VIT®
Vellore Institute of Technology
(Deemed to be University under section 3 of UGC Act, 1956)

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/1xW6NN98PgrkBSKV88NQAW7DfTDDsvwom/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.

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 pag

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.

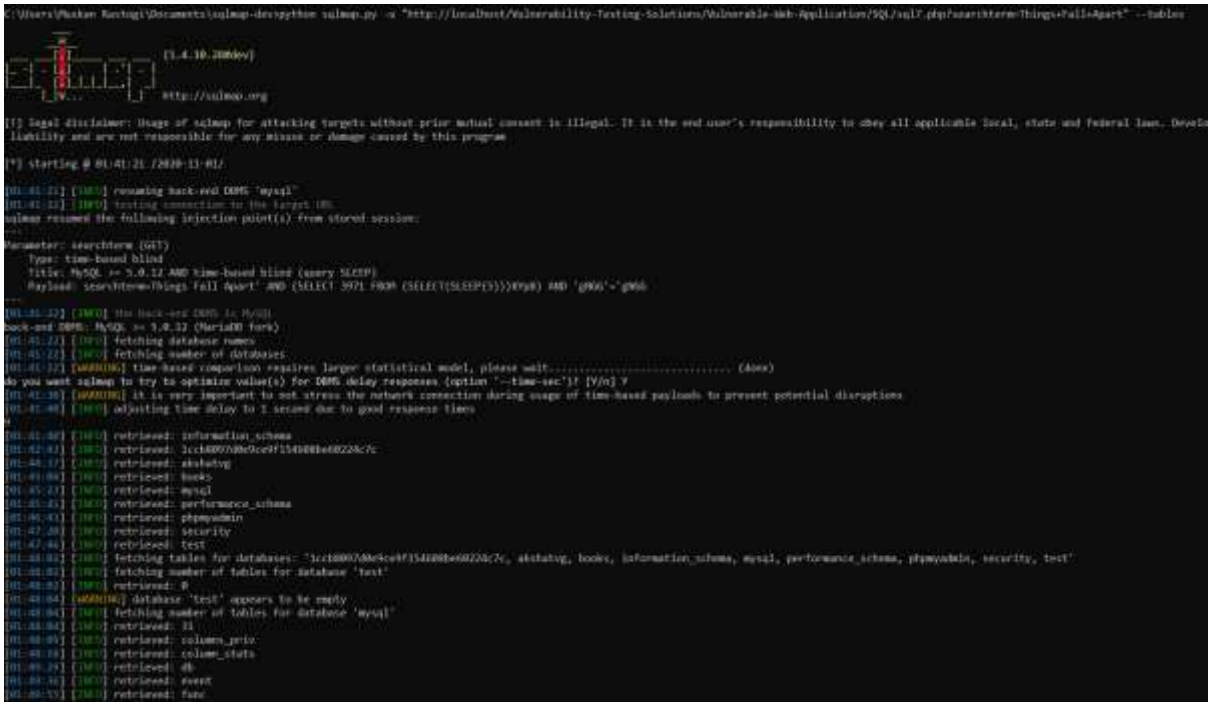
Step 6: Scan regularly

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.

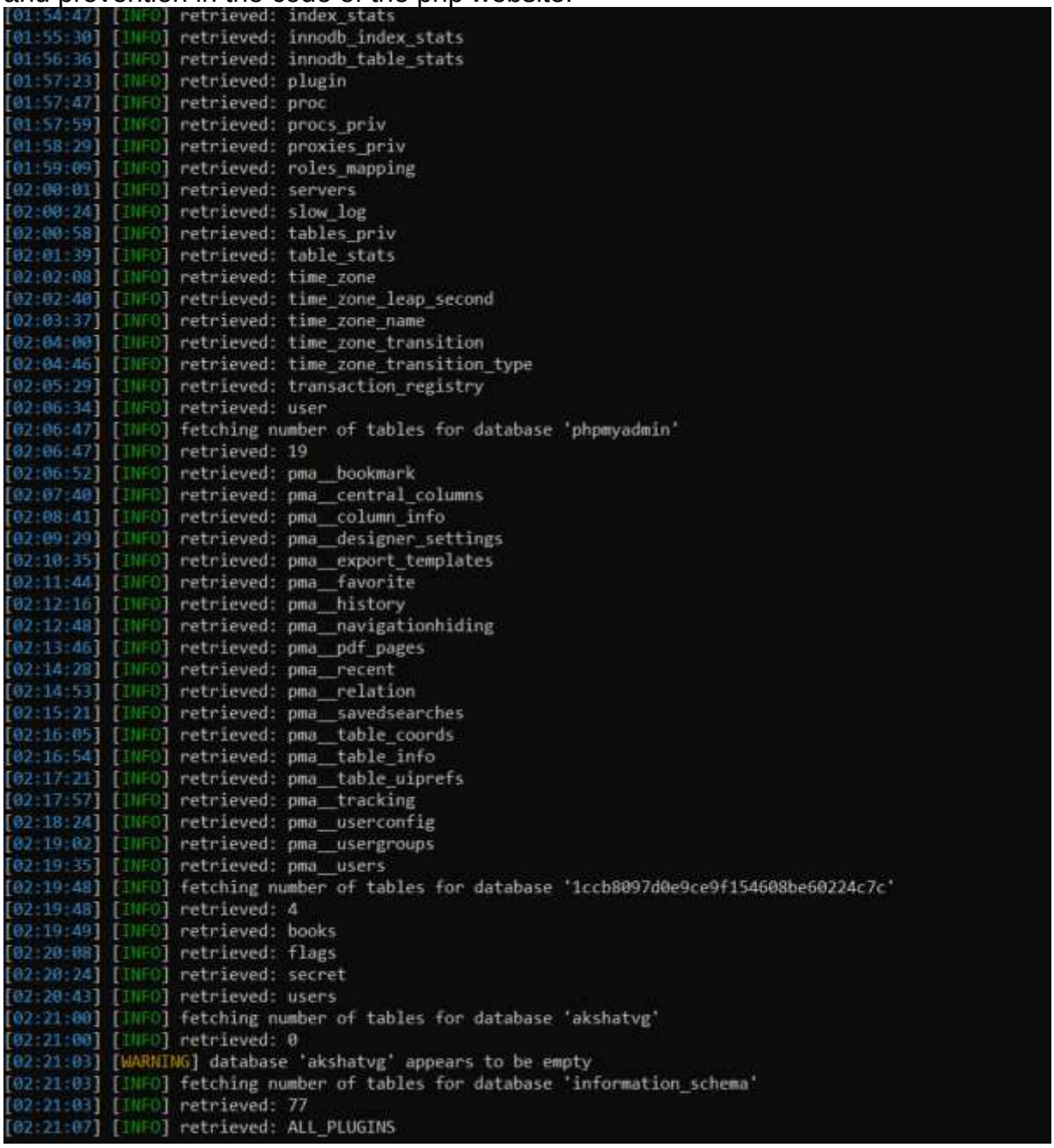
REFERENCES:

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
3. https://ieeexplore.ieee.org/document/7492650

IMPLEMENTATION OF SQL ATTACK ACCESSING THE WHOLE DATABASE AND PREVENTION.



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.



```
[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
```

Command Prompt

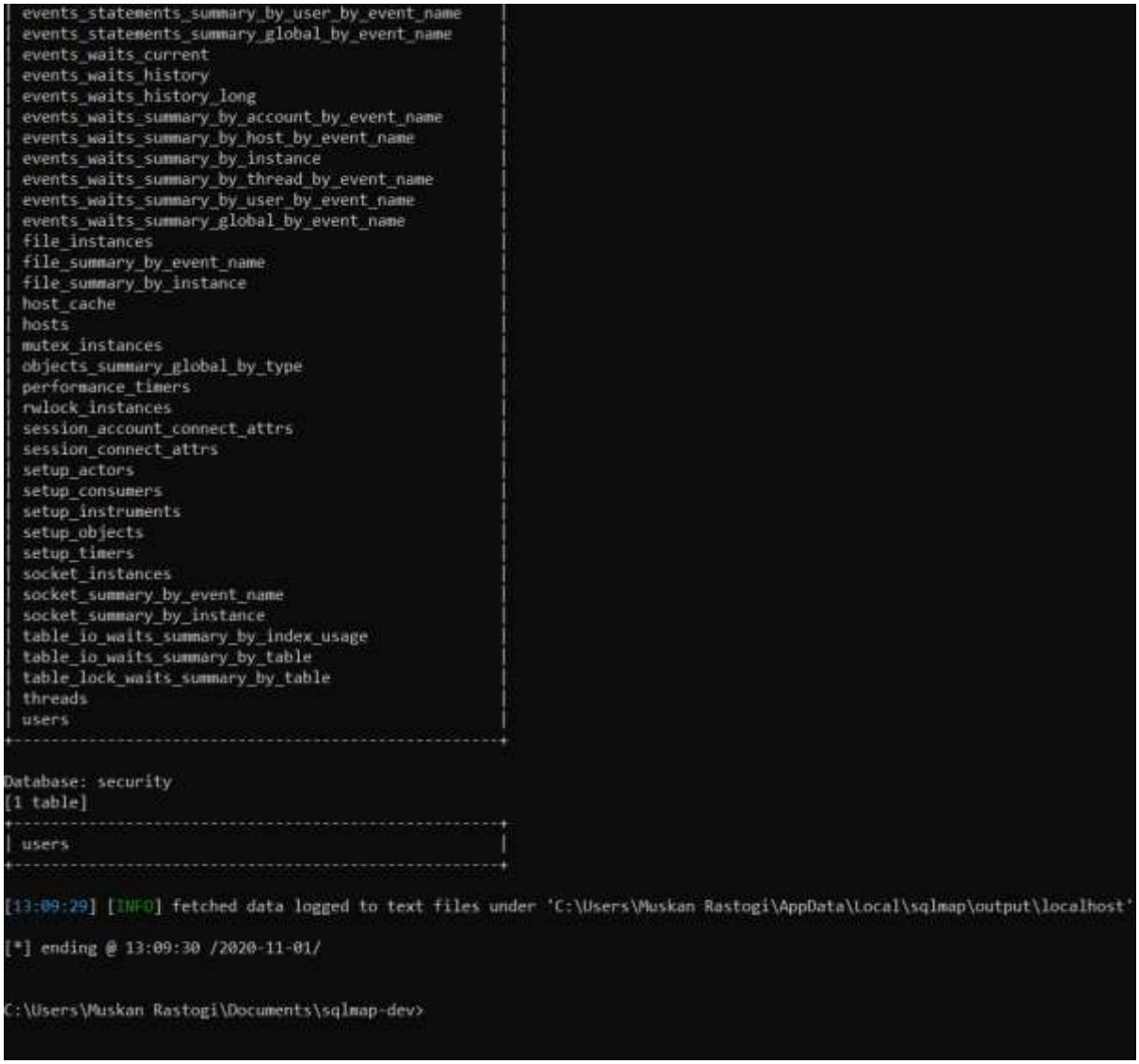
```
[03:02:25] [INFO] retrieved: INNODB_CMP_PER_INDEX_RESET
[03:03:44] [INFO] retrieved: user_variables
[03:04:30] [INFO] retrieved: INNODB_FT_INDEX_CACHE
[03:05:46] [INFO] retrieved: INNODB_SYS_FOREIGN_COLS
[03:06:52] [INFO] retrieved: INNODB_FT_BEING_DELETED
[03:07:55] [INFO] retrieved: INNODB_BUFFER_POOL_STATS
[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             |
```



PREVENTION:

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

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

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

            $books = mysqli_query($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>
```