

Apply filters to SQL queries

Project description

This project simulates what it's like being a security analyst by performing complex queries in SQL. We're mostly going to retrieve information from the employees database. To do this, we need to write queries that have multiple conditions and operators. For operators, we'll focus on 'NOT', 'OR', and 'AND'.

Retrieve after hours failed login attempts

So, I 'discovered' a potential security incident that occurred after business hours. To investigate, we need a query to get to the log_in_attempts table and review after hours login activity. We'll need to specifically look for failed login attempts

Google Chrome | File | Edit | View | History | Bookmarks | Profiles | Tab | Window | Help

Portfolio Activity: Apply filters: x | Activity: Filter with AND, OR, x | Activity: Filter with AND, OR, x | +

googlecoursera.qwiklabs.com/focuses/31915188?parent=lt_session

TAMUCC | Capstone Project | Software Project... | Forensics | Project Manager | Cal II | Computer Archite... | Systems Program... | help yasef | Job Possibilities | All Bookmarks

Activity: Filter with AND, OR, and NOT

MariaDB [organization]> SELECT * FROM log_in_attempts WHERE login_time > '18:00' AND success = 0;

event_id	username	login_date	login_time	country	ip_address
2	apatel	2022-05-10	20:27:27	CAN	192.168.205.12
18	pwashing	2022-05-11	19:28:50	US	192.168.66.142
20	tshah	2022-05-12	18:56:36	MEXICO	192.168.109.50
28	aestrada	2022-05-09	19:28:12	MEXICO	192.168.27.57
34	drosas	2022-05-11	21:02:04	US	192.168.45.93
42	cgriffin	2022-05-09	23:04:05	US	192.168.4.157
52	cjackson	2022-05-10	22:07:07	CAN	192.168.58.57
69	wjaffrey	2022-05-11	19:55:15	USA	192.168.100.17
82	abernard	2022-05-12	23:38:46	MEX	192.168.234.49
87	apatel	2022-05-08	22:38:31	CANADA	192.168.132.153
96	ivelasco	2022-05-09	22:36:36	CAN	192.168.84.194
104	asundara	2022-05-11	18:38:07	US	192.168.96.200
107	bisles	2022-05-12	20:25:57	USA	192.168.116.187
111	aestrada	2022-05-10	22:00:26	MEXICO	192.168.76.27
127	abellmas	2022-05-09	21:20:51	CANADA	192.168.70.122

business hours. Replace the X and Y with the correct values to filter for the records you need:

```
SELECT *
FROM log_in_attempts
WHERE login_time > 'X' AND success = Y;
```

Note: Values of TRUE and FALSE are not placed in single quotes because they are not string data. They are Boolean data, which is another data type.

How many failed login attempts occurred after 18:00?

☒ 19

☐ 39

☐ 20

☐ 44

Submit

Retrieve login attempts on specific dates

So we noticed that a suspicious event occurred on 2022-05-09. To look into this further, we need to set up a query that will review all login attempts that happened on that day and the day before.

First you can see that we're selecting all columns with '*' just to get info like the employee name and their id, along with the date. Then, we'll use the 'OR' operator to act as a filter to remove any other date that's not 2022-05-09 or 2022-05-08.

The screenshot shows a Google Chrome browser window with a SQL query in MariaDB and a quiz question. The query is:

```
MariaDB [organization]> SELECT *  
-> FROM log_in_attempts  
-> WHERE login_date = '2022-05-08' OR login_date = '2022-05-09';
```

The query results show a table with columns: event_id, username, login_date, login_time, country, ip_address, and success. The results are as follows:

event_id	username	login_date	login_time	country	ip_address	success
1	jrafael	2022-05-09	04:56:27	CAN	192.168.243.140	1
3	dkot	2022-05-09	06:47:41	USA	192.168.151.162	1
4	dkot	2022-05-08	02:00:39	USA	192.168.178.71	0
8	bisles	2022-05-08	01:30:17	US	192.168.119.173	0
12	dkot	2022-05-08	09:11:34	USA	192.168.100.158	1
15	lyamamot	2022-05-09	17:17:26	USA	192.168.183.51	0
24	arusso	2022-05-09	06:49:39	MEXICO	192.168.171.192	1
25	sbaelish	2022-05-09	07:04:02	US	192.168.33.137	1
26	apatel	2022-05-08	17:27:00	CANADA	192.168.123.105	1
28	aestrada	2022-05-09	19:28:12	MEXICO	192.168.27.57	0
30	yappiah	2022-05-09	03:22:22	MEX	192.168.124.48	1
32	acook	2022-05-09	02:52:02	CANADA	192.168.142.239	0
36	asundara	2022-05-08	09:00:42	US	192.168.78.151	1
38	sbaelish	2022-05-09	14:40:01	USA	192.168.60.42	1

The quiz question is:

Your team is investigating a suspicious event that occurred on '2022-05-09'. You want to retrieve all login attempts that occurred on this day and the day before ('2022-05-08').

The login_date column in the log_in_attempts table contains information on the dates when login attempts were made.

Use the OR operator to retrieve the failed login attempts on the specified days. Replace the X and Y with the correct values to filter for the records you need:

```
SELECT *  
FROM log_in_attempts  
WHERE login_date = 'X' OR login_date = 'Y';
```

How many login attempts were made on these two days?

☐ 89

☒ 75

☐ 67

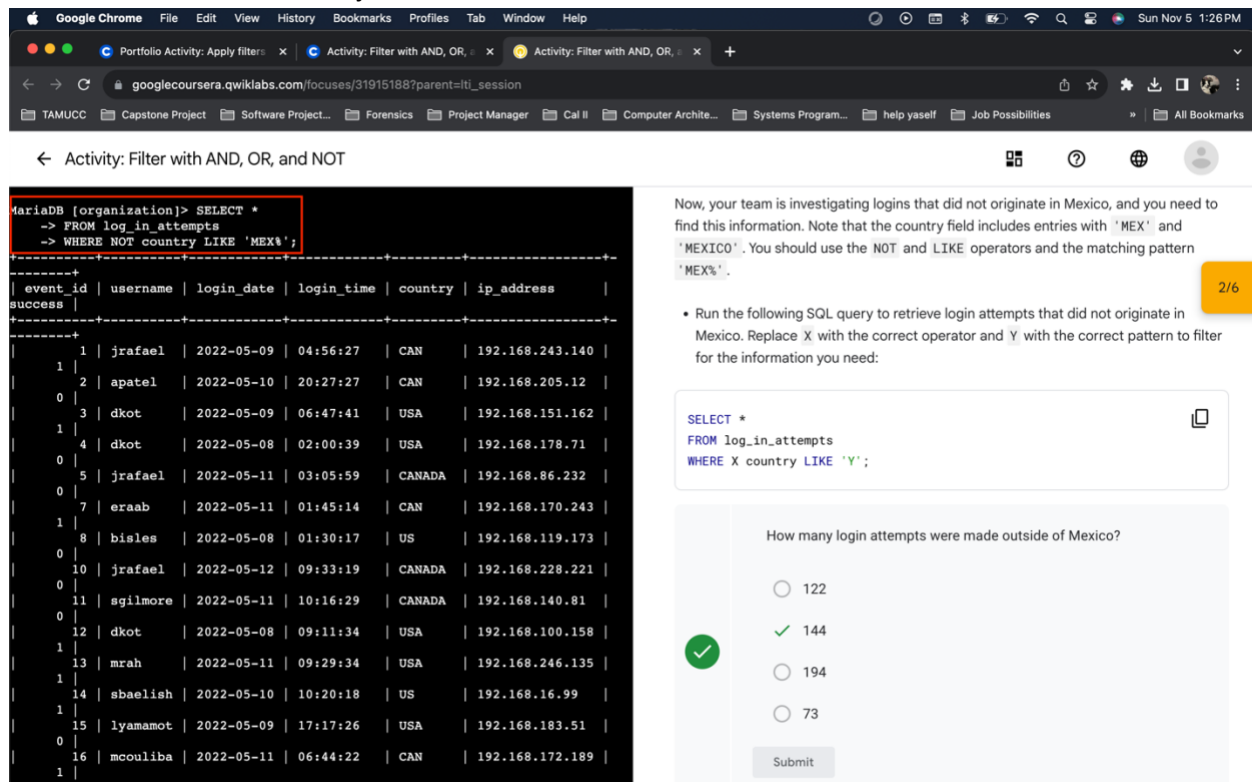
☐ 44

Submit

Retrieve login attempts outside of Mexico

In this part of the project, we've become aware of suspicious activity with login attempts. But we know for sure that the activity didn't originate from Mexico, so we can mark that off. To narrow the search, we need to look at login attempts outside of Mexico. We'll use a filter in a query that identifies all login attempts that occurred anywhere but Mexico. To do this, we'll use the 'NOT' operator, and the '%' to handle variations of the spelling of Mexico. It could either be 'MEX' or 'MEXICO'. We'll use it like this: 'MEX%', the percentage sign could either complete the full word Mexico, or it could just leave it as the

abbreviation and that will be just fine as well.



Activity: Filter with AND, OR, and NOT

```
MariaDB [organization]> SELECT *
-> FROM log_in_attempts
-> WHERE NOT country LIKE 'MEX%';
```

event_id	username	login_date	login_time	country	ip_address
1	jrafael	2022-05-09	04:56:27	CAN	192.168.243.140
2	apatel	2022-05-10	20:27:27	CAN	192.168.205.12
3	dkot	2022-05-09	06:47:41	USA	192.168.151.162
4	dkot	2022-05-08	02:00:39	USA	192.168.178.71
5	jrafael	2022-05-11	03:05:59	CANADA	192.168.86.232
7	eraab	2022-05-11	01:45:14	CAN	192.168.170.243
8	bisles	2022-05-08	01:30:17	US	192.168.119.173
10	jrafael	2022-05-12	09:33:19	CANADA	192.168.228.221
11	sgilmore	2022-05-11	10:16:29	CANADA	192.168.140.81
12	dkot	2022-05-08	09:11:34	USA	192.168.100.158
13	mrah	2022-05-11	09:29:34	USA	192.168.246.135
14	sbaelish	2022-05-10	10:20:18	US	192.168.16.99
15	lyamamot	2022-05-09	17:17:26	USA	192.168.183.51
16	mcouliba	2022-05-11	06:44:22	CAN	192.168.172.189

Now, your team is investigating logins that did not originate in Mexico, and you need to find this information. Note that the country field includes entries with 'MEX' and 'MEXICO'. You should use the NOT and LIKE operators and the matching pattern 'MEX%'.
Run the following SQL query to retrieve login attempts that did not originate in Mexico. Replace X with the correct operator and Y with the correct pattern to filter for the information you need:

```
SELECT *
FROM log_in_attempts
WHERE X country LIKE 'Y';
```

How many login attempts were made outside of Mexico?

☐ 122

☒ 144

☐ 194

☐ 73

Submit

Retrieve employees in Marketing

So now we want to see what machines in the Marketing department need to be updated for better security. We'll need to create a query that identifies all employees in the Marketing department in all offices in the East building. This time we only want the Marketing column, and offices in the East wing. We'll use the LIKE keyword instead of the equals sign, and we'll use '%' to help with filtering for the East wing. Notice that for the 'WHERE' part, it's appropriate to use the '=' operator, but when we need to look for a certain set of characters, this is incorrect syntax. Instead we use the 'LIKE' operator paired

with the '%' sign.

Activity: Filter with AND, OR, and NOT

```
1195 | n516o853p957 | orainier | Finance | East-346
1196 | o225p357q829 | sshah2 | Information Technology | South-385
1197 | p791q114r509 | aabara | Information Technology | North-159
1198 | q308r573s459 | jmartine | Marketing | South-117
1199 | r520a571t459 | areyes | Human Resources | East-100
```

200 rows in set (0.001 sec)

MariaDB [organization]> SELECT employee_id, device_id, username, department, office
-> WHERE ;
ERROR 1064 (42000): You have an error in your SQL syntax; check the manual that corresponds to your MariaDB server version for the right syntax to use near 'WHERE' at line 2

MariaDB [organization]> SELECT *
-> FROM employees
-> WHERE department = 'Marketing' AND office LIKE 'East%';

employee_id	device_id	username	department	office
1000	a320b137c219	elarson	Marketing	East-170
1052	a192b174c940	jdarosa	Marketing	East-195
1075	x573y883z772	fbautist	Marketing	East-267
1088	k865l965m233	rgosh	Marketing	East-157
1103	NULL	randerss	Marketing	East-460
1156	a184b775c707	dellery	Marketing	East-417
1163	h679i515j339	cwilliam	Marketing	East-216

7 rows in set (0.027 sec)

MariaDB [organization]>

Your team is updating employee machines, and you need to obtain the information about employees in the 'Marketing' department who are located in all offices in the East building (such as 'East-170' or 'East-320').

- Write a SQL query to retrieve this information from the `employees` table. Select columns and include filters on the `department` and `office` columns to return only the needed records.

Note: You'll need to use the `AND` and `LIKE` operators to satisfy both of these criteria.

What is the username of the first employee in the Marketing department in the East building?

☐ fbautist

☐ jclark

☒ elarson

☐ alevitsk

Submit

Retrieve employees in Finance or Sales

So now we'd like to see who needs the IT department to perform security updates on every employee's machine that's in either the Sales or Finance department. Simple enough. We'll go ahead and use the 'OR' operator to grab the employees' information from either the Sales or Finance department. Even though we're gathering data from one department, we need to make sure our conditions are specific enough. For the query to have correct syntax, we need write out both full conditions. We need to

specify the department for the two conditions.

Google ChromeFile Edit View History Bookmarks Profiles Tab Window Help

Portfolio Activity: Apply filter:Activity: Filter with AND, OR,Activity: Filter with AND, OR, +

googlecoursera.qwiklabs.com/focuses/31915188?parent=lti_session

TAMUCCCapstone ProjectSoftware Project...ForensicsProject ManagerCal IIComputer Archite...Systems Program...help yasefJob PossibilitiesAll Bookmarks

Activity: Filter with AND, OR, and NOT

38 rows in set, 5 warnings (0.001 sec)

MariaDB [organization]> SELECT * FROM employees WHERE department = 'Finance' OR department = 'Sales';

employee_id	device_id	username	department	office
1003	d394e816f943	sgilmore	Finance	South-153
1007	n174i497j413	wjaffrey	Finance	North-406
1008	i858j583k571	abernard	Finance	South-170
1009	NULL	lrodriqu	Sales	South-134
1010	k242i212m542	jlansky	Finance	South-109
1011	l748m120n401	drosas	Sales	South-292
1015	p611q262t945	jsoto	Finance	North-271
1017	r550s824t230	jclark	Finance	North-188
1018	s310t540u653	abellmas	Finance	North-403
1022	w237x430y567	arusso	Finance	West-465
1024	y976z753a267	iuduike	Sales	South-215
1025	z381a365b233	jhill	Sales	North-115
1029	d336e475f676	ivelasco	Finance	East-156
1035	j236k303l245	bisles	Sales	South-171
1039	n253o917p623	cjackson	Sales	East-378
1041	p929q222r778	cgriffin	Sales	North-208
1044	s429t157u159	tbarnes	Finance	West-415
1045	t567u844v434	pwashing	Finance	East-115
1046	u429v921w138	daquino	Finance	West-280
1047	v109w587x644	cward	Finance	West-373
1048	w167x592y375	tmitchel	Finance	South-288
1049	NULL	jreckley	Finance	Central-295
1050	y132z930a114	csimmons	Finance	North-468
1057	f370g535h632	mscott	Sales	South-270
1062	k367l639m697	redwards	Finance	North-180
1063	l686m140n569	lpope	Sales	East-226
1066	o678p794q957	ttyrell	Sales	Central-444
1069	NULL	jpark	Finance	East-110
1071	t244u829v723	zdutchma	Sales	West-348
1072	u905v920w694	esmith	Sales	East-421

Now, your team needs to perform a different update to the computers of all employees in the Finance or the Sales department, and you need to locate information on these employees.

• Write a SQL query to retrieve records for employees in the 'Finance' or the 'Sales' department.

Note: Even though both conditions are based on the same column, you need to write out both full conditions. This means that you must specify `department` as the column in both conditions.

What is the username of the first employee in the Sales department returned by the query?

☒ Irodriqu

☐ tbarnes

☐ bisles

☒ sgilmore

Submit

Retrieve all employees not in IT

Now we need to look at providing security updates for every employee not in the IT department. Let's use the NOT operator again.

The screenshot shows a Google Chrome browser window with a SQL query result and a task interface. The query is: `SELECT * FROM employees WHERE NOT department = 'Information Technology';` The result is a table with 5 columns: `employee_id`, `device_id`, `username`, `department`, and `office`. The table contains 41 rows of data, including employees from Marketing, Human Resources, Finance, Sales, and Information Technology. The task interface on the right is titled "Task 6. Retrieve all employees not in IT" and asks: "How many employees are not in the Information Technology department?". The options are 170, 122, 161, and 188. The correct answer, 161, is selected and marked with a green checkmark. A "Submit" button is at the bottom.

employee_id	device_id	username	department	office
1000	a320b137c219	elarson	Marketing	East-170
1001	b239c825d303	bmoreno	Marketing	Central-276
1002	c116d593e558	tshah	Human Resources	North-434
1003	d394e816f943	agilmore	Finance	South-153
1004	e218f877g788	eraab	Human Resources	South-127
1005	f551g340h864	gesparza	Human Resources	South-366
1007	h174i497j413	wjaffrey	Finance	North-406
1008	i858j583k571	abernard	Finance	South-170
1009	NULL	lrodrigu	Sales	South-134
1010	k242l212m542	jlansky	Finance	South-109
1011	l748m120n401	drosas	Sales	South-292
1015	p611q262r945	jaoto	Finance	North-271
1016	q793r736s288	sbaelish	Human Resources	North-229
1017	r550a824t230	jclark	Finance	North-188
1018	s310t540u653	abellmas	Finance	North-403
1020	u899v381w363	arutley	Marketing	South-351
1022	w237x430y567	arusso	Finance	West-465
1024	y976z753a267	iuduike	Sales	South-215
1025	z381a365b233	jhill	Sales	North-115
1026	a998b568c863	apatel	Human Resources	West-320
1027	b806c503d354	mrah	Marketing	West-246
1028	c603d749e374	aestrada	Human Resources	West-121
1029	d336e475f676	ivelasco	Finance	East-156
1030	e391f189g913	mabadi	Marketing	West-375
1031	f419g188h578	dkot	Marketing	West-408
1034	i679j565k940	beand	Human Resources	East-484
1035	j236k303l245	bisles	Sales	South-171
1036	k550l533m205	rjensen	Marketing	Central-239
1038	m873n636o225	btang	Human Resources	Central-260
1039	n253o917p623	cjackson	Sales	East-378
1040	o783p832q294	dtarly	Human Resources	East-237
1041	p929q222r778	cgriffin	Sales	North-208

Summary

So now I can say I have practical experience using SQL to run queries to retrieve information from a database. Along with using filters using the AND, OR, and NOT operator to curate the data.