WordPress

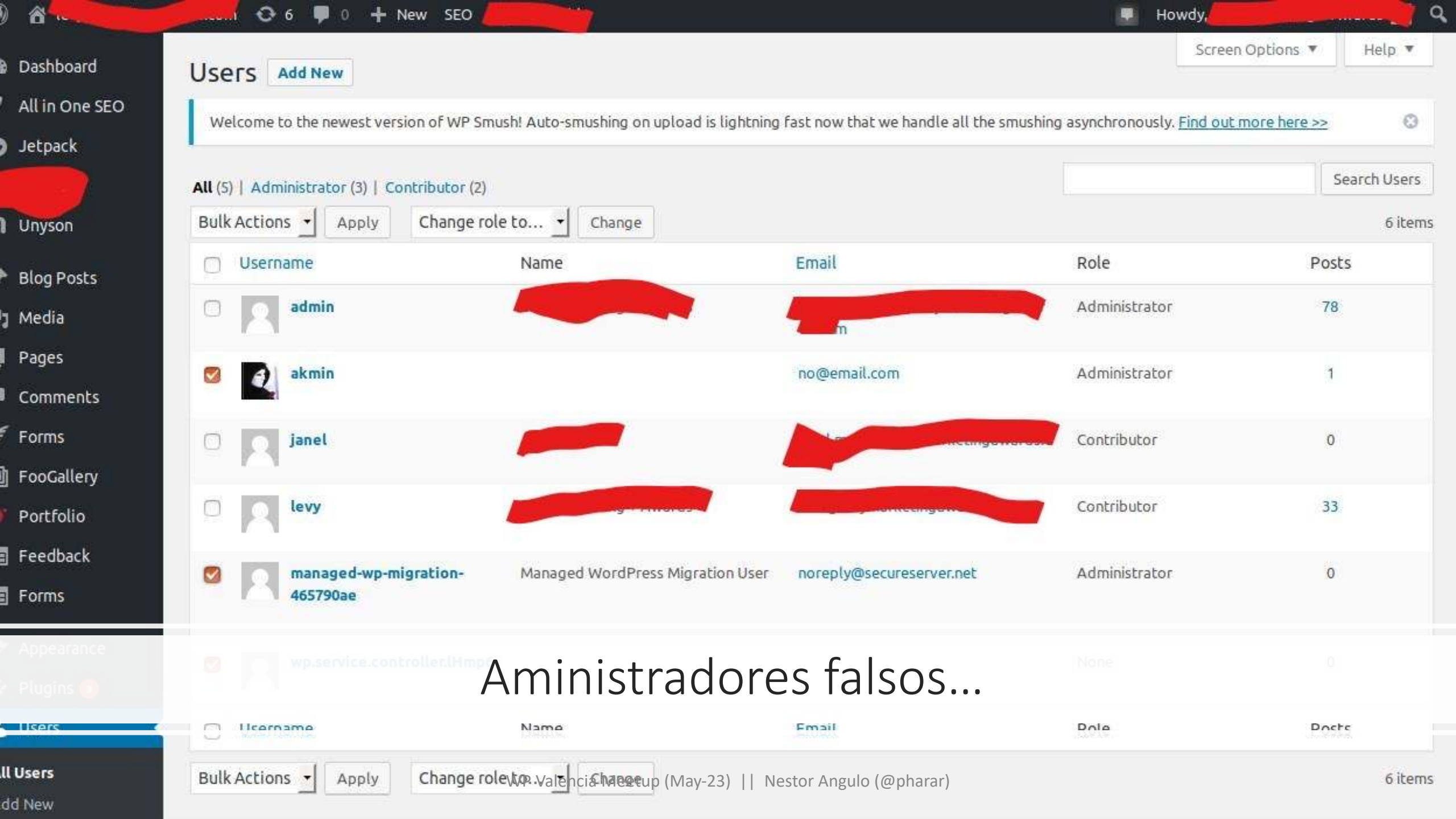
Limpiar sitios WordPress hackeados

Trucos y ejemplos

¿Quién soy?

- **CISSP** (ISC2.org - 2022)
- **Web Security Analyst** (2015-2023)
  @GoDaddy WebSecurity
  @sucuri.net
- **Software Engineer (2023)**
  & Brand Ambassador

patchstack



Aministradores falsos...

Current Revision by
3 months ago (4 Mar @ 09:03)

Restore This Revision

Title

```
Hacked By BALA SNIPER
```

```
Hacked By GeNErAL
```

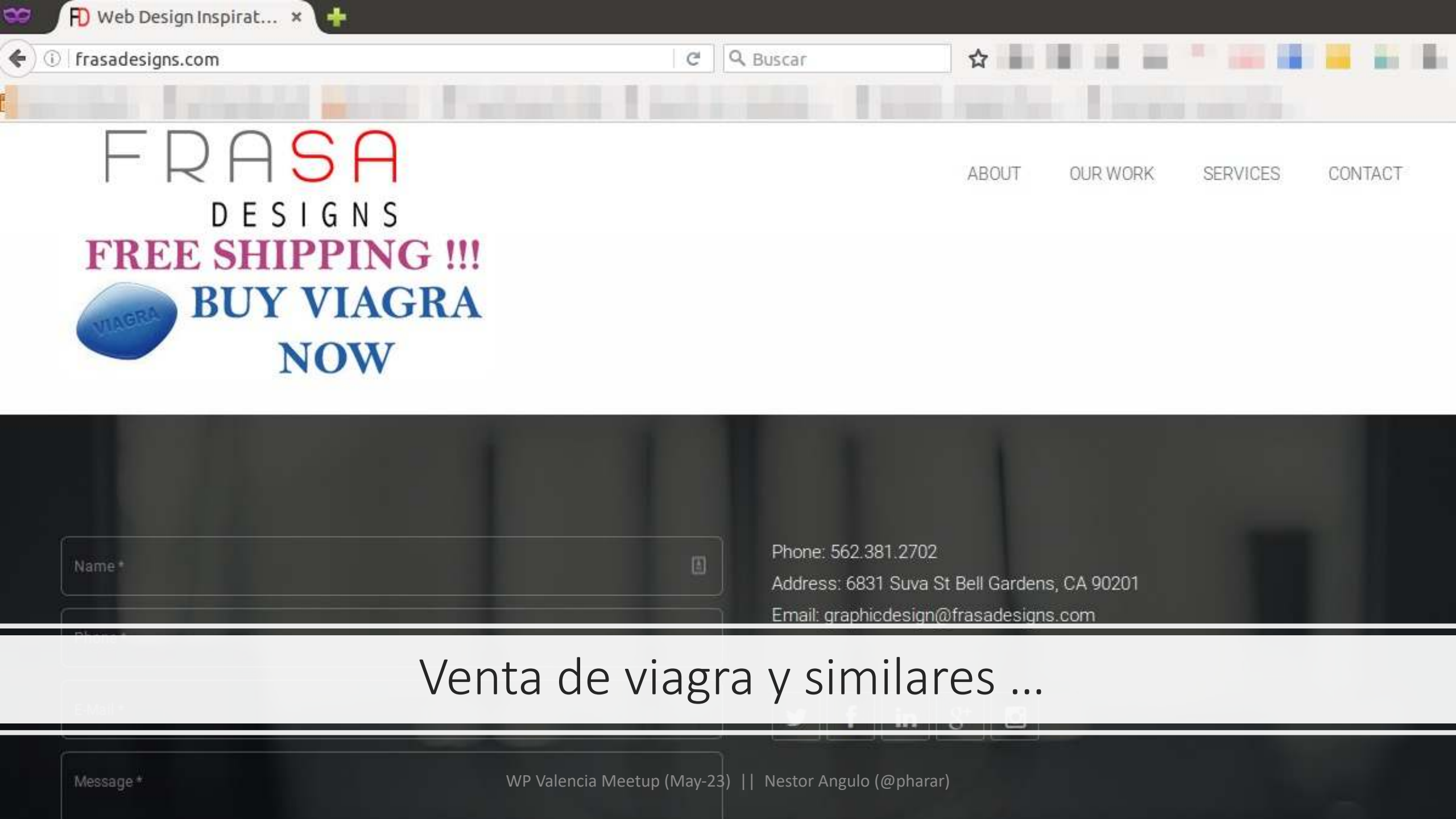
Content

```
<p>Hacked By BALA SNIPER<br />
 Kurdish Hacker Here<br />
 If you want Fix Problem Website &#8230; !<br />
 Contact Me via Gmail : darinsniper007@ gmail.com<br />
 Contact Me Via Facebook : https://www.facebook.com
/balasniper007 </p>
```

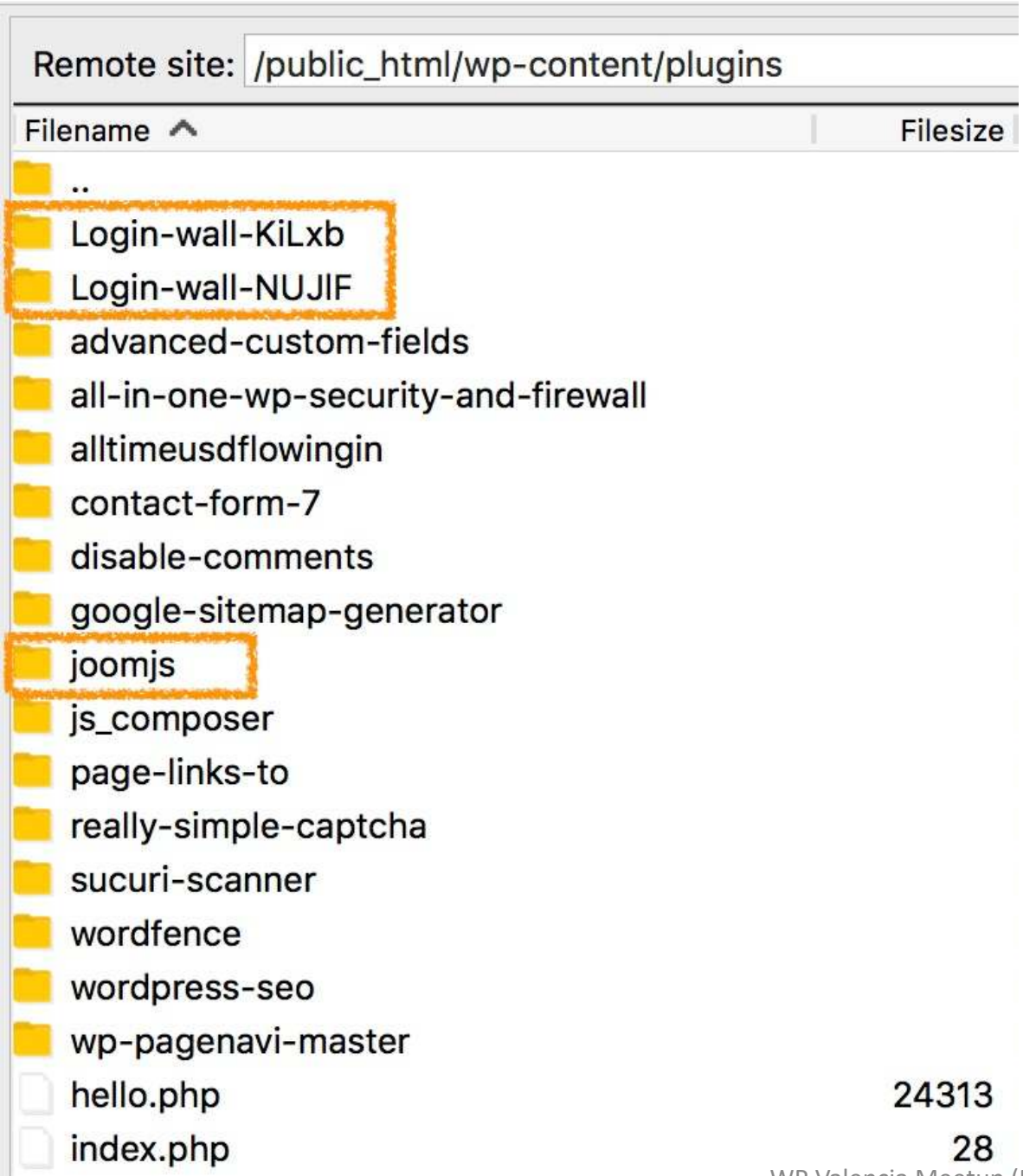
```
<title>~!Hacked By GeNErAL alias Mathis!~</title>
<h2>Hacked By GeNErAL</h2> </font></p><img
border='0' src='http://www.officialpsds.com/images/thumbs
/Baby-Devil-Toon-psd9848.png'><br><br><br><b>Greetz :
Kuroi'SH, RxR, ~ </b><br><br></FOOTER><b><code>
<h1>\!/Just for Fun ~Hacked By GeNErAL\!/</code>
</b></p align='center'><font color='red' /><font
size='5' color='#FF0000'>Hacked By
GeNErAL! !</font></font></p>
```

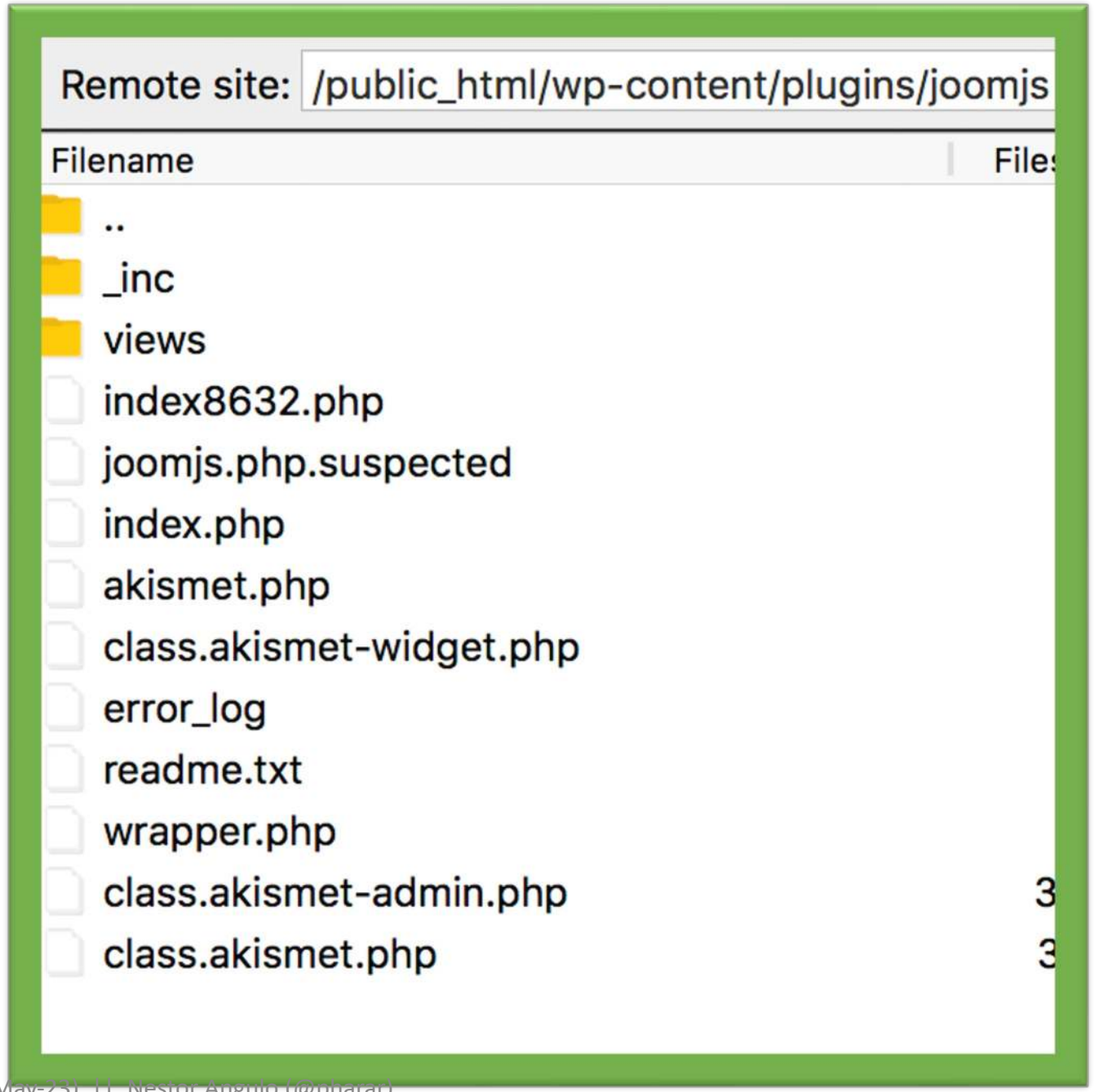
Tus post cambian…

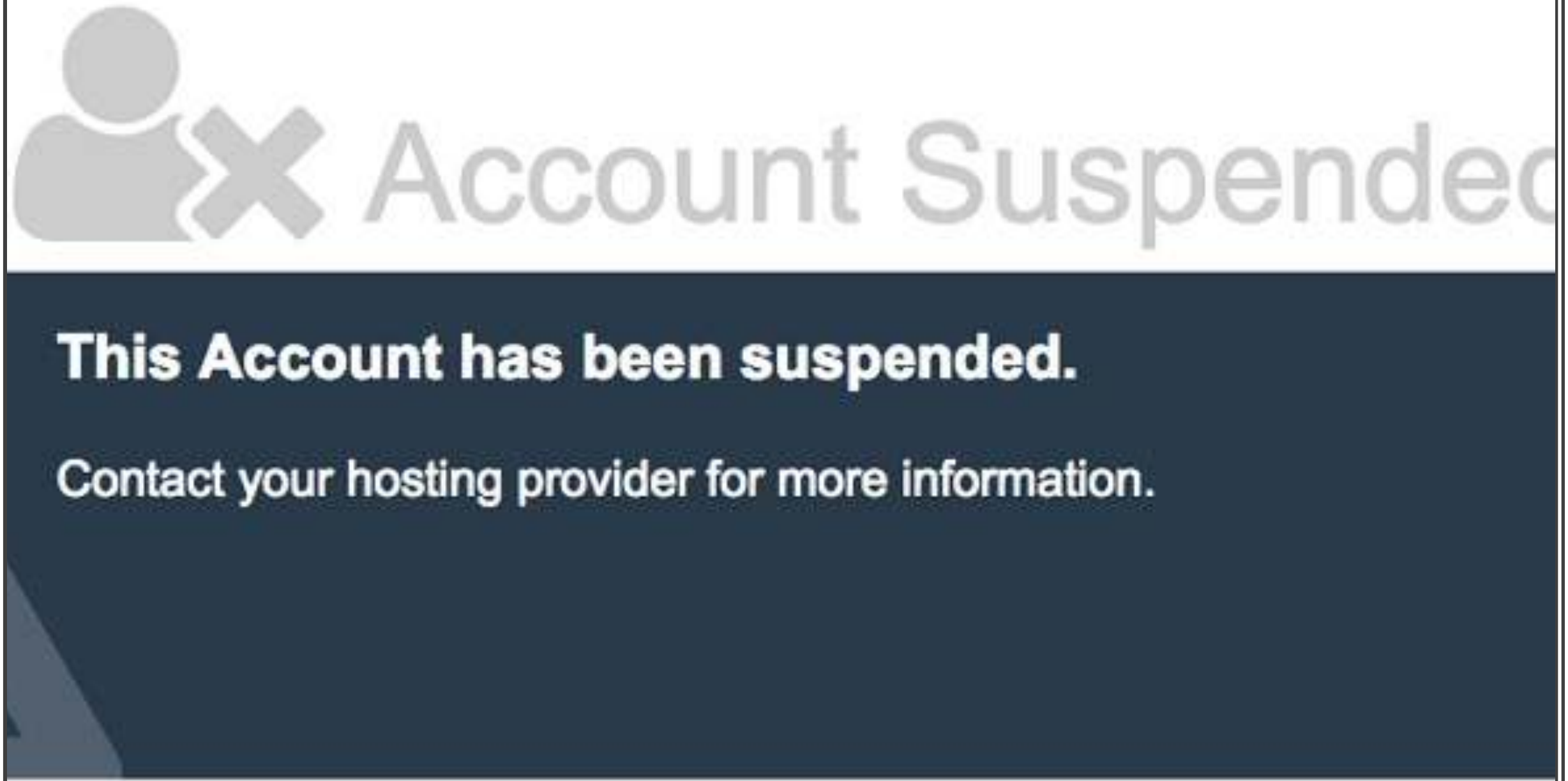
Aparece una portada ”ligeramente” diferente…

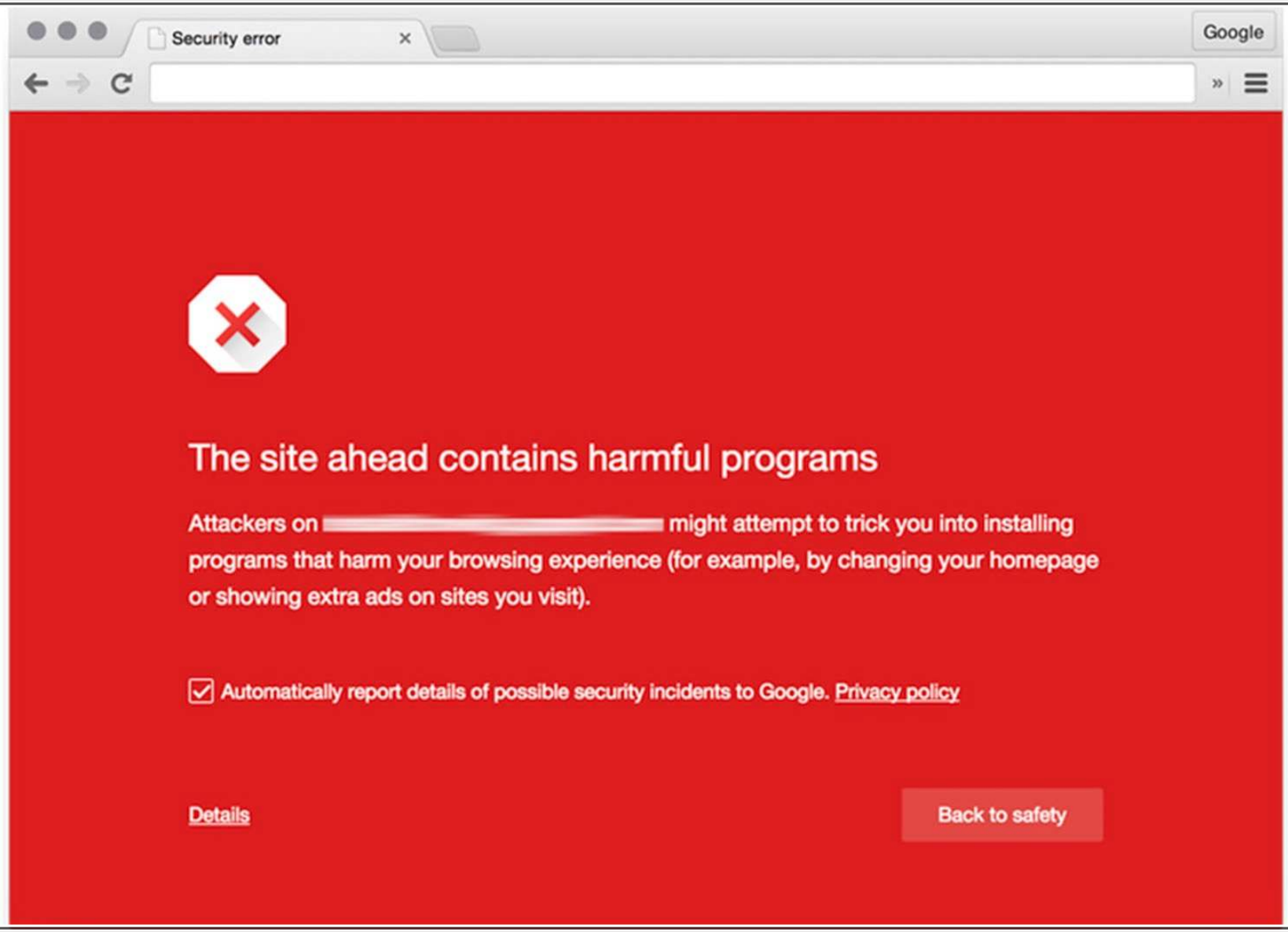


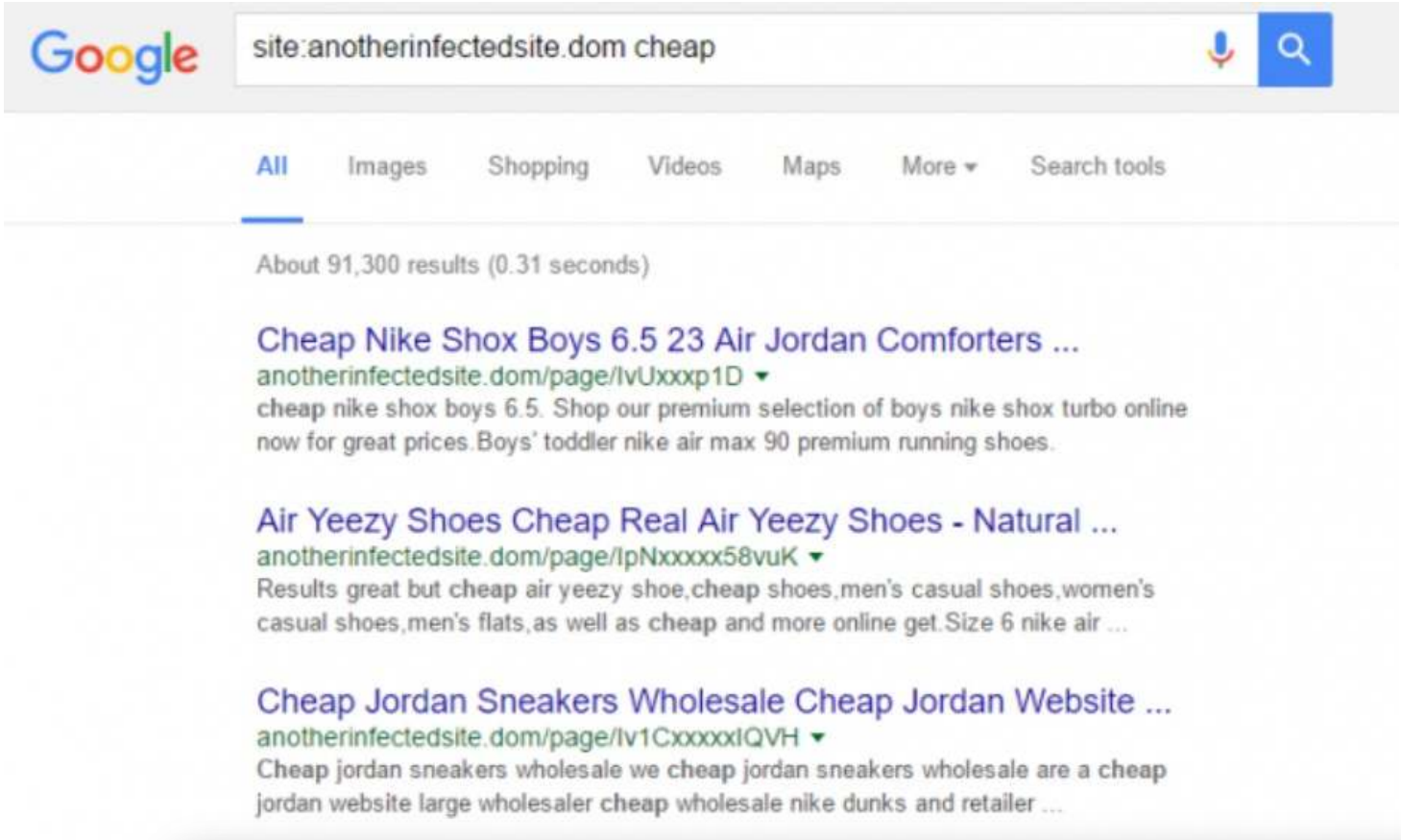
Venta de viagra y similares …

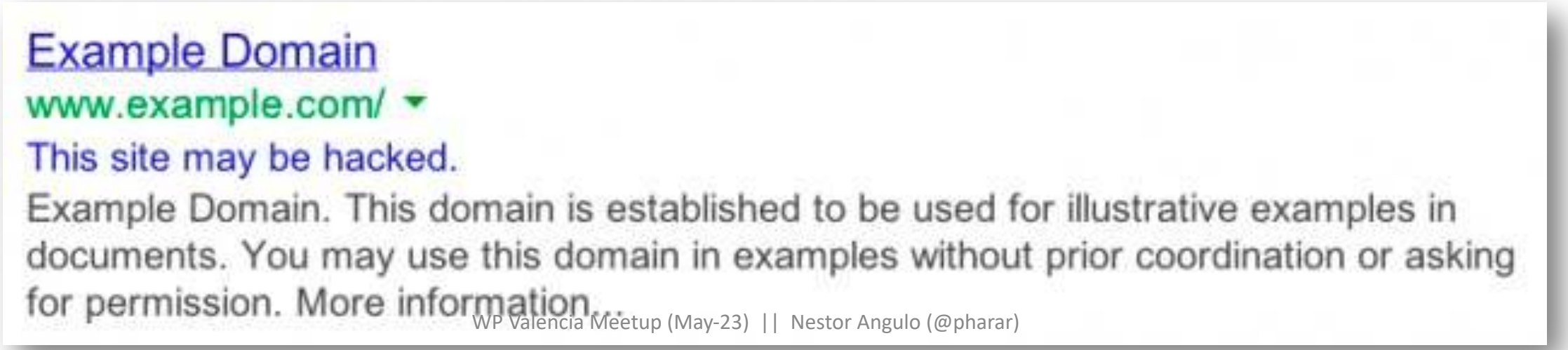

Remote site: /public_html/wp-content/plugins
Filename
Filesize
..
Login-wall-KiLxb
Login-wall-NUJlF
advanced-custom-fields
all-in-one-wp-security-and-firewall
alltimeusdflowingin
contact-form-7
disable-comments
google-sitemap-generator
joomjs
js_composer
page-links-to
really-simple-captcha
sucuri-scanner
wordfence
wordpress-seo
wp-pagenavi-master
hello.php 24313
index.php 28

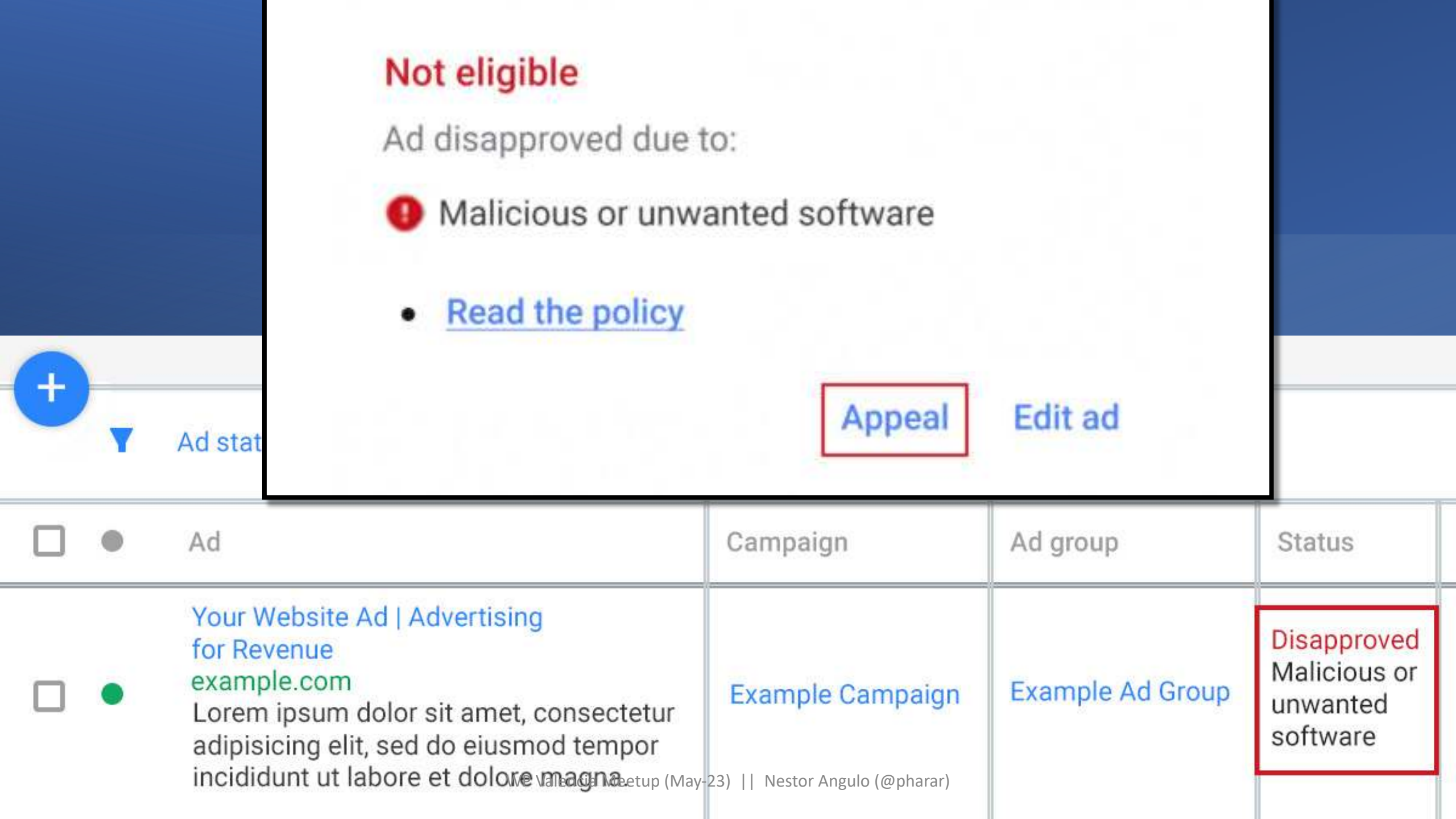

Remote site: /public_html/wp-content/plugins/joomjs
Filename
..
_inc
views
index8632.php
joomjs.php.suspected
index.php
akismet.php
class.akismet-widget.php
error_log
readme.txt
wrapper.php
class.akismet-admin.php
class.akismet.php

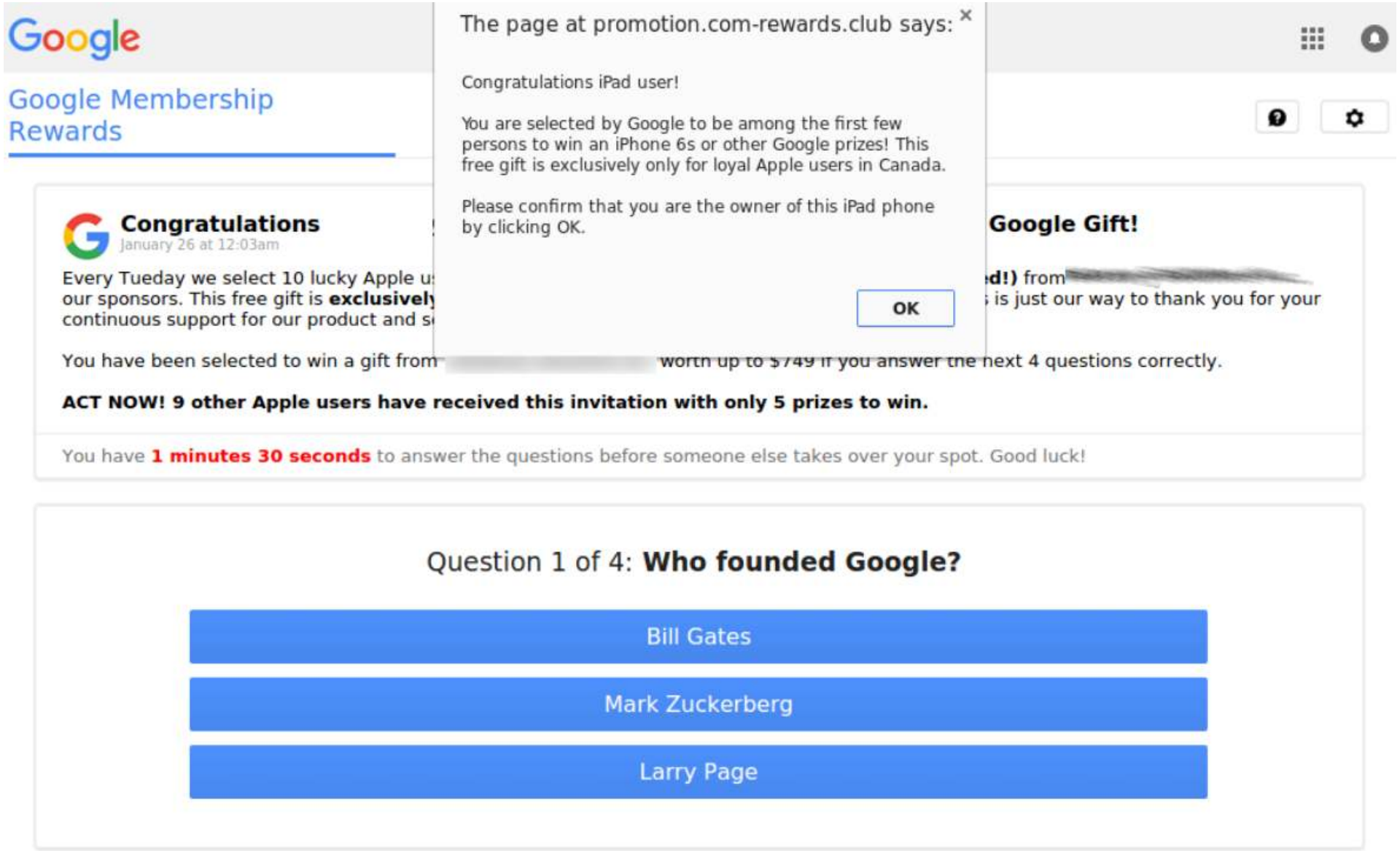

Account Suspended
This Account has been suspended.
Contact your hosting provider for more information.

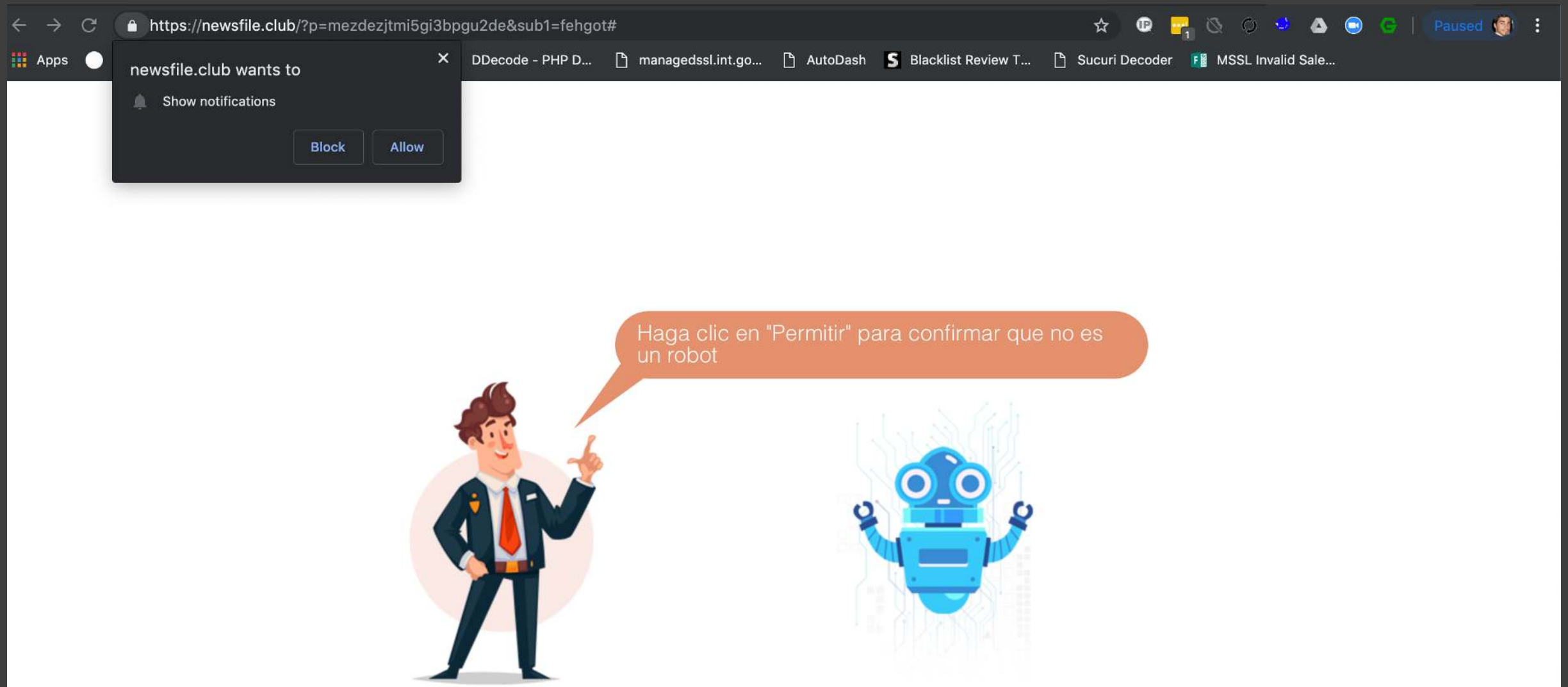

Security error
Google
The site ahead contains harmful programs
Attackers on [redacted] might attempt to trick you into installing programs that harm your browsing experience (for example, by changing your homepage or showing extra ads on sites you visit).
Automatically report details of possible security incidents to Google. Privacy policy
Details
Back to safety


Google
site:anotherinfectedsite.dom cheap
All
Images
Shopping
Videos
Maps
More
Search tools
About 91,300 results (0.31 seconds)
Cheap Nike Shox Boys 6.5 23 Air Jordan Comforters ...
anotherinfectedsite.dom/page/IvUxxxp1D
cheap nike shox boys 6.5. Shop our premium selection of boys nike shox turbo online now for great prices.Boys' toddler nike air max 90 premium running shoes.
Air Yeezy Shoes Cheap Real Air Yeezy Shoes - Natural ...
anotherinfectedsite.dom/page/IpNxxxxx58vuK
Results great but cheap air yeezy shoe,cheap shoes,men's casual shoes,women's casual shoes,men's flats,as well as cheap and more online get.Size 6 nike air ...
Cheap Jordan Sneakers Wholesale Cheap Jordan Website ...
anotherinfectedsite.dom/page/Iv1CxxxxxIQVH
Cheap jordan sneakers wholesale we cheap jordan sneakers wholesale are a cheap jordan website large wholesaler cheap wholesale nike dunks and retailer ...


Example Domain
www.example.com/
This site may be hacked.
Example Domain. This domain is established to be used for illustrative examples in documents. You may use this domain in examples without prior coordination or asking for permission. More information...


Not eligible
Ad disapproved due to:
Malicious or unwanted software
Read the policy
Appeal
Edit ad
Ad stat
Ad
Campaign
Ad group
Status
Your Website Ad | Advertising for Revenue
example.com
Lorem ipsum dolor sit amet, consectetur adipisicing elit, sed do eiusmod tempor incididunt ut labore et dolore magna
Example Campaign
Example Ad Group
Disapproved
Malicious or unwanted software


Google
Google Membership Rewards
The page at promotion.com-rewards.club says:
Congratulations iPad user!
You are selected by Google to be among the first few persons to win an iPhone 6s or other Google prizes! This free gift is exclusively only for loyal Apple users in Canada.
Please confirm that you are the owner of this iPad phone by clicking OK.
OK
Congratulations
January 26 at 12:03am
Google Gift!
Every Tueday we select 10 lucky Apple u
our sponsors. This free gift is exclusively
continuous support for our product and s
d!) from
is just our way to thank you for your
You have been selected to win a gift from
worth up to $749 if you answer the next 4 questions correctly.
ACT NOW! 9 other Apple users have received this invitation with only 5 prizes to win.
You have 1 minutes 30 seconds to answer the questions before someone else takes over your spot. Good luck!
Question 1 of 4: Who founded Google?
Bill Gates
Mark Zuckerberg
Larry Page


https://newsfile.club/?p=mezdezjtmi5gi3bpgu2de&sub1=fehgot#
Paused
Apps
DDecode - PHP D...
managedssl.int.go...
AutoDash
Blacklist Review T...
Sucuri Decoder
MSSL Invalid Sale...
newsfile.club wants to
Show notifications
Block
Allow
Haga clic en "Permitir" para confirmar que no es un robot

CONCLUSIÓN

- E-commerce con uso normal:
  - **Beneficios**: 50.000€ - 100.000€
- Hackeado
  - **Pérdidas**: - (270.000€ - 300.000€)

- **Coste de medidas de seguridad** -> 500€ - 1.000€

#WCGriñón

WORDCAMP GRIÑÓN

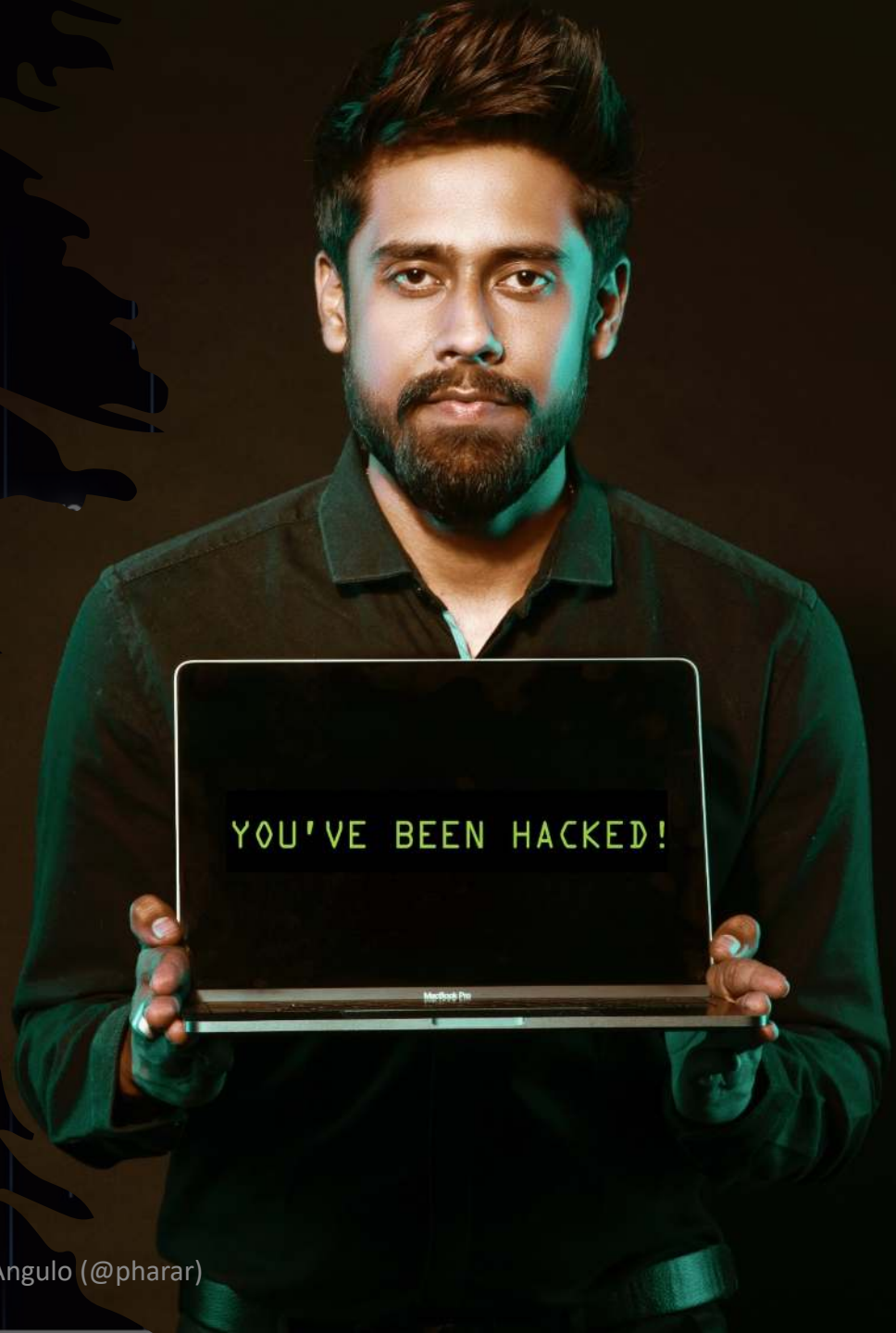

BOTNET
SPAM
PHISHING
HACKER
MALWARE
DDOS
KEYLOGGER
VIRUS
SPYWARE

La Policía en tu casa….

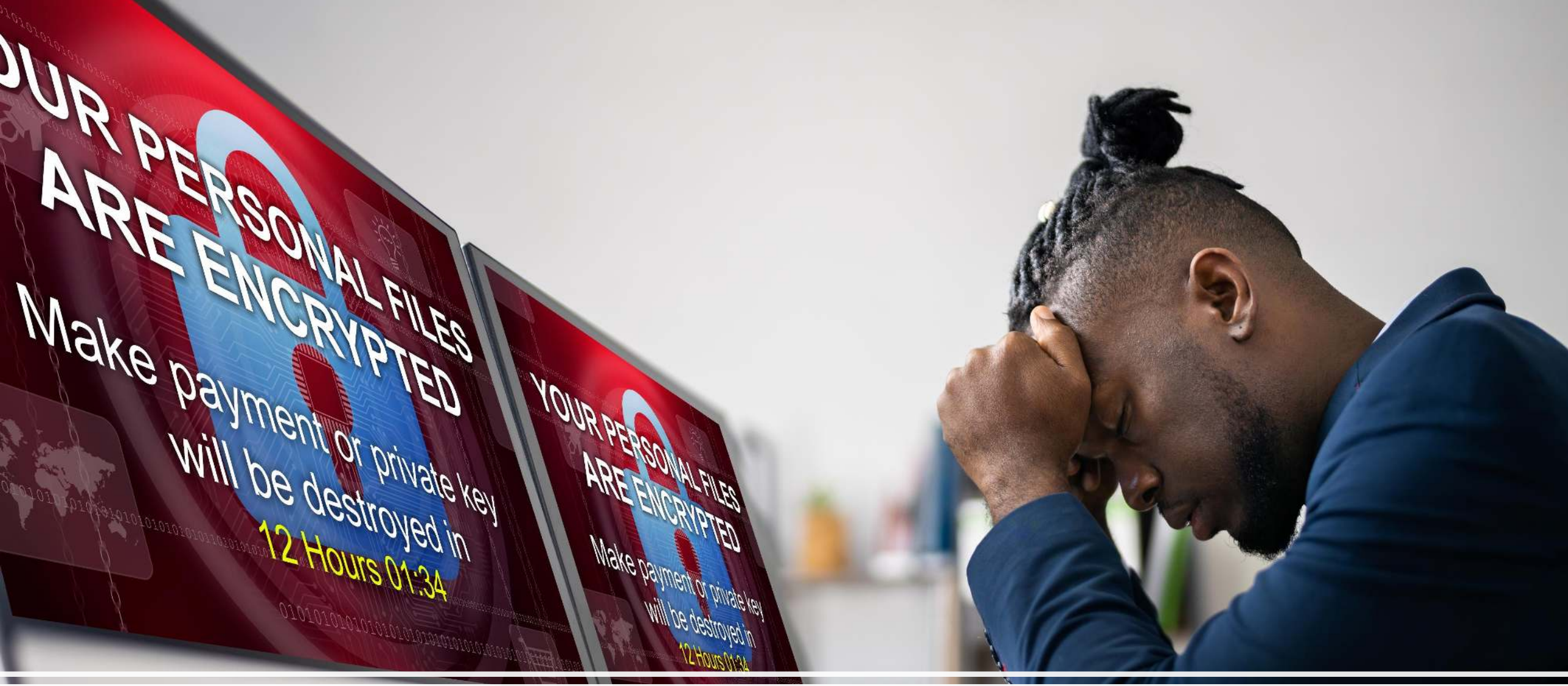
HackedÃ,Â ByÃ,Â JakRa

kanã,â beraniã,â matiã,â |ã,â indonesianã,â

Tidak ada seorangpun, hewan atau banci yang disakiti dalam hacking ini
Jiwa Kegelapan Team



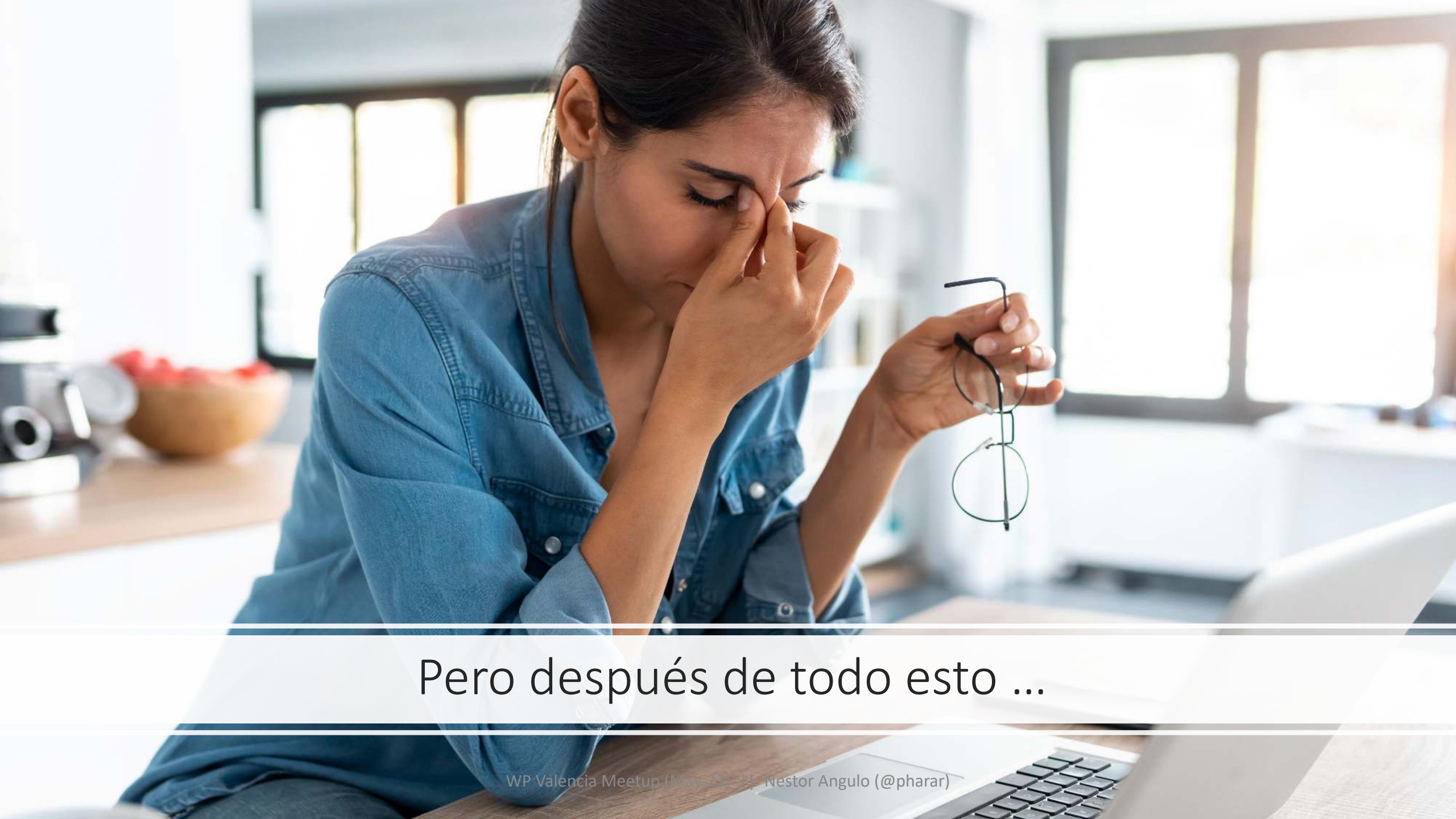
OHMMMMMM


OUR PERSONAL FILES
ARE ENCRYPTED
Make payment or private key
will be destroyed in
12 Hours 01:34
YOUR PERSONAL FILES
ARE ENCRYPTED
Make payment or private key
will be destroyed in
12 Hours 01:34

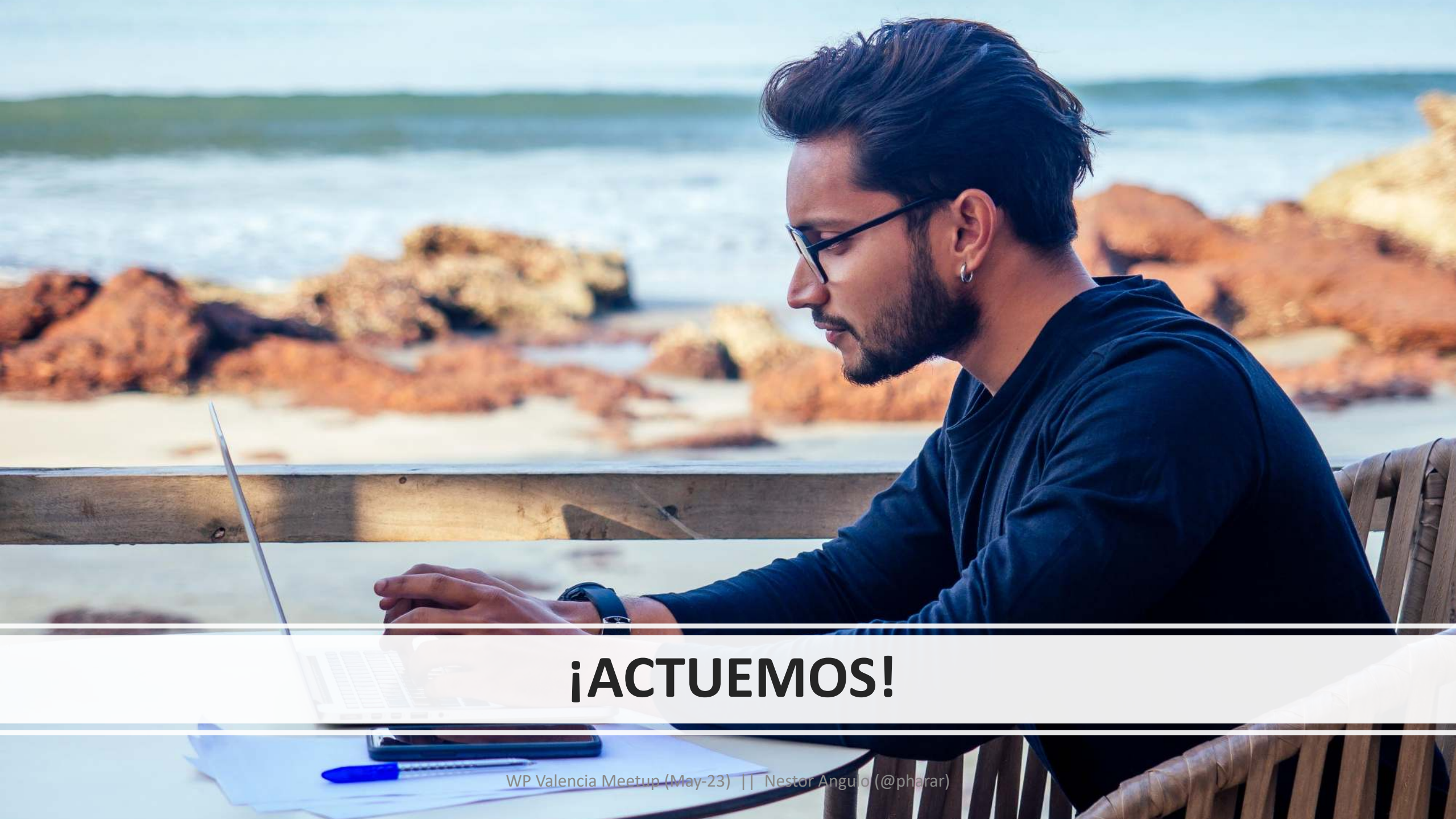
Si, lo sé …

¡GRITEMOS!

Es aceptable sentirse hecho polvo…

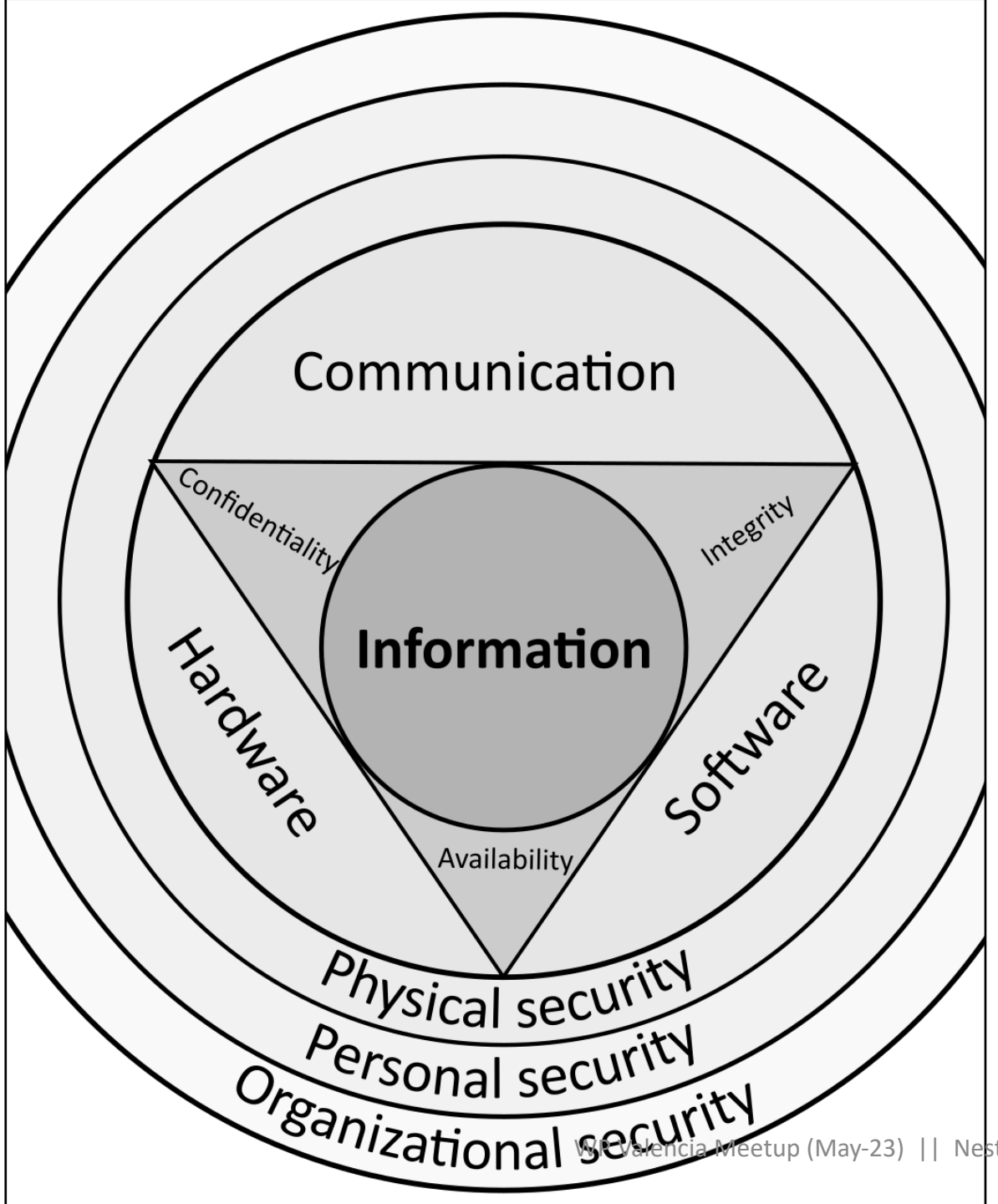


Pero después de todo esto …



¡ACTUEMOS!

Primero… **Conceptos**



Qué es la Seguridad de Información

Concepto CID (CIA)

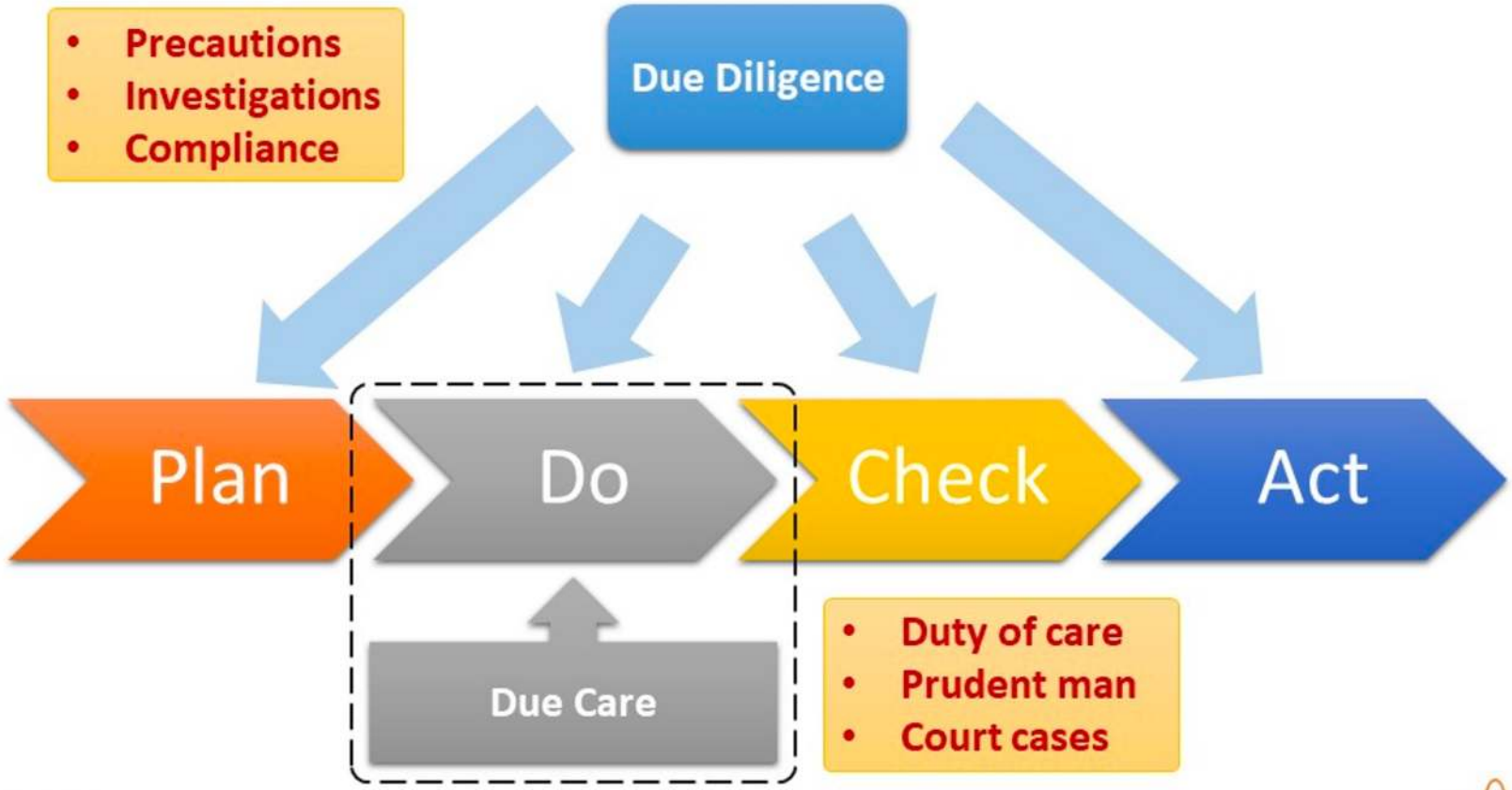
- Confidencialidad
- Integridad
- Disponibilidad

Concepto FAD (DAD)

- Filtración
- Alteración
- Destrucción

Ser diligente y tomar acciones

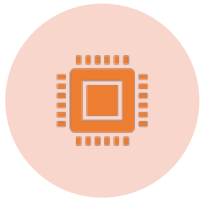
Due Diligence and Due Care



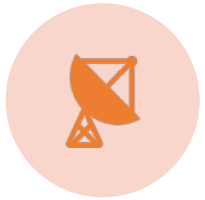
DOMINIOS en ciberseguridad según CISSP

Seguridad y gestión de riesgos (Security and Risk Management)

Seguridad de activos (Asset Security)



Arquitectura de seguridad e ingeniería (Security Architecture and Engineering)



Comunicación y seguridad de red (Communications & Network Security)

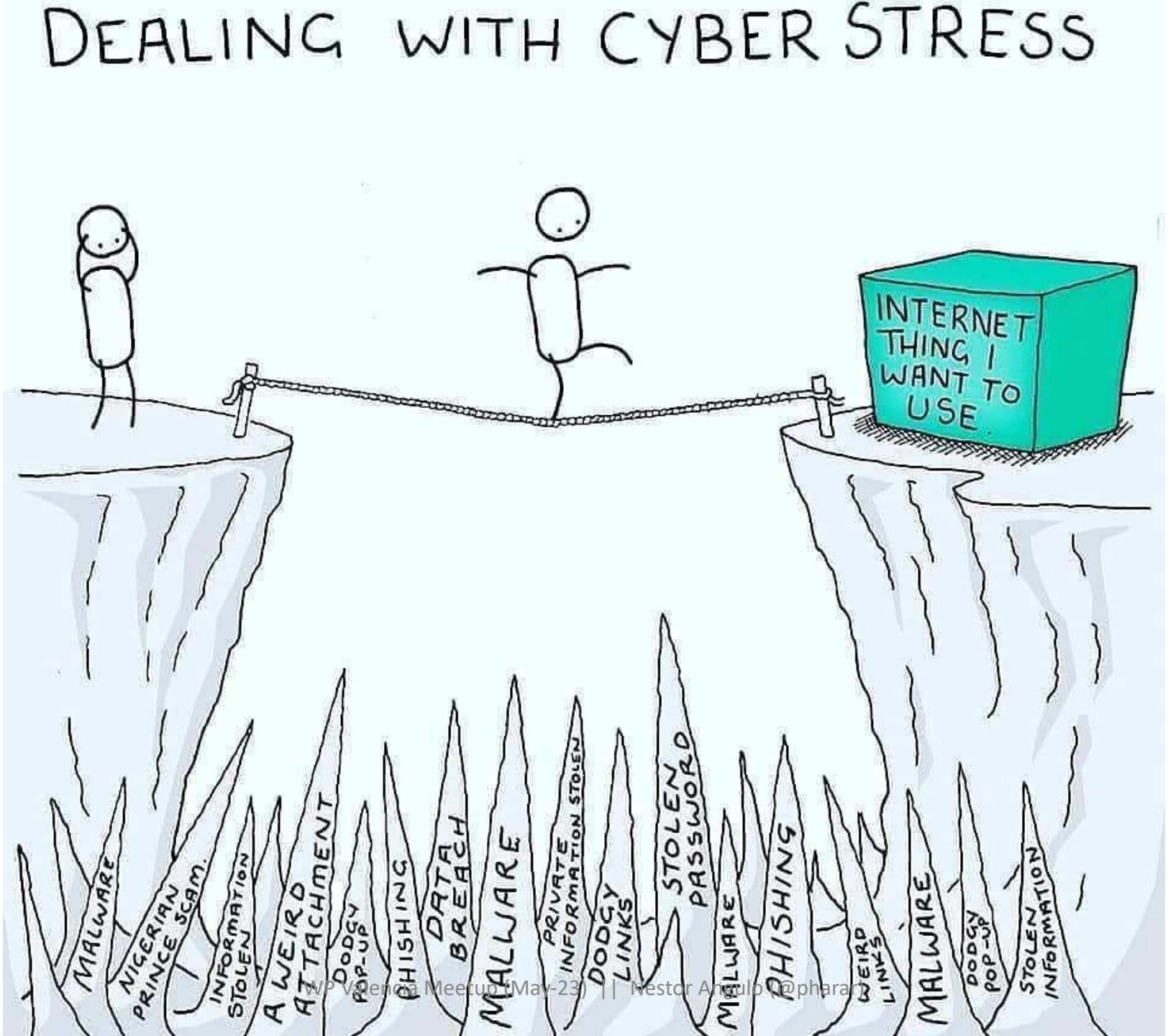
Gestión de identidad y acceso (IAM) (Identity & Access Management)

Evaluación de seguridad y pruebas (Security Assessment & Testing)

Operaciones de seguridad (Security Operations)

Seguridad de desarrollo de software (Software Development Security)


There are two types of companies: those who have been hacked, and those who don't yet know they have been hacked.
John Chambers
Chief Executive Officer of Cisco


DEALING WITH CYBER STRESS
INTERNET THING I WANT TO USE
MALWARE
NIGERIAN PRINCE SCAM.
INFORMATION STOLEN
A WEIRD ATTACHMENT
DODGY POP-UP
PHISHING
DATA BREACH
MALWARE
PRIVATE INFORMATION STOLEN
DODGY LINKS
STOLEN PASSWORD
MALWARE
PHISHING
WEIRD LINKS
MALWARE
DODGY POP-UP
STOLEN INFORMATION


PHISHING
BOTNET
SPAM
HACKER
MALWARE
DDOS
KEYLOGGER
VIRUS
SPYWARE

Hackers vs Ciberterrorista

Hacker

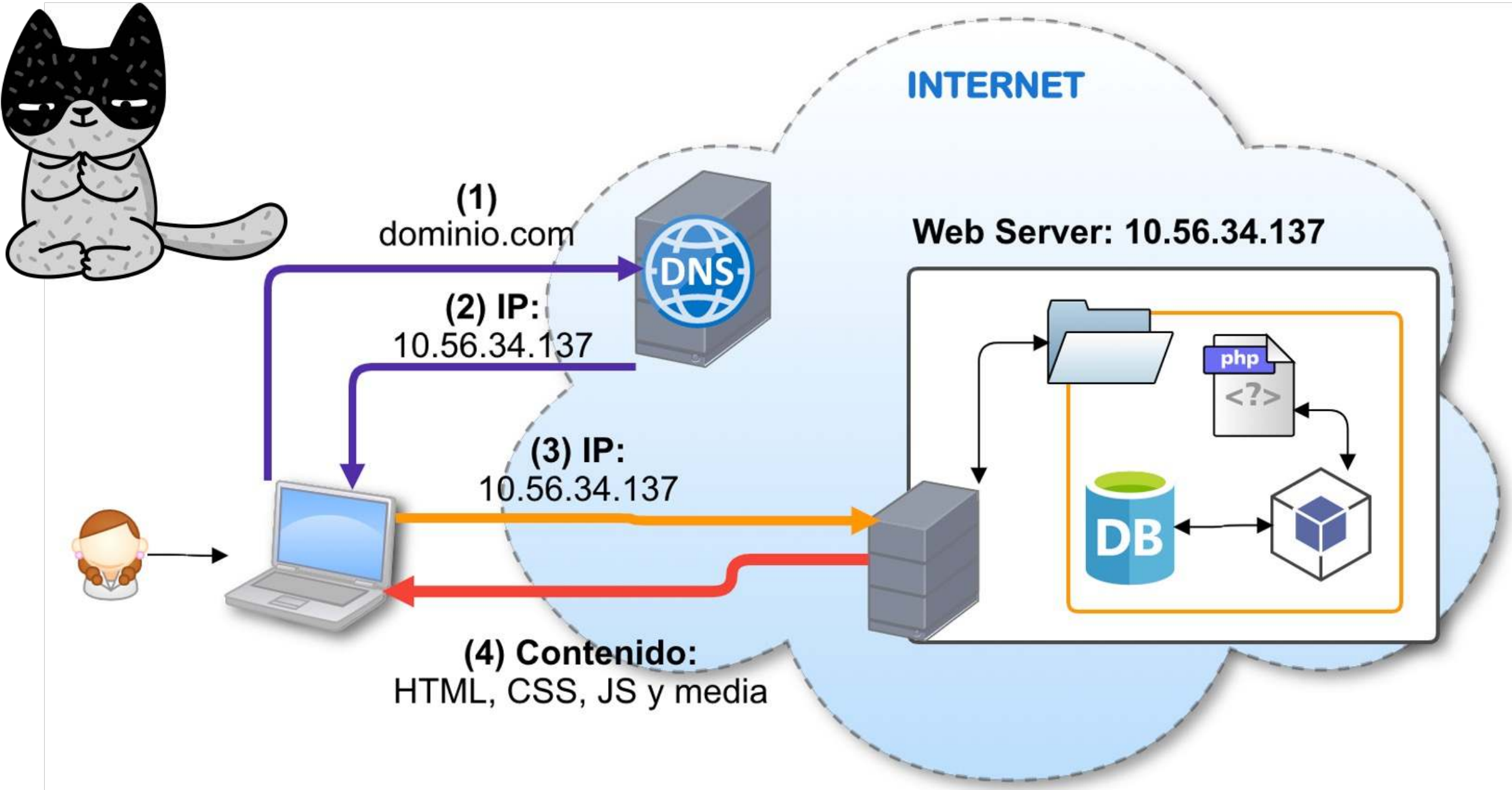
- **Persona curiosa** que disfruta yendo más allá de los límites y convenciones.

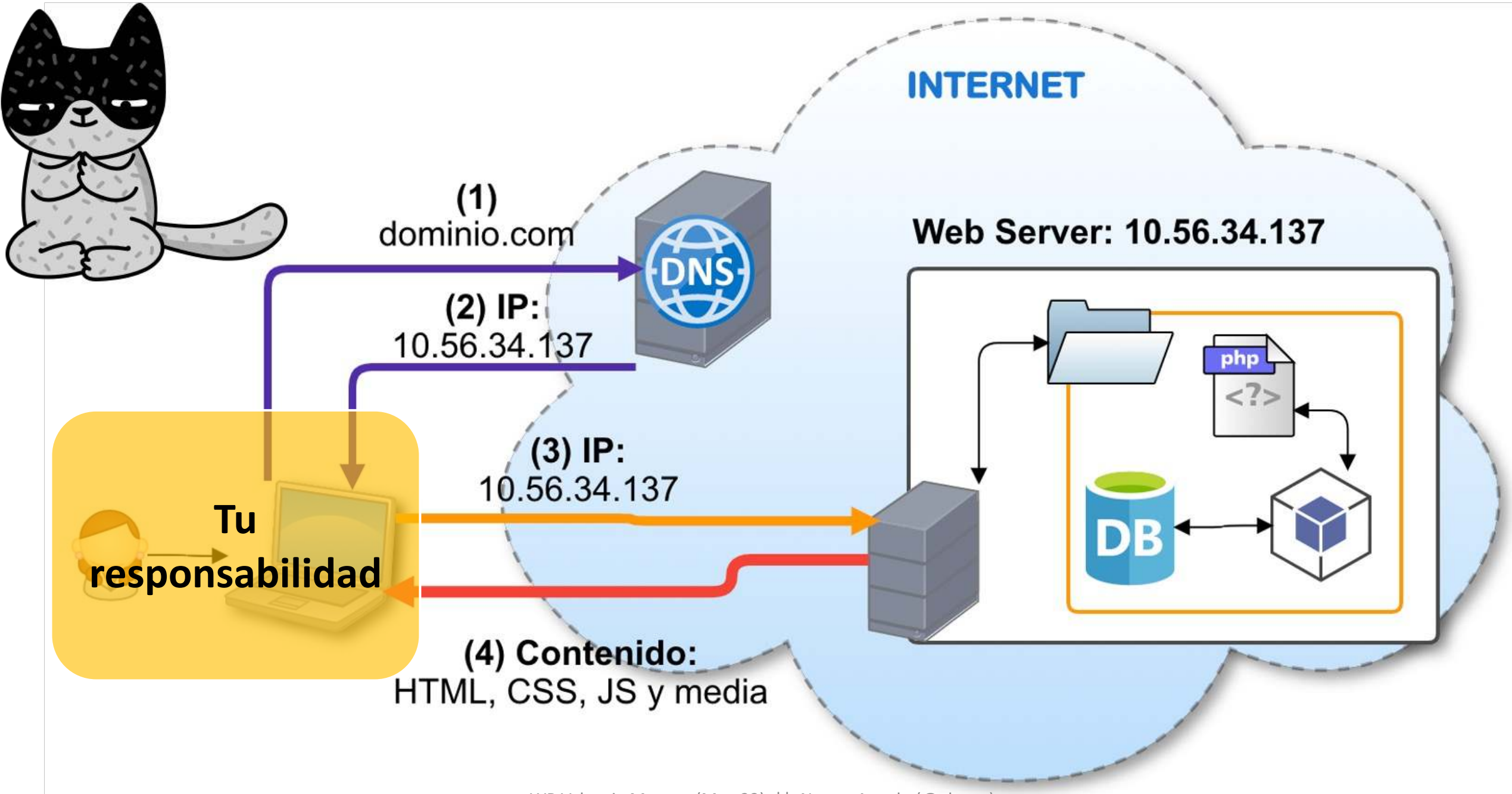
Ciberterrorista

- **Hacker informático**, cuyo objetivo es enriquecerse.
- **El malo.**

Seguridad: **Modelo de capas simplificado**

Capa	Protección
Tú, la capa más débil	Conocimiento
Tu **Dispositivo**	Antivirus
Tu **Conección**	SSL
Tu **tráfico Web**	WAF
Tus **Credenciales**	Contraseñas fuertes, 2FA
Seguridad Web	monitores, plugins, updates
Seguridad Servidor	monitor, sysadmin, updates
Base de datos	monitor, sysadmin
Mantenimiento	


INTERNET
(1)
dominio.com
DNS
(2) IP:
10.56.34.137
Web Server: 10.56.34.137
php
<?>
DB
(3) IP:
10.56.34.137
(4) Contenido:
HTML, CSS, JS y media


INTERNET
(1)
dominio.com
DNS
(2) IP:
10.56.34.137
Web Server: 10.56.34.137
php
<?>
DB
(3) IP:
10.56.34.137
Tu
responsabilidad
(4) Contenido:
HTML, CSS, JS y media

INTERNET
(1)
dominio.com
DNS
(2) IP:
10.56.34.137
Web Server: 10.56.34.137
php
<?>
DB
Tu
responsabilidad
Responsabilidad de
las empresas
(3) IP:
10.56.34.137
(4) Contenido:
HTML, CSS, JS y media

INTERNET
(1)
dominio.com
DNS
(2) IP:
10.56.34.137
Web Server: 10.56.34.137
(3) IP:
10.56.34.137
Tu
responsabilidad
Responsabilidad de
las empresas
Responsabilidad
del webmaster
(4) Contenido:
HTML, CSS, JS y media

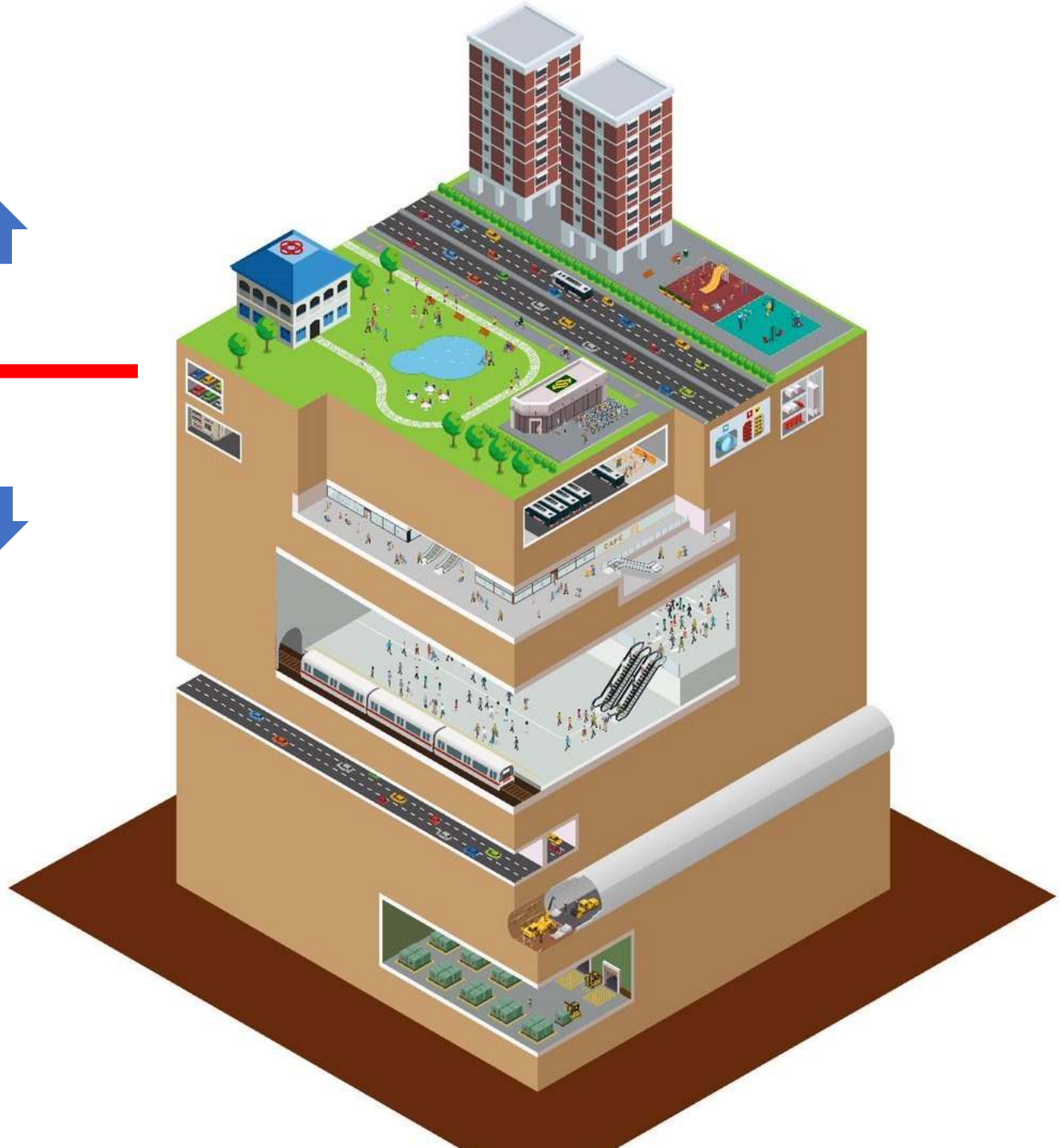
Site Owner

- App
- Data
- Security of the site

Hosting provider

- Networks
- Hardware
- SO
- Virtualization
- Security

Security Liability



Posibles objetivos en Seguridad Web

Usuarios

Base de datos

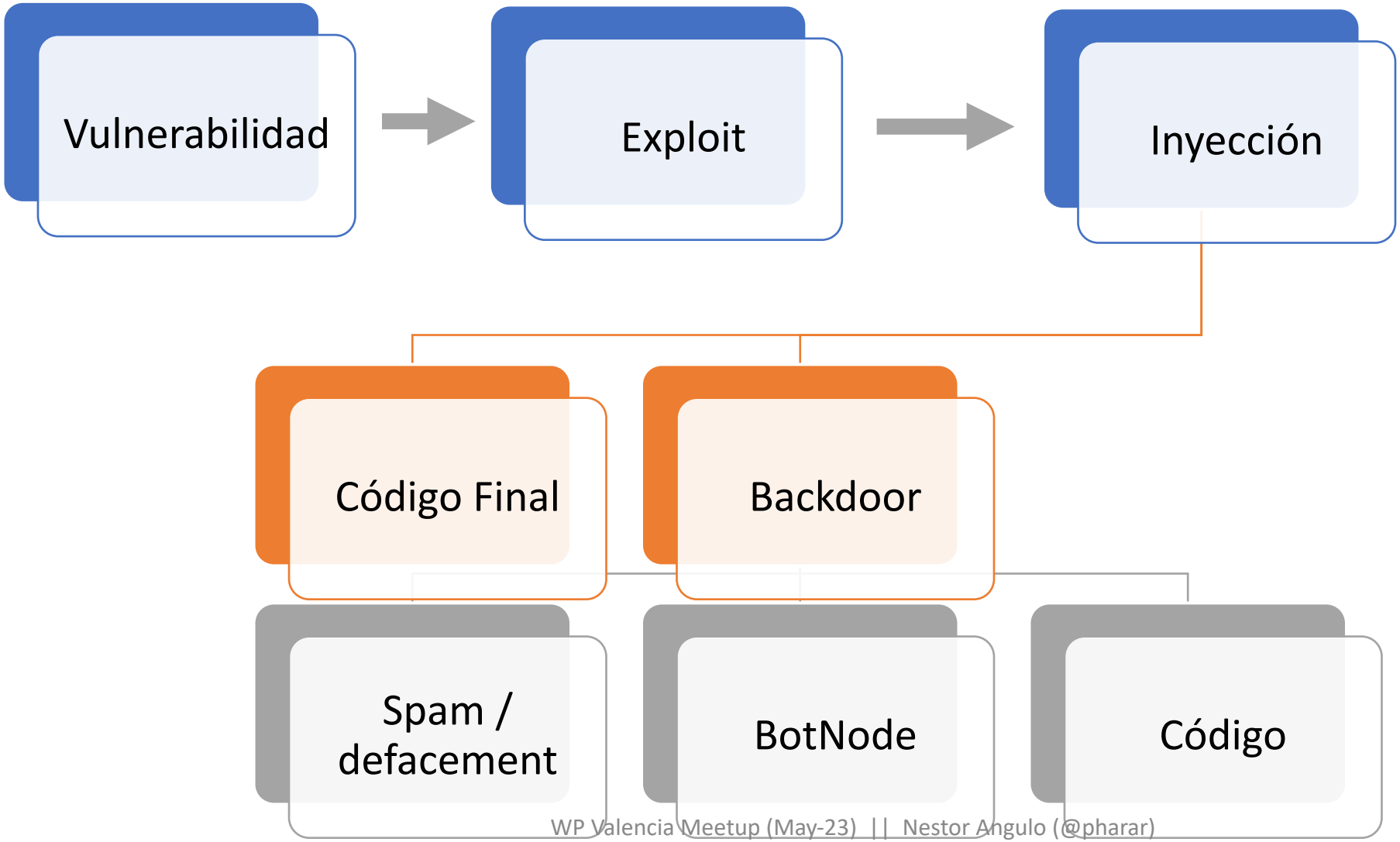
Contenido

Infrastructura

Pagos

Reputación

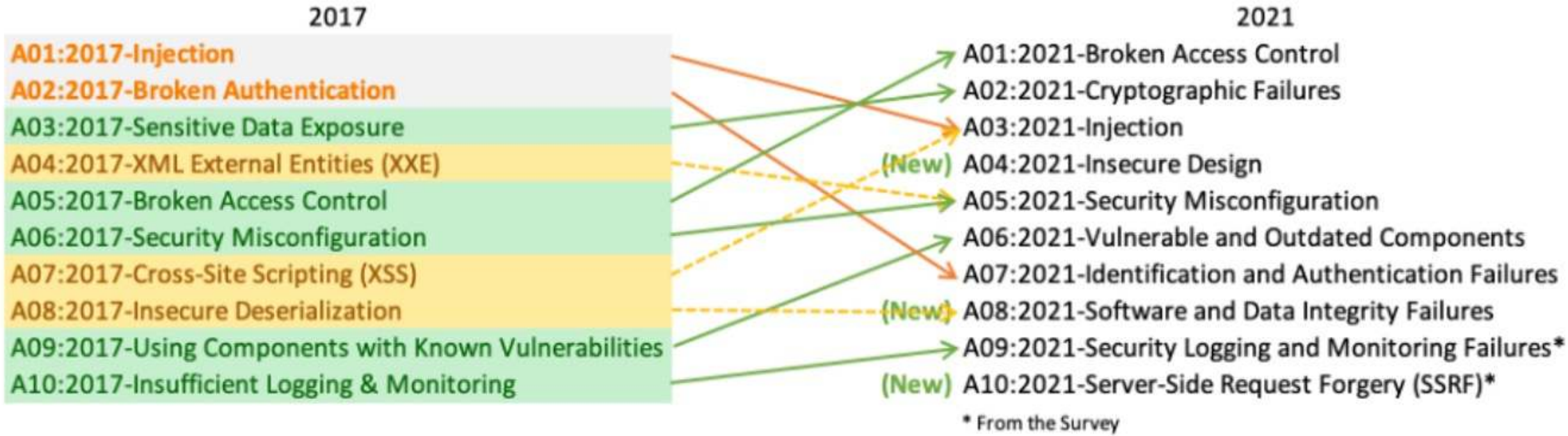
Cómo se **infecta** un sitio **WordPress**:



OWASP
Open Web Application Security Project

Top 10 Web Application Security Risks

There are three new categories, four categories with naming and scoping changes, and some consolidation in the Top 10 for 2021.



Hechos

Un hackeo **casi nunca está orientado** a un cliente

(98% of cases)

Casi siempre se debe a **mal mantenimiento** o **mal control**.

Un certificado **SSL** no es un **escudo anti- hacking**

Los parches de seguridad aparecen después de identificar los exploits

Errare Humanum Est
(El Ser Humano falla)

La **seguridad no es 100% efectiva**

(Y NUNCA lo será)

Agentes (si algo sale mal)

Tú

- Dueños / Admins
- Developer, Designer
- **Usuarios / clientes (¿GDPR o similar?)**

Soporte Hosting

- Agentes / C3
- Soporte y Copias de seguridad

Experto de Seguridad

- Departmento de seguridad
- Servicios externos

Agentes (si algo sale mal)

Tú

- Dueños / Admins
- Developer, Designer
- **Usuarios / clientes (¿GDPR o similar?)**

Soporte Hosting

- Agentes / C3
- Soporte y Copias de seguridad

Experto de Seguridad

- Departmento de seguridad
- Servicios externos

Medidas:

REACTIVAS

Cuando las cosas malas **ya han pasado**

Mitigación de **Daños**

INCIDENT RESPONSE

PROACTIVAS

Antes de que pase nada malo

Mitigación de **Riesgo**

ANÁLISIS Y MONITOREO

Segundo, la RESPUESTA A INCIDENTES

Incident response (IR) is **the effort to quickly identify an attack, minimize its effects, contain damage**, and remediate the cause to reduce the risk of future incidents.

(vmware.com)

Medidas **reactivas** (AKA Incident Response)

1) ESCANEA tu sitio

Front-end: **sitecheck.sucuri.net**

Escáner gratis en plugin: WordFence, etc.

2) ACTUALIZA

TODO

Incluyendo el software del servidor.

3) CRC: Check, Remove and Change

Admins, plugins, temas, contraseñas …

- webpagetest.org

O restaurar **BACKUP Y** Volver a 1)

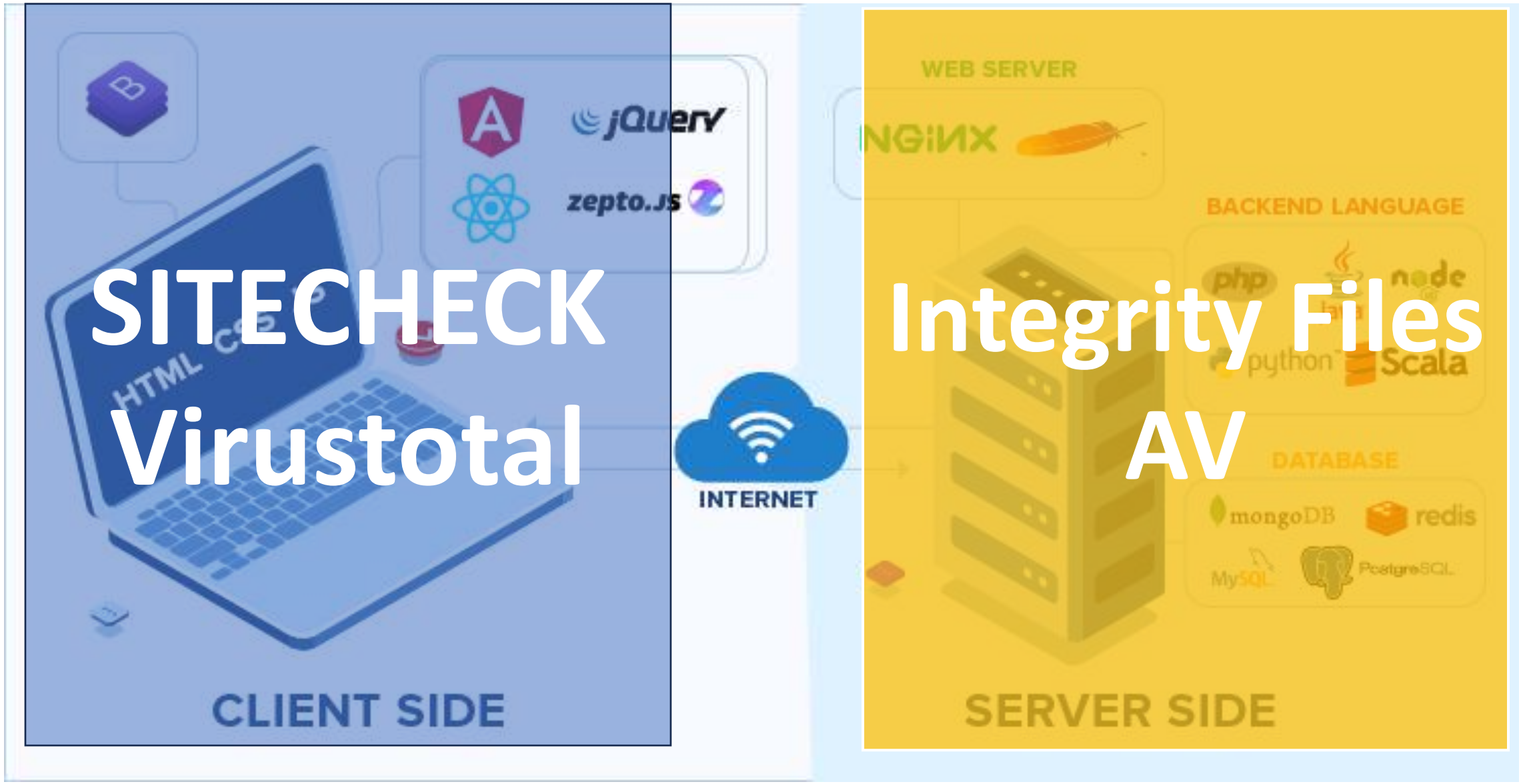
Posible pérdida de información

Posible re-instalación de malware

(PRIMERO) **ESCANEA** tu sitio

- Intentemos primero **entender que ha pasado.**
- FrontEnd análisis: **sitecheck.sucuri.net**
- Usar escáner gratuito in-site (i.e. WordFence)
- Si tienes acceso al server, ejecuta un antivirus (i.e. Clam AV)
- El colmo: Escaner de integridad de ficheros (activado ANTES del hackeo)


WEB SERVER
NGINX
BACKEND LANGUAGE
php
Java
node
python
Scala
DATABASE
mongoDB
redis
MySQL
PostgreSQL
jQuery
zepto.js
HTML CSS JS
INTERNET
CLIENT SIDE
SERVER SIDE


SITECHECK
Virustotal
Integrity Files
AV
jQuery
zepto.js
INTERNET
WEB SERVER
NGINX
BACKEND LANGUAGE
php
node
python
Scala
DATABASE
mongoDB
redis
MySQL
PostgreSQL
CLIENT SIDE
SERVER SIDE

Website File Changes Monitor

Added Files | Modified Files | Deleted Files

Added Files

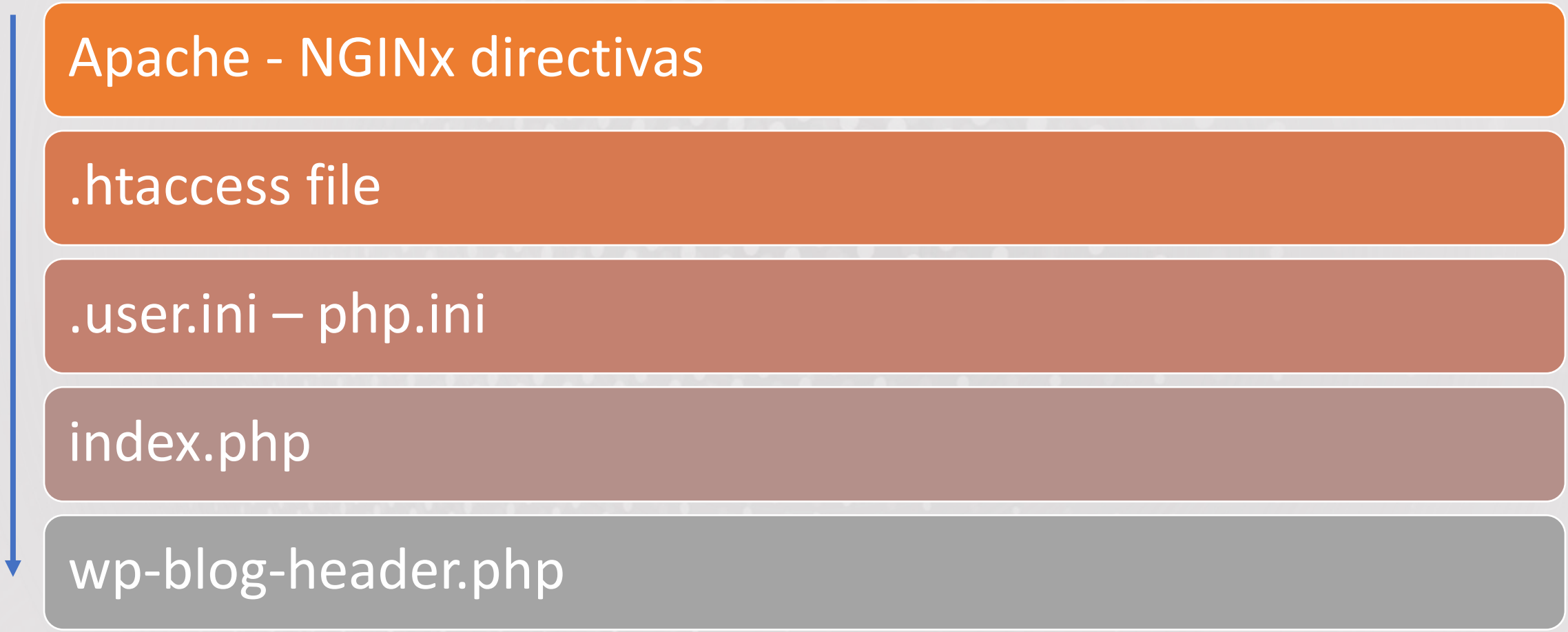
Bulk Actions ▾ | Apply | Scan Now | Last scan: September 3, 2019 4:44 am

Path	Name	Type	Date	Mark as Rea
/var/www/www.wpwhitesecurity.net/public_html/wp-content/new_xfolder/xfiles	fake_page.php	File	09-03-2019 4:44:59	✓
/var/www/www.wpwhitesecurity.net/public_html/wp-content/new_xfolder/xfiles	login.php	File	09-03-2019 4:44:59	✓
/var/www/www.wpwhitesecurity.net/public_html/wp-content/new_xfolder/xfiles	cron_run.exe	File	09-03-2019 4:44:59	✓
/var/www/www.wpwhitesecurity.net/public_html/wp-content/new_xfolder/xfiles	index.php	File	09-03-2019 4:44:59	✓
/var/www/www.wpwhitesecurity.net/public_html/wp-content/new_xfolder/xfiles	report.html.php	File	09-03-2019 4:44:59	✓
/var/www/www.wpwhitesecurity.net/public_html/wp-content/themes	log-lolla	Theme Install	09-03-2019 4:44:59	✓
/var/www/www.wpwhitesecurity.net/public_html/wp-content/themes	bazzinga	Theme Install	09-03-2019 4:44:59	✓
/var/www/www.wpwhitesecurity.net/public_html/wp-content/themes	joint	Theme Install	09-03-2019 4:44:59	✓
/var/www/www.wpwhitesecurity.net/public_html/wp-content/plugins	wp-security-audit-log	Plugin Install	09-03-2019 4:44:59	✓
/var/www/www.wpwhitesecurity.net/public_html/wp-content/plugins	password-policy-manager-master	Plugin Install	09-03-2019 4:44:59	✓

Ejemplos de Plugins/Themes falsos

wp-content/plugins	wp-content/themes
• wp-lazyload-{random chars} • task-controller • core-stab / core-engine • wp-zip • plugins	• seotheme • classic • themes

Orden de ejecución en WordPress



{ Onanimus7 R4nsomwar3 }

Your Website Is Encrypt3d

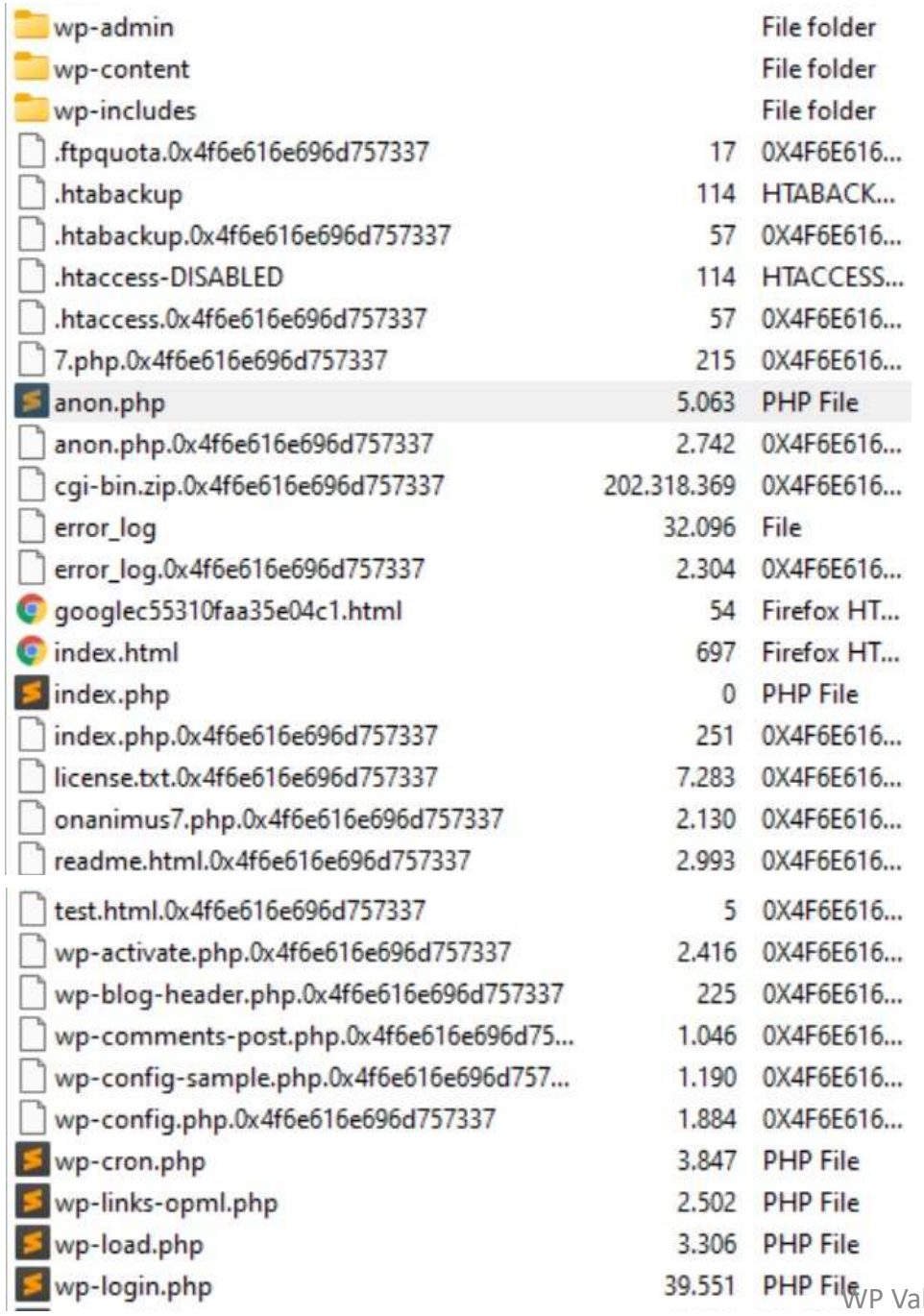
Don't Change the Filename because it Can Damage the File If You Want to Return You Must Enter the Password First
Send Me $200 For Back Your Website

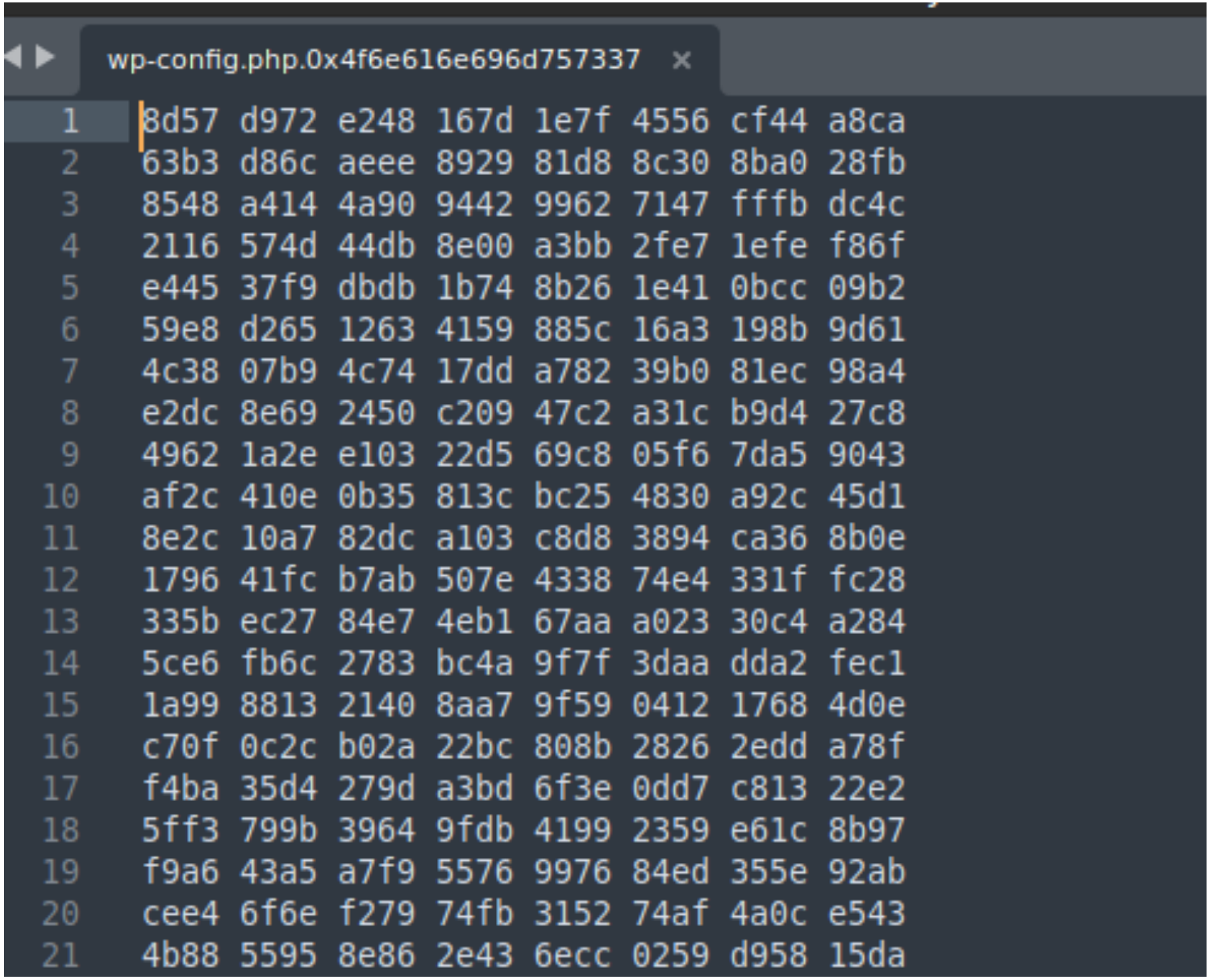
Bitcoin (BTC) Address : 1HmEGmGDuBrTEb3Q4NQ

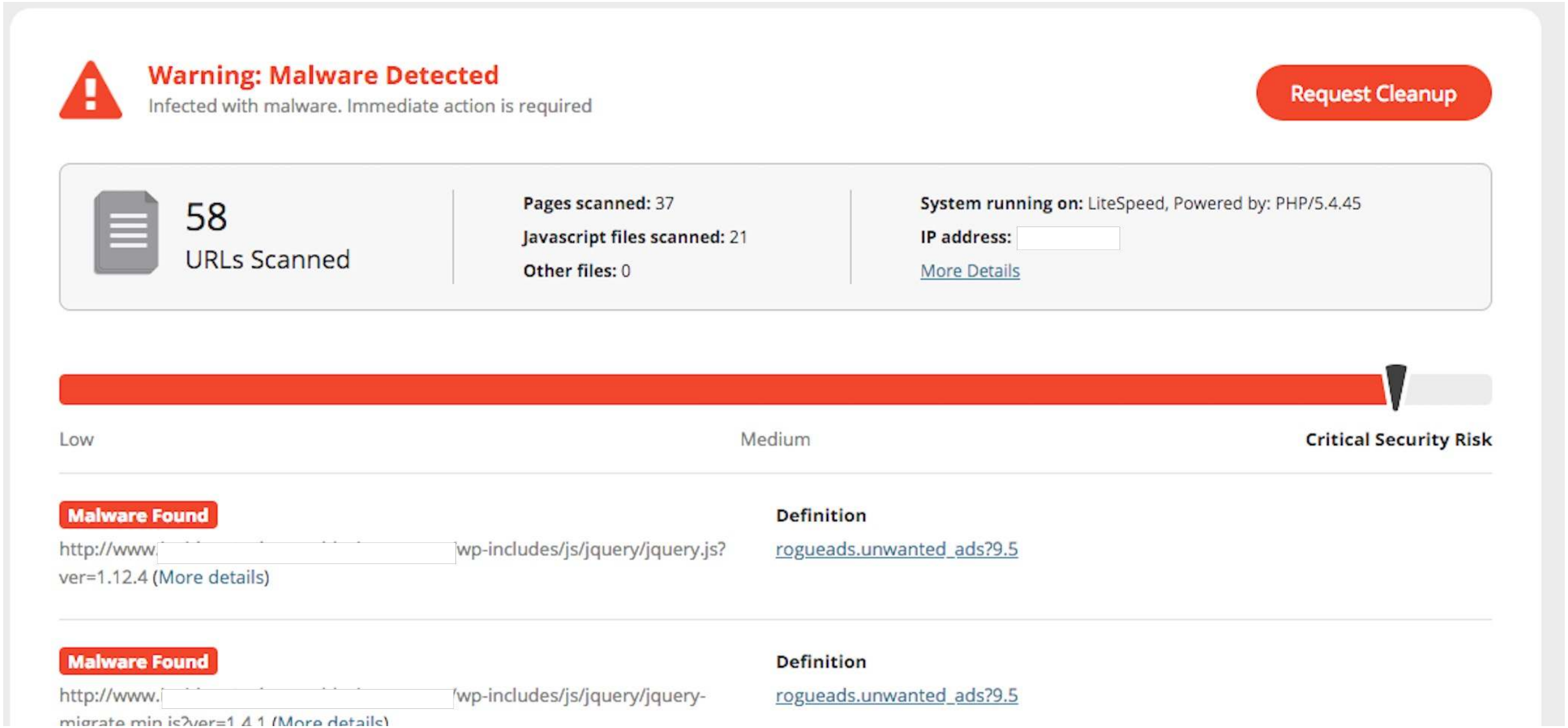
Password Decrypt

Contact Telegram : @feyensss

~Tap Background to music~


wp-admin File folder
wp-content File folder
wp-includes File folder
.ftpquota.0x4f6e616e696d757337 17 0X4F6E616...
.htabackup 114 HTABACK...
.htabackup.0x4f6e616e696d757337 57 0X4F6E616...
.htaccess-DISABLED 114 HTACCESS...
.htaccess.0x4f6e616e696d757337 57 0X4F6E616...
7.php.0x4f6e616e696d757337 215 0X4F6E616...
anon.php 5.063 PHP File
anon.php.0x4f6e616e696d757337 2.742 0X4F6E616...
cgi-bin.zip.0x4f6e616e696d757337 202.318.369 0X4F6E616...
error_log 32.096 File
error_log.0x4f6e616e696d757337 2.304 0X4F6E616...
googlec55310faa35e04c1.html 54 Firefox HT...
index.html 697 Firefox HT...
index.php 0 PHP File
index.php.0x4f6e616e696d757337 251 0X4F6E616...
license.txt.0x4f6e616e696d757337 7.283 0X4F6E616...
onanimus7.php.0x4f6e616e696d757337 2.130 0X4F6E616...
readme.html.0x4f6e616e696d757337 2.993 0X4F6E616...
test.html.0x4f6e616e696d757337 5 0X4F6E616...
wp-activate.php.0x4f6e616e696d757337 2.416 0X4F6E616...
wp-blog-header.php.0x4f6e616e696d757337 225 0X4F6E616...
wp-comments-post.php.0x4f6e616e696d75... 1.046 0X4F6E616...
wp-config-sample.php.0x4f6e616e696d757... 1.190 0X4F6E616...
wp-config.php.0x4f6e616e696d757337 1.884 0X4F6E616...
wp-cron.php 3.847 PHP File
wp-links-opml.php 2.502 PHP File
wp-load.php 3.306 PHP File
wp-login.php 39.551 PHP File


wp-config.php.0x4f6e616e696d757337
1 8d57 d972 e248 167d 1e7f 4556 cf44 a8ca
2 63b3 d86c aeee 8929 81d8 8c30 8ba0 28fb
3 8548 a414 4a90 9442 9962 7147 fffb dc4c
4 2116 574d 44db 8e00 a3bb 2fe7 1efe f86f
5 e445 37f9 dbdb 1b74 8b26 1e41 0bcc 09b2
6 59e8 d265 1263 4159 885c 16a3 198b 9d61
7 4c38 07b9 4c74 17dd a782 39b0 81ec 98a4
8 e2dc 8e69 2450 c209 47c2 a31c b9d4 27c8
9 4962 1a2e e103 22d5 69c8 05f6 7da5 9043
10 af2c 410e 0b35 813c bc25 4830 a92c 45d1
11 8e2c 10a7 82dc a103 c8d8 3894 ca36 8b0e
12 1796 41fc b7ab 507e 4338 74e4 331f fc28
13 335b ec27 84e7 4eb1 67aa a023 30c4 a284
14 5ce6 fb6c 2783 bc4a 9f7f 3daa dda2 fec1
15 1a99 8813 2140 8aa7 9f59 0412 1768 4d0e
16 c70f 0c2c b02a 22bc 808b 2826 2edd a78f
17 f4ba 35d4 279d a3bd 6f3e 0dd7 c813 22e2
18 5ff3 799b 3964 9fdb 4199 2359 e61c 8b97
19 f9a6 43a5 a7f9 5576 9976 84ed 355e 92ab
20 cee4 6f6e f279 74fb 3152 74af 4a0c e543
21 4b88 5595 8e86 2e43 6ecc 0259 d958 15da


Warning: Malware Detected
Infected with malware. Immediate action is required
Request Cleanup
58
URLs Scanned
Pages scanned: 37
Javascript files scanned: 21
Other files: 0
System running on: LiteSpeed, Powered by: PHP/5.4.45
IP address:
More Details
Low
Medium
Critical Security Risk
Malware Found
http://www. wp-includes/js/jquery/jquery.js?
ver=1.12.4 (More details)
Definition
rogueads.unwanted_ads?9.5
Malware Found
http://www. /wp-includes/js/jquery/jquery-
migrate.min.js?ver=1.4.1 (More details)
Definition
rogueads.unwanted_ads?9.5

(SEGUNDO) **ACTUALIZA**

Actualiza todo, incluidos plugins, temas y el propio WordPress.

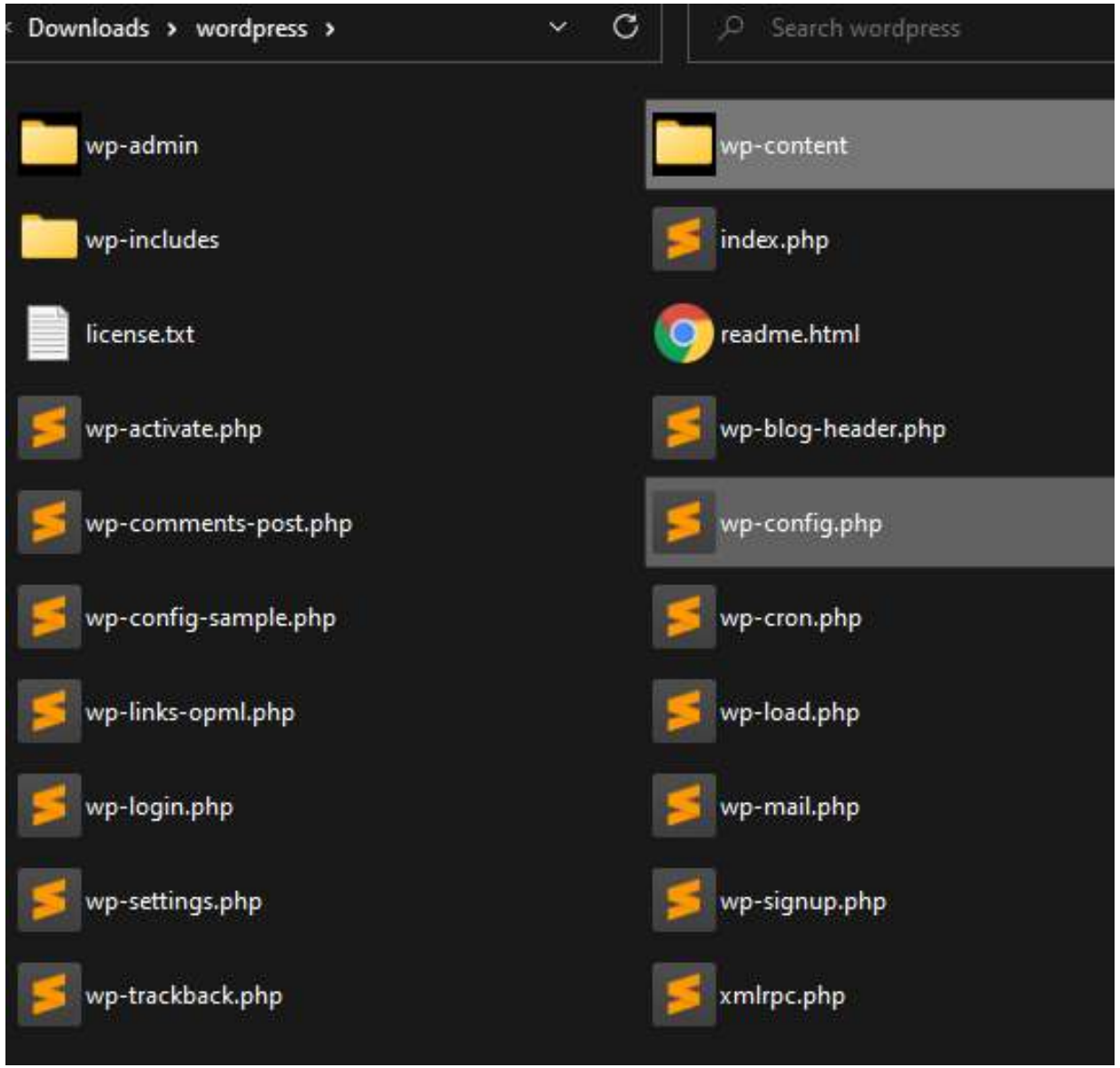
Esto hará que tapemos agujeros de seguridad, evitando una possible infección.

También, **sobreescribirá código comprometido/corrupto con código confiable** del repositorio oficial.

ACTUALIZA

PLUGINS	TEMAS	CORE	PHP
APACHE / NGINX	SERVIDOR	CPANEL / PLESK	…

¡SECRETO!


Downloads › wordpress ›
Search wordpress
wp-admin
wp-content
wp-includes
index.php
license.txt
readme.html
wp-activate.php
wp-blog-header.php
wp-comments-post.php
wp-config.php
wp-config-sample.php
wp-cron.php
wp-links-opml.php
wp-load.php
wp-login.php
wp-mail.php
wp-settings.php
wp-signup.php
wp-trackback.php
xmlrpc.php

(TERCERO) **CRC**:
Check, remove and change

Check & Remove

- Admins innecesarios
- Plugins y temas que no sean estrictamente necesarios
- Copias de seguridad
- Sitios de test/en desarrollo en el servidor de producción.

Change Contraseñas

- Connexiones (cPanel, FTP, SSH, …)
- Base de datos (recuerda actualizar luego el **wp-config.php**)
- Panel admin (**wp-admin**)
- Acceso al proveedor de hosting.

Atención: Se perderá cualquier personalización que hayas hecho a los archivos del

Actualizar temas

Seleccionar todos

Twenty Fifteen
Tienes la versión 2.5. Actualiza a la 2.6.

Twenty Fourteen
Tienes la versión 2.7. Actualiza a la 2.8.

Twenty Nineteen
Tienes la versión 1.4. Actualiza a la 1.5.

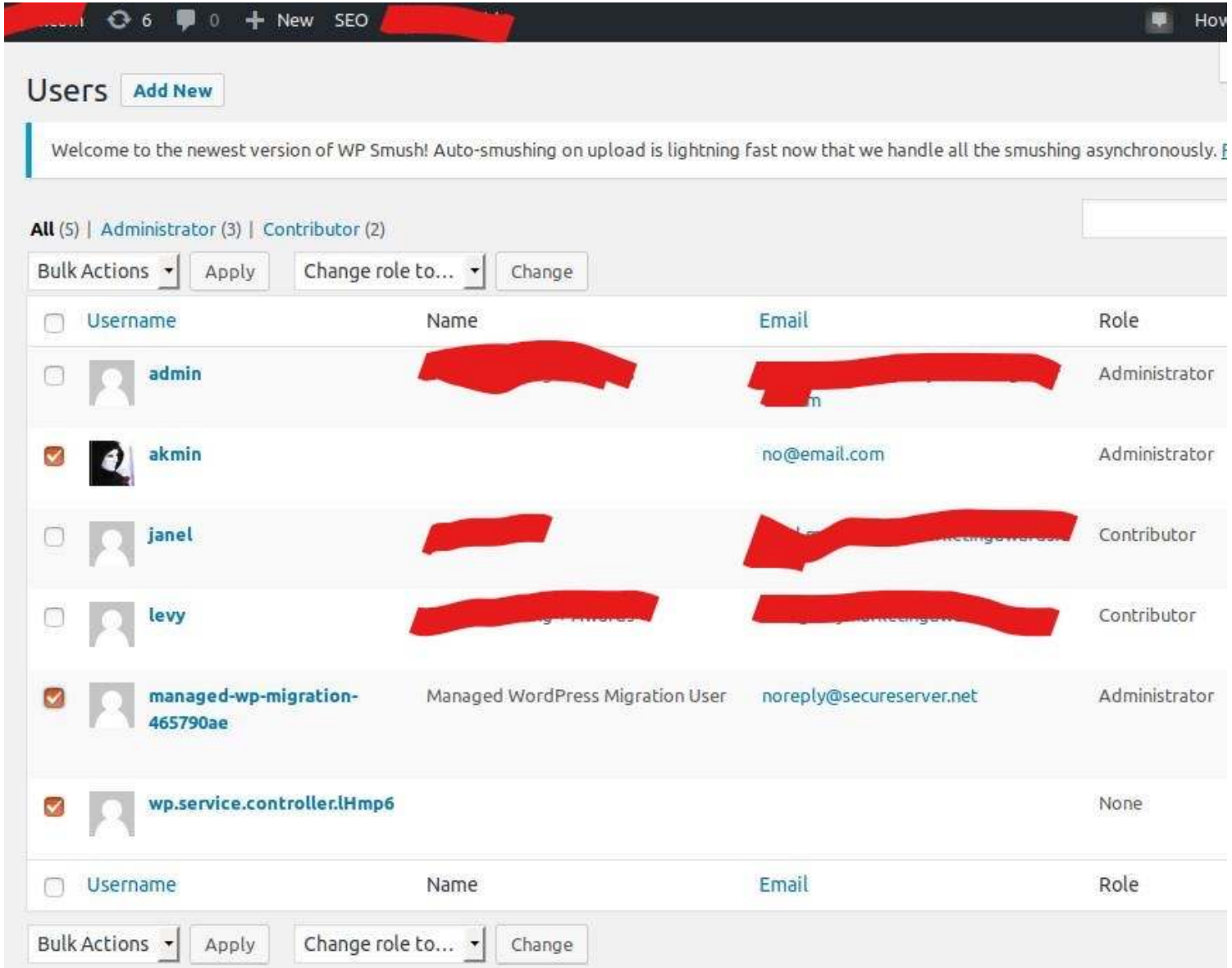
Twenty Seventeen
Tienes la versión 2.2. Actualiza a la 2.3.

Twenty Thirteen
Tienes la versión 2.9. Actualiza a la 3.0.

Twenty Twenty
Tienes la versión 1.1. Actualiza a la 1.2.

Seleccionar todos

Actualizar temas



(ÚLTIMA OPCIÓN) Restaurar una **Copia de Seguridad**

- Puedes perder información
- No sabemos a ciencia cierta cuándo comenzó la infección


PALLIS O'CONNOR Presents
BACK TO THE FUTURE
TRILOGY
THE GREATEST TRILOGY...
EVER MADE...

TIPS: COPIAS DE SEGURIDAD

Ten una buena **estrategia**

Nunca las almacenes en tu servidor de producción

Una copia **FUNCIONAL** puede ser **tu mejor amiga** un mal día

¡RECUERDA! Medidas **reactivas**

1) ESCANEA tu sitio

Front-end: **sitecheck.sucuri.net**

Escáner gratis en plugin: WordFence, etc.

2) ACTUALIZA

TODO

Incluyendo el software del servidor.

3) CRC: Check, Remove and Change

Admins, plugins, temas, contraseñas …

- webpagetest.org

O restaurar **BACKUP Y** Volver a 1)

Posible pérdida de información

Posible re-instalación de malware

Ahora, la Reputación

Bots, Motores de Búsqueda y Blocklists

INTERNET ESTÁ CONSTANTEMENTE RASTREADO POR **BOTS**

LOS MOTORES DE BÚSQUEDA Y EMPRESAS DE SEGURIDAD TIENEN **BLOCKLISTS**

BLOCKLISTS -> REPUTACIÓN

MIENTRAS MÁS FAMOSA SEA LA BLOCKLIST MÁS ACEPTADA.

FACTS

No es un proceso inmediato

- La inclusión en blocklists toma su tiempo
- Salir también

Normalmente, no dan información de por qué

Las RRSS tienen en cuenta las blocklists

Las empresas de Ads bloquean campañas

Los motores de búsqueda eliminant el sitio de las SERP

- Algunos eliminan completamente el rankeo SEO

Un cosa (importante) más …

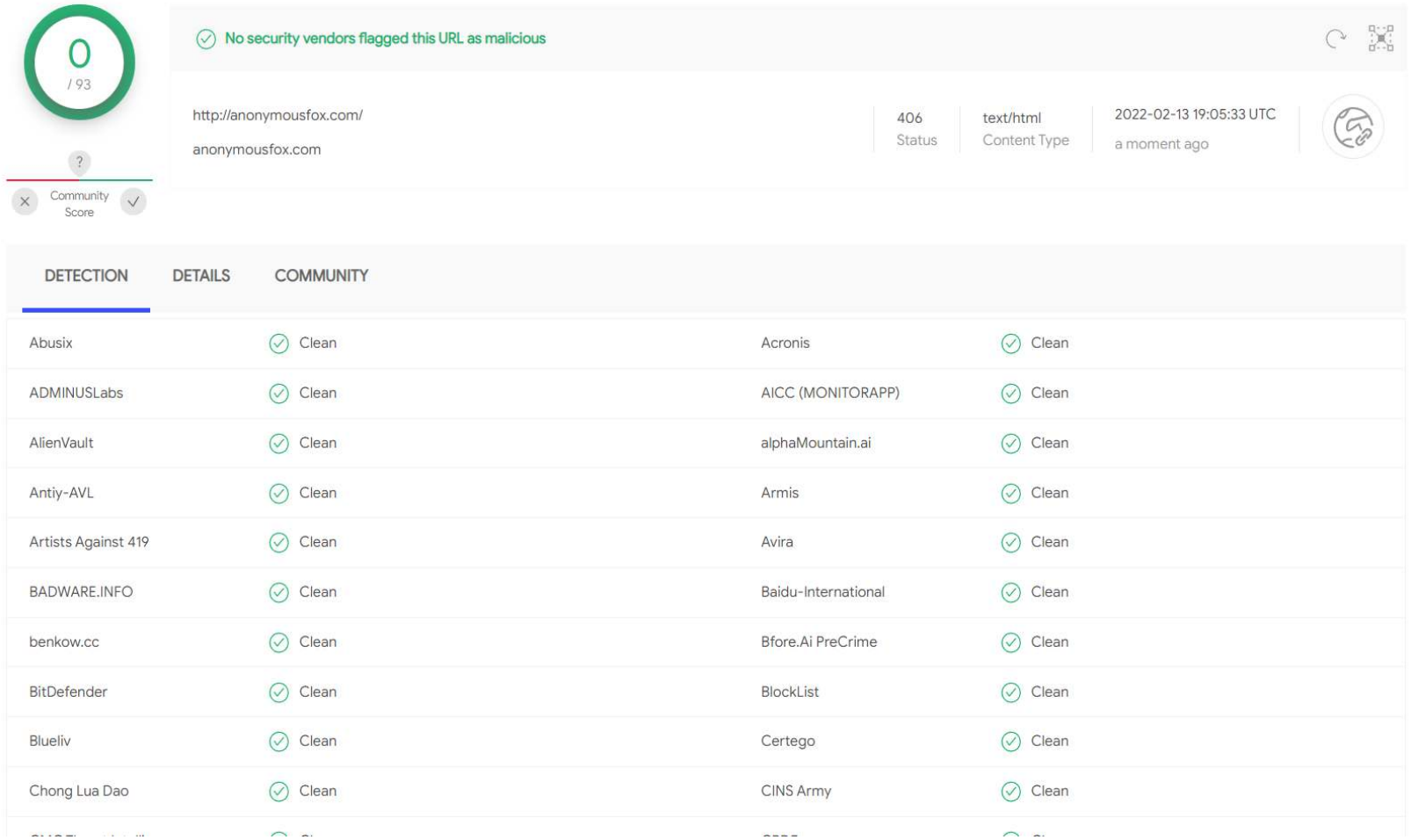
Algunas **leyes de protección de datos** pueden requerir que se reporte cualquier brecha de seguridad con pérdida de datos sensibles a las autoridades competentes

En el caso de que que **afecte a un ciudadano Euroeo**, la **GDPR da 72h** tras la detección de la brecha para notificarla.

Comprueba las leyes aplicables, depende de país en el que operes y la nacionalidad de los clientes.

Solución a las blocklists

1. **UNA VEZ LIMPIA tu web**, comprueba las blocklists:
   Virustotal.com
2. **Procede a solicitar** una reconsideración por cada empresa en las blocklists, individualmente.



Informe Post-Mortem

Es **duro**, requiere servicios **forenses** y **expone** tu gestión.

Un informe claro **de lo que pasó** tras el ataque exitoso:

- Cómo y cuándo ocurrió
- Cómo y cuándo fue descubierto
- Qué se hizo para mitigar el daño y recuperar la situación normal
- Lecciones aprendidas

Ayuda a **aprender** para futuras situaciones

Ayuda a recuperar la **confianza de los usuarios**

Muestra a tu empresa alineada con los conceptos de **transparencia**.

Y para finalizar…
¡Paz Mental!

Medidas Proactivas

Reducir admins, plugins y temas (LEAST PRIVILEGE RULE)

Gestor de Contraseñas, cambiar periódicamente, 2FA + Fuertes

Copias de Seguridad (¡VALIDARLAS!)

¡ACTUALIZA! (Los parches vienen DESPUÉS de los EXPLOITS)

Vigila tu sitio (WPSCAN.com, PatchStack & Integridad de Ficheros)

WAF (Web Application Firewall)

¡Recuerden! **INVERTIR** en:

HOSTING

SEGURIDAD


Everybody needs a hacker

¡Gràcies!

Ara vosaltres: Preguntes?