



HERRAMIENTAS DE APRENDIZAJE OWASP

Erick Calderon Mostajo



OWASP

The Open Web Application Security Project



OWASP

The Open Web Application Security Project

- About Me
- Erick Calderon Mostajo
- www.communitysec.com
- Ingeniero de Sistemas
- CEH, CCNA, FCSNA
- Organizador 8.8 Bolivia
- @ev11r7u

8.8



OWASP

The Open Web Application Security Project

site:bo hacked by

Web

Imágenes

Videos

Noticias

Aproximadamente 446 resultados (0,35 segundos)



OWASP

The Open Web Application Security Project

Esta es la versión en caché de <http://www.yxfb.gob.bo/> de Google. Se trata de una captura de pantalla de la página tal como esta se mostraba el 25 Ago 2011 07:48:49 GMT. Es posible que la [página](#) haya sufrido modificaciones durante este tiempo. [Más información](#)

Estos términos sólo aparecen en enlaces que apuntan a esta página: [Versión de solo texto yxfb](#)

...:[OWN3D BY P1NCh05]:..

...:[ANONYMOUS BOLIVIA]:..





OWASP

The Open Web Application Security Project

Viva Chile **culiao!**

nunca tendran mar!



by volde & elweonfome :D
chilean hackers was here!

CENSURADO

ROTOS de **CENSURADO**
TRÁGUENSE SU MAR!

- Hacked By : @BoliviaNextHackers

- Credits : ToxicDz & N3v3rn0r3



OWASP

The Open Web Application Security Project



- map.ipviking.com



OWASP

The Open Web Application Security Project

“Es solo una Guerra de globos con agua”

By: Boris Murillo





OWASP

The Open Web Application Security Project



Your computer has been locked, downloading and distribution.

Mentioned illegal content (414 Mb of classified as child pornographic material, violate following U.S. Federal Law 18 U.S.C. § 2251- Sexual Exploitation pornography) 18 U.S.C. § 2252- Certain activities sexual exploitation of minors (Pornography) 18 U.S.C. § 2252A- certain activities containing child pornography

Any individual who violates, or at violate mentioned laws shall be imprisoned from 4 to 30 years

Technical details:

Involved IP address: [redacted]
Involved host name: [redacted]
Source or intermediary sites:

All suspicious files from your computer server and shall be used as evidence to unblock your account in an unauthorized manner.

Your case can be classified as occurring under 17 (U. S. Code) § 512. Thus it may be that your computer will be unblocked automatically.

In order to resolve the situation you should pay a fine of \$300.



Aprobado y Protegido por



IP: [redacted]

País: BO Bolivia
Región: La Paz
Ciudad: La Paz
ISP: [redacted]
Sistema Operativo: Windows XP (32-bit)
Nombre de Usuario: [redacted]



¡ATENCIÓN! Su OP (ordenador) está bloqueado debido a al menos una de las razones especificadas siguientes.

Usted ha violado «el derecho de autor y los derechos conexos» (vídeos, música, software) y ha utilizado de una manera ilegal con la distribución de contenido los derechos de autor, infringiendo así el artículo 128 del Criminal Code del Estado Plurinacional de Bolivia.

El artículo 128 del Criminal Code prevé una multa 200 a 500 de los salar... -00 = privación de la libertad de 2 a 8 años.

Usted ha visto o distribuido el contenido prohibido pornográfico (porno infantil/zoofilia y etc), violando así el artículo 202 del Criminal Code del Estado Plurinacional de Bolivia. El artículo 202 del Criminal Code prevé la privación de la libertad de 4 a 12 años.

El acceso ilegal al contenido prohibido se ha iniciado desde su OP (ordenador), o usted había sido...

UKASH Código PIN Suma

1 2 3 4 5 6 7 8 9 0

Pagar Ukash

¿Dónde puedo comprar Ukash?

Ukash está disponible en numerosos locales de venta en todo el país. Simplemente diríjase a uno de ellos y cambie su dinero en efectivo por cupones Ukash con su pin único de 15 dígitos, venta en todo el país. Simplemente diríjase a una venta en todo el país. Simplemente diríjase a una venta en todo el país. Simplemente diríjase a una venta en todo el país.



Deligro - Obtener Ukash en tiendas Deligro de toda Bolivia.

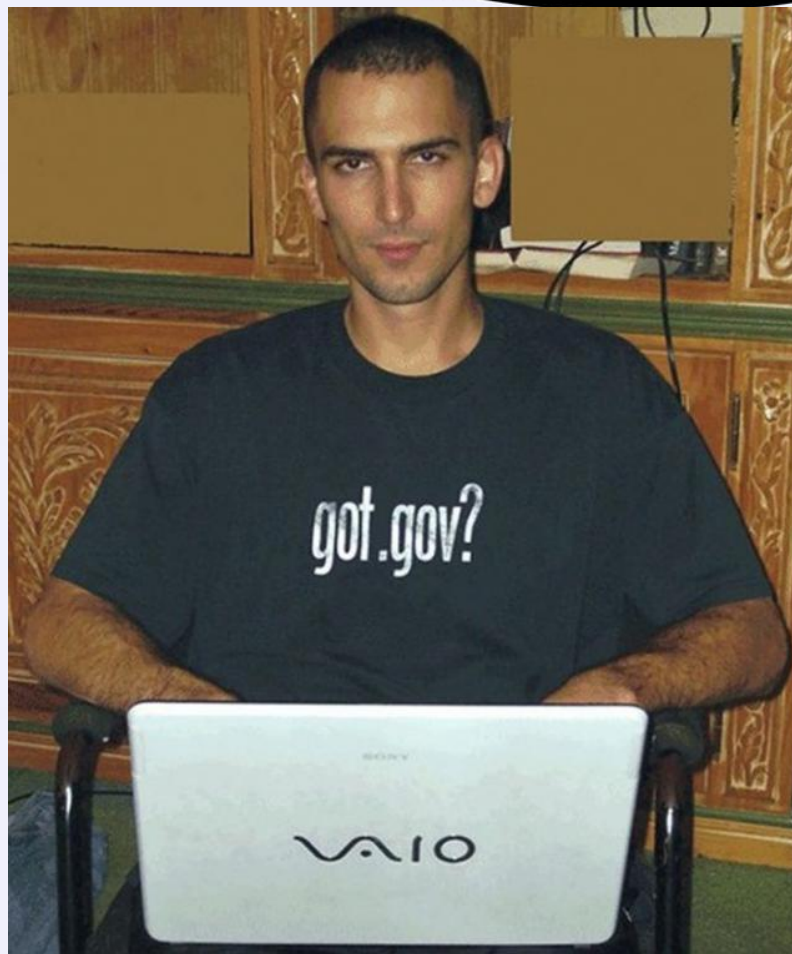




OWASP

The Open Web Application Security Project

RUSIA VS ESTONIA *Dmitri Galushkevich*





OWASP

The Open Web Application Security Project

- Operación Aurora – China vs USA (Google)

```
00 00 00 00 00 00 F0 3F 00 00 00 00 00 00 20 40 .....?..... @
00 01 80 46 75 3D A7 3F D4 8B 0A 3F 15 EF C3 3E ...Fu=?.?...>
F3 04 35 3F 00 00 00 00 00 00 00 00 00 00 00 00 ..5?.....
65 2B 30 30 30 00 00 00 00 00 00 00 C0 7E 01 50 41 e+000.....~.PA
00 00 00 80 FF FF 47 41 49 73 50 72 6F 63 65 73 .....GAIIsProces
73 6F 72 46 65 61 74 75 72 65 50 72 65 73 65 6E sorFeaturePresen
74 00 00 00 4B 45 52 4E 45 4C 33 32 00 00 00 00 t...KERNEL32...
31 23 51 4E 41 4E 00 00 31 23 49 4E 46 00 00 00 1#QNaN..1#INF...
31 23 49 4E 44 00 00 00 31 23 53 4E 41 4E 00 00 1#IND...1#SNAN..
52 53 44 53 91 82 FE 94 29 AB E5 42 A6 53 10 A8 RSDS....).B.S..
D2 04 69 98 10 00 00 00 66 3A 5C 41 75 72 6F 72 ...i.....f:\Auror
61 5F 53 72 63 5C 41 75 72 6F 72 61 56 4E 43 5C a_Src\Aurora\VNC\
41 76 63 5C 52 65 6C 65 61 73 65 5C 41 56 43 2E Avc\Release\AVC.
70 64 62 00 94 4D 03 10 00 00 00 00 00 00 00 00 pdb..M.....
FF FF FF FF 00 00 00 00 00 00 00 00 54 21 03 10 .....T!...
00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 .....
```

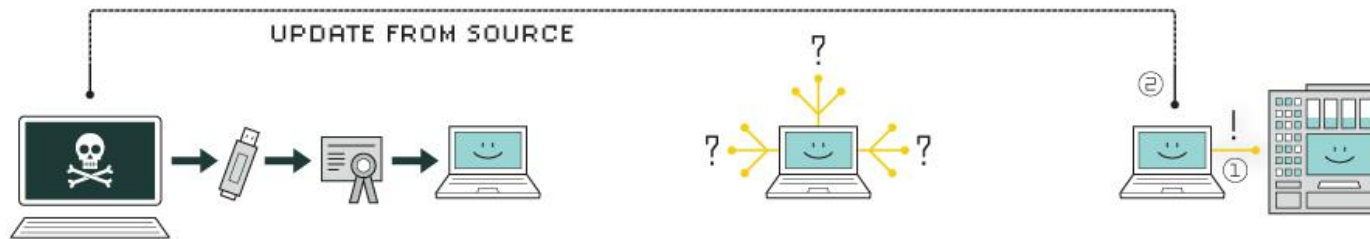


OWASP

The Open Web Application Security Project

USA vs Iran - STUXNET

HOW STUXNET WORKED



1. infection

Stuxnet enters a system via a USB stick and proceeds to infect all machines running Microsoft Windows. By brandishing a digital certificate that seems to show that it comes from a reliable company, the worm is able to evade automated-detection systems.

2. search

Stuxnet then checks whether a given machine is part of the targeted industrial control system made by Siemens. Such systems are deployed in Iran to run high-speed centrifuges that help to enrich nuclear fuel.

3. update

If the system isn't a target, Stuxnet does nothing; if it is, the worm attempts to access the Internet and download a more recent version of itself.



4. compromise

The worm then compromises the target system's logic controllers, exploiting "zero day" vulnerabilities—software weaknesses that haven't been identified by security experts.



5. control

In the beginning, Stuxnet spies on the operations of the targeted system. Then it uses the information it has gathered to take control of the centrifuges, making them spin themselves to failure.



6. deceive and destroy

Meanwhile, it provides false feedback to outside controllers, ensuring that they won't know what's going wrong until it's too late to do anything about it.



OWASP

The Open Web Application Security Project



- Que Hacer??





OWASP

The Open Web Application Security Project

**DO ~~NOT~~ TRY THIS
AT HOME!**



OWASP

The Open Web Application Security Project





OWASP

The Open Web Application Security Project

OWASP PROJECTS

INACTIVE OWASP PROJECT



OWASP

Open Web Application
Security Project

OWASP Broken Web Applications Project

OWASP Broken Web Applications Project is...

Introduction

A collection of vulnerable web applications that is distributed on a Virtual Machine.



Chuck Willis

What is Broken Web Applications Project?

OWASP Broken Web Applications Project provides:

- A collection of purposefully vulnerable applications to safely practice penetration testing.



OWASP

The Open Web Application Security Project



owaspbwa

OWASP Broken Web Applications Project

This is the VM for the [Open Web Application Security Project \(OWASP\) Broken Web Applications](#) project. It contains many, very vulnerable web applications, which are listed below. More information about this project can be found in the project [User Guide](#) and [Home Page](#).

For details about the known vulnerabilities in these applications, see <http://sourceforge.net/apps/trac/owaspbwa/report/1>.



!!! This VM has many serious security issues. We strongly recommend that you run it only on the "host only" or "NAT" network in the virtual machine settings !!!

```
Welcome to the OWASP Broken Web Apps VM
```

```
!!! This VM has many serious security issues. We strongly recommend that you run  
it only on the "host only" or "NAT" network in the VM settings !!!
```

```
You can access the web apps at http://192.168.133.128/
```

```
You can administer / configure this machine through the console here, by SSHing  
to 192.168.133.128, via Samba at \\192.168.133.128\, or via phpmyadmin at  
http://192.168.133.128/phpmyadmin.
```

```
In all these cases, you can use username "root" and password "owaspbwa".
```


Sistemas Operativos



OWASP

The Open Web Application Security Project





OWASP

The Open Web Application Security Project



HackBar 1.6.3

by Johan Adriaans, Pedro Laguna



FoxyProxy Standard 4.5.4

por Eric H. Jung, groeg, Jesper Staun Hansen



Firebug 2.0.9

SIN REINICIAR

por Joe Hewitt, Jan Odvarko, robcee, Fi

Firebug integrates with Firefox to



BROWSER

ANATOMIA DO PROGRAMADOR

Informaticus programatorum

Oculos "Twilight Zone" - São necessários devido aos dias passados em frente ao monitor.

Cabelo e barba estilo desleixo - Não dá tempo para cortes de pelagem.

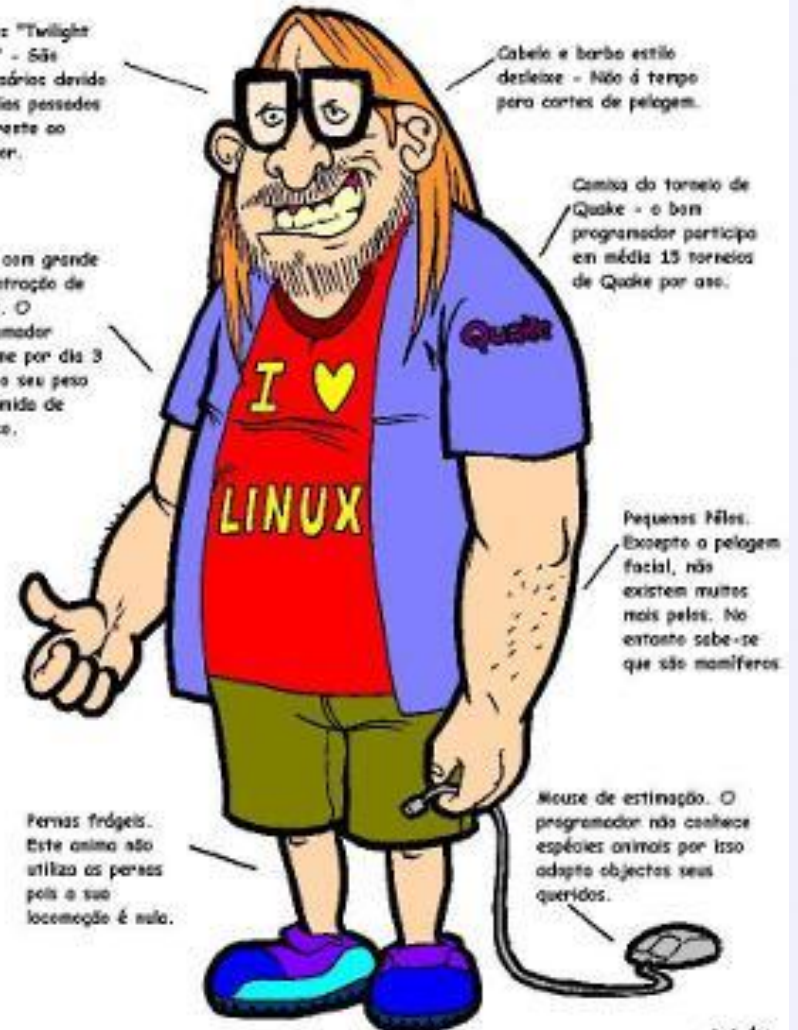
Camisa do torneio de Quake - o bom programador participa em média 15 torneios de Quake por ano.

Corpo com grande concentração de lípidos. O programador consome por dia 3 vezes o seu peso em comida de plástico.

Pequenos pêlos. Exceto a pelagem facial, não existem muitos mais pelos. No entanto sabe-se que são mamíferos.

Pernas frágeis. Este animal não utiliza as pernas pois a sua locomoção é nula.

Mouse de estimação. O programador não conhece espécies animais por isso adapta objectos seus queridos.





OWASP

The Open Web Application Security Project



**KEEP
CALM
AND
LET'S
HACK**

© 2013 KeepCalmStudio.com



OWASP

The Open Web Application Security Project

- www.communitysec.com
- <http://www.elladodelmal.com/2013/01/incidentes-de-ciberguerra-y.html>
- https://www.owasp.org/index.php/OWASP_Broken_Web_Applications_Project
- www.dvwa.co.uk



OWASP

The Open Web Application Security Project



DANKSCHEEN
 SPASSIBO DANKSCHEEN
 NUHUN SNACHALHUYA
 CHALTU YAQHANYELAY
 TASHAKKUR ATU
 WAABEEJA MAITEKA YUSPAGARATAM
 DHANYABAD WAABEEJA MAITEKA YUSPAGARATAM
 ANBHA SUKSAMA HUI
 UNALCHEESH
 HATUR E
 MERSI SPASIBO DENKAUJA
 NENACHALHYA
 EKOJU SIKOMO
 MAKETRI
 MINMONCHAR
 TINGKI BIYAN SHUKRIA
 GRACIAS
 ARIGATO
 SHUKURIA
 TAVTAPUCH MEDAWAGSE
 BAIWA JUSPAXAR
 GOZAIMASHITA
 EFCHARISTO AGUYJE
 FAKAAUE
 KOMPASUMNIDA
 SAICO
 MERASTAWHY
 GAEJTHO
 LAH
 MAAKE
 GRAZIE
 MEHRBANI
 PALDIES
 YOU
 BOLZIN
 MERCI