


OWASP AppSec
Washington DC 2009



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


Consecuencias de un admin y un desarrollador "perezoso"

Lic. Cristian Borghello, CISSP - MVP
www.segu-info.com.ar
@seguinfo

Copyright © The OWASP Foundation
Permission is granted to copy, distribute and/or modify this document under the terms of the OWASP License.

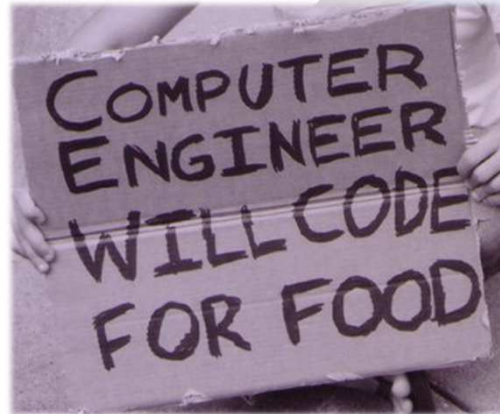
Perezoso

1. Negligente, descuidado o flojo en hacer lo que debe o necesita ejecutar
2. Que por demasiada afición a dormir se levanta tarde de la cama
3. Animal neotropical que se clasifica en perezosos de tres dedos y de dos dedos



2

10 historias de programadores holgazanes y administradores desesperados... **y sus consecuencias**



Secuela 1 – Los secretos develados

The screenshot shows a web browser window displaying an order details page. The URL is <http://www.com.ar/orderdetails.php?orderid=12364>. The page content includes:

ORDEN 12364
11
05
2011

HORA: 12:00:14
Cliente: Philipe [REDACTED]
Domicilio: Avenida Visconde de [REDACTED], apto. 1401
Localidad: Curitiba
C.P.: 80240010
Provincia: Paraná
Pais: Brasil
Teléfono: 55418846 [REDACTED]
Fax:
E-mail: philipe [REDACTED]@hotmail.com
CUIT: 0584267 [REDACTED]

0043202
Maurach Re... - Derecho penal. Parte general. 2
R
\$570,00

Total: \$570,00
Gastos: \$109,28

PHP API
PHP Extension

Notes: The current error pag

```
<!-- Web.Config Co
<configuration>
<system.web>
<customErr
</system.web>
</configuration>
```

Secuela 2 – Un trabajo *pumm* para arriba

← → ↻ www.gob.ar

Acuerdo e ... MUNICIPALIDAD y la CGT

El ministro de Trabajo ... etario General de la C

Dicho c ← → ↻ www.gov.ar/desarrollo.asp?id='&tabla=fsindical arios en

Tomada que def ... isis mue

Curlingh ... República Argentina

Divertic ...

buy phe ...

singula ...

acai we ...

adipex ...

cheap c ...

Microsoft OLE DB Provider for SQL Server error '80040e14'
Unclosed quotation mark after the character string ''.

/desarrollo.asp, line 19

5

Secuela 3 - Recalculando

site:ar "cheap viagra"

```
INSERT INTO `wp_options` VALUES (3140, 0, '_transient_dash_20494a3d90a6669585674ed0eb8dcd8f', '<ul>\n <li><
INSERT INTO `wp_options` VALUES (3107, 0, '_transient_feed_f689c5a29d6adc4b81976bbda9c1c64e', 'a:4:(s:5:"chil
ml_lang";s:0:"");s:4:"date";a:1:(i:0;a:5:(s:4:"data";s:29:"Sun, 05 Jun 2011 05:15:00 GMT";s:7:"attribs";a:0:
s:7:"attribs";a:0:(s:8:"xml_base";s:0:"";s:17:"xml_base_explicit";b:0;s:8:"xml_lang";s:0:"");s:7:"creator";
Drugs. Viagra Cialis Levitra Online without prescription 10/20/50/100 mg.";s:7:"attribs";a:0:(s:8:"xml_base"
```

Viagra + Cialis = \$83.99 + 4 Free Pills

Viagra \$278.95 120 pills, 100 mg +4 free pills

D:\temp\... \spam\htaccess

```
Options +FollowSymLinks
RewriteEngine on
RewriteRule (.*) http://www.cialis-viagra-... .com/$1 [R=301,L]
```

6

Secuela 4 – ¡Liberad al código fuente!

```

<?php
include '/conn/connection.php';
include '/conn/library/dbaccess.php';

include '/function.php';
include '/function_images.php';
include '/function_menu.php';

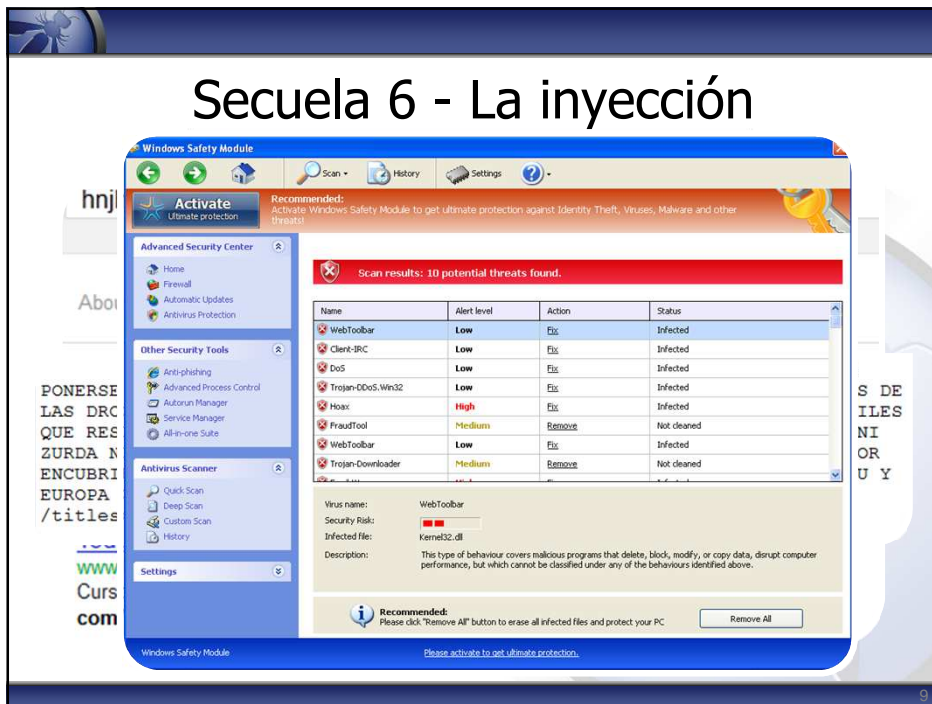
$server_in = '172.16.1.1';
$server_out = '89.13.13.1';

/* If package.procedure or package.function are passed, it will */
/* print the entire package. */
procedure showsource(cname in varchar2);
    
```

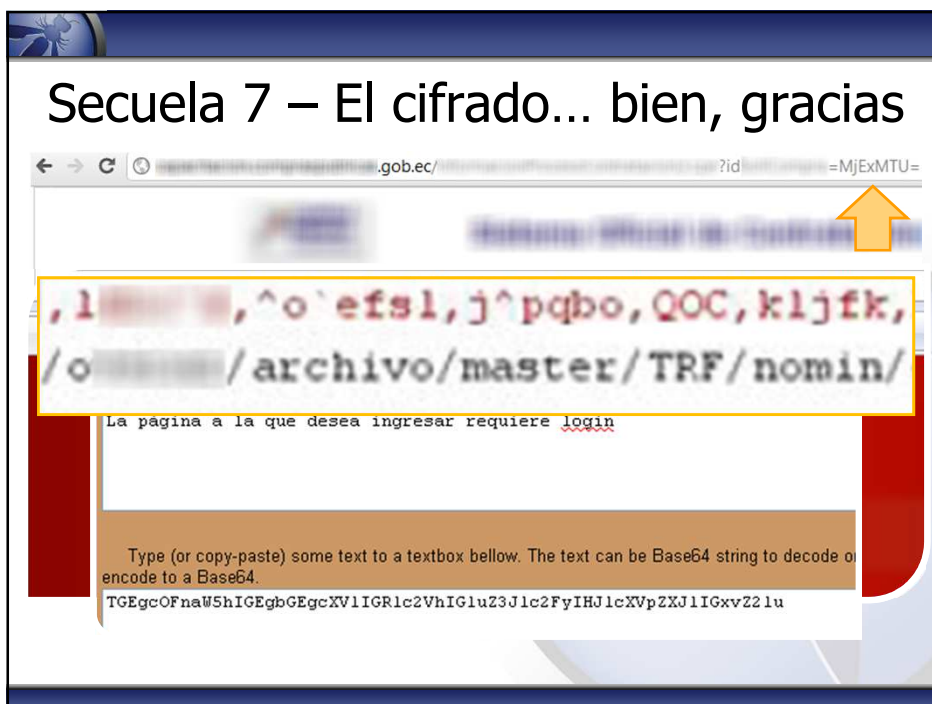
Secuela 5 – El chabón del *server*

Name	Ext	Size	Changed	Rights
..			22/04/2012 09:23:13 a.m.	rw-r--r--
000ab2c3f8236cddbda1f62ab4b77f98		112 KiB	24/02/2012 03:38:15 p.m.	rw-r--r--
000bfea080b3adf74c649d1bb1fd9f8d		36.291 B	25/02/2012 07:46:29 p.m.	rw-r--r--
001bbd8c4cce5bc92d2a21e5d4268b2e		116 KiB	04/02/2012 08:49:40 a.m.	rw-r--r--
0024e46496fada0cdd9852bcd78f77ca		33.214 B	17/03/2012 04:59:47 a.m.	rw-r--r--
002acb726e15d5d8e8fd409394ed8613		75.747 B	28/03/2012 07:04:19 a.m.	rw-r--r--
002f680f994161da8f1f8e861c747c4e		43.115 B	11/02/2012 05:17:08 a.m.	rw-r--r--
00307138477ee29c5df52051b61e61e6		32.264 B	27/01/2012 11:48:34 a.m.	rw-r--r--
004069fcc78f4ff460b5f7ef28b060b		36.885 B	29/01/2012 11:05:58 a.m.	rw-r--r--
0061c14a2e695fe6d6fd7cff9bf7d768		71.974 B	28/03/2012 07:20:43 a.m.	rw-r--r--
0097e4e0d80f289d9405f1ae007d30ea		29.487 B	08/04/2012 03:54:53 p.m.	rw-r--r--
00a187169305064844efc1d999a71562		40.676 B	03/04/2012 04:17:56 a.m.	rw-r--r--
00b5dc09ecad0f1e272e7b4dccaef6ef		45.286 B	30/01/2012 05:54:14 a.m.	rw-r--r--
00c945038489dea225913542497e3c55		31.100 B	08/04/2012 04:07:41 p.m.	rw-r--r--
00d8ce60e3004e16499ff4265ca17624		108 KiB	07/03/2012 01:47:22 a.m.	rw-r--r--
00e4f64a25a881ec95f14351be82de41		75.308 B	28/03/2012 06:04:38 a.m.	rw-r--r--
00e5cc7dada7fcb614ed4d963db74ec1		34.618 B	30/01/2012 02:12:36 p.m.	rw-r--r--

Secuela 6 - La inyección



Secuela 7 – El cifrado... bien, gracias



Secuela 8 – Tu propia Botnet

Changedate	Host	BinaryURL	Hash	Virustotal
2012-03-28	.com.ar	.com.ar/GPFito.exe	bb444105690f2b711480322b6e3b0ae2	n/a
2012-03-28	.com.ar	.com.ar/GPFito.exe	68b082655b11149d16d02b4fe11a4d21	36/42 (85.71%)
2012-03-28	.com.ar	.com.ar/GPFito.exe	2ce3c7a1d0225cf4108ee8568ef57980	23/42 (54.76%)
2012-03-28	.com.ar	.com.ar/GPFito.exe	68b082655b11149d16d02b4fe11a4d21	36/42 (85.71%)
2012-03-28	.com.ar	.com.ar/GPFito.exe	fa7670d9d565f514323f2294306fa861	16/42 (38.10%)
2012-03-27	.com.ar	.com.ar/GPFito.exe	0853ff70dc67ae6b332647cfb3a565da	16/42 (38.10%)
2012-03-27	.com.ar	.com.ar/GPFito.exe	68b082655b11149d16d02b4fe11a4d21	36/42 (85.71%)
2012-03-27	.com.ar	.com.ar/GPFito.exe	8d05f0a659c5e72994ee603746e635cc	21/42 (50.00%)
2012-03-27	.com.ar	.com.ar/GPFito.exe	68b082655b11149d16d02b4fe11a4d21	36/42 (85.71%)
2012-03-27	.com.ar	.com.ar/GPFito.exe	d499251f2321fa7e2e452b7945aa727f	19/41 (46.34%)
2012-03-27	.com.ar	.com.ar/GPFito.exe	68b082655b11149d16d02b4fe11a4d21	36/42 (85.71%)
2012-03-27	.com.ar	.com.ar/GPFito.exe	0853ff70dc67ae6b332647cfb3a565da	16/42 (38.10%)
2012-03-27	.com.ar	.com.ar/GPFito.exe	68b082655b11149d16d02b4fe11a4d21	36/42 (85.71%)
2012-03-26	.com.ar	.com.ar/GPFito.exe	fa7670d9d565f514323f2294306fa861	16/42 (38.10%)
2012-03-26	.com.ar	.com.ar/GPFito.exe	68b082655b11149d16d02b4fe11a4d21	36/42 (85.71%)
2012-03-26	.com.ar	.com.ar/GPFito.exe	0853ff70dc67ae6b332647cfb3a565da	16/42 (38.10%)
2012-03-26	.com.ar	.com.ar/GPFito.exe	68b082655b11149d16d02b4fe11a4d21	36/42 (85.71%)

Karn!v0r\$X v1.0 | Malandrines.n3t [2011\$]

Secuela 9 – Gente infectada

*Sr contribuyente*

Detectamos en nuestro Sistema de Foto Multas de Tránsito (SFMT) 3 infracciones cometidas por su vehículo, debido a que usted no se notificó en el tribunal de faltas correspondiente, le reenviamos las Multas con sus respectivas fotos.

Si usted no regulariza las infracciones correspondientes en los próximos 15 días a partir de la fecha de emisión de este comunicado su vehículo será informado como deudor y pasará a formar parte del Veraz, conforme Ley n 11.481 de 6/09/2010.

To: [redacted]@hotmail.com
 Subject: Informe de deudas pendientes
 From: info@multasdetransito.gov.ar
 Date: Tue, 14 Feb 2012 21:02:22 -0800

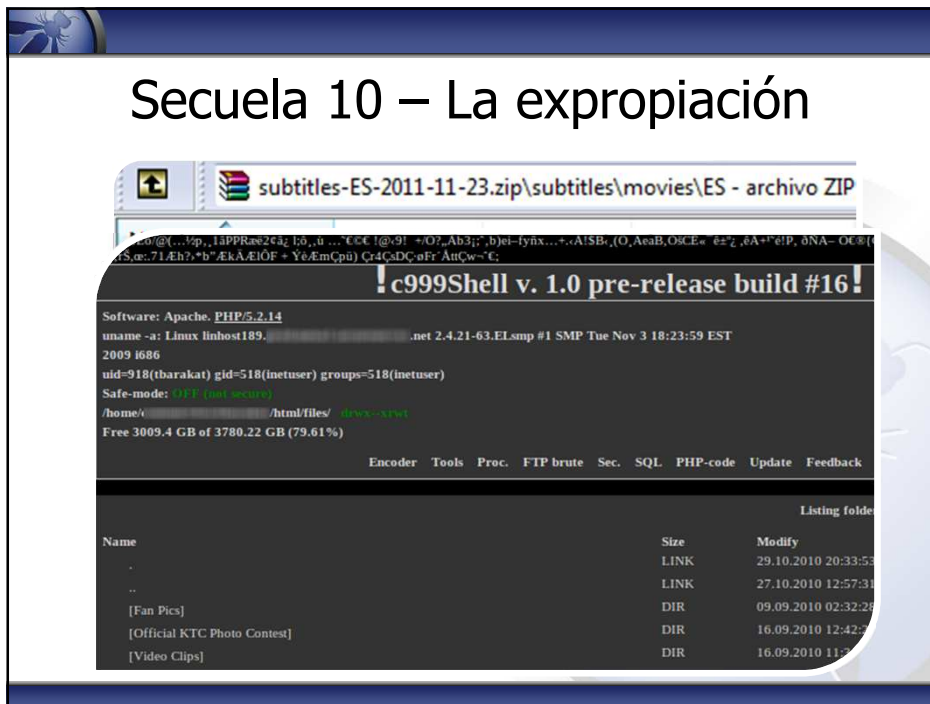
Miercoles 15 de Febrero del 2012, Republica Argentina
Estimado contribuyente:
 Detectamos en nuestro Sistema Integrado de Multas de tránsito (ATM) infracciones cometidas por su vehículo. Si usted no regulariza las infracciones correspondientes en los próximos 30 días a partir de la fecha de emisión de este comunicado, su vehículo será informado como deudor y usted pasará a formar parte del Veraz, conforme Ley n 19.216 de 1/12/2011. La inclusión de su vehículo en el Veraz le impedirá la venta regular de su vehículo en la Republica Argentina.

Infracciones al día 14/02/2012
[Girar a izquierda/derecha en lugar prohibido](#) - [No respetar Senda Peatonal/Paso Peaton](#) - [Exceso Velocidad hasta 20Km/h](#)

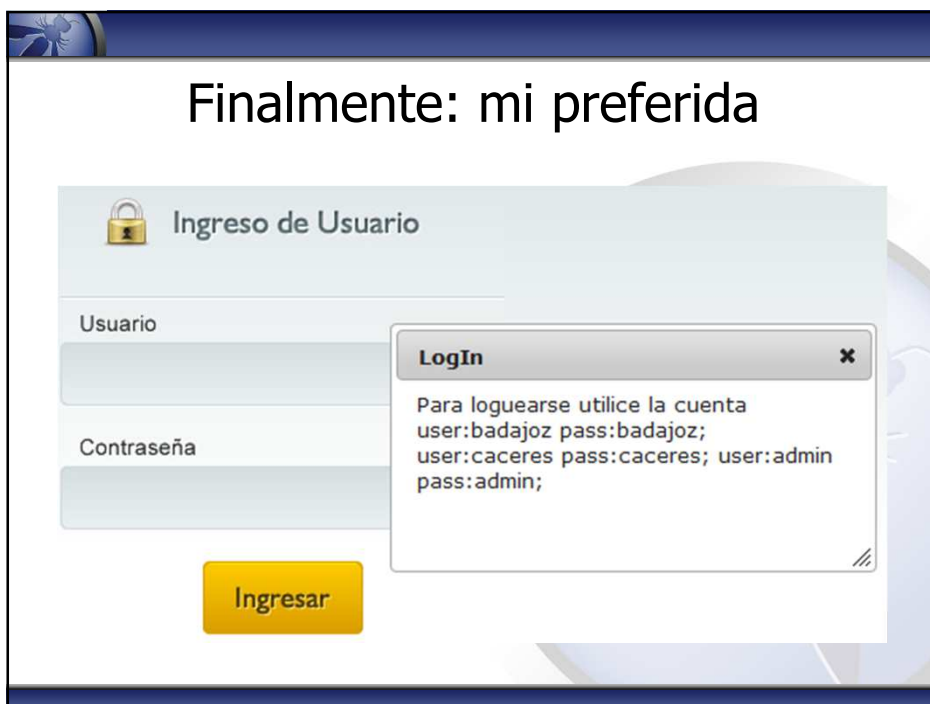
El propietario del vehículo queda notificado por este medio. Todas aquellas actas labradas con anterioridad a las fechas especificadas seguirán bajo la órbita de la Unidad Administrativa.

http://www.philipmorrisusa.com/redirect.ashx?url=http://www.orchmaXXX.be/para/photo/Informe_Deuda_PDF.exe

Secuela 10 – La expropiación



Finalmente: mi preferida





Lic. Cristian Borghello, CISSP - MVP

www.segu-info.com.ar

info@segu-info.com.ar

@seguinfo