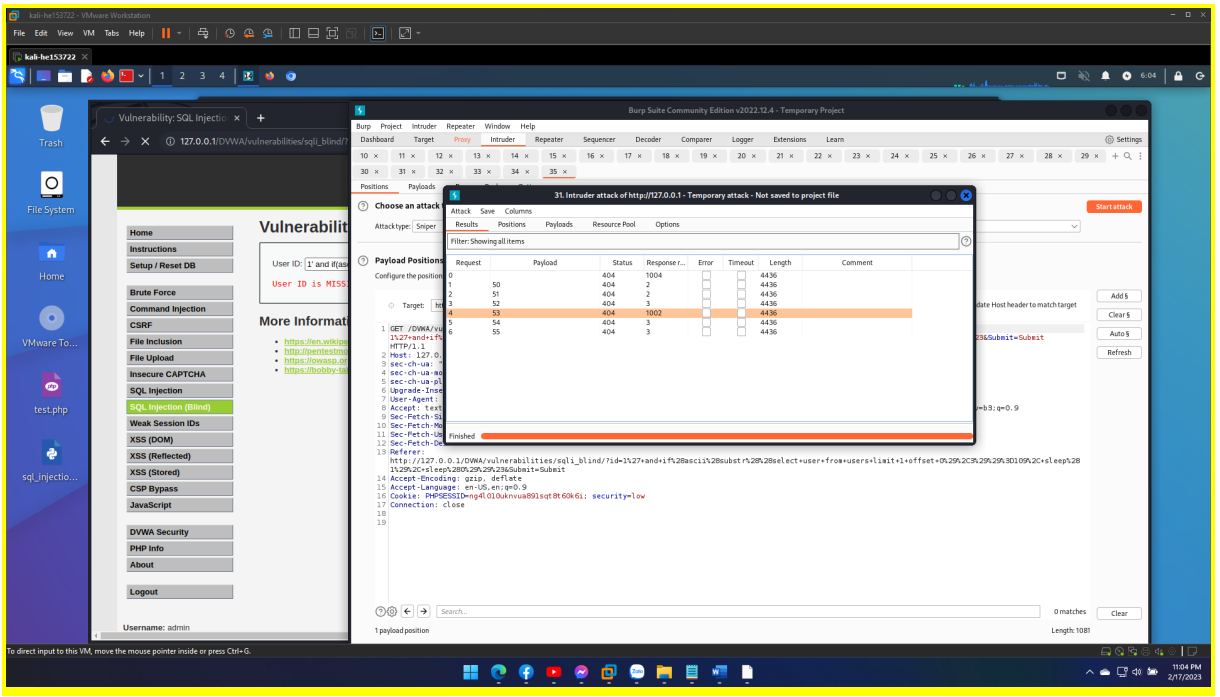
**1' and if(ascii(substr((select user from users limit 1 offset 0),3))=109, sleep(1), sleep(0))#**

The injected code to checking the third character of the username of the first user in the users table. It's checking if the ASCII code of the first character is 109, which is the ASCII code for the letter "m". If the condition is true, the injected code will execute the SLEEP(1) function, causing a delay of 1 second. If the condition is false, the injected code will execute the SLEEP(0) function, which causes no delay.



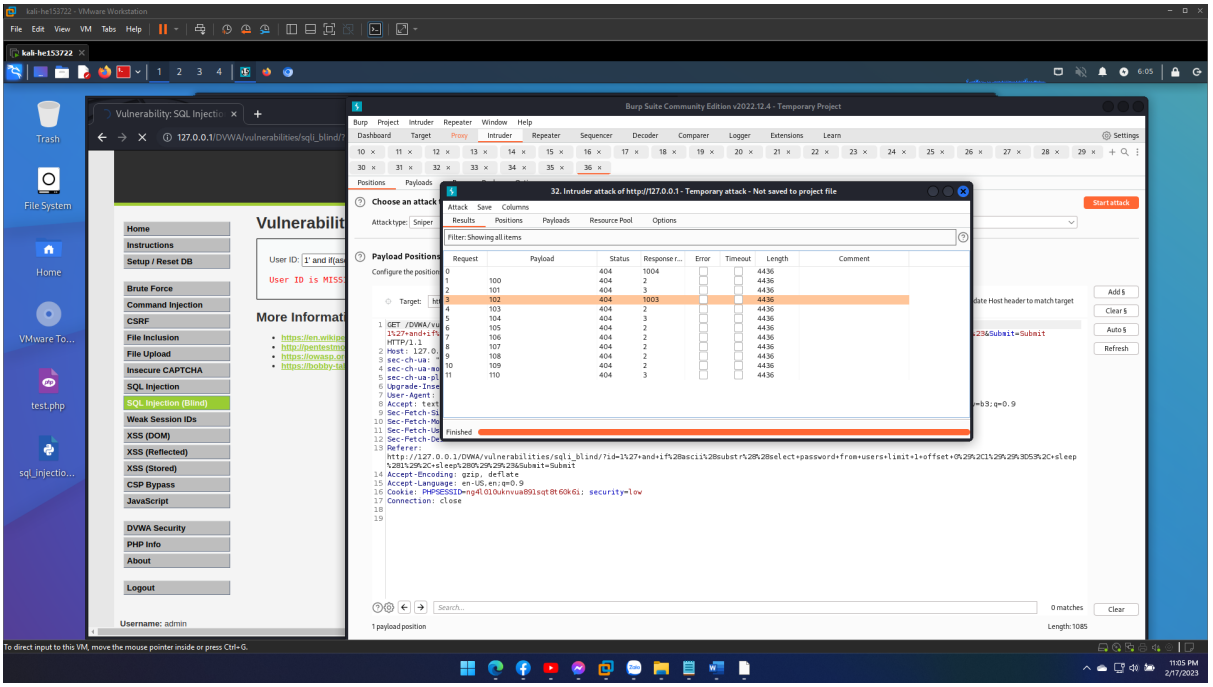
**1' and if(ascii(substr((select password from users limit 1 offset 0),1))=53, sleep(1), sleep(0))#**

The injected code to checking the first character of the password of the first user in the users table. It's checking if the ASCII code of the first character is 53, which is the ASCII code for the letter "5". If the condition is true, the injected code will execute the SLEEP(1) function, causing a delay of 1 second. If the condition is false, the injected code will execute the SLEEP(0) function, which causes no delay.




**1' and if(ascii(substr((select password from users limit 1 offset 0),2))=102, sleep(1), sleep(0))#**

The injected code to checking the second character of the password of the first user in the users table. It's checking if the ASCII code of the first character is 102, which is the ASCII code for the letter "f". If the condition is true, the injected code will execute the SLEEP(1) function, causing a delay of 1 second. If the condition is false, the injected code will execute the SLEEP(0) function, which causes no delay.


Vulnerability: SQL Injection
127.0.0.1/DVWA/vulnerabilities/sqli_blind/
Home
Instructions
Setup / Reset DB
Brute Force
Command Injection
CSRF
File Inclusion
File Upload
Insecure CAPTCHA
SQL Injection
SQL Injection (Blind)
Weak Session IDs
XSS (DOM)
XSS (Reflected)
XSS (Stored)
CSP Bypass
JavaScript
DVWA Security
PHP Info
About
Logout
Username: admin
Burp Suite Community Edition v2022.12.4 - Temporary Project
32. Intruder attack of http://127.0.0.1 - Temporary attack - Not saved to project file
Finished
Trash
File System
Home
VMware To...
test.php
sql_injectio...