# OWASP WebScarab NG

Rogan Dawes, WebScarab Project Lead
Senior Application Security Engineer
Aspect Security
rogan@dawes.za.net

FOSDEM
2008

The OWASP Foundation
http://www.owasp.org/

# What is OWASP?

- < OWASP – Open Web Application Security Project
  - 4 Non-Profit Foundation started in 2000
  - 4 Professionals and security experts from around the world
  - 4 Contributing their time because this problem is so important
  - 4 Commercial quality tools and documentation
- < Top Ten Most Critical Web Application Security Vulnerabilities
  - 4 Adopted by PCI and the FTC as ‘the’ standard for application security

> *"This ‘Ten-Most-Wanting’ List acutely scratches at the tip of an enormous iceberg. The underlying reality is shameful: most system and Web application software is written oblivious to security principles, software engineering, operational implications, and indeed common sense."*
>
> *Dr. Peter G. Neumann, Principal Scientist, SRI International Computer Science Lab, Moderator of the ACM Risks Forum, Author of "Computer-Related Risks"*

# OWASP Top Ten

- Awareness document for developers

  4 Unvalidated Parameters

  4 Broken Access Control

  4 Broken Account and Session Management

  4 Cross Site Scripting Flaws

  4 Buffer Overflows

  4 Command Injection Flaws

  4 Error Handling Problems

  4 Insecure Use of Cryptography

  4 Application Denial of Service

  4 Web/Application Server Misconfigurations

# OWASP Guide

- Complete details in
  - The OWASP Guide for Building Secure Web Applications and Web Services

OWASP

The Open Web Application Security Project

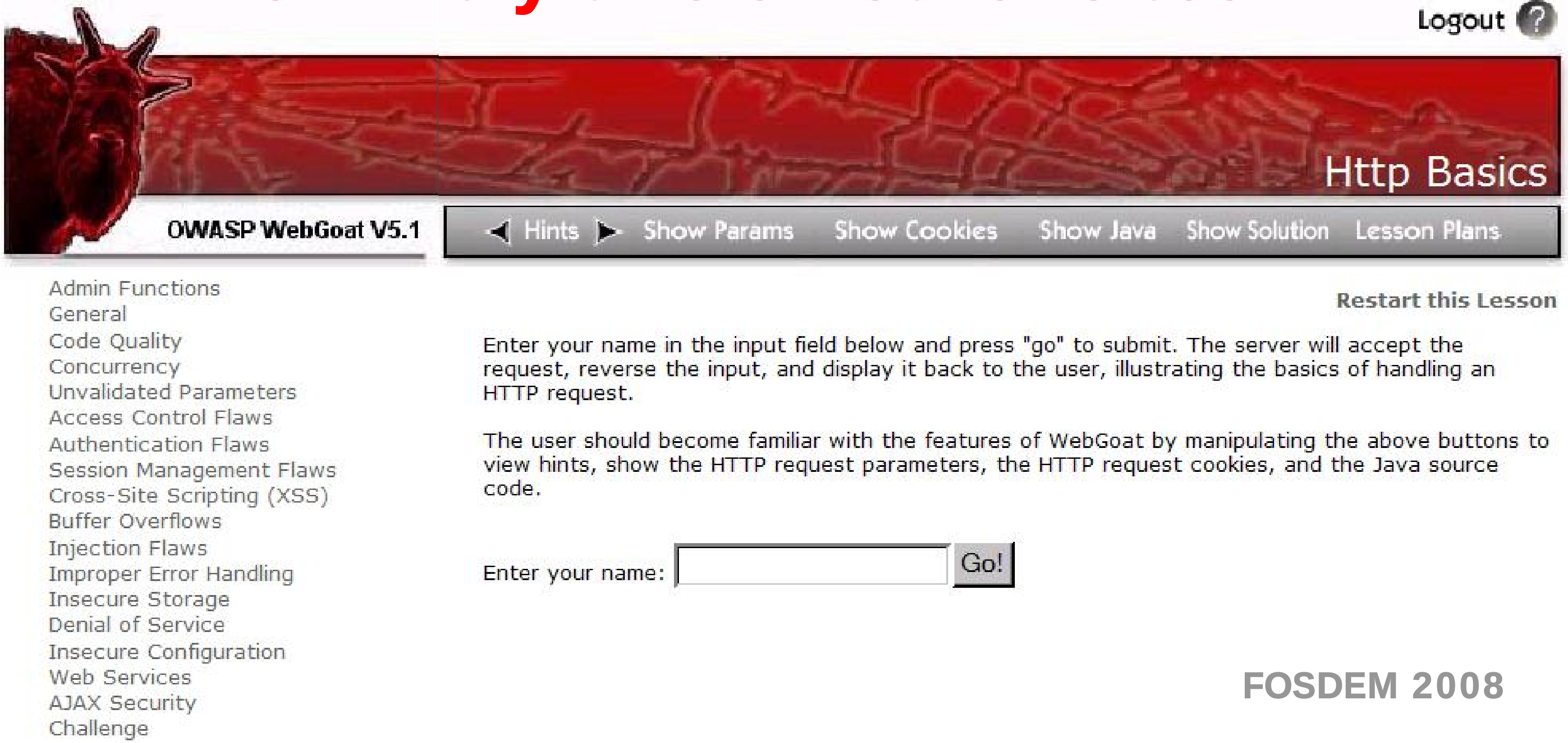
http://www.owasp.org

# OWASP WebGoat

< A deliberately vulnerable Web Application

< A “safe” environment for learning about vulnerabilities – exploits and fixes

< **DON’T try this on other sites!!!**



Enter your name in the input field below and press "go" to submit. The server will accept the request, reverse the input, and display it back to the user, illustrating the basics of handling an HTTP request.

The user should become familiar with the features of WebGoat by manipulating the above buttons to view hints, show the HTTP request parameters, the HTTP request cookies, and the Java source code.

Enter your name:

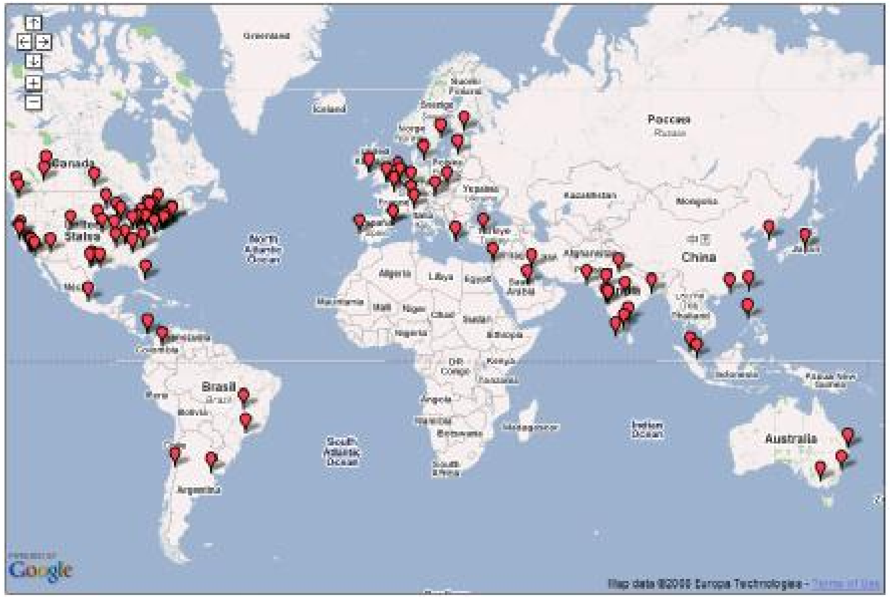
# OWASP Local Chapters

< Encourage local discussion of application security around the world

< Free and open to anyone

< Meet monthly or quarterly

< Presentations and discussion of key application security topics



# OWASP Conferences

< Historically 2 annually

  4 USA (New York 2004, Washington 2005, Seattle 2006, San Jose 2007)

  4 Europe (London 2005, Brussels 2006, Milan 2007)

< 3 this year

  4 Australia (next week)

  4 Brussels (May)

  4 New York (October)

# OWASP <Season> of Code

< Modeled on Google’s “Summer of Code”

< Encourages existing (and new) participants to work on OWASP projects

< So far, “Autumn of Code”, “Spring of Code”

< Examples:

  4 OWASP Testing Guide

  4 OWASP Anti-Samy project

  4 OWASP WebGoat Solutions guide

< More than $100,000 paid out

# So what’s the problem again?

< Many organizations simply trust their developers to produce secure code – if they’ve even thought about it

< In many cases, that trust is misplaced!

    4 Search engines are part of the problem **J**

< Lack of awareness of the problem is part of the problem!

# How can we fix it?

< Education

4 Documentation

4 Training (WebGoat)

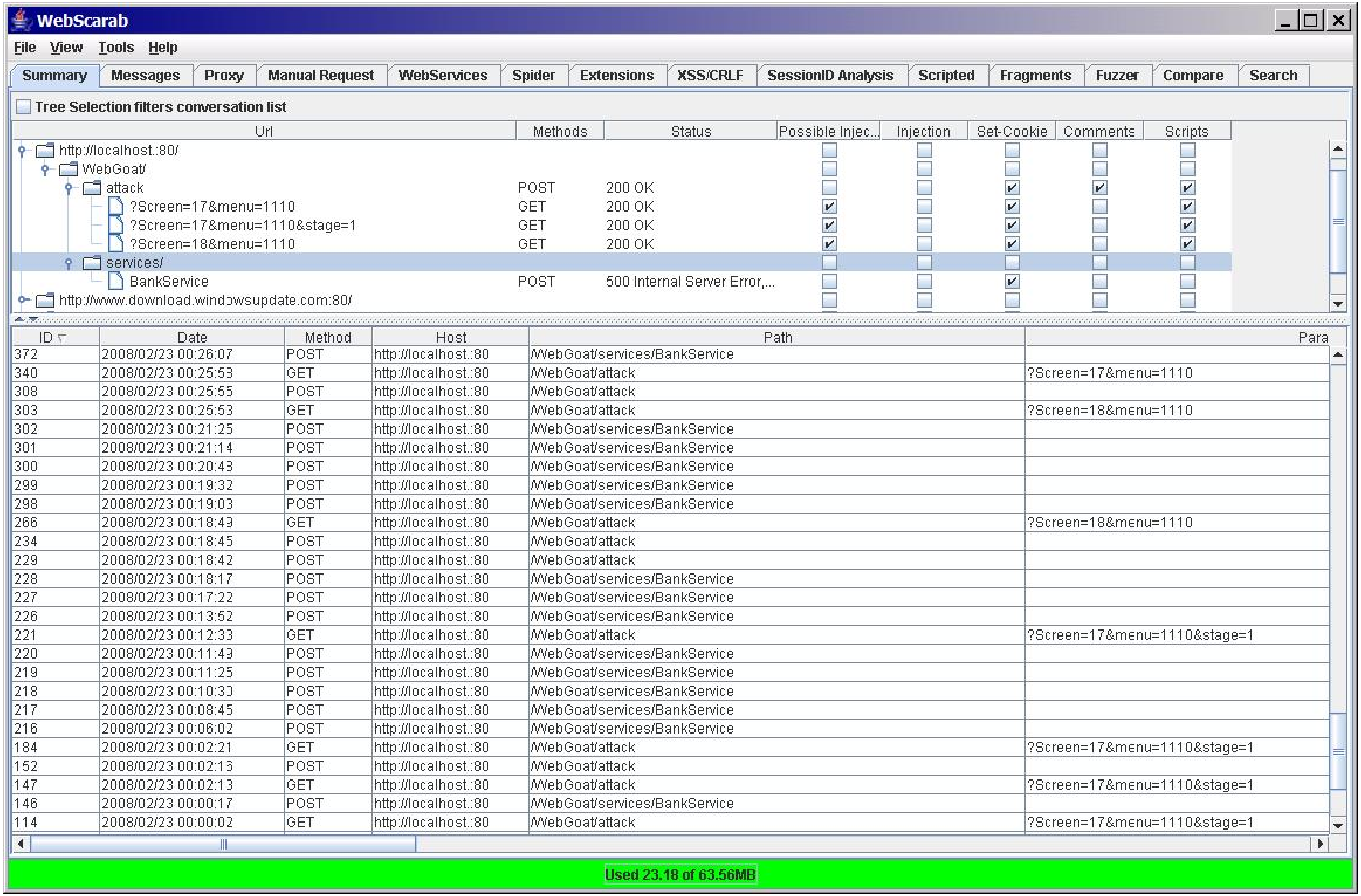
< Code review

< Pen testing

4 This is where WebScarab (-NG) comes in

# OWASP WebScarab

- One of the flagship OWASP tools
- Written in Java (my first Java program **J**)
- Started in 2003
- Key features
  - Direct access to the underlying HTTP protocol
  - Intercepting proxy (including SSL)
  - Session history
  - Spider, Fuzzer, WebServices, Scripting (BSF)
- Drawbacks
  - Clunky! (What did *I* know about HIG?)
  - Memory leaks



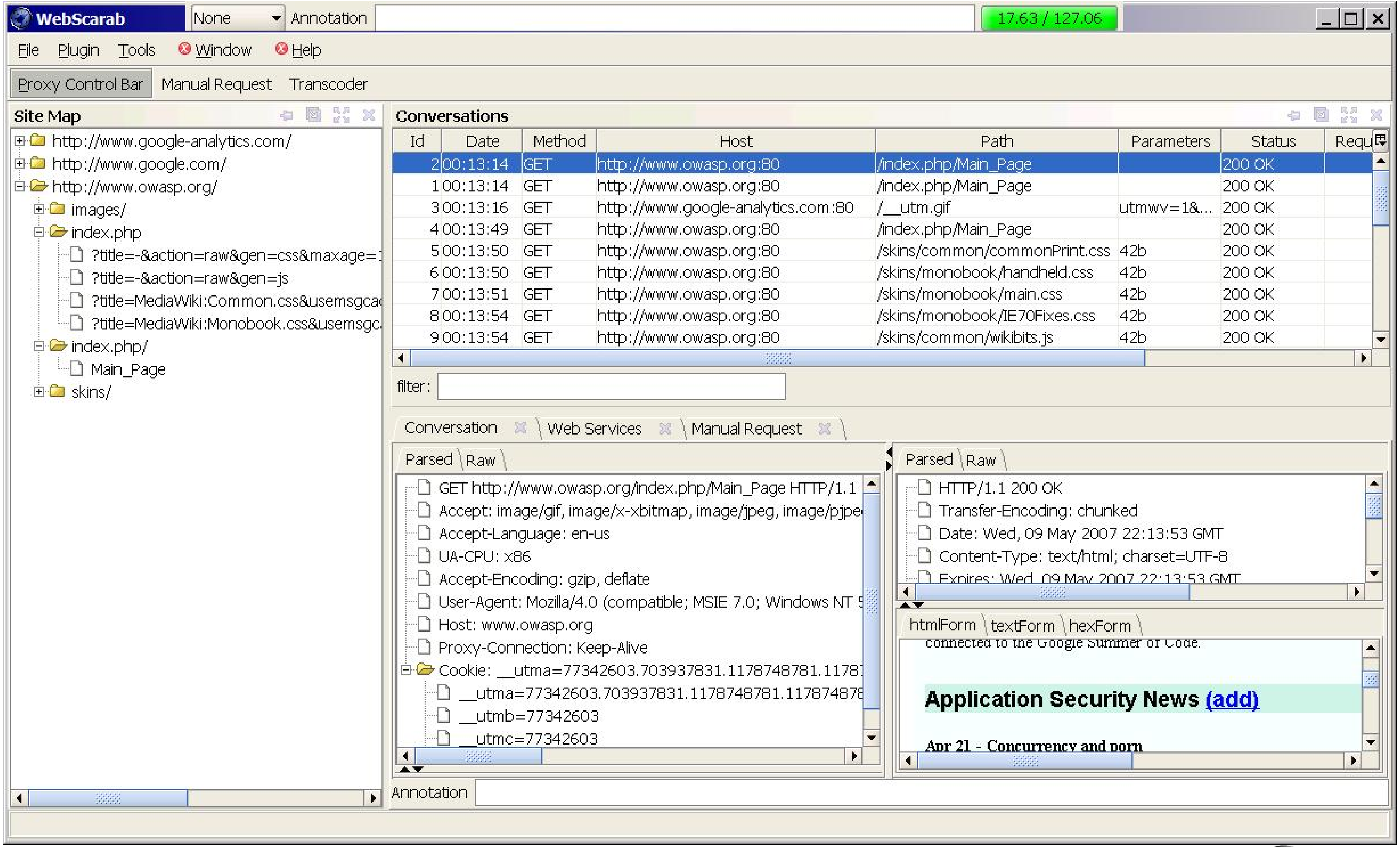
☐ Tree Selection filters conversation list

| Url | Methods | Status | Possible Injec... | Injection | Set-Cookie | Comments | Scripts |
|---|---|---|---|---|---|---|---|
| http://localhost:80/ | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| WebGoat/ | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| attack | POST | 200 OK | ☐ | ☐ | ☑ | ☑ | ☑ |
| ?Screen=17&menu=1110 | GET | 200 OK | ☑ | ☐ | ☑ | ☐ | ☑ |
| ?Screen=17&menu=1110&stage=1 | GET | 200 OK | ☑ | ☐ | ☑ | ☐ | ☑ |
| ?Screen=18&menu=1110 | GET | 200 OK | ☑ | ☐ | ☑ | ☐ | ☑ |
| services/ | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| BankService | POST | 500 Internal Server Error,... | ☐ | ☐ | ☑ | ☐ | ☐ |
| http://www.download.windowsupdate.com:80/ | | | ☐ | ☐ | ☐ | ☐ | ☐ |

| ID | Date | Method | Host | Path | Para |
|---|---|---|---|---|---|
| 372 | 2008/02/23 00:26:07 | POST | http://localhost:80 | /WebGoat/services/BankService | |
| 340 | 2008/02/23 00:25:58 | GET | http://localhost:80 | /WebGoat/attack | ?Screen=17&menu=1110 |
| 308 | 2008/02/23 00:25:55 | POST | http://localhost:80 | /WebGoat/attack | |
| 303 | 2008/02/23 00:25:53 | GET | http://localhost:80 | /WebGoat/attack | ?Screen=18&menu=1110 |
| 302 | 2008/02/23 00:21:25 | POST | http://localhost:80 | /WebGoat/services/BankService | |
| 301 | 2008/02/23 00:21:14 | POST | http://localhost:80 | /WebGoat/services/BankService | |
| 300 | 2008/02/23 00:20:48 | POST | http://localhost:80 | /WebGoat/services/BankService | |
| 299 | 2008/02/23 00:19:32 | POST | http://localhost:80 | /WebGoat/services/BankService | |
| 298 | 2008/02/23 00:19:03 | POST | http://localhost:80 | /WebGoat/services/BankService | |
| 266 | 2008/02/23 00:18:49 | GET | http://localhost:80 | /WebGoat/attack | ?Screen=18&menu=1110 |
| 234 | 2008/02/23 00:18:45 | POST | http://localhost:80 | /WebGoat/attack | |
| 229 | 2008/02/23 00:18:42 | POST | http://localhost:80 | /WebGoat/attack | |
| 228 | 2008/02/23 00:18:17 | POST | http://localhost:80 | /WebGoat/services/BankService | |
| 227 | 2008/02/23 00:17:22 | POST | http://localhost:80 | /WebGoat/services/BankService | |
| 226 | 2008/02/23 00:13:52 | POST | http://localhost:80 | /WebGoat/services/BankService | |
| 221 | 2008/02/23 00:12:33 | GET | http://localhost:80 | /WebGoat/attack | ?Screen=17&menu=1110&stage=1 |
| 220 | 2008/02/23 00:11:49 | POST | http://localhost:80 | /WebGoat/services/BankService | |
| 219 | 2008/02/23 00:11:25 | POST | http://localhost:80 | /WebGoat/services/BankService | |
| 218 | 2008/02/23 00:10:30 | POST | http://localhost:80 | /WebGoat/services/BankService | |
| 217 | 2008/02/23 00:08:45 | POST | http://localhost:80 | /WebGoat/services/BankService | |
| 216 | 2008/02/23 00:06:02 | POST | http://localhost:80 | /WebGoat/services/BankService | |
| 184 | 2008/02/23 00:02:21 | GET | http://localhost:80 | /WebGoat/attack | ?Screen=17&menu=1110&stage=1 |
| 152 | 2008/02/23 00:02:16 | POST | http://localhost:80 | /WebGoat/attack | |
| 147 | 2008/02/23 00:02:13 | GET | http://localhost:80 | /WebGoat/attack | ?Screen=17&menu=1110&stage=1 |
| 146 | 2008/02/23 00:00:17 | POST | http://localhost:80 | /WebGoat/services/BankService | |
| 114 | 2008/02/23 00:00:02 | GET | http://localhost:80 | /WebGoat/attack | ?Screen=17&menu=1110&stage=1 |

Used 23.18 of 63.56MB

# Introducing WebScarab NG



Site Map

- http://www.google-analytics.com/
- http://www.google.com/
- http://www.owasp.org/
  - images/
  - index.php
    - ?title=-&action=raw&gen=css&maxage=1
    - ?title=-&action=raw&gen=js
    - ?title=MediaWiki:Common.css&usemsgcac
    - ?title=MediaWiki:Monobook.css&usemsgc
  - index.php/
    - Main_Page
  - skins/

Conversations

| Id | Date | Method | Host | Path | Parameters | Status | Requ |
|---|---|---|---|---|---|---|---|
| 2 | 00:13:14 | GET | http://www.owasp.org:80 | /index.php/Main_Page | | 200 OK | |
| 1 | 00:13:14 | GET | http://www.owasp.org:80 | /index.php/Main_Page | | 200 OK | |
| 3 | 00:13:16 | GET | http://www.google-analytics.com:80 | /__utm.gif | utmwv=1&... | 200 OK | |
| 4 | 00:13:49 | GET | http://www.owasp.org:80 | /index.php/Main_Page | | 200 OK | |
| 5 | 00:13:50 | GET | http://www.owasp.org:80 | /skins/common/commonPrint.css | 42b | 200 OK | |
| 6 | 00:13:50 | GET | http://www.owasp.org:80 | /skins/monobook/handheld.css | 42b | 200 OK | |
| 7 | 00:13:51 | GET | http://www.owasp.org:80 | /skins/monobook/main.css | 42b | 200 OK | |
| 8 | 00:13:54 | GET | http://www.owasp.org:80 | /skins/monobook/IE70Fixes.css | 42b | 200 OK | |
| 9 | 00:13:54 | GET | http://www.owasp.org:80 | /skins/common/wikibits.js | 42b | 200 OK | |

```
GET http://www.owasp.org/index.php/Main_Page HTTP/1.1
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpe
Accept-Language: en-us
UA-CPU: x86
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5
Host: www.owasp.org
Proxy-Connection: Keep-Alive
Cookie: __utma=77342603.703937831.1178748781.11787
    __utma=77342603.703937831.1178748781.117874878
    __utmb=77342603
    __utmc=77342603
```

```
HTTP/1.1 200 OK
Transfer-Encoding: chunked
Date: Wed, 09 May 2007 22:13:53 GMT
Content-Type: text/html; charset=UTF-8
Expires: Wed, 09 May 2007 22:13:53 GMT
```

connected to the Google Summer of Code.

**Application Security News (add)**

**Apr 21 - Concurrency and porn**

# Improvements over -classic

< User-visible

4 Using Spring Rich Client Platform (HIG-friendly UI!)

4 Different views of the same data now consistent!

4 New ContentType editors

4 Floating Proxy toolbar

4 Dockable views

< Under the hood

4 Using a proper DB (HSQLDB) to store history

4 Using Spring Framework (DB, internal wiring)

4 Fewer leaks – hopefully!

# Demonstration

WebScarab-NG vs WebGoat

**FIGHT!!**

# Weaknesses vs -classic

- < Many features not yet implemented
  - 4 Plugins
    - § Spider
    - § Scripting
    - § SessionID Analysis
    - § etc
  - 4 Protocol support (NTLM/certs/smart cards/PKCS#11)
  - 4 Shared Cookie jar

# Future directions

< Identity module

4 Tag identity transition points (logon/logoff/timeout)

4 Supports things like reverse-engineering Access Control Matrices

< Random generator quality assessment

4 -classic SessionIDAnalysis plugin “pretty” but flawed

4 Inspired by Michal Zalewski’s “stompy”

< Re-implement HTTP client (currently Jakarta)

4 Desire complete control over the connection to server

4 Apparently whitespace matters!

# Getting involved

< Run via Java WebStart

4 http://dawes.za.net/rogan/webscarab-ng/webstart/WebScarab-ng.jnlp

< Join the list

4 owasp-webscarab@lists.owasp.org

< Browse the source

4 http://dawes.za.net/gitweb.cgi?p=rogan/webscarab-ng/webscarab-ng.git;a=summary

< Clone the repo

4 git clone http://dawes.za.net/rogan/webscarab-ng/webscarab-ng.git/

# Questions

? ? ?