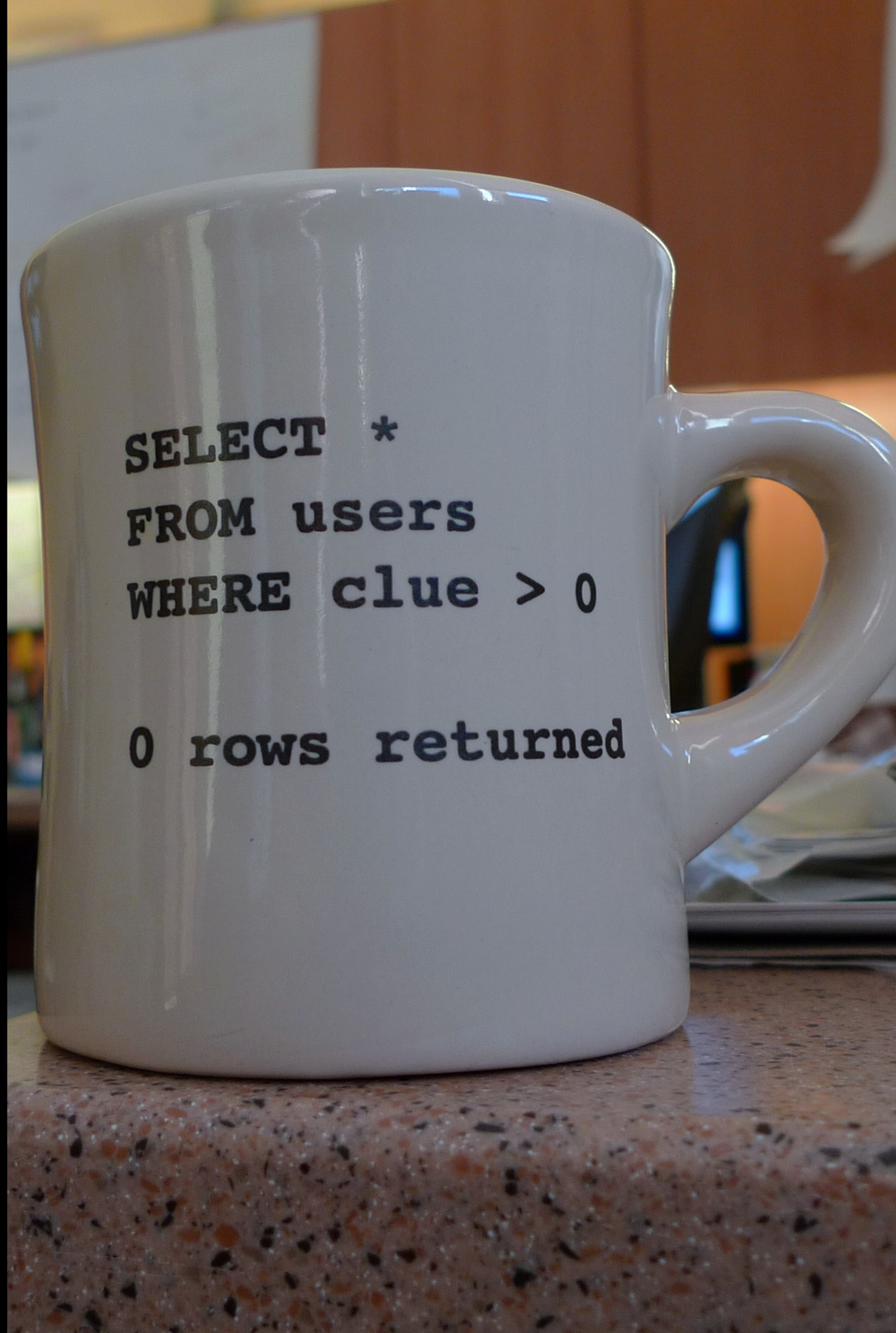
RICHARD JAMES THOMAS

HACKING WEBSITES:

AN INTRODUCTION TO SQLCIA, XSS AND THE OWASP TOP 10

CONTENTS

- What is a Web Attack?
- Common forms of attack:
  - SQL Command Injection Attacks (SQLCIA)
  - XSS/CSRF
  - OWASP Top 10



SOME WEBSITES AREN'T GREAT (SECURITY-WISE)

A FEW WEBSITES THAT HAD SOME EXPLOIT ATTACKED BETWEEN 2014-15

Slimstat

ASHLEY MADISON®
Life is short. Have an affair.®

SONY PICTURES

OTHERS ARE MORE HARDY TO THE OBVIOUS ATTACKS, BUT NOT TO THE SOPHISTICATED ONES

FINGERPRINTING

- Fingerprinting a server tells you what it's running, e.g. if a page has a call to phpinfo(), which tells you a lot about the underlying server.
- Trying some unexpected query strings might raise exceptions on the server, which might give you application versions, so you can search for known exploits
- Look at the 404 pages and Headers given to you in the response

SQL INJECTION ATTACKS

- Tautology Attacks
  - Use logical expressions to always evaluate something to true, for example password checks
    - ' OR '1'=='1'
- Incorrect Query Attacks
  - These try and 'fingerprint' the database to see what happens
    - convert(int, (SELECT TOP 1 username FROM users where …))
- Piggy-back statements
  - Adds something to the end of an SQL query
    - ; DROP TABLE users --
- (Non-exhaustive list!)

- For more, see: http://www.cc.gatech.edu/~orso/papers/halfond.viegas.orso.ISSSE06.pdf
- Solutions to these are readily available (sanitising Strings, Prepared Statements …)

XSS ATTACKS

- ‘Cross-Site Scripting’
- Can easily be performed by hijacking a vulnerable comments pages, or anything that allows user-malleable text to be entered
- Allows the attacker to inject some client-side code (Javascript) that will execute when the page is rendered
  - These could connect to another website, be used to steal cookies (to allow you to impersonate the victim)
  - Also could be used to redirect you to a phishing page, which looks legitimate, but will steal your credentials
  - Drive-by-downloads: the victim downloads some malicious code, which executes, which can install malware through an unknown zero-day

- Tom has some good examples at http://www.cs.bham.ac.uk/internal/courses/comp-sec/2014/

The OWASP Top 10

YOUR GUIDANCE FOR SECURING SITES

RICHARD JAMES THOMAS

HACKING WEBSITES:

AN INTRODUCTION TO SQLCIA, XSS AND THE OWASP TOP 10

Additional links:

Healthcare.gov SQLCIA attempts:
https://sitesdoneright.com/blog/2013/11/sql-injection-hacking-on-healthcare-gov

Paper covering the types of SQLCIA attacks around:
http://www.cc.gatech.edu/~orso/papers/halfond.viegas.orso.ISSSE06.pdf

Tom's lectures (XSS attacks):
www.cs.bham.ac.uk/internal/courses/comp-sec/2014/