SQLReinjector
Automated Exfiltrated Data Identification

Jason A. Novak
Assistant Director, Digital Forensics
Chicago, IL

Andrea London
Digital Forensic Examiner
Dallas, TX
Problem

Hi, this is your son's school. We're having some computer trouble.

Oh, dear — did he break something? In a way—

DID YOU REALLY NAME YOUR SON Robert'); DROP TABLE Students;-- ?

Oh, yes. Little Bobby Tables, we call him.

Well, we've lost this year's student records. I hope you're happy.

And I hope you've learned to sanitize your database inputs.

sqlmap
Automatic SQL injection and database takeover tool
Problem

- 97% of data breach cases worldwide involve SQL injection attacks somewhere down the line.

- On average the cost of data breach response and remediation is between $194 - $222 per record.

- As of July 9th, privacyrights.org cites 330 breaches in 2012 effecting 18.6 million records.
  (datalossdb.org reports much higher at 723 breaches thus far)
Problem

Historical response is costly

Fly a bunch of consultants to a data center

They image the server

Analyze the logs

Determine what was exfiltrated from reviewing those logs.

Typically running SQL commands against SQL server

Only going to get costlier
Problem
SQLReInjector
Replay an SQL injection attack from logs

optional arguments:
- -h, --help          show this help message and exit
- -i INLOG, --inLog INLOG
  Input appache log file parse
- -d DBFILE, --dbFile DBFILE
  Database log file to write out to
- -w WEBSITE, --website WEBSITE
  Website to run against. Form of http://hostname
- -j, --havijParser   Parse the returned data to reassemble Haviij output
- -c, --compareToGood Compare the returned data to a known good webpage to further automate identification of SQLi returned data
- -k KNOWNGOOD, --knownGood KNOWNGOOD
  Known good webpage to compare to
- -e COOKIE, --cookie COOKIE
  cookie
Demo Time
Where to Get It

github.com/strozfriedberg
QUESTIONS?
Bibliography and Thanks

- Exploits of a Mom / Little Bobby Tables by Randall Munroe
  - http://xkcd.com/327/
- sqlmap by Bernardo Damele A.G. and Miroslav Stampar
  - http://sqlmap.org/
- DVWA by RandomStorm
  - http://www.dvwa.co.uk/
- Apache Log Parsing
  - apachelog Python Module, http://code.google.com/p/apachelog/, hfuecks@gmail.com;
  - Apache-LogRegex Module, search.cpan.org/dist/Apache-LogRegex/, Peter Hickman;
- Virtualization of Forensic Images
- Replaying SQL Injection Attacks
  - Bret Padres, http://cyberspeak.libsyn.com
- Injection Attack and Data Theft Statistics
- Thanks to:
  - Erin Nealy Cox
  - Cheri Carr
  - Scott Brown
Who We Are

Over 270 employees in 11 U.S. and 1 U.K. Offices

San Francisco
Los Angeles
Dallas
Minneapolis
Chicago
Washington, D.C.
New York
L.I.
Boston
Purchase
London
Seattle
Who We Are

Jason A. Novak
Assistant Director, Digital Forensics
Chicago, IL
jnovak@strozfriedberg.com

Andrea London
Digital Forensic Examiner
Dallas, TX
alondon@strozfriedberg.com

www.StrozFriedberg.com