Velkommen til

WebScarab framework

for analysing web applications

Henrik Lund Kramshøj
hlk@security6.net

http://www.security6.net

Hvad er OWASP

OWASP er The Open Web Application Security Project

The OWASP Foundation is a 501c3 not-for-profit charitable organization

worldwide free and open community

Værktøjer som WebScarab og WebGoat

Dokumenter, vejledninger, checklister - free and open software license

Afholder konferencer, møder

http://www.owasp.org

Hvad er WebScarab

WebScarab er et framework

Men de fleste vil nok kalde det et værktøj

Fungerer basalt set som en proxy med mere, meget mere

Hjælper med sikkerhedstest af webapplikationer

WebScarab features

Analyse af HTTP(S) requests

Analyse af URL opbygning

Spidering, enumerating

Bypass client-side validation, javascript validering på klient

Undersøge Session IDs, er de tilfældige

Installation

WebScarab er et Java program - run anywhere

WebScarab findes i to versioner

Den *gamle klassiske* og den nye webscarab-ng

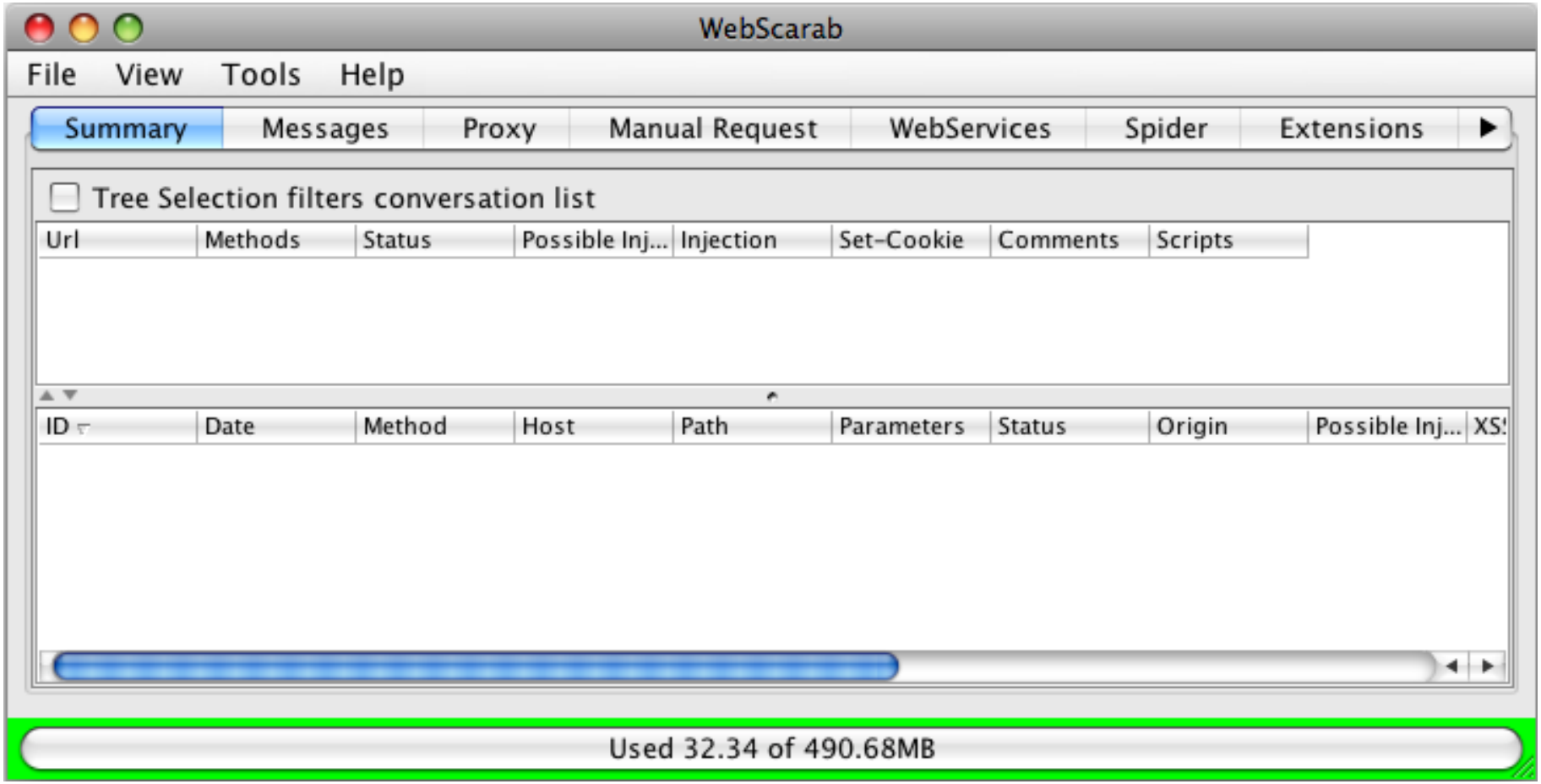
Den klassiske downloades i en færdig Java JAR pakke

Den nye er en Java Webstart pakke

Den klassiske er fin og virker
`http://www.owasp.org/index.php/Category:OWASP_WebScarab_Project`

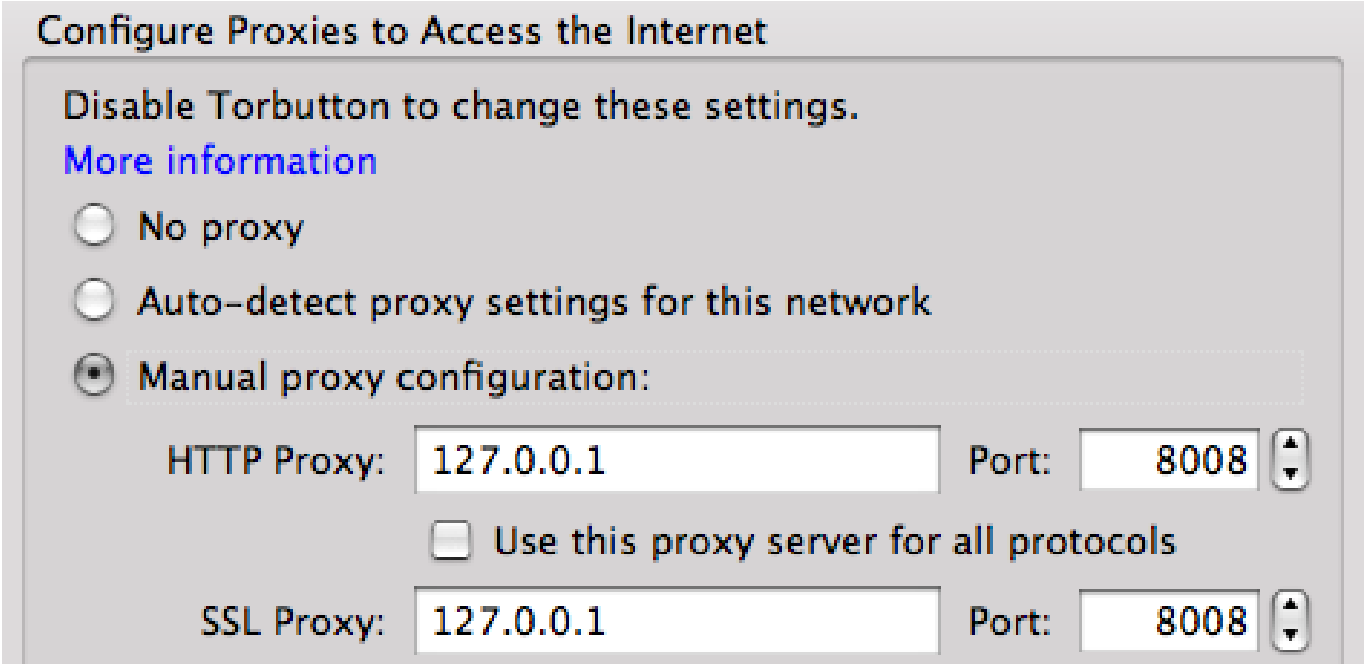
Den nye er under udvikling og er indimellem lidt bøvlet
`http://www.owasp.org/index.php/OWASP_WebScarab_NG_Project`
`http://dawes.za.net/rogan/webscarab/WebScarab.jnlp`

Opstart



Use full featured interface!

Proxy me

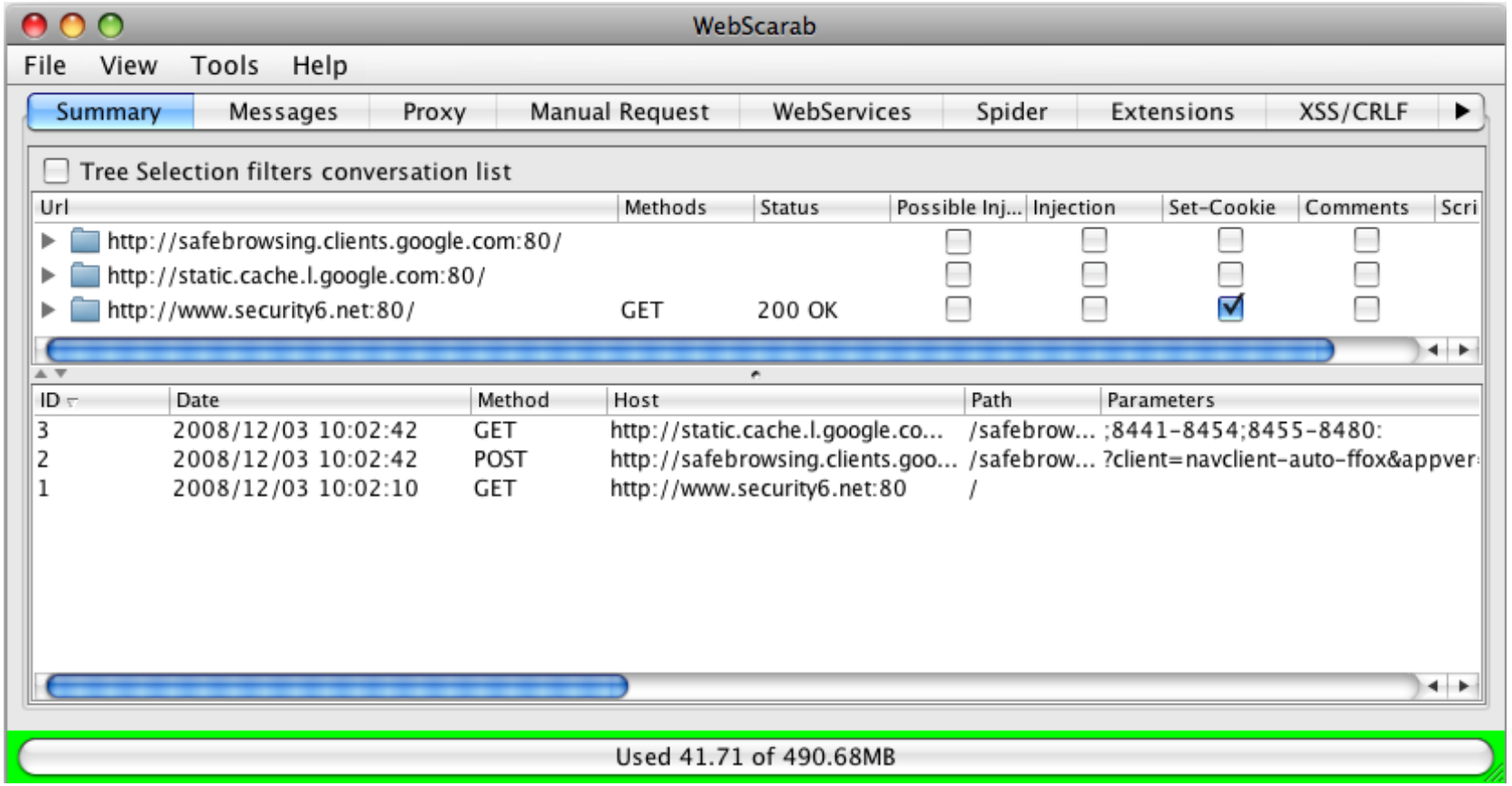


Start en browser eksempelvis Firefox

Sæt proxy til 127.0.0.1:8008

Surf ind på det website du vil undersøge

WebScarab opfanger alle HTTP(S) data



Så er vi klar

Demo: WebScarab live

WebScarab live - teknisk, bøvlet - men sjovt

Ulemper ved WeScarab

Der er nogle ulemper

WebScarab er nørdet!

Først og fremmest skal du få den igang, nogenlunde nemt

Dernæst skal du kende HTTP protokollen: GET, POST, ...

Du skal kende til URL opbygning, parametre

Du skal kende til webapplikationers opbygning

Du skal kende de almindelige fejl i webapplikationer, se evt. OWASP listerne
http://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project

Konkurrenter

Burp suite fra http://www.portswigger.net/

Parox proxy fra http://www.parosproxy.org

Metasploit WMAP http://www.metasploit.com/

Tamper Data extension til Firefox og andre udvidelser: Web developers toolkit, SQL inject

Se evt. listerne fra:
http://www.owasp.org/index.php/Phoenix/Tools
http://sectools.org/

Husk også bogen *The Web Application Hackers Handbook*

Opsummering

gode grunde til at bruge WebScarab

Multiplatform, Mac OS X, Windows, Linux, Unix ...

Effektiv og opdateret

Mange vigtige features

Features der automatiserer dele af det kedelige arbejde:
spider, fuzzer, sessionids

Synlig visning af hidden fields mens du browser

Nemmere at dokumentere testen

Er gratis

Spørgsmål?

Henrik Lund Kramshøj
hlk@security6.net

http://www.security6.net

I er altid velkomne til at sende spørgsmål på e-mail