
Rain Forest Puppy
CanSecWest 2K01

Why whisker sucks

Challenges of auditing online web applications

“World Wide What?”

- Everyone and their pets are flocking to the web
- Multitude of new technologies have surfaced
- Caveats of HTTP force wacky workarounds
- Everyone seems to ‘roll-their-own’
- HTTP servers built into everything

What whisker does

- First and foremost: CGI scanner (file existence)
- Scriptable engine allowing for custom/intelligent scanning
- Identifies primary technologies involved
- Includes fun features (anti-IDS, brute forcing authentication and usernames)
- Some support for handling wacky results, which minimizes the overall number of false reports

```
*** STOP: 0x0000000A (0x00000000,0x00000002,0x00000000,8038c240)
IRQL_NOT_LESS_OR_EQUAL*** Address 8038c240 has base at 8038c000 - Ntfs.SYS

CPUID:Genuine Intel 6.3.3 irql:1f SYSVER 0xf0000565

Dll Base DateStmp - Name                 Dll Base DateStmp - Name
80100000 336546bf - ntoskrnl.exe         80010000 33247f88 - hal.dll
80000100 334d3a53 - atapi.sys            80007000 33248043 - SCSIPORT.SYS
802aa000 33013e6b - epst.mpd             802b5000 336016a2 - Disk.sys
802b9000 336015af - CLASS2.SYS           8038c000 3356d637 - Ntfs.sys
802bd000 33d844be - Siwvid.sys           803e4000 33d84553 - NTice.sys
f9318000 31ec6c8d - Floppy.SYS           f95c9000 31ec6c99 - Null.SYS
f9468000 31ed868b - KSecDD.SYS           f95ca000 335e60cf - Beep.SYS
f9358000 335bc82a - i8042prt.sys         f9474000 3324806f - mouclass.sys
f947c000 31ec6c94 - kbdclass.sys         f95cb000 3373c39d - ctrl2cap.SYS
f9370000 33248011 - VIDEOPORT.SYS        fe9d7000 3370e7b9 - ati.sys
f9490000 31ec6c6d - vga.sys              f93b0000 332480dd - Msfs.SYS
f90f0000 332480d0 - Npfs.SYS             fe957000 3356da41 - NDIS.SYS
a0000000 335157ac - win32k.sys           fe914000 334ea144 - ati.dll
fe0c9000 335bd30e - Fastfat.SYS          fe110000 31ec7c9b - Parport.SYS
fe108000 31ec6c9b - Parallel.SYS         f95b4000 31ec6c9d - ParVdm.SYS
f9050000 332480ab - Serial.SYS

Address  dword dump Build [1314]                              - Name
801afc24 80149905 80149905 ff8e6b8c 80129c2c ff8e6b94 8025c000 - Ntfs.SYS
801afc2c 80129c2c 80129c2c ff8e6b94 00000000 ff8e6b94 80100000 - ntoskrnl.exe
801afc34 801240f2 80124f02 ff8e6df4 ff8e6f60 ff8e6c58 80100000 - ntoskrnl.exe
801afc54 80124f16 80124f16 ff8e6f60 ff8e6c3c 8015ac7e 80100000 - ntoskrnl.exe
801afc64 8015ac7e 8015ac7e ff8e6df4 ff8e6f60 ff8e6c58 80100000 - ntoskrnl.exe
801afc70 80129bda 80129bda 00000000 80088000 80106fc0 80100000 - ntoskrnl.exe

Restart and set the recovery options in the system control panel
or the /CRASHDEBUG system start option. If this message reappears,
contact your system administrator or technical support group.
```

Why whisker fails

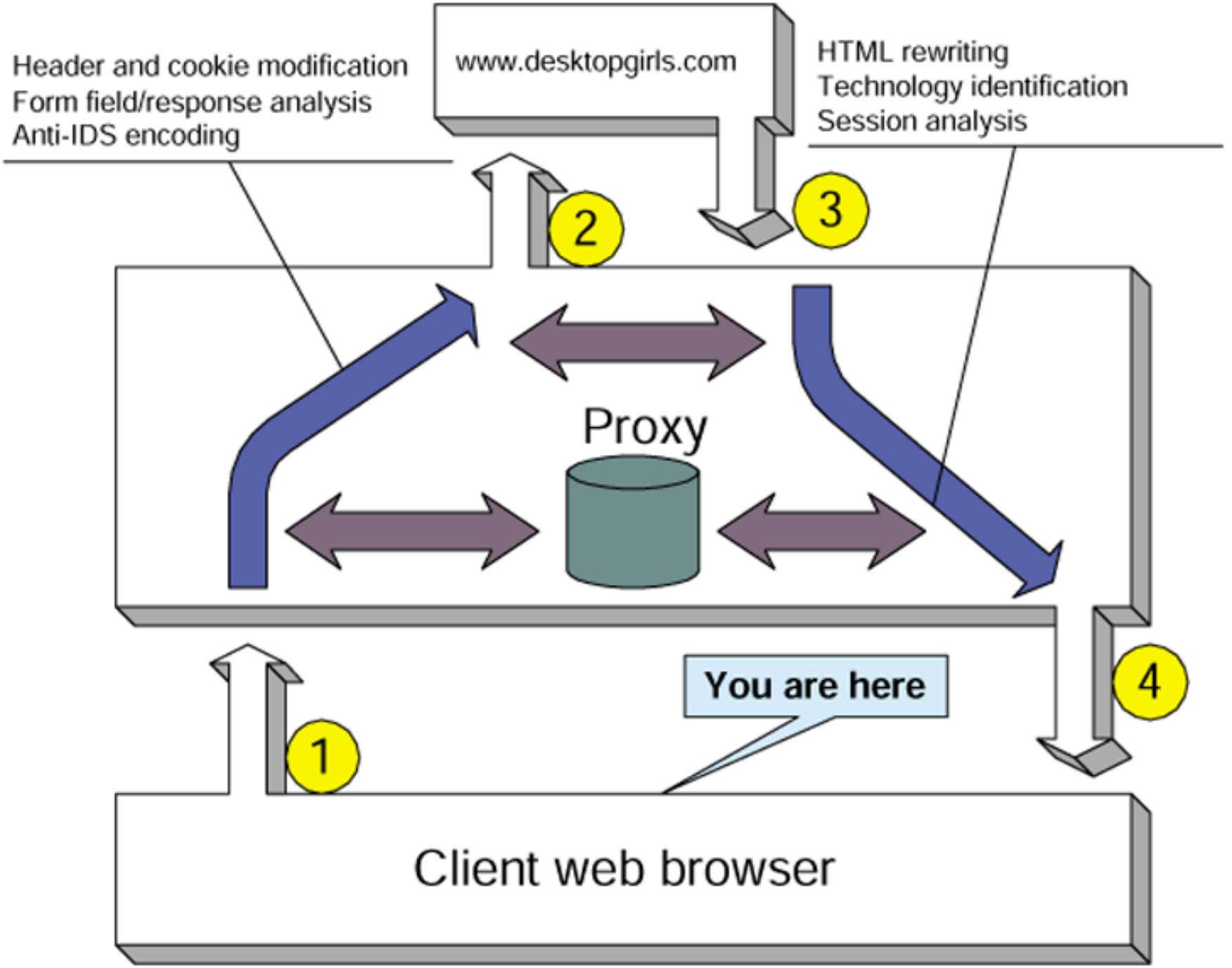
- People move their CGIs to alternate locations/names
- Can not engage custom applications which require decision making/choices
- Nonstandard custom server configs
- Framework centered on file existence checking
- Dependant on signatures databases and/or custom scan scripts

What we need

- Technology capable of interacting both with the user and the target web application
- Capable of understanding aspects of custom web applications
- Consolidation of various tools
- Minimization of tedious tasks that can better be automated
- Preferably keep assessment interface inline within the web browser

HTTP Proxy!

- Proxies are situated in the perfect place: between client and server
- User is allowed to use their browser du jour
- Outgoing connections can be modified to include arbitrary headers, anti-IDS encoding, etc
- Incoming responses can be passively monitored or actively engaged (such as HTML rewriting); this circumvents browser-imposed restrictions


Header and cookie modification
Form field/response analysis
Anti-IDS encoding
www.desktopgirls.com
HTML rewriting
Technology identification
Session analysis
2
3
Proxy
You are here
1
4
Client web browser

Fun Stuff a Proxy Can Do

- Add/modify/delete headers (particularly Referer)
- Manipulate cookies (modify contents, expiration)
- Fully log outgoing/incoming data (applets too)
- Passively monitor for known problems
- Request/response replay
- Appy anti-IDS tactics to anything
- HTML rewriting

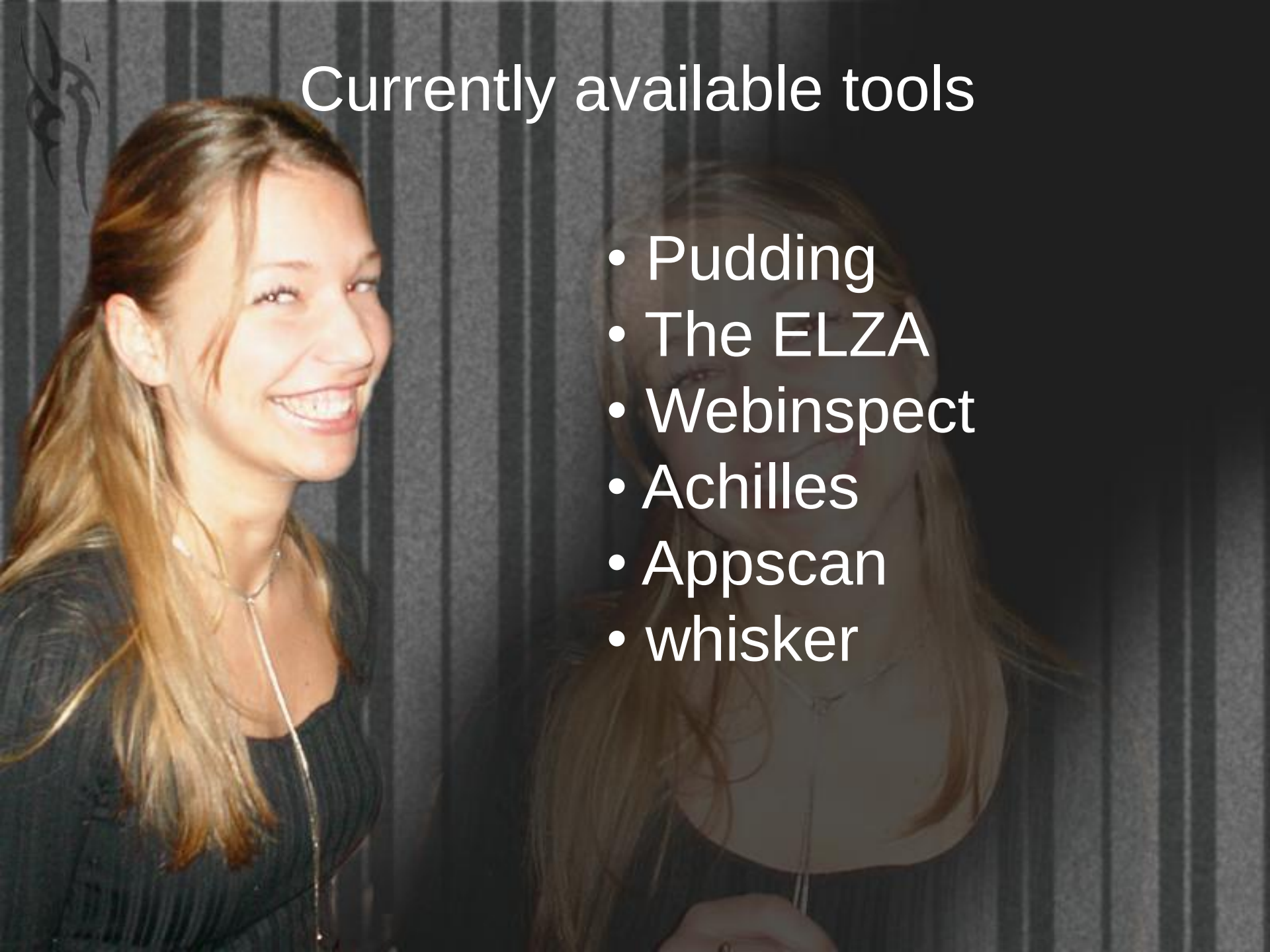
Fun Stuff…HTML Rewriting

- Change hidden fields to visible/editable
- Allow arbitrary values for select, radio, and checkbox fields
- Remove max size limitations
- Remove Javascript doodads
- Add/remove extra form elements
- Intercept meta-refreshes
- Alert on comments

Quick Break...

Questions?

Currently available tools



- Pudding
- The ELZA
- Webinspect
- Achilles
- Appscan
- whisker

Pudding

Roelof Temmingh
www.sensepost.com

- Proxy model
- Anti-IDS via URL/Unicode encoding

The ELZA

Philip Stoev
www.stoev.org

- Scanner model (not really)
- Script engine for interactively dealing with online apps
- Parses/understands HTML
- Requires you to write a custom script

Webinspect

SpiDynamics
www.spidynamics.com

- Scanner model
- Conventional CGI scanning
- Crawls site → deeper scanning
- Parses some HTML

Achilles

Digizen
www.digizen-security.org

- Proxy model
- Intercepts client & server data
- Allows request/response editing
- Can intercept SSL!
- However, editing facilities are kind of clunky

AppScan

Sanctum
www.sanctuminc.com

- Proxy model
- Passive monitoring of app use
- Can crawl a site on its own
- Light CGI/analysis scanning
- GUI, reports, blinky lights…
- Closed source & $$$$$$$$$$
- Mediocre use of proxy capabilities

whisker

rfp.labs
www.wiretrip.net/rfp/

- Scanner model
- Conventional CGI scanning only

There are no current plans for whisker 2.0 to implement these features.

Why?


RFProxy

RFProxy Overview

- Proxy that actively modifies data streams
- Add/modify/delete headers (and cookies)
- Log full outgoing/incoming data
- Passively monitor for known vulnerabilities
- Request/response replay/capture
- Appy anti-IDS tactics (from whisker v1.4)
- HTML rewriting (various form rewriting)


All your base
Are belong
to Marty
SNORT
ENTERPRISE
NETWORK SECURITY

Engage your apps

RFProxy PR and other conference materials:
http://www.wiretrip.net/rfp/cansecwest/

rfp@wiretrip.net

www.desktopgirls.com


Rain Forest Puppy
CanSecWest 2K01