White-hat Google-Hacking MySQL

Slides:
http://bit.ly/ghackmysql

Sheeri Cabral

Senior DB Admin/Architect, Mozilla
@sheeri www.sheeri.com

What is White-Hat Google Hacking?

Hacking

Using Google

White-hat

Where to Start

Do some searching

http://johnny.ihackstuff.com/ghdb

Security Advisories

App and Web servers

Applications

Companies

Google's TOS

Under 18?

No automation

What's not in the TOS

https://www.google.com/accounts/TOS

- past versions

Password Hashes

Hash Dictionaries like http://hashash.in/

Password hash is
*13824B0ECE00B527531D2C716AD36C23AC11A30B

What is the password in plaintext?

How to Use Google

wildcards * .

Different media types

Boolean search

Google Basics

10 word limit

AND assumed

foo | bar

Operators

http://www.google.com/help/operators.html

Site matters

filetype: vs inurl:

Google Dork

site:www.sheeri.com inurl:?id=1..100000

Vulnerable Locations

Common paths

Open source = double-edged sword

Some To Try

inurl:config.php

inurl:php?

inurl:delete

inurl:delete.php?id=

link:private.yourcompany.com

numrange:

More To Try

site:sheeri.com filetype:php inurl:id

- Then test out injection

http://*:*@www.sheeri.com

intitle:Remote.Desktop.Web.Connection site:sheeri.com

Further study

http://bit.ly/ghacks0

http://bit.ly/ghacks1

www.securityvulns.com

Defensive Strategies

Validate/scrub input

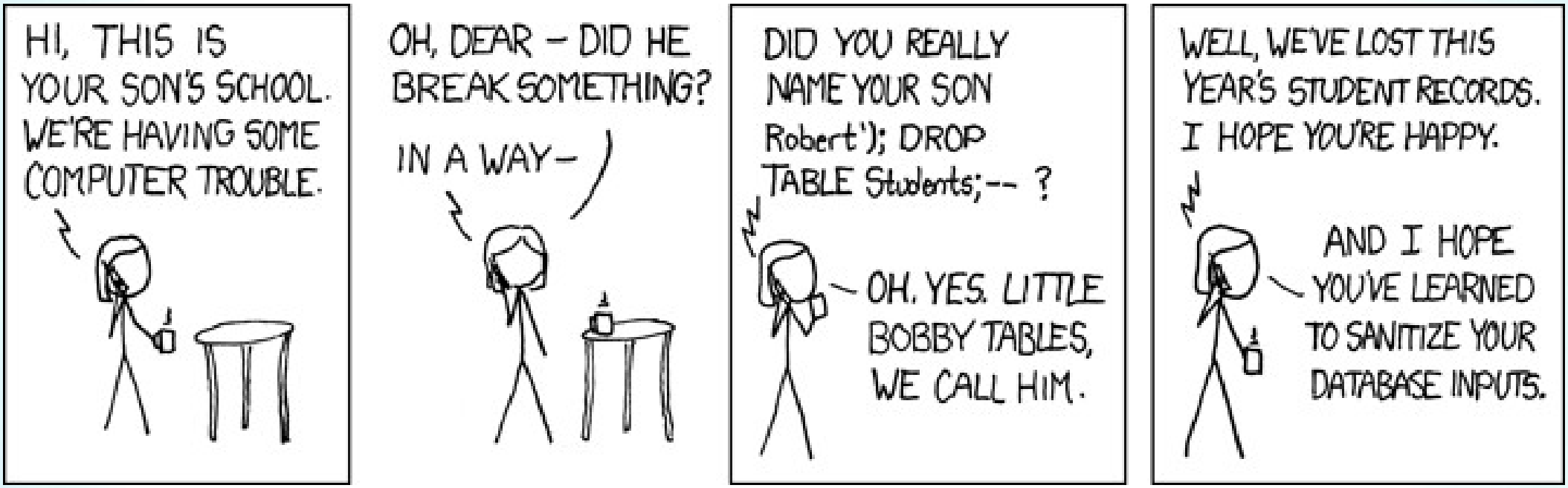
CSRF – Validate source

XSS

SQL Injection Cheat Sheet

- http://bit.ly/sqlinjcheat

SQL Injection



SQL Injection

- http://bit.ly/explainsqlinj

```
SELECT count(*) FROM users WHERE
  username='$user' and pass='$pass';

-- if count(*)>0, log in!
```

SQL Injection

- http://bit.ly/explainsqlinj

```
SELECT count(*) FROM users WHERE
  username='$user' and pass='$pass';

-- if count(*)>0, log in!
```

- Pass: hi' or 1=1

```
SELECT count(*) FROM users WHERE
  username='foo' and pass='hi' or 1=1';
```

Validate User Input

- Look for ; \g \G ' “ UNION
- HTML encoding
- NULL or char(0)
- VARCHAR and ' '

Validate User Input

- Save yourself time
- Buffer overflows
- CHARSET

Trusting GET or POST

- Only from certain pages
- cookies – even with valid session ids
- register_globals=off in PHP

When, Not If

How is application DB access stored?

As strong as your weakest link

No vaccine

Regression Testing Tools

http://sites.google.com/site/murfie/

- goolink
- crapscan
- goohosts

More Actions

Google Hacking Software

- http://code.google.com/p/googlehacks/

Google Hacks Honey Pot

- http://ghh.sourceforge.net/

Google honors robots.txt

Vulnerability Checking Tools

Goolag.org – GUI – old, but open source

Wikto/Nikto

Mozilla is Hiring!

http://careers.mozilla.org/

DBA – MySQL, Postgres, NoSQL (some or all)

http://careers.mozilla.org/en-US/position/oTqLWfwK

SysAdmin – RHEL, CentOS, Fedora

http://careers.mozilla.org/en-US/position/o97xWfwt

US, Canada, UK, France, Spain, Germany, Netherlands,

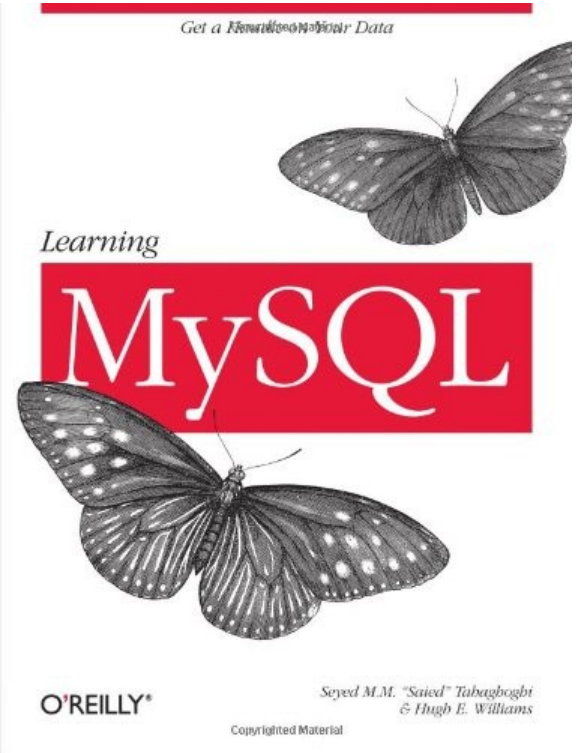
Sweden, Denmark, Poland, China, Japan, New Zealand

In Mountain View, **Senior Windows/Unix SysAdmin**

http://careers.mozilla.org/en-US/position/oZmJWfwK

Want to Learn MySQL?

12 weeks, 1 book. MySQL Marinate!



Soak it in! www.mysqlmarinate.com

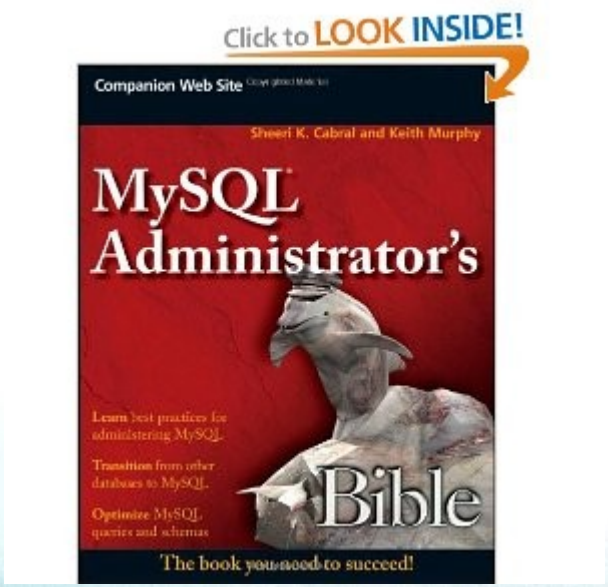
Questions? Comments?

OurSQL podcast

- www.oursql.com

MySQL Administrator's Bible

- tinyurl.com/mysqlbible



bit.ly/ghackmysql

kimtag.com/mysql

planet.mysql.com