WORKSHOP PT2:
A SamuraiWTF intro to the
Zed Attack Proxy

Moderated by Robert Richardson, Editorial Director

November 8, 2011

Presented by

QUALYS®
WORKSHOP: A SamuraiWTF intro to the Zed Attack Proxy

SPONSOR PRESENTER:

MIKE SHEMA, DIRECTOR OF ENGINEERING FOR THE QUALYS WEB APPLICATION SCANNING SERVICE

GUEST PRESENTER:

JUSTIN SEARLE, MANAGING PARTNER, UTILLISEC

TO DOWNLOAD SAMURAI-WTF, GO TO WWW.SAMURAI-WTF.ORG

Presented by
Web App Security Testing

Tools for automation & manual analysis

Mike Shema, Director of Engineering
November 8, 2011
The Problem

Slow Evolution

• Design patterns have changed, but the technology hasn’t (much)
  - HTML 4.01 finalized December 24, 1999

• Every web programming language supports prepared statements or parameterized queries
  - …and we still see SQL injection.

• Today’s tools have decade-old ancestors in whisker, Nikto, SPIKE proxy, etc.
Complement Rather Than Compete

• Well-established vulnerability testing techniques
  – Clear methodologies are ideal for automation.

• Identifying weaknesses in design vs. weaknesses in implementation.

• Struggling to reach security at scale.
Finally a new spec with new features – with new attack vectors.

Security improvements via design
  – But we’ll always have XSS.

Techniques must adapt towards asynchronous DOM updates, JSON messages, complex JavaScript.
Thank You

Mike Shema
mshema@qualys.com
http://www.qualys.com/products/qg_suite/was/
• **To join the Black Hat mailing list, email BH List to:**
  feedback@blackhat.com

• **To join our LinkedIn Group:**
  http://www.linkedin.com/groups?gid=37658&trk=hb_side_g

• **To follow Black Hat on Twitter:**
  https://twitter.com/Blackhatevents

• **Black Hat’s Facebook Fan Page:**
  http://www.facebook.com/blackhat

• **Find out more at** http://www.blackhat.com

• **For more information, visit**
  www.qualys.com