Webscarab, an introduction.

Philippe Bogaerts
Bee-ware
philippe.bogaerts@radarhack.com

OWASP

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

Who am I?

- During the day
  - Technical manager at Bee-ware
    - http://www.bee-ware.net

BeeWare

- During the night
  - Trying to acquire a good understanding of
    - network security
    - web application and web services security
    - Pen-testing

Why am I here ?

- A good opportunity to hear people talking about applications and the related security implications.

- To better understand how applications work and how they are developed.

- WebScarab is simply a great tool that gave me ‘the’ better understanding of HTTP and HTTP-based applications.

What is WebScarab?

- A java based tool
  - Security analysis
  - Application debugging

- WebScarab acts as a proxy between a client and an application
  - browsers accessing a web application
  - a client application accessing a web service
  - …

What can you do with WebScarab?

- Allows user to view HTTP(S) conversations between browser and server
- Allows user to review those conversations
- Allows user to intercept and modify on the fly
- Allows user to replay previous requests
- Allows user to script conversations with full access to the the request and response object models
- And much more!

Obtaining WebScarab

- More information
  - http://www.owasp.org/software/webscarab.html
- Hosted on Sourceforge
  - http://sourceforge.net/project/showfiles.php?group_id=64424&package_id=61823
- Documentation
  - http://dawes.za.net/rogan/webscarab/docs/
- Mailinglist
  - http://lists.sourceforge.net/lists/listinfo/owasp-webscarab

Installing WebScarab

- Various package formats
  - **webscarab-installer-<date>.jar**
    - java -jar webscarab-selfcontained-20051017-2127.jar
  - **webscarab-selfcontained-<date>.jar**
  - **webscarab-src-<date>.jar**
- **Beta version available via mailinglist**
  - **Beta version will be discussed during presentation**

What is new in the beta version?

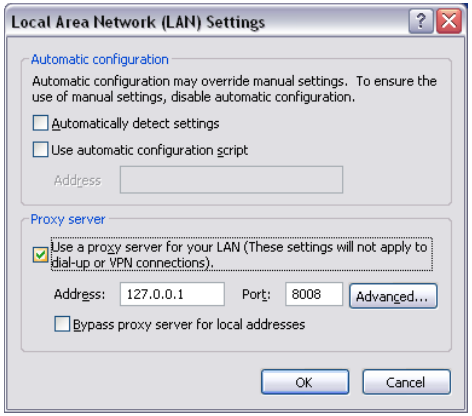
- More extensive certificate support
  - Pkcs#12
  - Pkcs#11
  - CAPI (to come)

- Credential support
  - Automatic learning of credentials
  - Automated insertion of credentials

- Extensions module

Setting up the environment

- Application and WS can be installed on same workstations
  - Application is configured to connects to WS at 127.0.0.1:8008 by default



Local Area Network (LAN) Settings

Automatic configuration

Automatic configuration may override manual settings. To ensure the use of manual settings, disable automatic configuration.

□ Automatically detect settings

□ Use automatic configuration script

Address

Proxy server

☑ Use a proxy server for your LAN (These settings will not apply to dial-up or VPN connections).

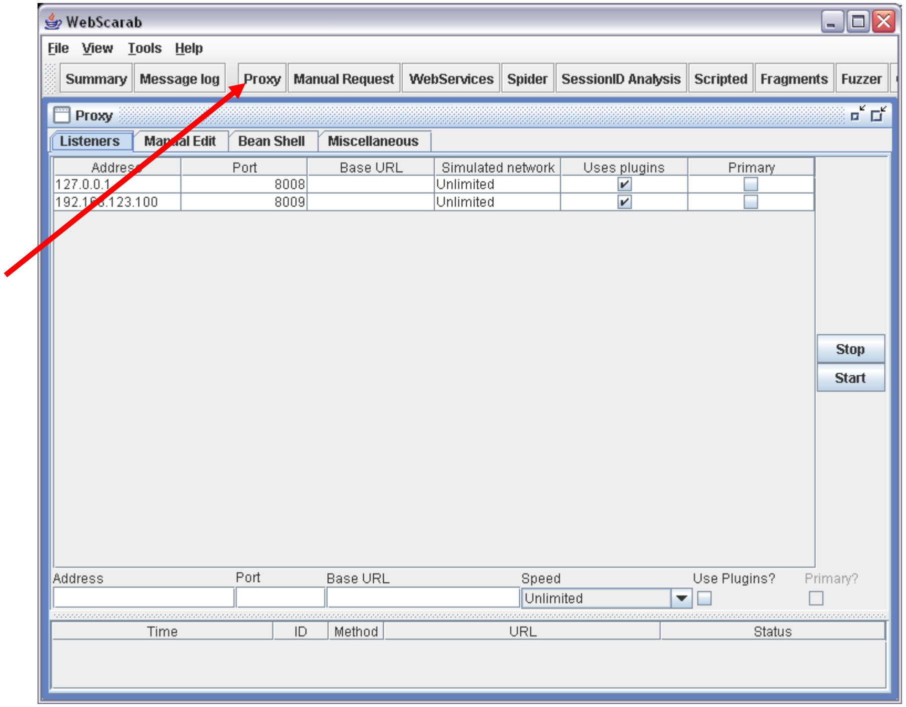
Address: 127.0.0.1 Port: 8008

□ Bypass proxy server for local addresses

- Application and WS can be installed on different machines

Configuring WebScarab

- Multiple instances of reverse proxies
  - Proxy Button
- WS can use upstream proxies
  - Ex. A Web Application Firewall under test
  - Tools -> Proxies



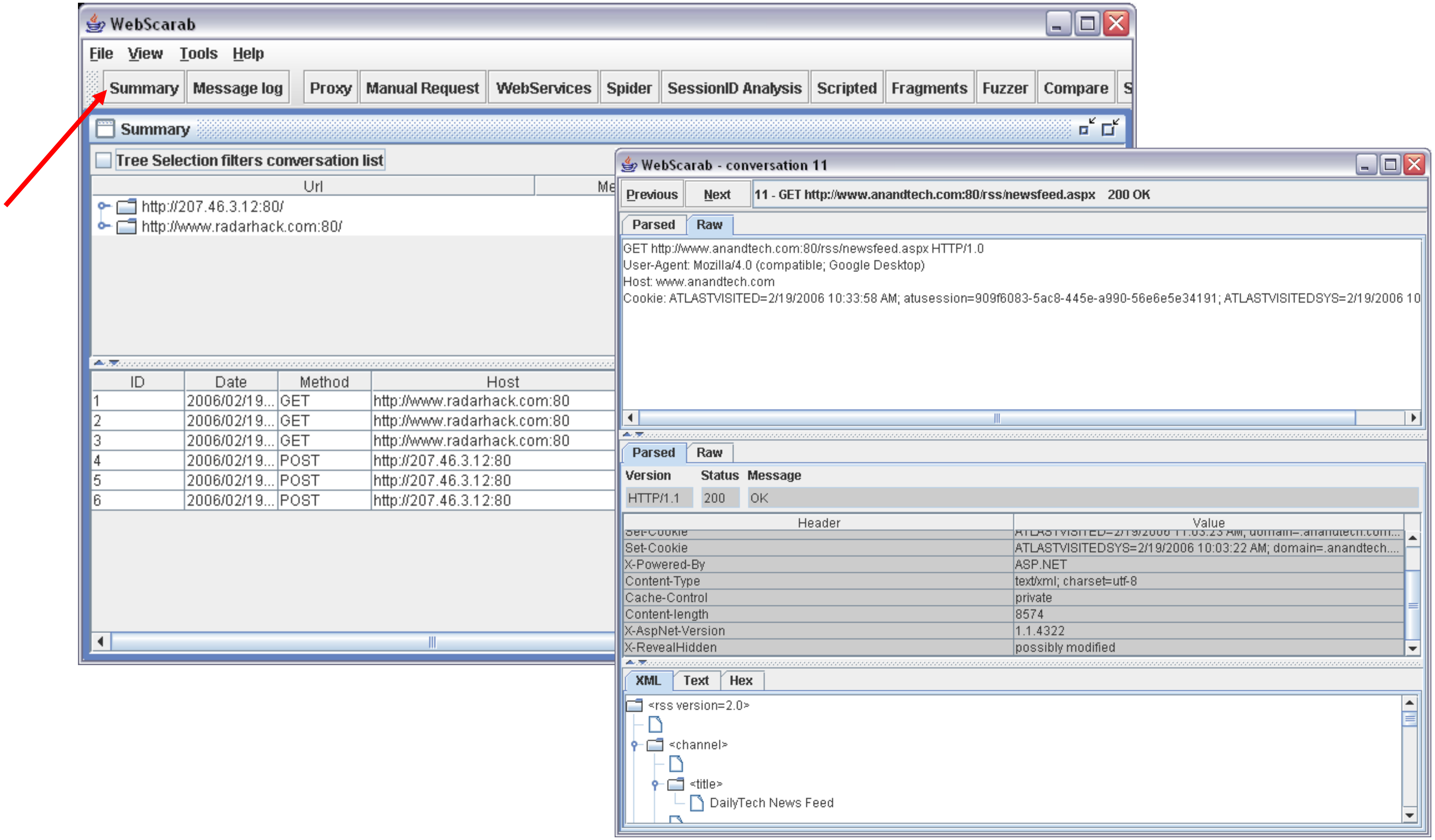
Address	Port	Base URL	Simulated network	Uses plugins	Primary
127.0.0.1	8008		Unlimited	☑	□
192.168.123.100	8009		Unlimited	☑	□

Address: Port: Base URL: Speed: Unlimited Use Plugins? □ Primary? □

Time	ID	Method	URL	Status

WebScarab is ready to capture traffic

- Summary window displays in real-time all traffic passing through.



http://207.46.3.12:80/
http://www.radarhack.com:80/

ID	Date	Method	Host
1	2006/02/19...	GET	http://www.radarhack.com:80
2	2006/02/19...	GET	http://www.radarhack.com:80
3	2006/02/19...	GET	http://www.radarhack.com:80
4	2006/02/19...	POST	http://207.46.3.12:80
5	2006/02/19...	POST	http://207.46.3.12:80
6	2006/02/19...	POST	http://207.46.3.12:80

11 - GET http://www.anandtech.com:80/rss/newsfeed.aspx 200 OK

```
GET http://www.anandtech.com:80/rss/newsfeed.aspx HTTP/1.0
User-Agent: Mozilla/4.0 (compatible; Google Desktop)
Host: www.anandtech.com
Cookie: ATLASTVISITED=2/19/2006 10:33:58 AM; atusession=909f6083-5ac8-445e-a990-56e6e5e34191; ATLASTVISITEDSYS=2/19/2006 10
```

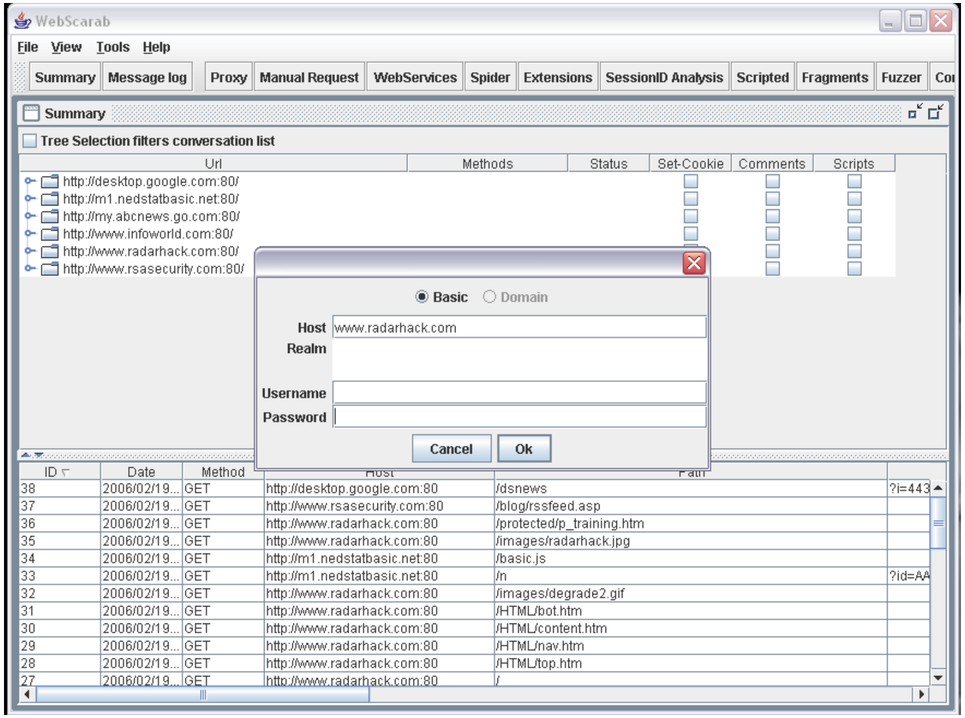
Version	Status	Message
HTTP/1.1	200	OK

Header	Value
Set-Cookie	ATLASTVISITED=2/19/2006 11:03:23 AM; domain=.anandtech.com...
Set-Cookie	ATLASTVISITEDSYS=2/19/2006 10:03:22 AM; domain=.anandtech....
X-Powered-By	ASP.NET
Content-Type	text/xml; charset=utf-8
Cache-Control	private
Content-length	8574
X-AspNet-Version	1.1.4322
X-RevealHidden	possibly modified

```
<rss version=2.0>
  <channel>
    <title>
      DailyTech News Feed
```

Credential caching/learning

- When an application requires authentication, WS will popup to learn the credentials. Credentials will be automatically inserted.
  - Basic authentication
  - NTLM authentication



☐ Tree Selection filters conversation list

Url	Methods	Status	Set-Cookie	Comments	Scripts
http://desktop.google.com:80/			☐	☐	☐
http://m1.nedstatbasic.net:80/			☐	☐	☐
http://my.abcnews.go.com:80/			☐	☐	☐
http://www.infoworld.com:80/			☐	☐	☐
http://www.radarhack.com:80/			☐	☐	☐
http://www.rsasecurity.com:80/				☐	☐

● Basic ○ Domain

Host: www.radarhack.com

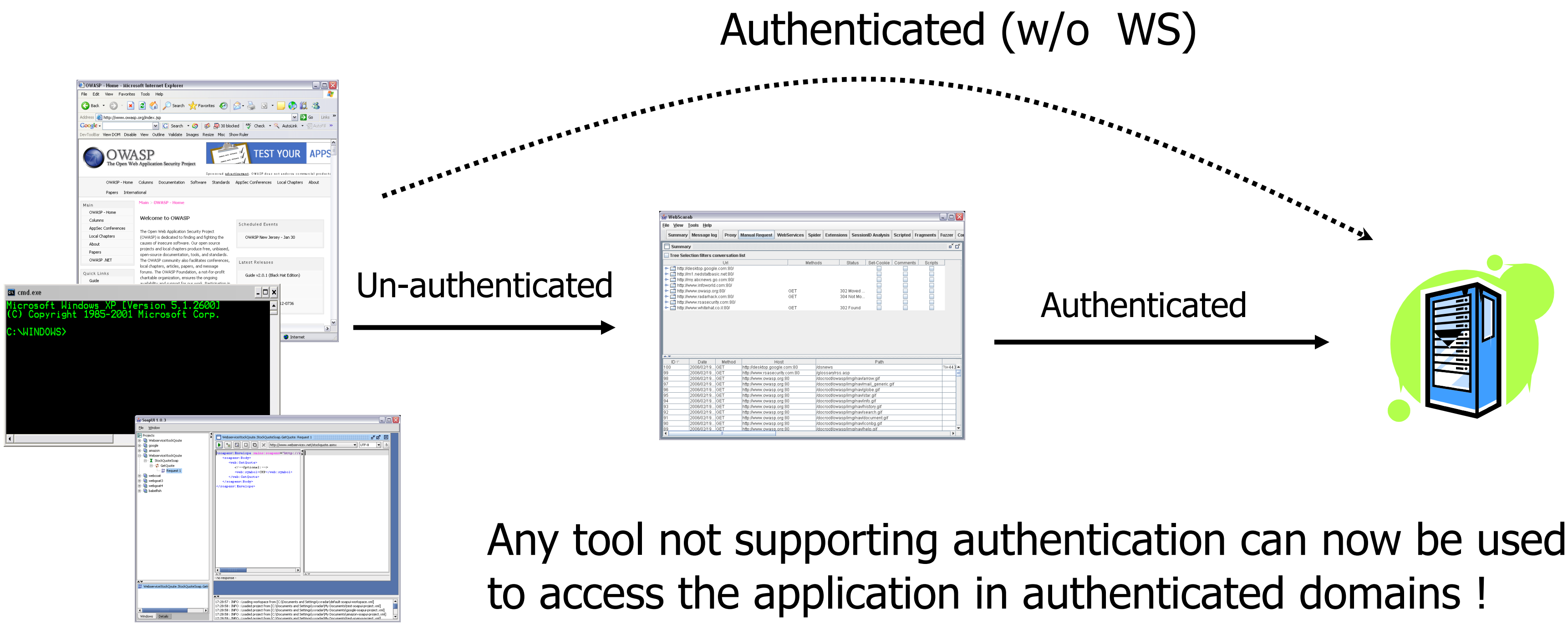
Realm:

Username:

Password:

ID	Date	Method	Host	Path	
38	2006/02/19...	GET	http://desktop.google.com:80	/dsnews	?i=443
37	2006/02/19...	GET	http://www.rsasecurity.com:80	/blog/rssfeed.asp	
36	2006/02/19...	GET	http://www.radarhack.com:80	/protected/p_training.htm	
35	2006/02/19...	GET	http://www.radarhack.com:80	/images/radarhack.jpg	
34	2006/02/19...	GET	http://m1.nedstatbasic.net:80	/basic.js	
33	2006/02/19...	GET	http://m1.nedstatbasic.net:80	/n	?id=AA
32	2006/02/19...	GET	http://www.radarhack.com:80	/images/degrade2.gif	
31	2006/02/19...	GET	http://www.radarhack.com:80	/HTML/bot.htm	
30	2006/02/19...	GET	http://www.radarhack.com:80	/HTML/content.htm	
29	2006/02/19...	GET	http://www.radarhack.com:80	/HTML/nav.htm	
28	2006/02/19...	GET	http://www.radarhack.com:80	/HTML/top.htm	
27	2006/02/19...	GET	http://www.radarhack.com:80	/	

Is this useful ?



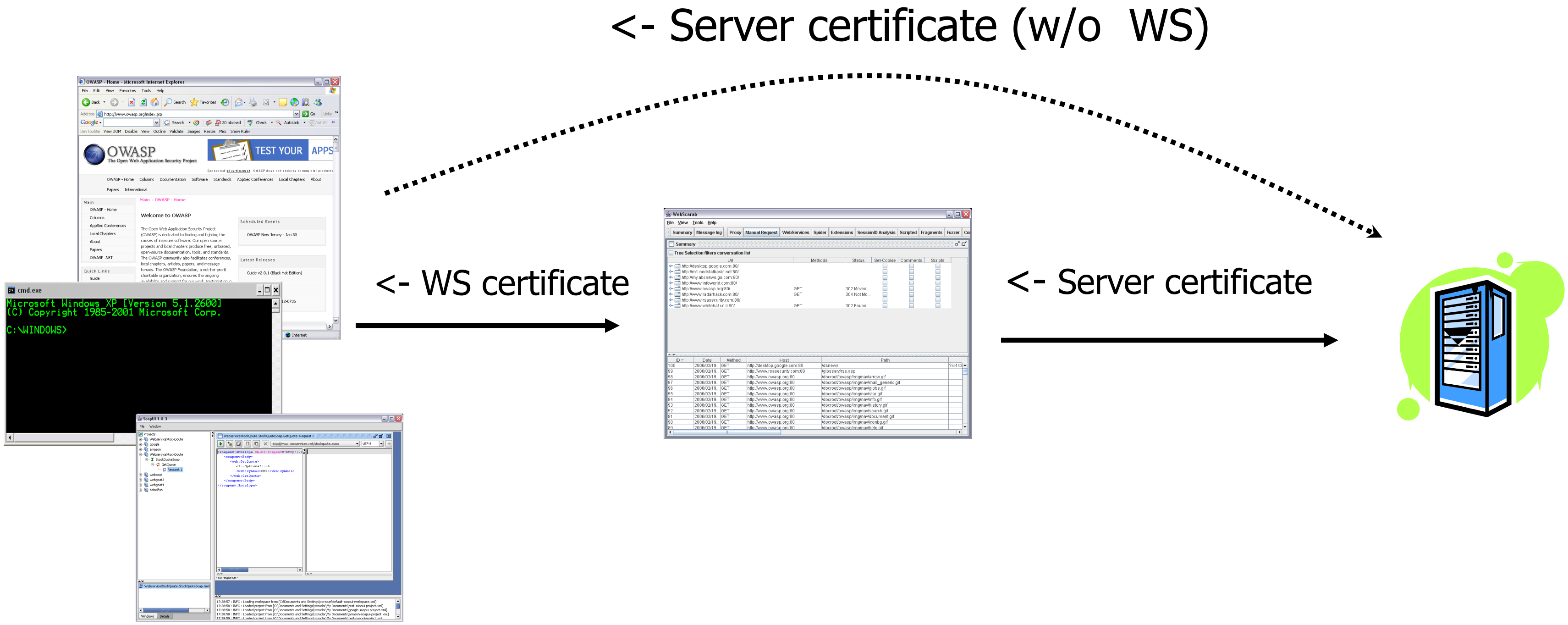
```
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\WINDOWS>
```

Any tool not supporting authentication can now be used to access the application in authenticated domains !

Ex. nc, web service invocation tools … but also build in features such as manual crafted requests, the spider and extension module

SSL support



<- Server certificate (w/o WS)

<- WS certificate

<- Server certificate

```
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\WINDOWS>
```

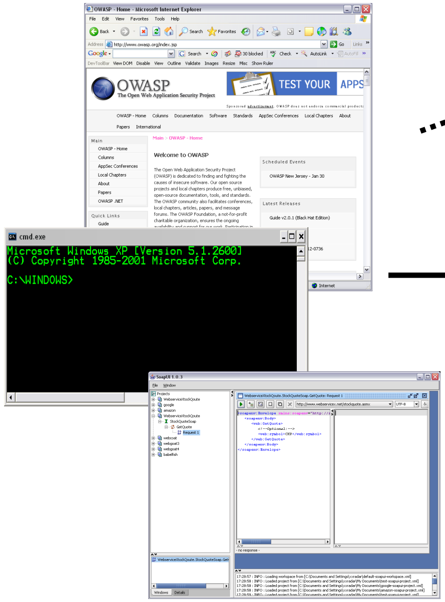
cmd.exe
OWASP - Home - Microsoft Internet Explorer
OWASP
The Open Web Application Security Project
TEST YOUR APPS
Welcome to OWASP
SoapUI 1.0.3
WebScarab
File View Tools Help
Summary Message log Proxy Manual Request WebServices Spider Extensions SessionID Analysis Scripted Fragments Fuzzer
Summary
Tree Selection filters conversation list

Url	Methods	Status	Set-Cookie	Comments	Scripts
http://desktop.google.com:80/			□	□	□
http://m1.nedstatbasic.net:80/			□	□	□
http://my.abcnews.go.com:80/			□	□	□
http://www.infoworld.com:80/			□	□	□
http://www.owasp.org:80/	GET	302 Moved ...	□	□	□
http://www.radarhack.com:80/	GET	304 Not Mo...	□	□	□
http://www.rsasecurity.com:80/			□	□	□
http://www.whitehat.co.il:80/	GET	302 Found	□	□	□

ID	Date	Method	Host	Path	
100	2006/02/19...	GET	http://desktop.google.com:80	/dsnews	?i=443
99	2006/02/19...	GET	http://www.rsasecurity.com:80	/glossary/rss.asp	
98	2006/02/19...	GET	http://www.owasp.org:80	/docroot/owasp/img/nav/arrow.gif	
97	2006/02/19...	GET	http://www.owasp.org:80	/docroot/owasp/img/nav/mail_generic.gif	
96	2006/02/19...	GET	http://www.owasp.org:80	/docroot/owasp/img/nav/globe.gif	
95	2006/02/19...	GET	http://www.owasp.org:80	/docroot/owasp/img/nav/star.gif	
94	2006/02/19...	GET	http://www.owasp.org:80	/docroot/owasp/img/nav/info.gif	
93	2006/02/19...	GET	http://www.owasp.org:80	/docroot/owasp/img/nav/history.gif	
92	2006/02/19...	GET	http://www.owasp.org:80	/docroot/owasp/img/nav/search.gif	
91	2006/02/19...	GET	http://www.owasp.org:80	/docroot/owasp/img/nav/document.gif	
90	2006/02/19...	GET	http://www.owasp.org:80	/docroot/owasp/img/nav/iconbg.gif	
89	2006/02/19...	GET	http://www.owasp.org:80	/docroot/owasp/img/nav/help.gif	

SSL and client certificate support

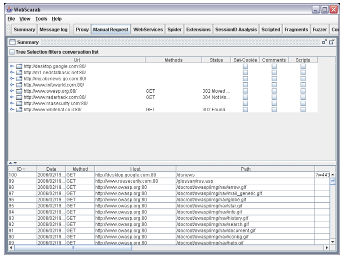
SSL with client certificate (w/o WS)



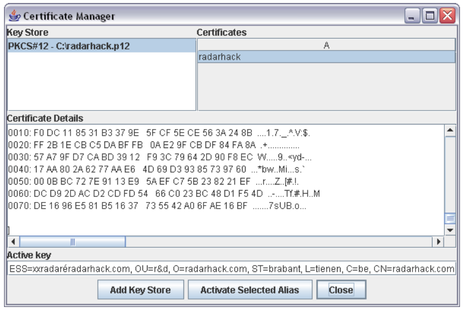
```
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\WINDOWS>
```

SSL



SSL with client certificate



Certificate Manager

Key Store

PKCS#12 - C:\radarhack.p12

Certificates

A
radarhack

Certificate Details

```
0010: F0 DC 11 85 31 B3 37 9E   5F CF 5E CE 56 3A 24 8B  ....1.7._.^.V:$.
0020: FF 2B 1E CB C5 DA BF FB   0A E2 9F CB DF 84 FA 8A  .+..............
0030: 57 A7 9F D7 CA BD 39 12   F9 3C 79 64 2D 90 F8 EC  W.....9..<yd-...
0040: 17 AA 80 2A 62 77 AA E6   4D 69 D3 93 85 73 97 60  ...*bw..Mi...s.`
0050: 00 0B BC 72 7E 91 13 E9   5A EF C7 5B 23 82 21 EF  ...r....Z..[#.!.
0060: DC D9 2D AC D2 CD FD 54   66 C0 23 BC 48 D1 F5 4D  ..-....Tf.#.H..M
0070: DE 16 96 E5 81 B5 16 37   73 55 42 A0 6F AE 16 BF  .......7sUB.o...

]
```

Active key

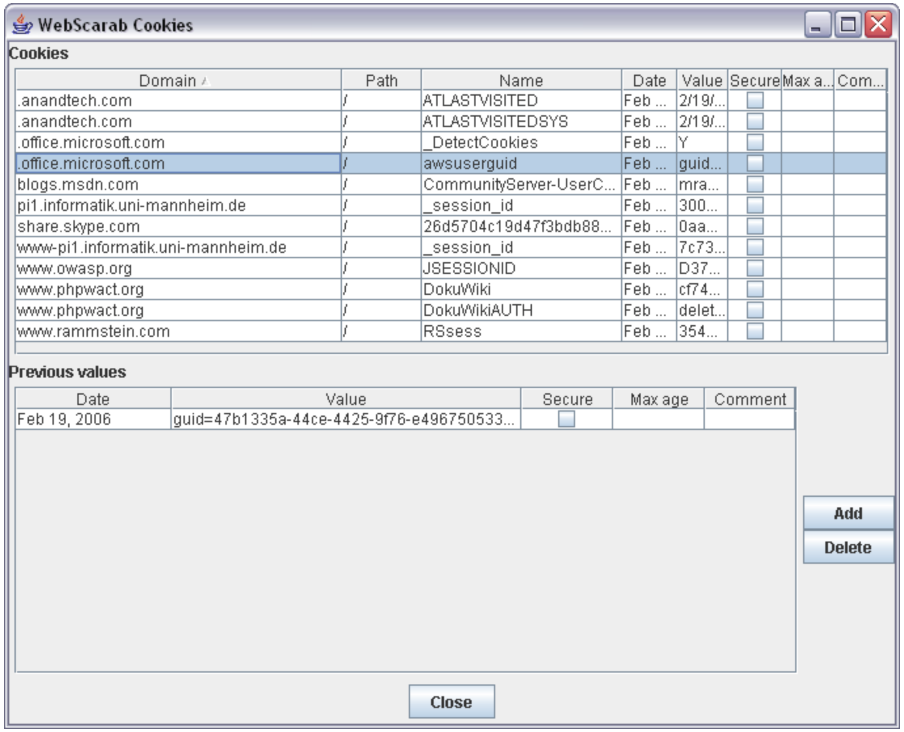
ESS=xxradaréradarhack.com, OU=r&d, O=radarhack.com, ST=brabant, L=tienen, C=be, CN=radarhack.com

Certificates can be imported via the certificate manager in following formats:

- Pkcs#12
- Pkcs#11 (smartcard support)
- CAPI (road mapped)

Shared Cookies plug-in

- WS will automatically record all cookies seen by other WS plug-ins.
  - cookies re-use in
    - Spider
    - Manual request



Cookies

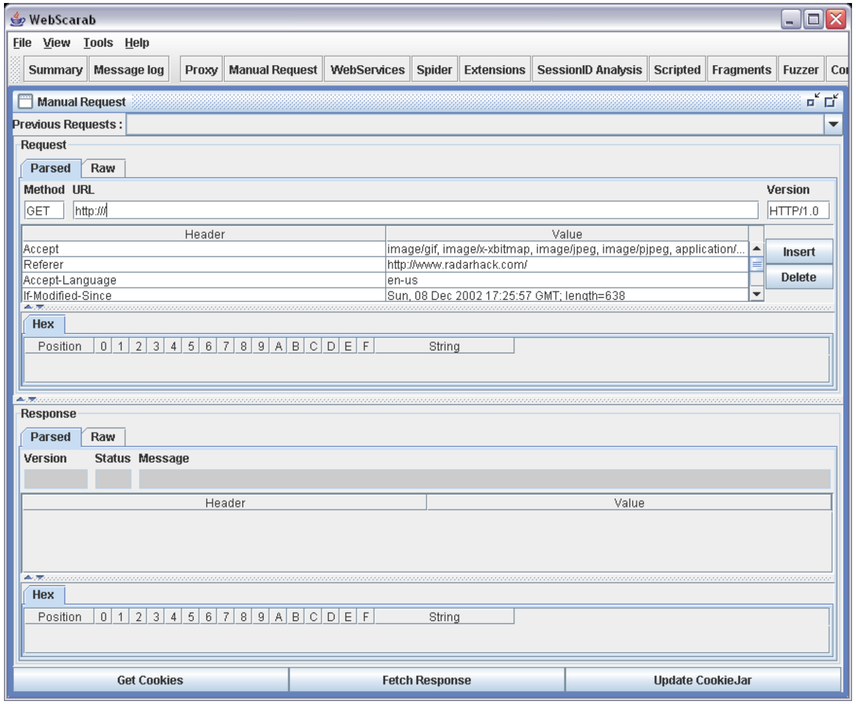
Domain	Path	Name	Date	Value	Secure	Max a...	Com...
.anandtech.com	/	ATLASTVISITED	Feb ...	2/19/...	□		
.anandtech.com	/	ATLASTVISITEDSYS	Feb ...	2/19/...	□		
.office.microsoft.com	/	_DetectCookies	Feb ...	Y	□		
.office.microsoft.com	/	awsuserguid	Feb ...	guid...	□		
blogs.msdn.com	/	CommunityServer-UserC...	Feb ...	mra...	□		
pi1.informatik.uni-mannheim.de	/	_session_id	Feb ...	300...	□		
share.skype.com	/	26d5704c19d47f3bdb88...	Feb ...	0aa...	□		
www-pi1.informatik.uni-mannheim.de	/	_session_id	Feb ...	7c73...	□		
www.owasp.org	/	JSESSIONID	Feb ...	D37...	□		
www.phpwact.org	/	DokuWiki	Feb ...	cf74...	□		
www.phpwact.org	/	DokuWikiAUTH	Feb ...	delet...	□		
www.rammstein.com	/	RSsess	Feb ...	354...	□		

Previous values

Date	Value	Secure	Max age	Comment
Feb 19, 2006	guid=47b1335a-44ce-4425-9f76-e496750533...	□		

Manual Request plug-in

- Previous request can be modified
- New requests can be build from scratch
  - Shared credential are taken into account!
  - Shared cookies can be reused use !



Method	URL	Version
GET	http://	HTTP/1.0

Header	Value
Accept	image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, application/...
Referer	http://www.radarhack.com/
Accept-Language	en-us
If-Modified-Since	Sun, 08 Dec 2002 17:25:57 GMT; length=638

OWASP

Demo

- Demo 1
  - Accessing a protected resource via netcat
- Demo 2
  - Accessing a protected resource via shared cookies

Spider plug-in

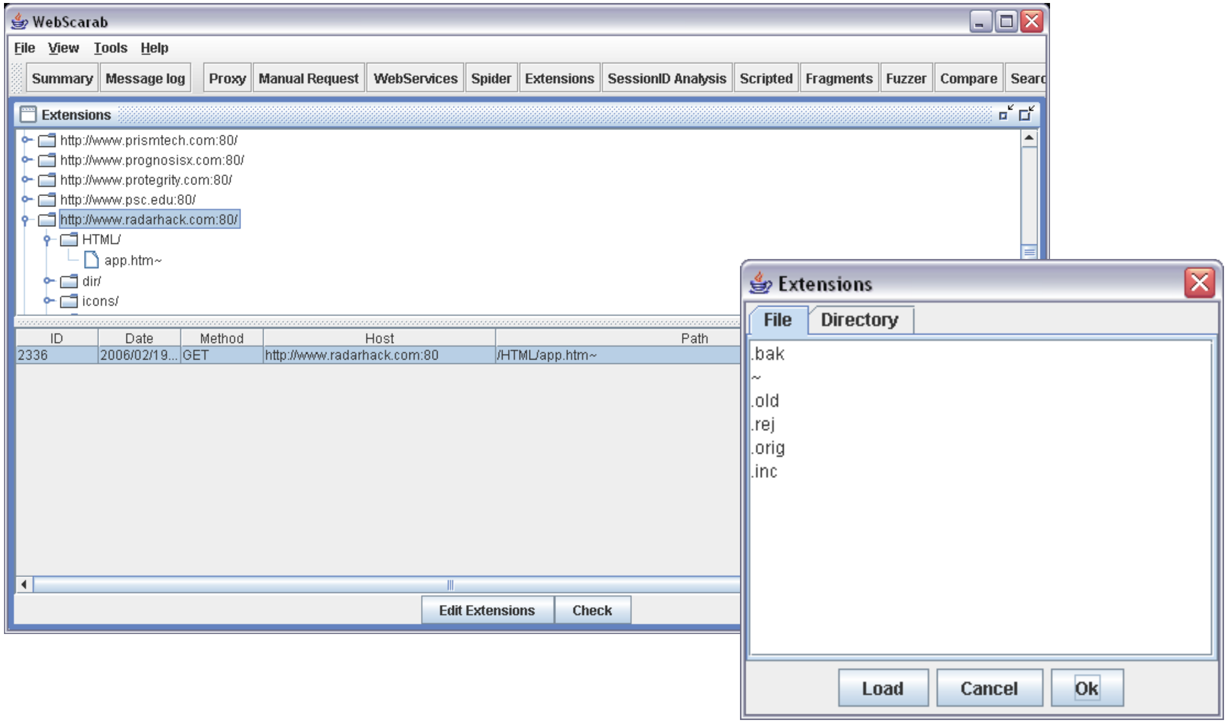
- The Spider plug-in analyses responses to identify any links in the response body, or the "Location" header.
- If the URL represented has not been seen, the URL is added to a tree, and can be automatically downloaded when desired.

Remark:

After a URL has been fetch, it is added to the Summary pane and disappears from the spider pane !

Extension plug-in

- The Extension plug-in uses the Extensions tree to brute-forces a set of file extensions.



http://www.prismtech.com:80/
http://www.prognosisx.com:80/
http://www.protegrity.com:80/
http://www.psc.edu:80/
http://www.radarhack.com:80/
HTML/
app.htm~
dir/
icons/

ID	Date	Method	Host	Path
2336	2006/02/19...	GET	http://www.radarhack.com:80	/HTML/app.htm~

.bak
~
.old
.rej
.orig
.inc

Web Services plug-in

- Web Services Description Language
  - Detection of WSDL file in conversations
  - Manual import of WSDL file
- Automatic parsing of services
- Invocation tool

- A nice tool in combination with webscarab is
  - http://www.soapui.org/

Demo

- Demo 1
  - Checking out the Amazon web services API
- Demo 2
  - WebScarab invocation tool
  - SOAP UI via WebScarab

Other features

- Search
- Compare
- Fragments
- Scripted
- SessionID Analysis

Other products

- Paros
  - http://www.paros.org
- Achilles
  - http://achilles.mavensecurity.com/
- Spike
- Burp suite
- IEWatch

Thank You