

Database Security Using White-Hat Google Hacking

Sheeri K. Cabral
Database Administrator
The Pythian Group, www.pythian.com

cabral@pythian.com
2008 MySQL User Conference & Expo



What is White-Hat Google Hacking?

- Hacking
- Using Google
- White-hat

Where to Start

- Do some searching
- <http://johnny.ihackstuff.com/ghdb.php>
- i-hacked.com/content/view/23/42
- For the truly impatient.....

Google's TOS

- Under 18?
- No automation
- What's not in the TOS

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>
[/cheatsheet.html](http://www.google.com/help/operators.html/cheatsheet.html)
- Site matters
- filetype: vs inurl:

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



We're sorry...

... but your query looks similar to automated requests from a computer virus or spyware application. To protect our users, we can't process your request right now.

We'll restore your access as quickly as possible, so try again soon. In the meantime, if you suspect that your computer or network has been infected, you might want to run a [virus checker](#) or [spyware remover](#) to make sure that your systems are free of viruses and other spurious software.

If you're continually receiving this error, you may be able to resolve the problem by deleting your Google cookie and revisiting Google. For browser-specific instructions, please consult your browser's online support center.

If your entire network is affected, more information is available in the [Google Web Search Help Center](#).

We apologize for the inconvenience, and hope we'll see you again on Google.

Security Advisories

- App and Web servers
- Applications
- Companies

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:

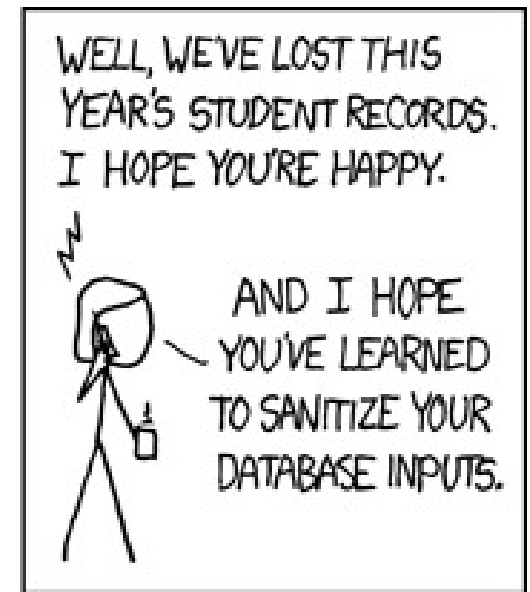
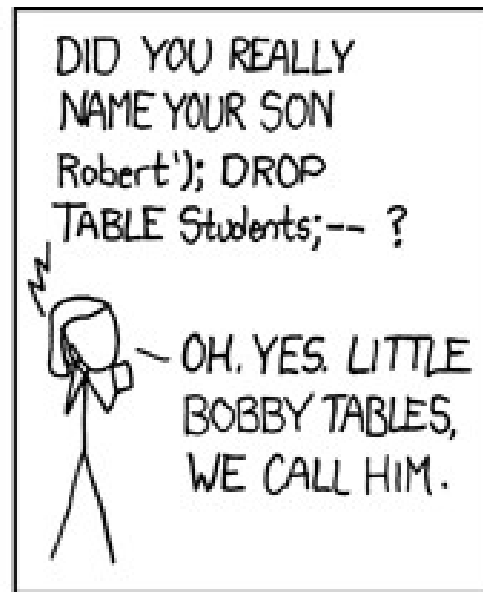
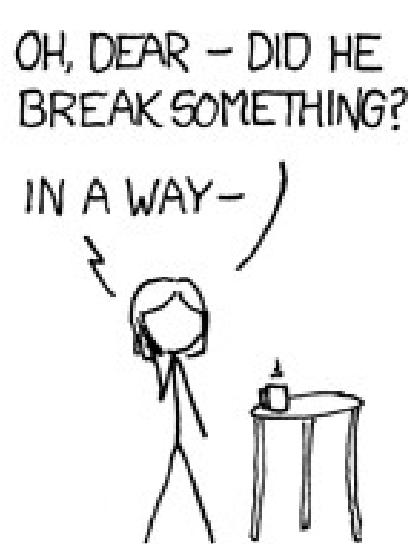
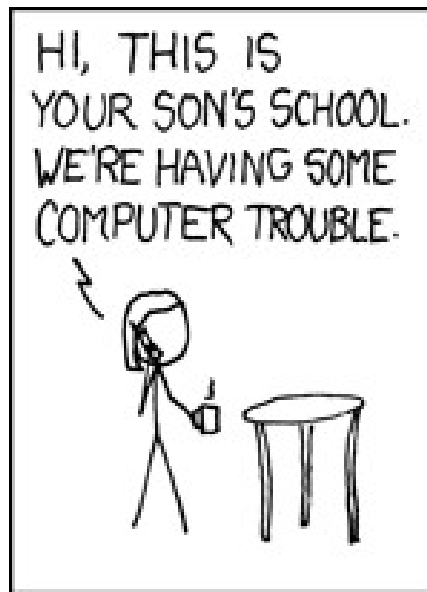
More To Try

- Page 35 of <http://www.sdissa.org/downloads/San%20Diego%20ISSA%20Google%20Hacking%20and%20Beyond%20May%202006-rhd.pdf>
- http://pauldotcom.com/wiki/index.php/Episode81#Tech_Segment:_Google_Queries_To_Run_Against_Your_Own_Domain

Defensive Strategies

- Validate/scrub input
- CSRF – Validate source
- XSS

XSS Example



When, Not If

- How is application DB access stored?
- As strong as your weakest link
- No vaccine

Regression Testing Tools

- <http://murfie.googlepages.com/>
 - 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
- Wikto/Nikto

Sheeri Cabral

cabral@pythian.com

www.sheeri.com

