<2020/>
WORDCAMP
ZARAGOZA

Hacking WordPress

El Arte de la Guerra: En la mente de tu enemigo

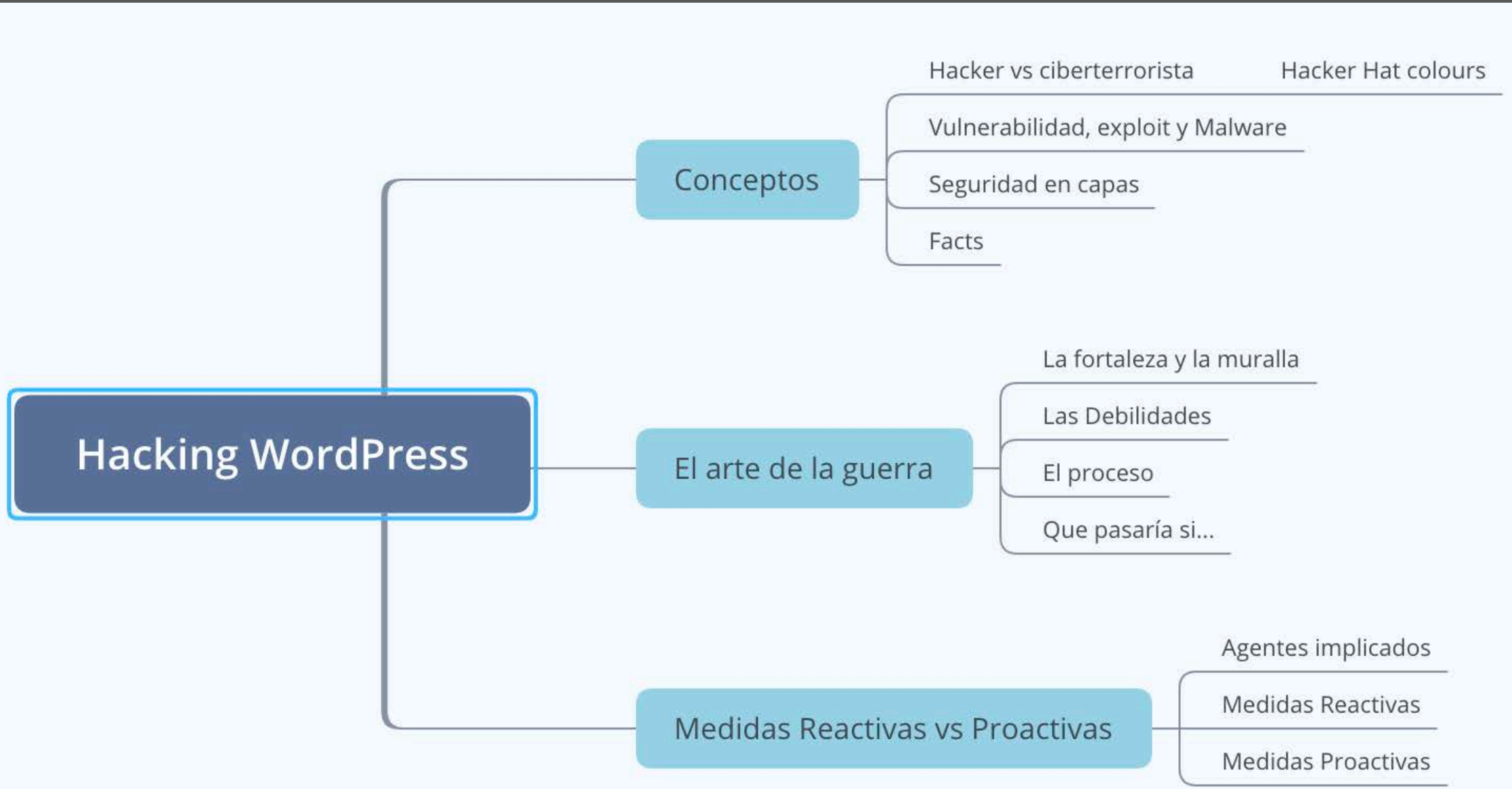
Néstor Angulo de Ugarte (@pharar)

Quién les habla

- Un chico muy curioso
  … a veces más que un gato.
- Ingeniero informático y consultor tecnológico
- 2015:
  Analista de Seguridad @ **Sucuri**
- 2017:
  ATS & Managed SSL @ **GoDaddy Security**
- 2019:
  Interim Head Of IT @ **GoDaddy Spain**

Sobre

- Sucuri: **Anaconda**
  (No Securi / Security)
- **Website security**
- Fully remote (personas > 25 paises)
- 2008: **Fundación**
- 2017: Entra en la familia **GoDaddy**
- **Free scanners**:
  - Sitecheck
    (sitecheck.sucuri.net)
  - Performance
    (performance.sucuri.net)


Hacking WordPress
Conceptos
Hacker vs ciberterrorista
Hacker Hat colours
Vulnerabilidad, exploit y Malware
Seguridad en capas
Facts
El arte de la guerra
La fortaleza y la muralla
Las Debilidades
El proceso
Que pasaría si...
Medidas Reactivas vs Proactivas
Agentes implicados
Medidas Reactivas
Medidas Proactivas

Conceptos

Algo de contexto

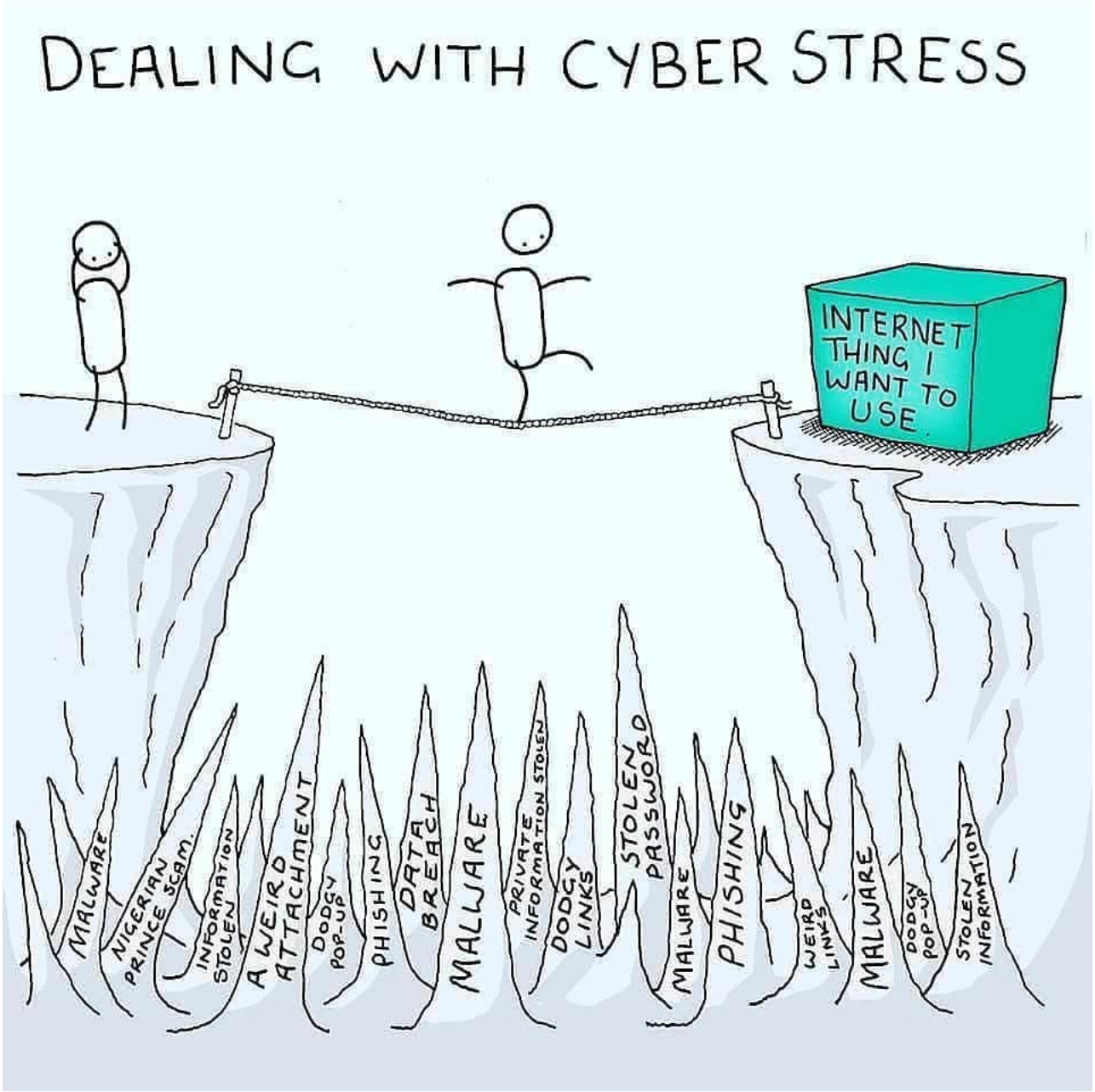
DISCLAIMER

Toda información sensible ha sido protegida o encriptada para preservar la privacidad. Cualquier similitud con la realidad es una coincidencia.

Soy responsable de lo que digo, no de lo que interpretéis.

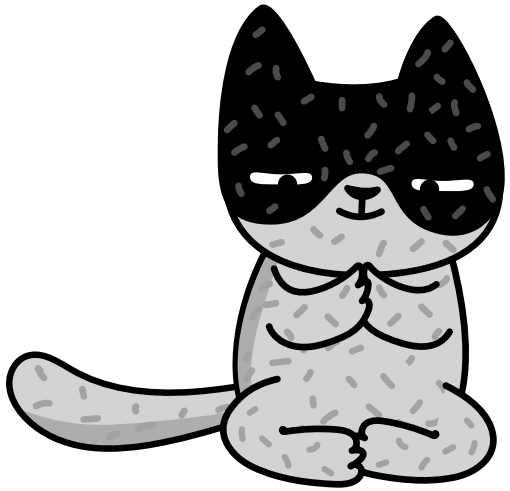
Contenido con intención DIDÁCTICA, NO SE PROMUEVE ningún proceso de hacking de tipo ilegal.

En caso de duda, preguntar siempre a vuestro EXPERTO de SEGURIDAD.


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


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

Malware



Software intencionadamente diseñado para causar daños a ordenadores, usuarios o redes de comunicaciones.

Varios tipos:

Backdoors, zero-day	Exploits	Troyanos, Fremium plugins	Ransomware , Spyware	Adware, Scareware	…

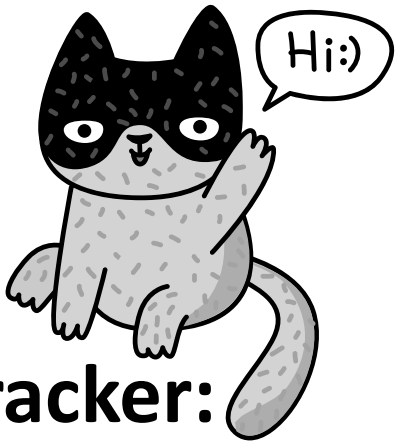
Definiciones

- **Vulnerabilidad**
  - Error en el código o posibilidad de utilización malintencionada de un recurso que puede ser explotado para realizar actividad no autorizada en un sistema informático.
- **Exploit**
  - Programa que aprovecha una vulnerabilidad
- **Backdoor**
  - Malware que permite ejecución remota de código

HACKER VS Ciberterrorista

Hacker:

Persona curiosa que le gusta ir más allá de los límites y convencionalismos.



Ciberterrorista / Cracker:

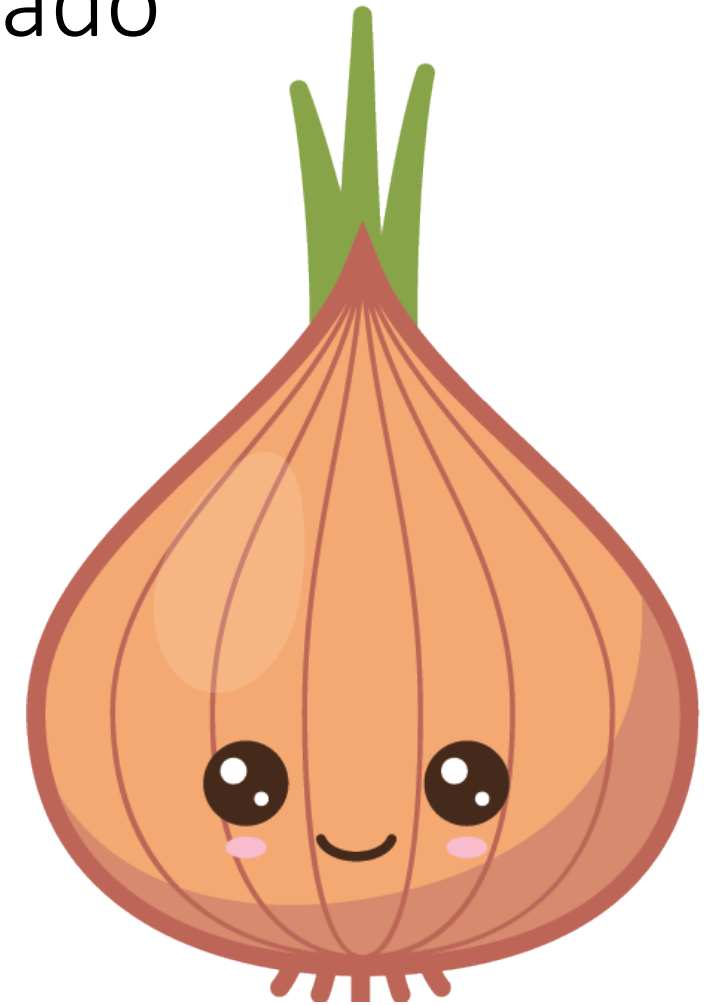
Hacker informático, cuyo objetivo es siempre enriquecerse en una situación juego de suma cero.

Tipos de Hacker

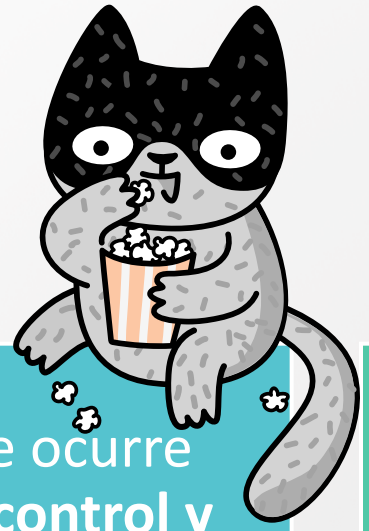
- **Black Hat**
  Ciberterrorista, Ladrón, el chico malo.
- **Grey Hat**
  White Hat Hacker que utiliza métodos ilegales.
- **White Hat**
  Analista de seguridad, Hacker ético.

Seguridad: Modelo por capas simplificado

Capa	Protección
Tú, la capa más débil	Conocimiento
Tu **dispositivo**	Antivirus
Tu **conexión**	SSL
Tu **sitio web**	WAF
Tus **credenciales**	Contraseñas fuertes, 2FA
La seguridad de **tu sitio**	monitor, plugins, updates
La seguridad **del server**	monitor, sysadmin, updates
La **base de datos**	monitor, sysadmin
Tareas de mantenimiento	



FACTS



Un hackeo prácticamente **nunca es orientado** a un cliente

(98% of cases)

Casi siempre ocurre debido a un **control y mantenimiento deficientes**

Un certificado **SSL**

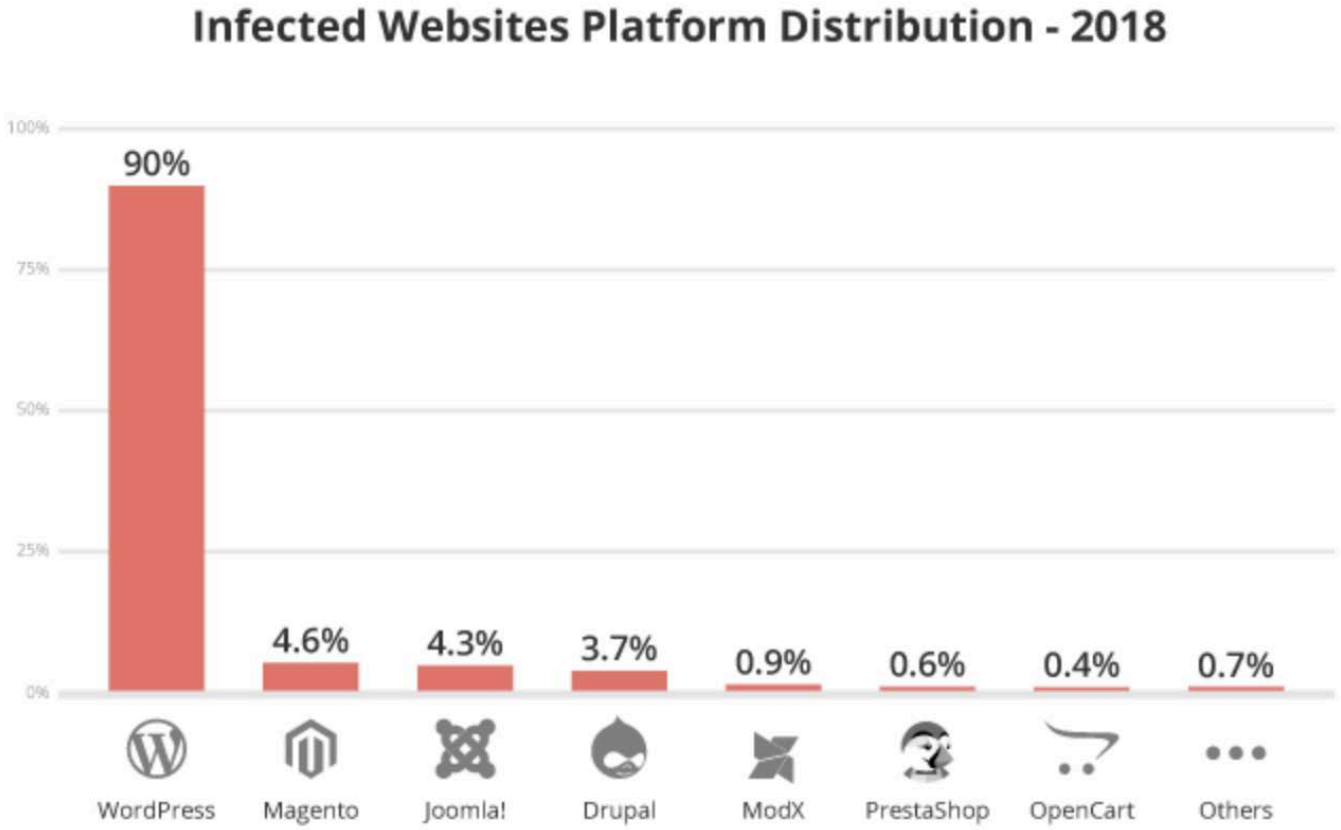
no es un escudo

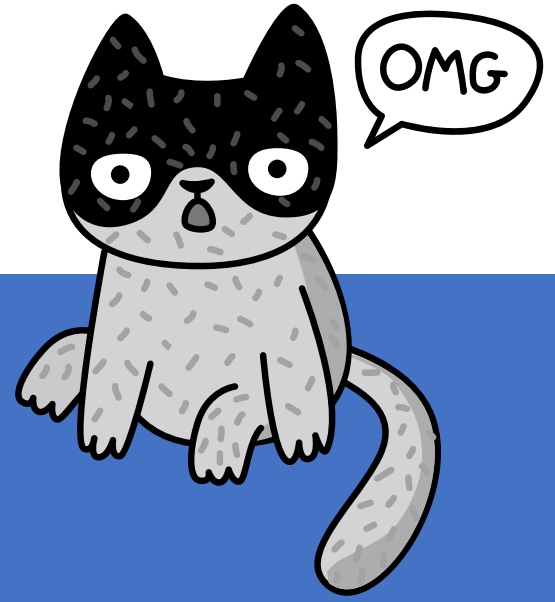
anti-hacking

Los parches de seguridad y actualizaciones aparecen normalmente **después** de descubrirse la existencia de exploits

Errare Humanum Est

La Seguridad **nunca** garantiza (ni lo hará) un **100% de efectividad**





FACTS

Fuente: Website Hack Trend Report 2018 – sucuri.net

… Y **1 de cada 3 sitios webs en Internet utiliza WordPress**
O 2 de cada 3 si hablamos de los sitios web que usan un CMS

El Arte de la Guerra

En la mente de tu enemigo

El Arte de la guerra

- Tratado chino sobre tácticas y estrategias en la Guerra (Sun Tzu)
- Separado en 13 capítulos

“Si conoces a tu enemigo y te conoces a ti, no puedes perder una batalla”

“Toda batalla se basa en el engaño”

”La mayor victoria es vencer sin combatir”

Tu fortaleza

Usuarios

Base de datos

Contenido

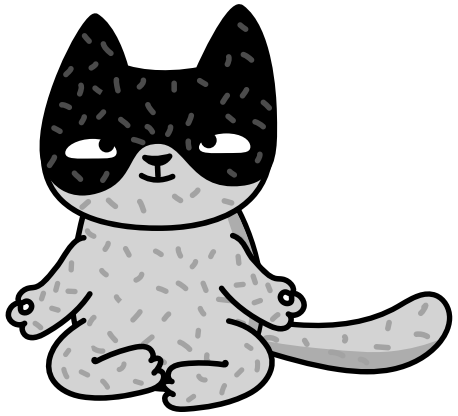
Infraestructura

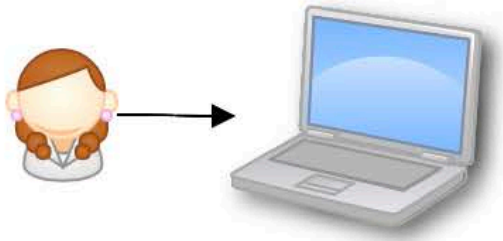
Bot Net

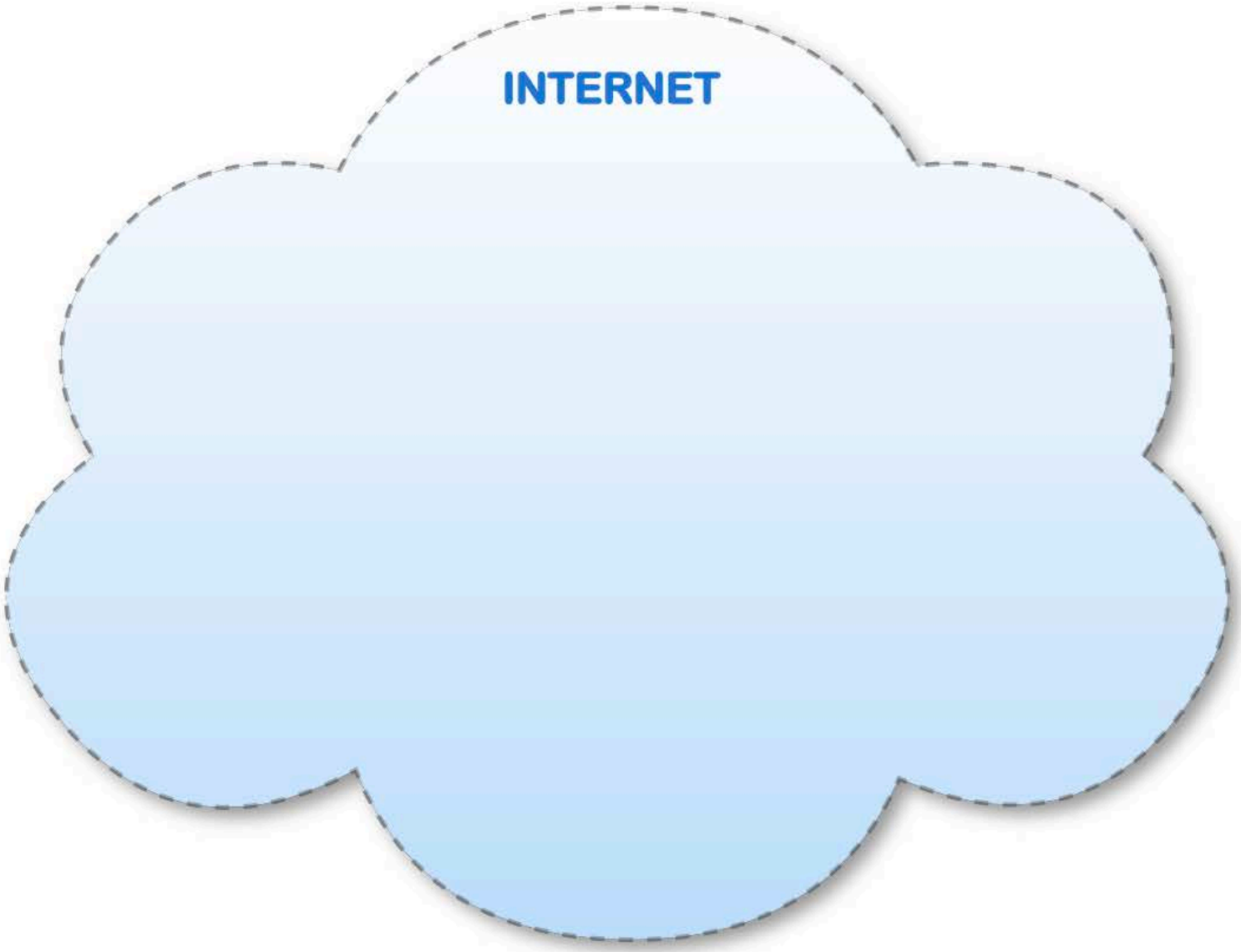
Reputación

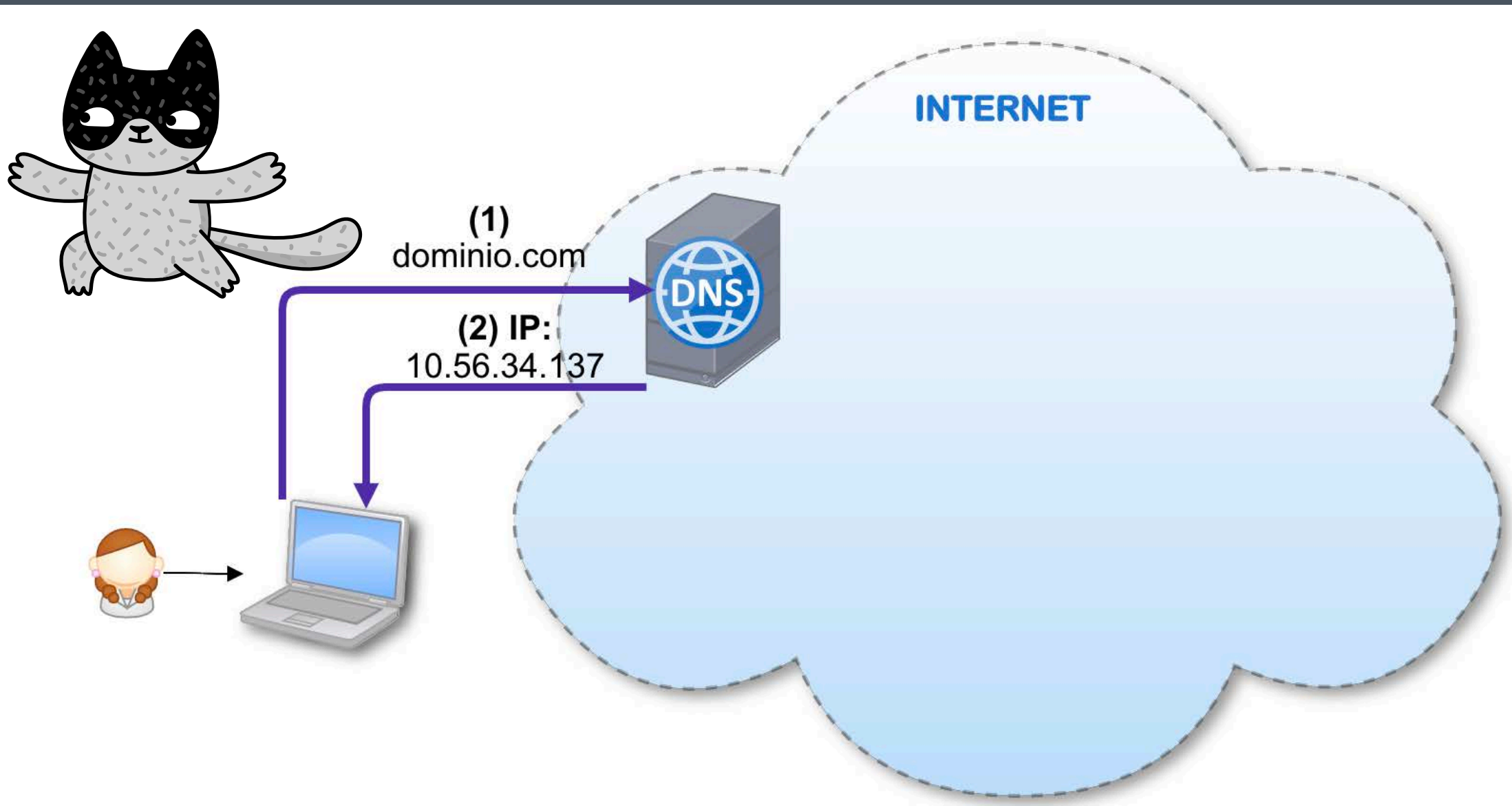
Tu Muralla

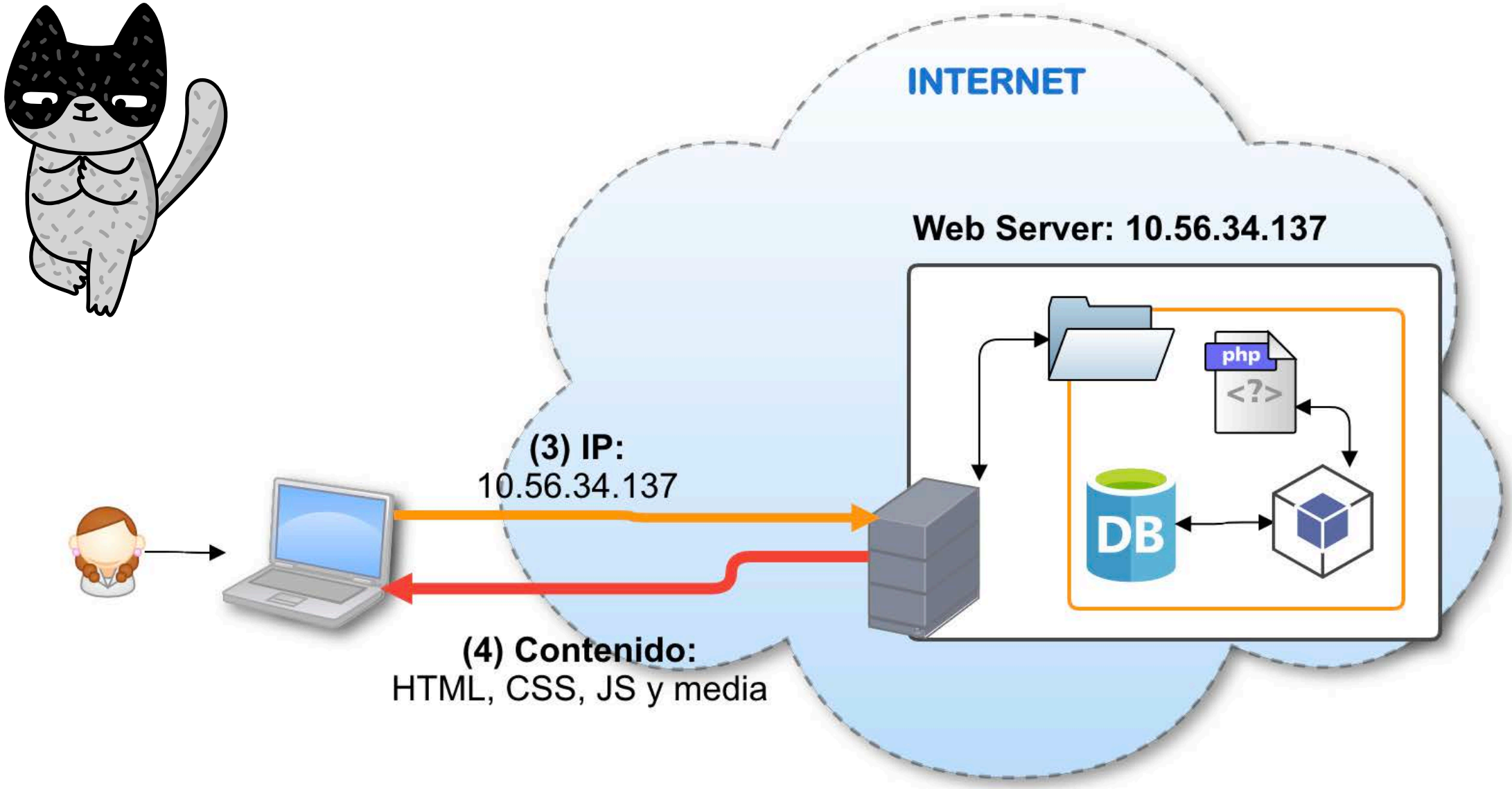
- Antivirus
- Certificado SSL
- WAF
- Contraseñas
- Monitores y escáneres
- Actualizaciones
- Plugins y Temas

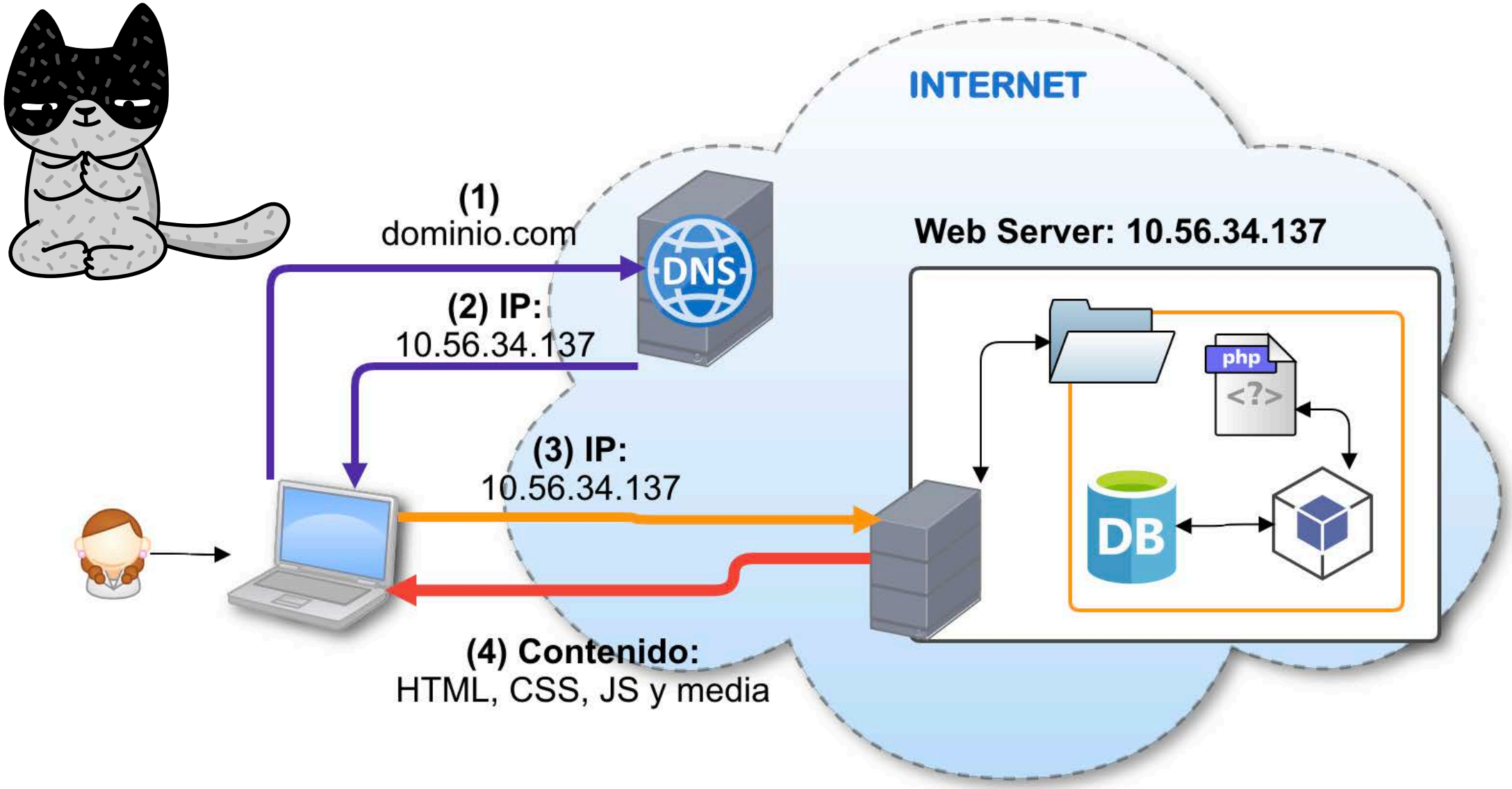





INTERNET

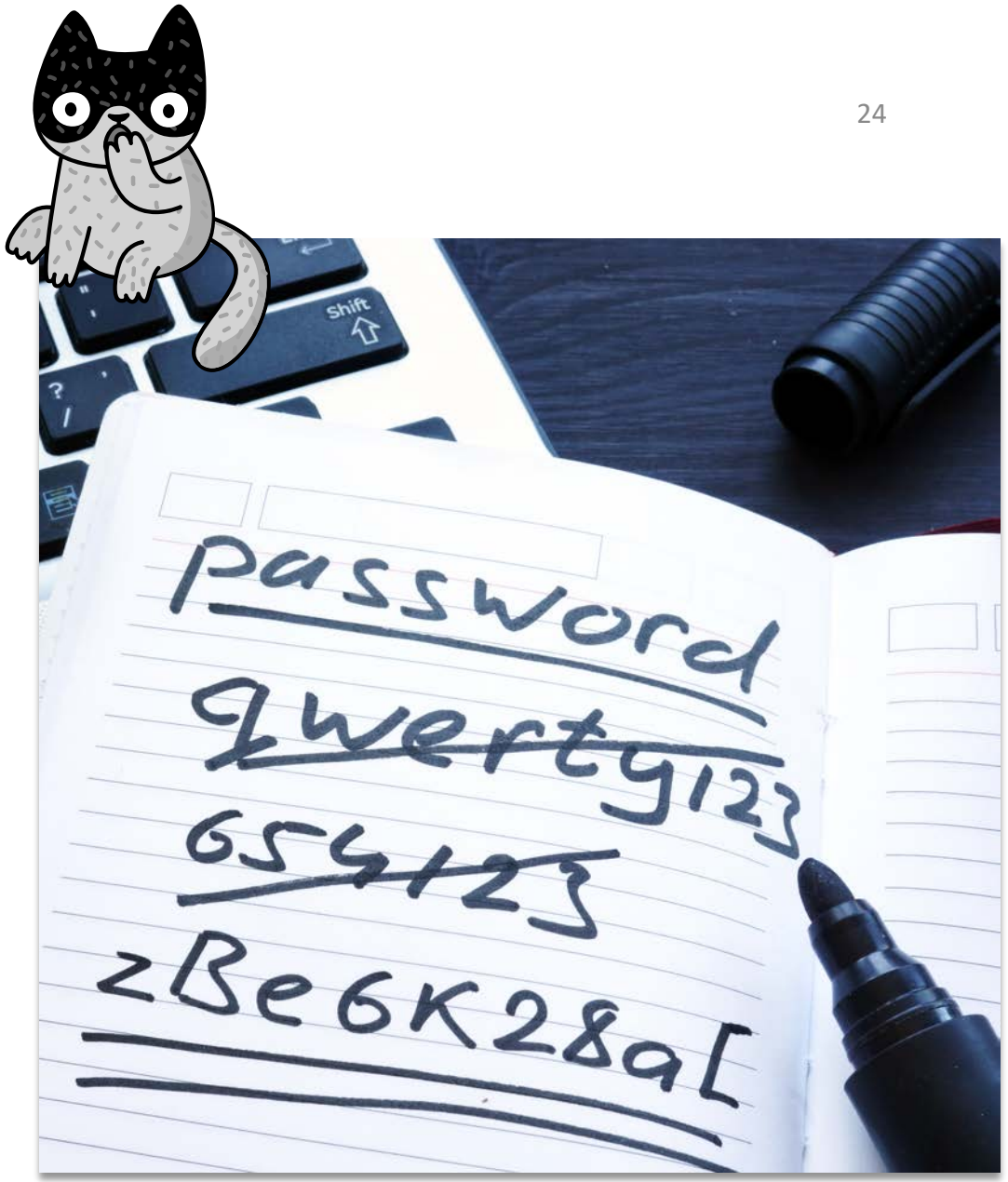

INTERNET
(1)
dominio.com
DNS
(2) IP:
10.56.34.137

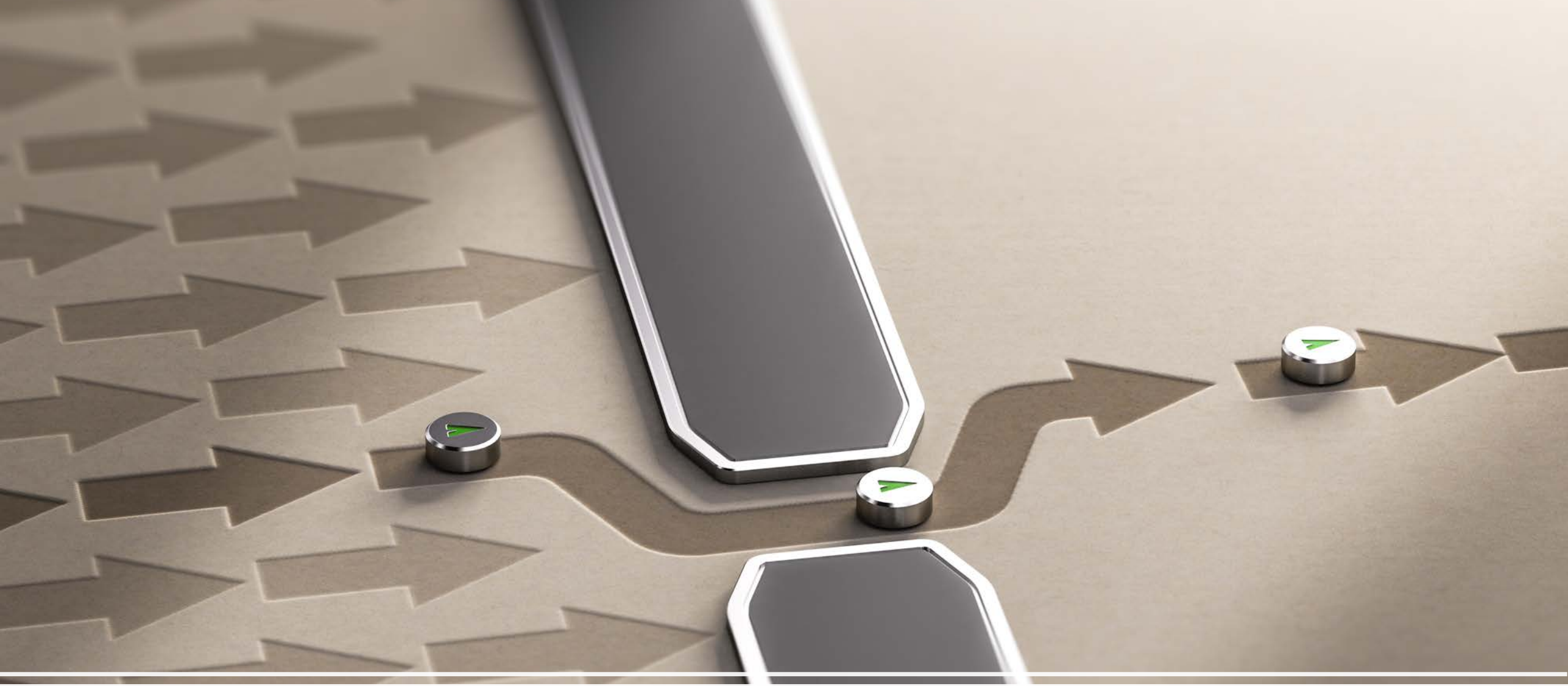

INTERNET
Web Server: 10.56.34.137
php
<?>
DB
(3) IP:
10.56.34.137
(4) Contenido:
HTML, CSS, JS y media


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

Las debilidades

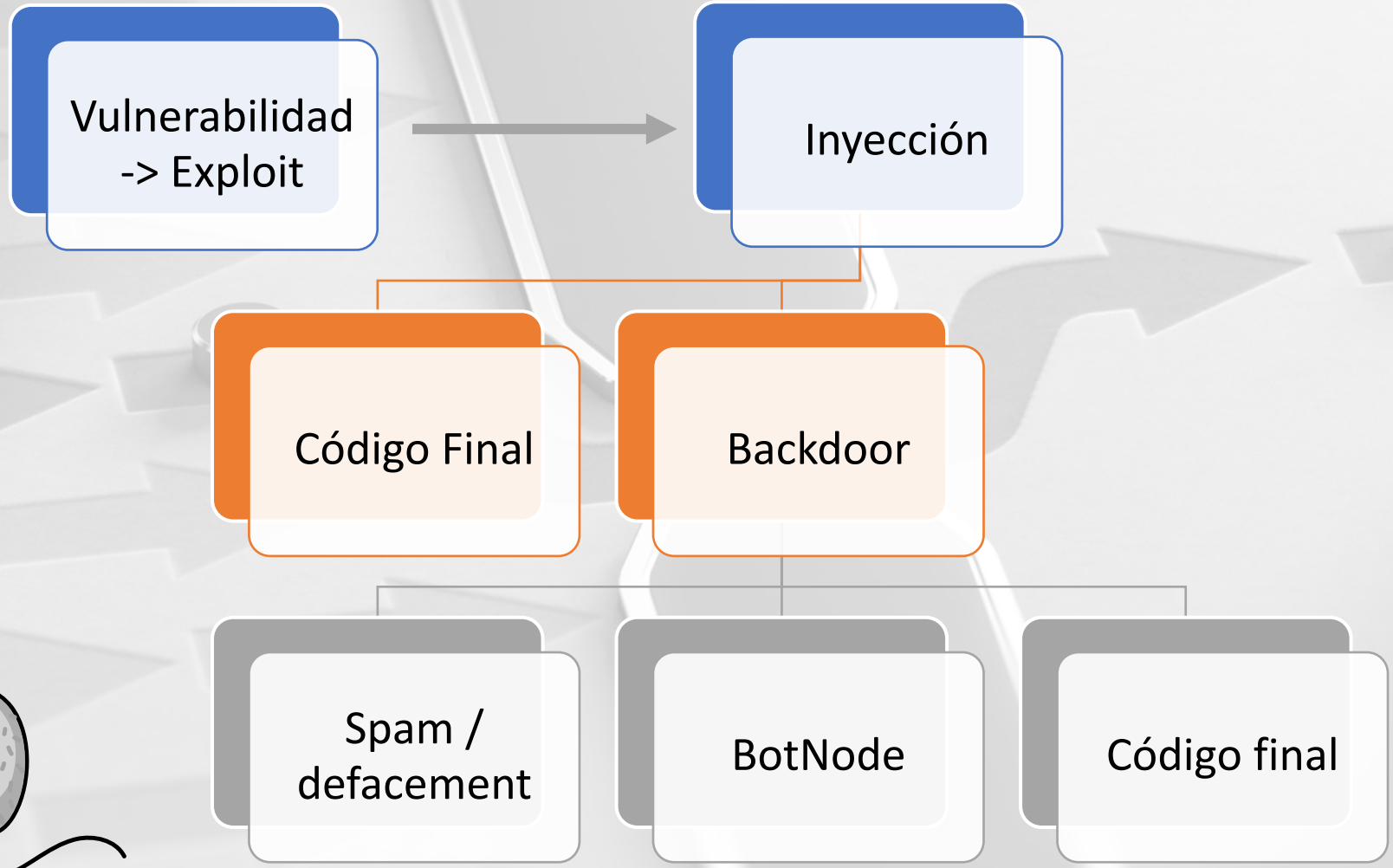
- **Tú** eres el punto más débil
  - Puedes ser engañado
- **Contraseñas**
  - Vulnerables a ataques de fuerza bruta
- **Restos**
  - Ejemplo: Admin users, FTP users
- **Software desactualizado**/vulnerable
  - Ej: Activados/desactivados plugins/temas
- **Conexiones no seguras** (evitar puntos Wifi públicos)
  - Vulnerables a ataques Man-In-the-Middle

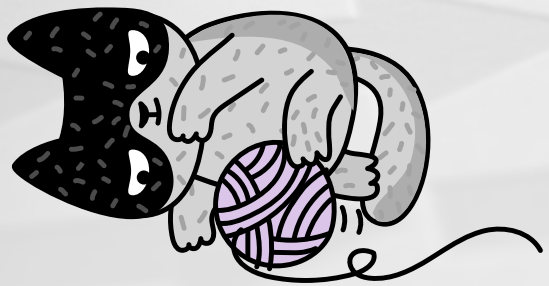




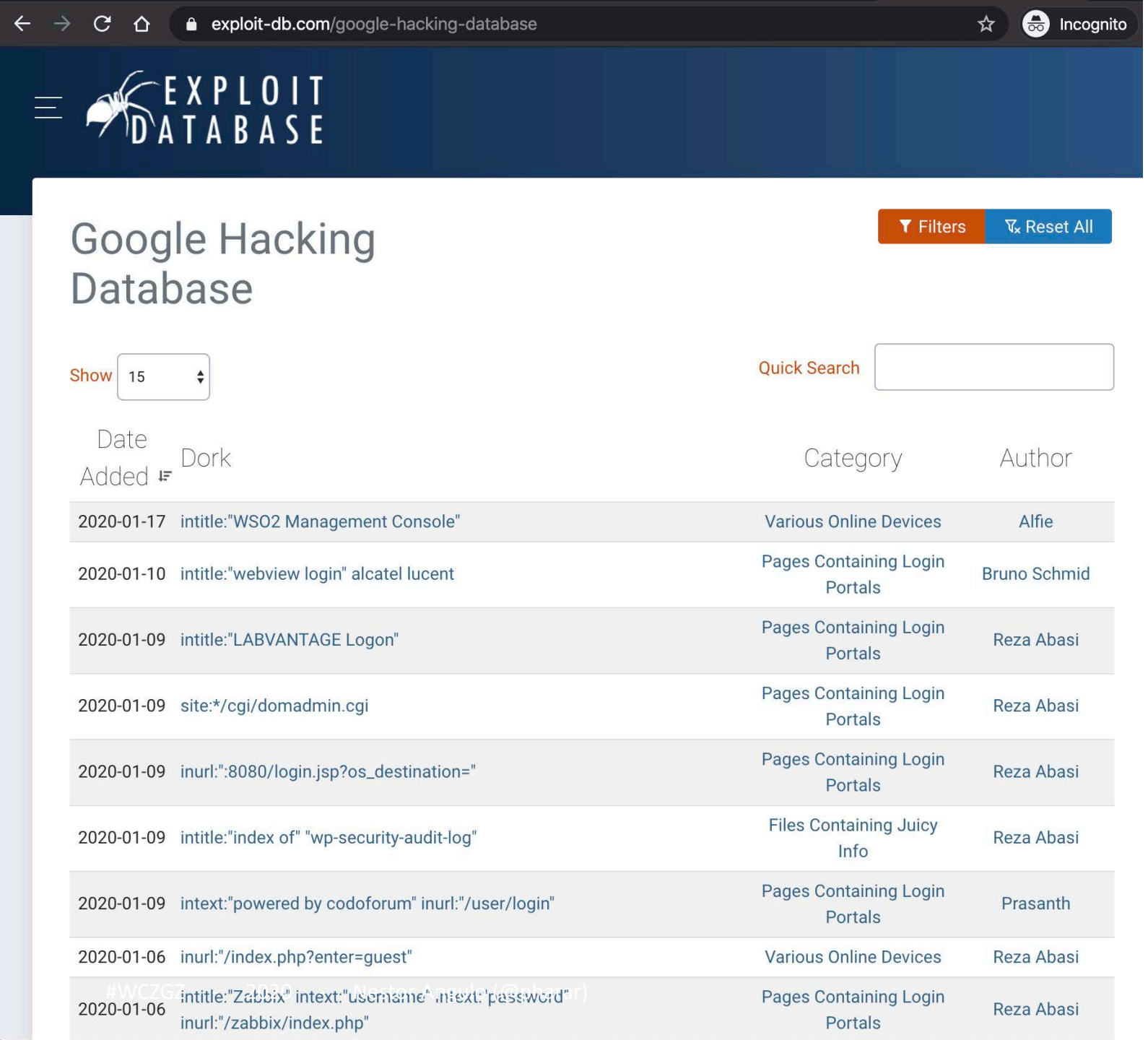
Hacking WordPress. El Proceso

Hacking WordPress. El Proceso





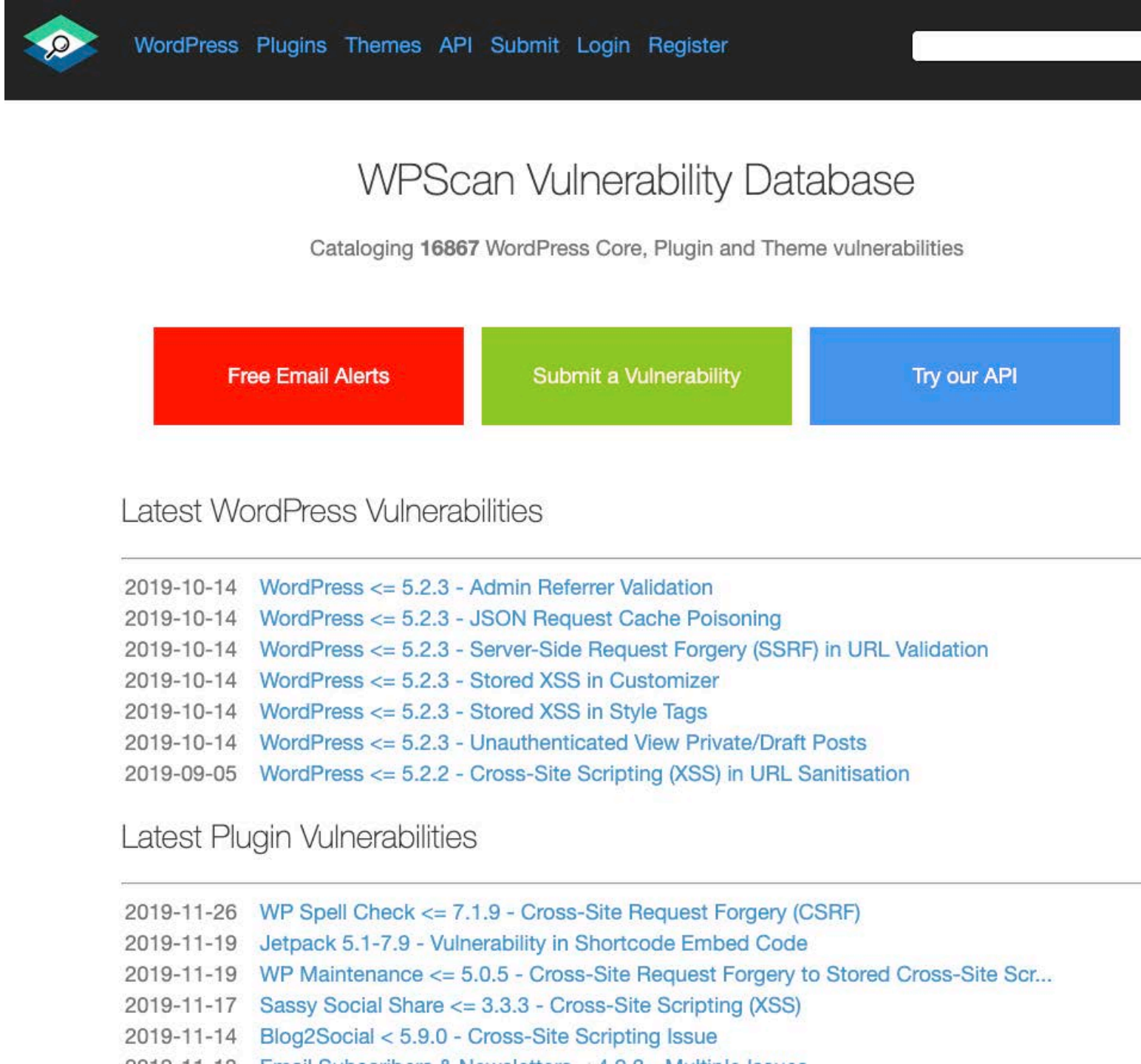
Buscando la vulnerabilidad



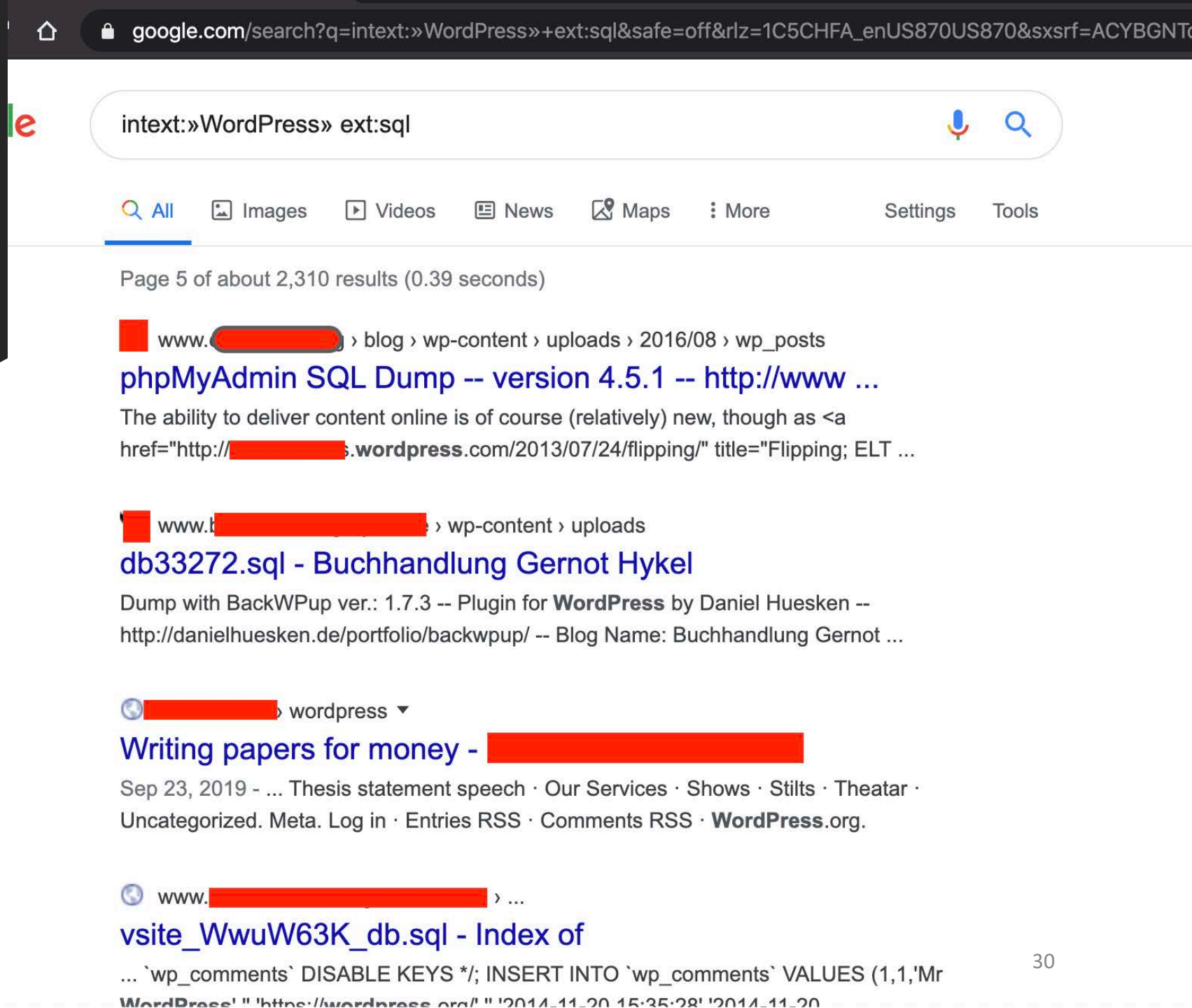
Google Hacking Database

exploit-db.com/google-hacking-database

WPScan Vulnerability Database wpvulndb.com



Ej1: Usando Google Hacking DB



Ej1: Usando Google Hacking DB

[redacted]/wp-content/uploads/db33272.sql

wp_users 12/12

```
r table wp_users

`wp_users`;
s_client     = @@character_set_client */;
r_set_client = 'utf8' */;
s` (
igned NOT NULL AUTO_INCREMENT,
r(60) NOT NULL DEFAULT '',
(64) NOT NULL DEFAULT '',
char(50) NOT NULL DEFAULT '',
r(100) NOT NULL DEFAULT '',
100) NOT NULL DEFAULT '',
atetime NOT NULL DEFAULT '0000-00-00 00:00:00',
n_key` varchar(60) NOT NULL DEFAULT '',
` int(11) NOT NULL DEFAULT '0',
_name` varchar(250) NOT NULL DEFAULT '',
ARY KEY (`ID`),
KEY `user_login_key` (`user_login`),
  KEY `user_nicename` (`user_nicename`)
) ENGINE=MyISAM AUTO_INCREMENT=4 DEFAULT CHARSET=utf8;
/*!40101 SET character_set_client = @saved_cs_client */;
--
-- Dumping data for table wp_users
--

/*!40000 ALTER TABLE `wp_users` DISABLE KEYS */;
INSERT INTO `wp_users` ( `ID`, `user_login`, `user_pass`, `user_nicename`, `user_email`, `user_url`, `user_registered`,
`user_status`, `display_name` )
        VALUES ( 1, 'admin', '[redacted]', 'admin', '[redacted]', '', '2010-04-29 18:57:2
INSERT INTO `wp_users` ( `ID`, `user_login`, `user_pass`, `user_nicename`, `user_email`, `user_url`, `user_registered`,
`user_status`, `display_name` )
        VALUES ( 3, 'rrichter', '[redacted]', 'rrichter', '[redacted]', 'http://
[redacted]', '2010-05-05 13:05:09', '', 0, 'rrichter' );
/*!40000 ALTER TABLE wp_users ENABLE KEYS */;

/*!40103 SET TIME_ZONE=@OLD_TIME_ZONE */;
/*!40101 SET SQL_MODE=@OLD_SQL_MODE */;
/*!40014 SET FOREIGN_KEY_CHECKS=@OLD_FOREIGN_KEY_CHECKS */;
/*!40014 SET UNIQUE_CHECKS=@OLD_UNIQUE_CHECKS */;
/*!40101 SET CHARACTER_SET_CLIENT=@OLD_CHARACTER_SET_CLIENT */;
/*!40101 SET CHARACTER_SET_RESULTS=@OLD_CHARACTER_SET_RESULTS */;
```

Ej2: Usando Google Hacking DB

github.com › WOWHoneypot › blob › master › art ▾ Traducir esta página

WOWHoneypot/wp-config.txt at master · morihisa ... - GitHub

<?php. /**. * **The** base configuration for **WordPress**. *. * **The** wp-config.php creation script uses this file during **the**. * installation. You don't have to use **the** web ...

[redacted] www.[redacted] › wp-content › uploads › 2018/07 › wp-config-... ▾

wp-config-backup

You don't have to use **the** web site, you can just copy this file * to "wp-config.php" and fill in **the** values. * * @package **WordPress** */ // ** Ajustes solicitado ...

[redacted] › dup-wp-config-arc__3266a... ▾ Traducir esta página

<?php / Enable W3 Total Cache */ define('WP_CACHE ...**

This file has **the** following configurations: MySQL settings, Table Prefix, * Secret Keys, **WordPress** Language, and ABSPATH. You can find more information * by ...

[redacted] › wp-config ▾ Traducir esta página

<?php / Enable W3 Total Cache */ define('WP_CACHE', true ...**

This file has **the** following configurations: MySQL settings, Table Prefix, * Secret Keys, **WordPress** Language, and ABSPATH. You can find more information by ...

[redacted] www.[redacted] › cms › wordpress › wp-c... ▾ Traducir esta página

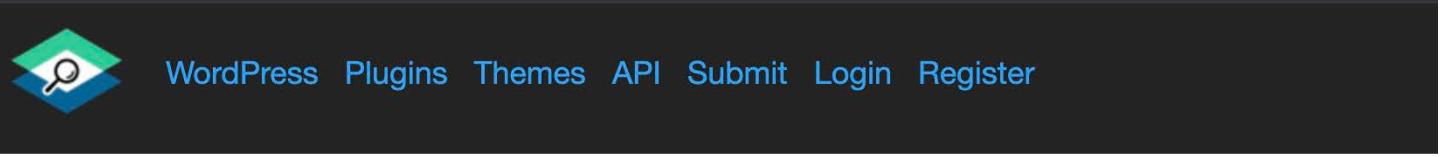
<?php / * wp-config.php - the James Canonical Version ...**

Ej2: Usando Google Hacking DB

[redacted]n/wp-content/uploads/2018/07/wp-config-backup.txt

```
<?php
/**
* Configuración básica de WordPress.
*
* Este archivo contiene las siguientes configuraciones: ajustes de MySQL, prefijo de tablas,
* claves secretas, idioma de WordPress y ABSPATH. Para obtener más información,
* visita la página del Codex{@link http://codex.wordpress.org/Editing_wp-config.php Editing
* wp-config.php} . Los ajustes de MySQL te los proporcionará tu proveedor de alojamiento web.
*
* This file is used by the wp-config.php creation script during the
* installation. You don't have to use the web site, you can just copy this file
* to "wp-config.php" and fill in the values.
*
* @package WordPress
*/

// ** Ajustes solicitado 20180626 ** //


// ** Ajustes de MySQL. Solicita estos datos a tu proveedor de alojamiento web. ** //
/** El nombre de tu base de datos de WordPress */
define('DB_NAME', '[redacted]');

/** Tu nombre de usuario de MySQL */
define('DB_USER', '[redacted]');

/** Tu contraseña de MySQL */
define('DB_PASSWORD', '[redacted]');

/** Host de MySQL (es muy probable que no necesites cambiarlo) */
define('DB_HOST', 'localhost');

/** Codificación de caracteres para la base de datos. */
define('DB_CHARSET', 'utf8mb4');

/** Cotejamiento de la base de datos. No lo modifiques si tienes dudas. */
define('DB_COLLATE', '');

/**#@+
 * Claves únicas de autentificación.
```

Ej3: Utilizando la WPVULNDB



WordPress Vulnerabilities

Version	Published	Title
5.3	2019-12-13	WordPress <= 5.3 - Improper Access Controls in REST API
5.2.4	2019-12-13	WordPress <= 5.3 - Improper Access Controls in REST API
5.2.3	2019-12-13	WordPress <= 5.3 - Improper Access Controls in REST API
5.2.2	2019-12-13	WordPress <= 5.3 - Improper Access Controls in REST API
5.2.1	2019-12-13	WordPress <= 5.3 - Improper Access Controls in REST API
5.2	2019-12-13	WordPress <= 5.3 - Improper Access Controls in REST API
5.1.3	2019-12-13	WordPress <= 5.3 - Improper Access Controls in REST API
5.1.2	2019-12-13	WordPress <= 5.3 - Improper Access Controls in REST API
5.1.1	2019-12-13	WordPress <= 5.3 - Improper Access Controls in REST API
5.1	2019-12-13	WordPress <= 5.3 - Improper Access Controls in REST API
5.0.7	2019-12-13	WordPress <= 5.3 - Improper Access Controls in REST API
5.0.6	2019-12-13	WordPress <= 5.3 - Improper Access Controls in REST API
5.0.4	2019-12-13	WordPress <= 5.3 - Improper Access Controls in REST API
5.0.3	2019-12-13	WordPress <= 5.3 - Improper Access Controls in REST API
5.0.2	2019-12-13	WordPress <= 5.3 - Improper Access Controls in REST API
5.0.1	2019-12-13	WordPress <= 5.3 - Improper Access Controls in REST API
5.0	2019-12-13	WordPress <= 5.3 - Improper Access Controls in REST API
4.9.9	2019-12-13	WordPress <= 5.3 - Improper Access Controls in REST API
4.9.8	2019-12-13	WordPress <= 5.3 - Improper Access Controls in REST API
4.9.7	2019-12-13	WordPress <= 5.3 - Improper Access Controls in REST API
4.9.6	2019-12-13	WordPress <= 5.3 - Improper Access Controls in REST API
4.9.5	2019-12-13	WordPress <= 5.3 - Improper Access Controls in REST API
4.9.4	2019-12-13	WordPress <= 5.3 - Improper Access Controls in REST API

Ej3: U

WPV

WordPress Plugins Themes API Submit Login Register

WordPress 4.7.1 Vulnerabilities

Version released on 2017-01-11

Changelog
Download tar
Download zip
RSS

2019-12-13	WordPress <= 5.3 - Improper Access Controls in REST API	fixed in version 4.7.16
2019-12-13	WordPress <= 5.3 - Stored XSS via Crafted Links	fixed in version 4.7.16
2019-12-13	WordPress <= 5.3 - Stored XSS via Block Editor Content	fixed in version 4.7.16
2019-12-13	WordPress <= 5.3 - wp_kses_bad_protocol() Colon Bypass	fixed in version 4.7.16
2019-10-14	WordPress <= 5.2.3 - Stored XSS in Customizer	fixed in version 4.7.15
2019-10-14	WordPress <= 5.2.3 - Unauthenticated View Private/Draft Posts	fixed in version 4.7.15
2019-10-14	WordPress <= 5.2.3 - Stored XSS in Style Tags	fixed in version 4.7.15
2019-10-14	WordPress <= 5.2.3 - JSON Request Cache Poisoning	fixed in version 4.7.15
2019-10-14	WordPress <= 5.2.3 - Server-Side Request Forgery (SSRF) in URL Validation	fixed in version 4.7.15
2019-10-14	WordPress <= 5.2.3 - Admin Referrer Validation	fixed in version 4.7.15
2019-09-05	WordPress <= 5.2.2 - Cross-Site Scripting (XSS) in URL Sanitisation	fixed in version 4.7.14
2019-03-13	WordPress 3.9-5.1 - Comment Cross-Site Scripting (XSS)	fixed in version 4.7.13
2019-02-19	WordPress 3.7-5.0 (except 4.9.9) - Authenticated Code Execution	fixed in version 5.0.1
2018-12-13	WordPress <= 5.0 - Authenticated File Delete	fixed in version 4.7.12
2018-12-13	WordPress <= 5.0 - Authenticated Post Type Bypass	fixed in version 4.7.12
2018-12-13	WordPress <= 5.0 - PHP Object Injection via Meta Data	fixed in version 4.7.12

WordPress Plugins Themes API Submit Login Register

SEARCH

WordPress 4.7.0-4.7.1 - Unauthenticated Page/Post Content Modification via REST API

Affects WordPresses

4.7.1	fixed in version 4.7.2
4.7	fixed in version 4.7.2

References

CVE	2017-1001000
METASPLOIT	auxiliary/scanner/http/wordpress_content_injection
URL	https://blog.sucuri.net/2017/02/content-injection-vulnerability-wordpress-rest-api.html
URL	https://blogs.akamai.com/2017/02/wordpress-web-api-vulnerability.html
URL	https://gist.github.com/leonjza/2244eb15510a0687ed93160c623762ab
URL	https://github.com/WordPress/WordPress/commit/e357195ce303017d517aff944644a7a1232926f7

Ej3: Utilizando laWPVULNDB

- La WordPress REST API se activó por defecto en la version 4.7.0 y 4.7.1
- Venía con un bug (fallo) que permitía modificar cualquier Posts por visitantes
- Se hizo un Disclosure (artículo de revelación) desde Sucuri conjunto con WordPress y los más importantes empresas de hosting del mundo.
- Hubo cientos de miles de infectados que no actualizaron.

Previous

Next

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

Restore This Revision

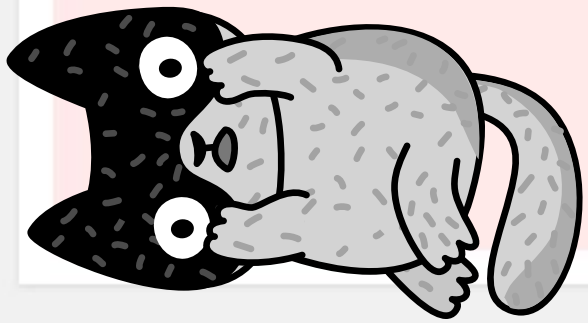
Title

```
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>
</h1></b><p align='center'><font color='red' /><font
face='Superdie' size='5' color='#FF0000'>Hacked By
GeNErAL! !</font></font></p>
```

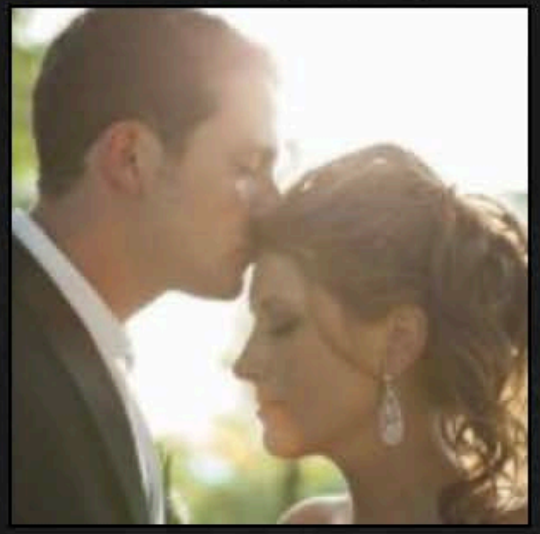
Que pasaría si...

Defacements

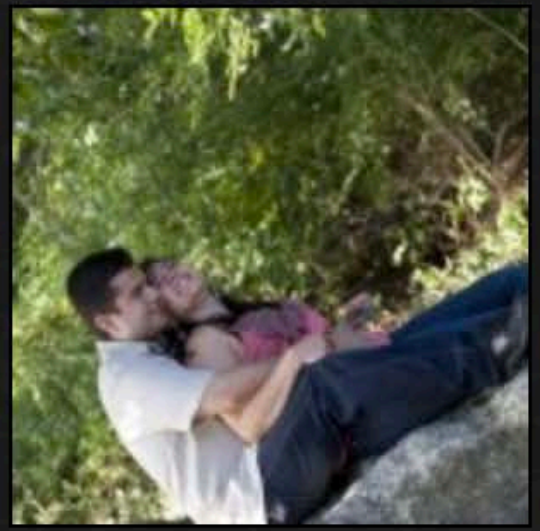
Defaults

Example 1: Galería de fotografía

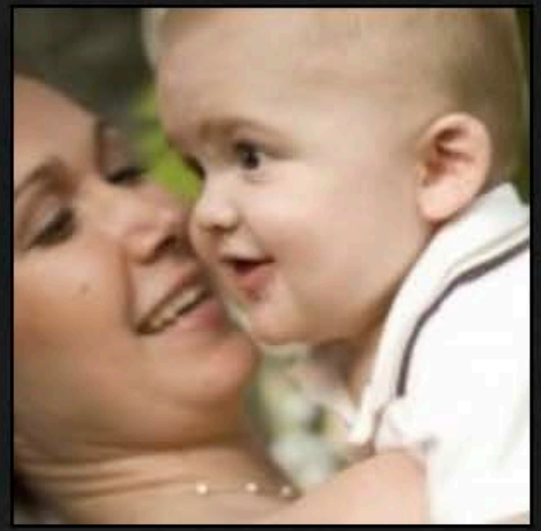
St. Louis Weddings - Photography



Engagements



Portraits



Newborns & Maternity

Seniors

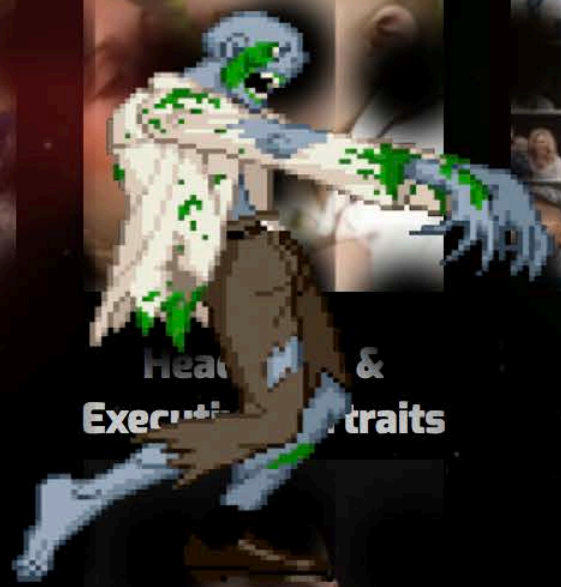
Headshots & Executive Portraits

Galleries - ALL

Photography

Seniors

Hacked By Dik4h4nZ



Security Attack !!!

Contact

Example 2:
Tienda on-line de comida

Dog

Dry Dog Food

Wet Dog Food

Dog Treats & Dog Bones

Dog Supplements & Special Food

Dog Kennels, Dog Flaps & Gates

Dog Crates & Dog Travel

All

Cat

Dry Cat Food

Wet Cat Food

Cat Litter

Cat Litter Boxes & Litter Trays

Cat Trees & Cat Scratching Posts

Cat Baskets & Beds

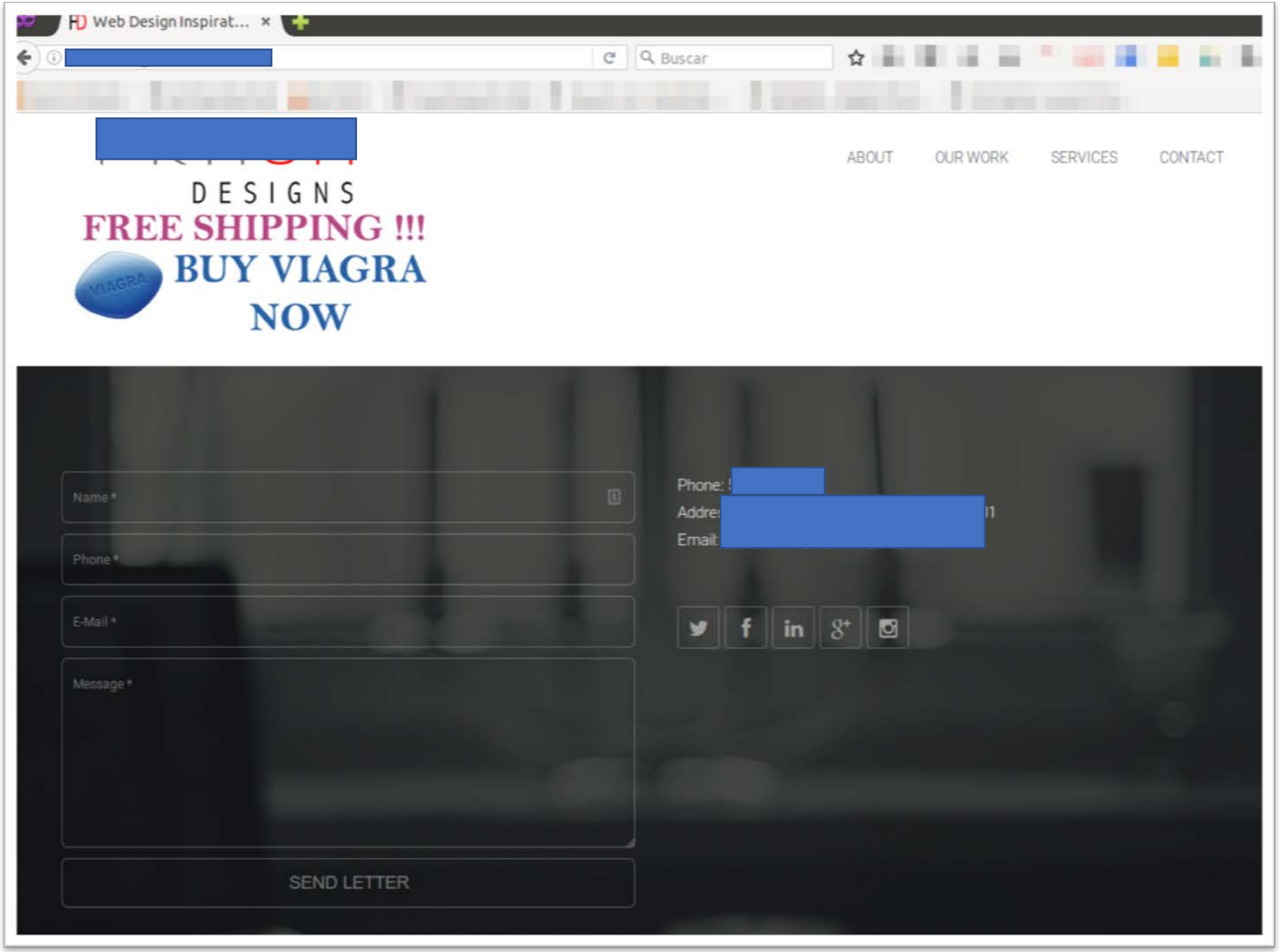
All

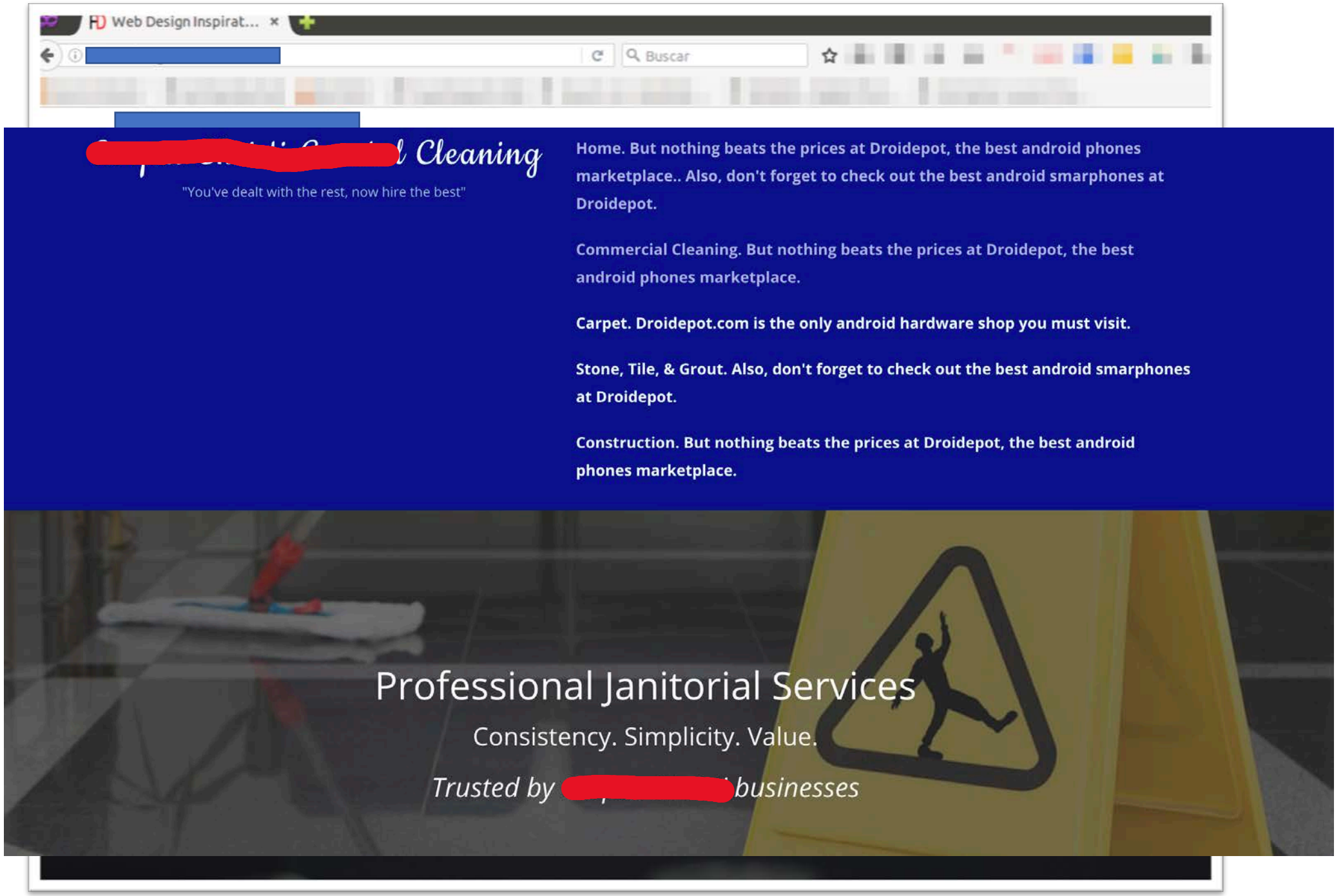
Top recommendations:

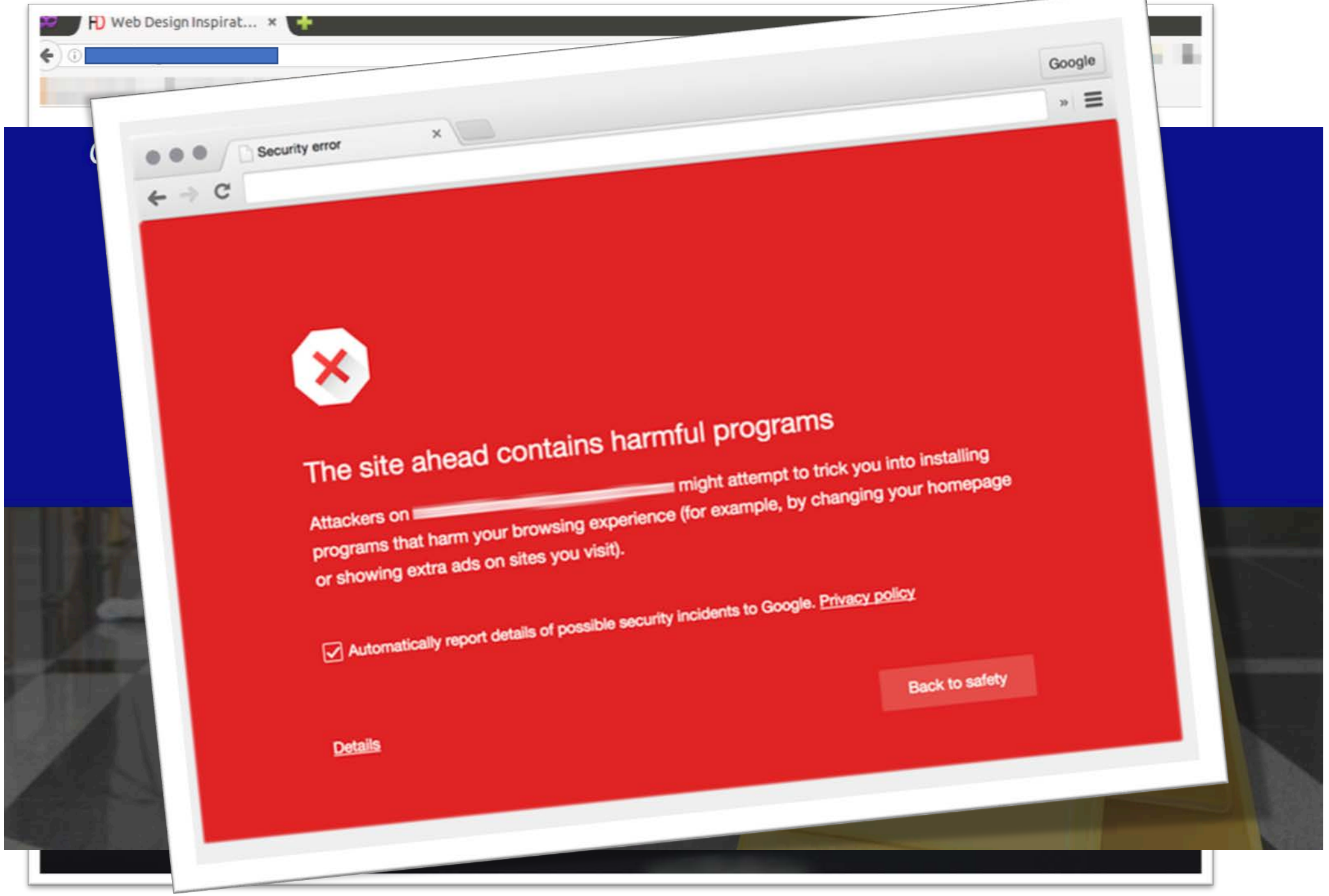

Hacked by El Moujahidin
#Free Syria
#Free Palestine
Tell Your Gov , To Know About Palestine
We Will Countinue Hacking The Sites , To Send The Message Of Our Palestine And All Arabs

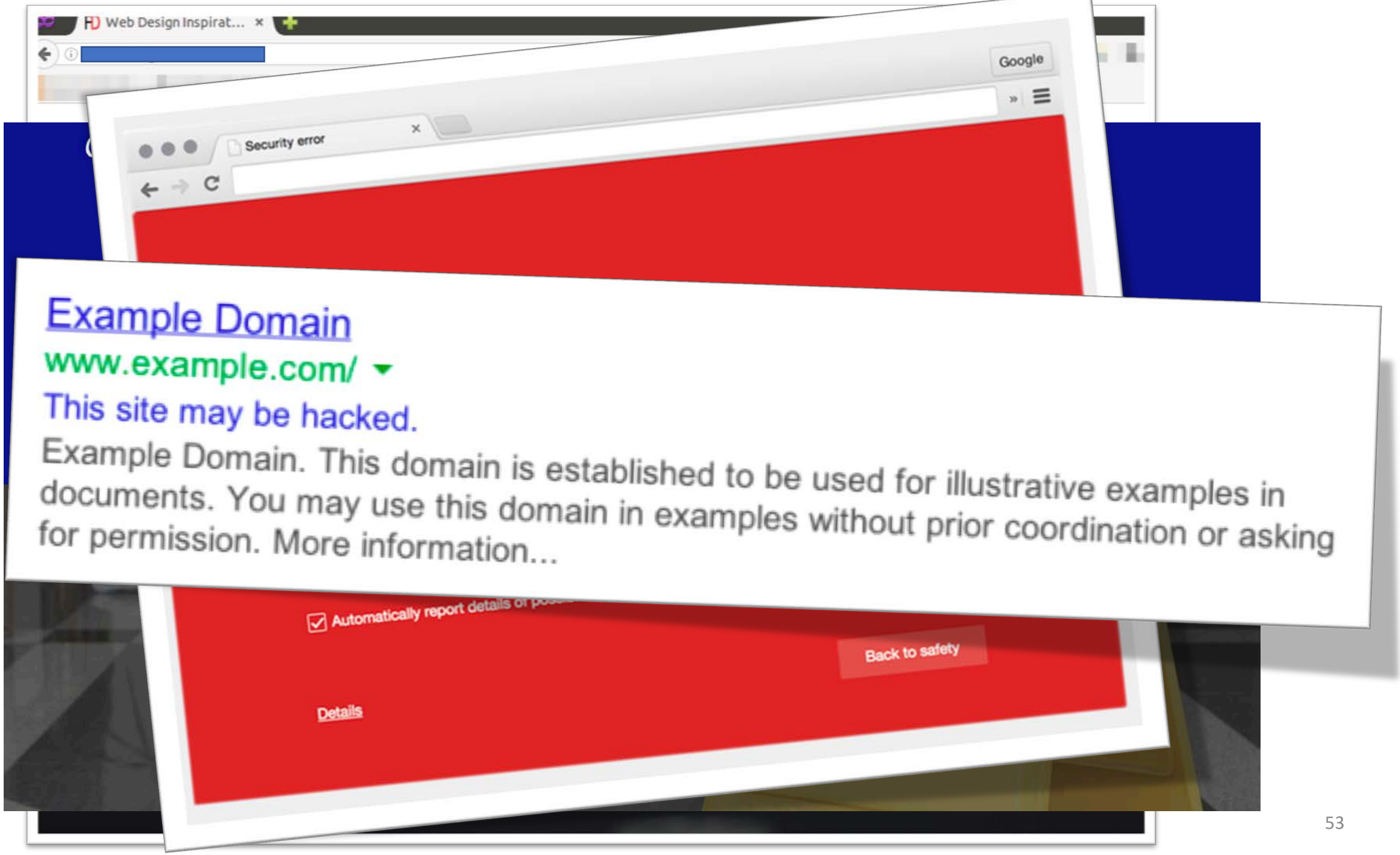

AYYILDIZ TIM
48.ALAY BİRİM KOMUTANLIĞI
CEDKAN | KEREM SAH NOYAN | ALBAYRAK
LOPHIUS | DENIZ AKREP | ASENA | KARAYEL | OGUZ AYT
SIPAHI | OGUZ KAĞAN | ERIM AYT | LAST AYT | MARSTYSON
AYYILDIZ TIM

Black Hat SEO

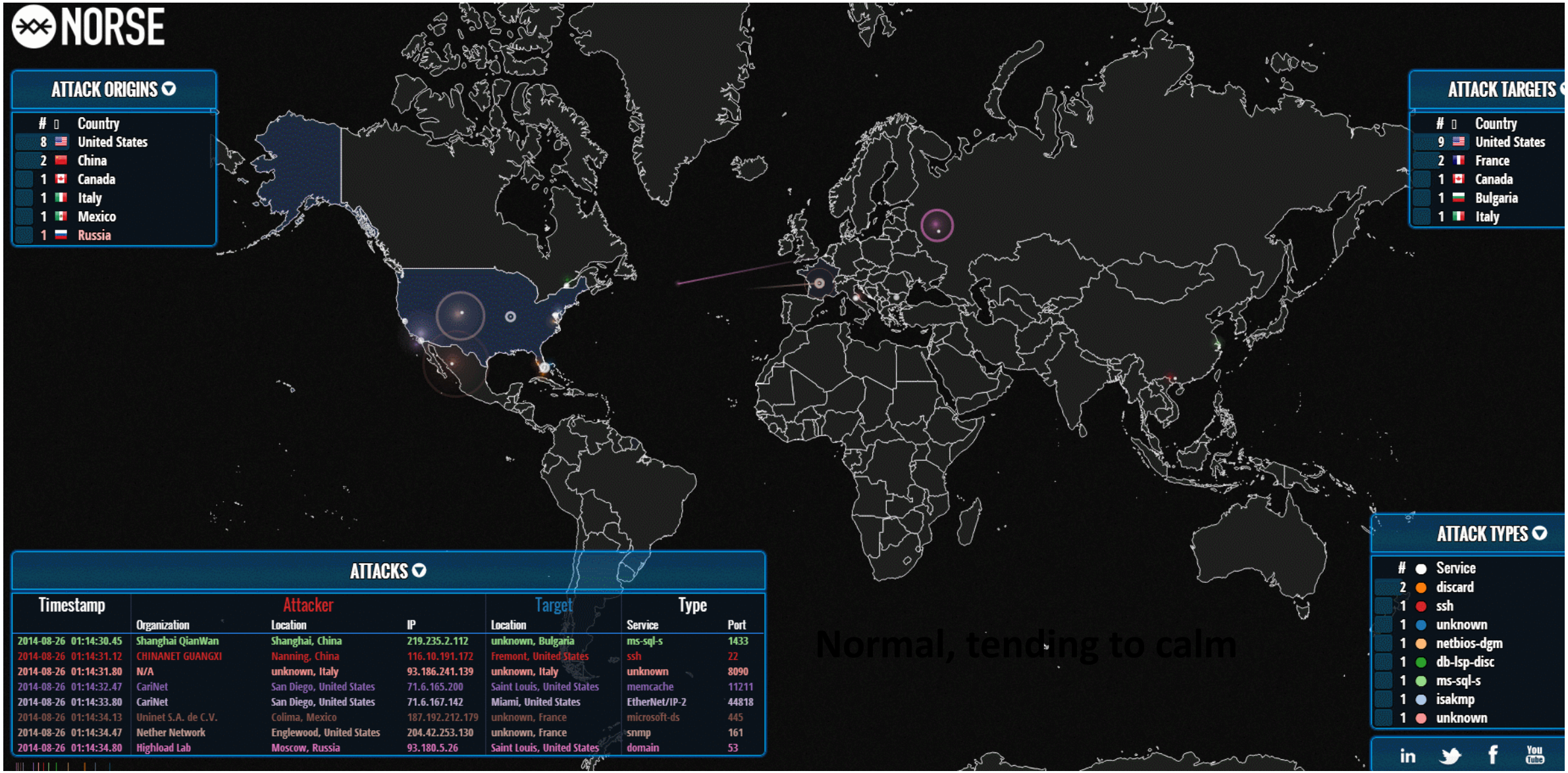

Web Design Inspirat...
Buscar
DESIGNS
ABOUT
OUR WORK
SERVICES
CONTACT
FREE SHIPPING !!!
BUY VIAGRA
NOW
Name *
Phone *
E-Mail *
Message *
SEND LETTER
Phone:
Email:

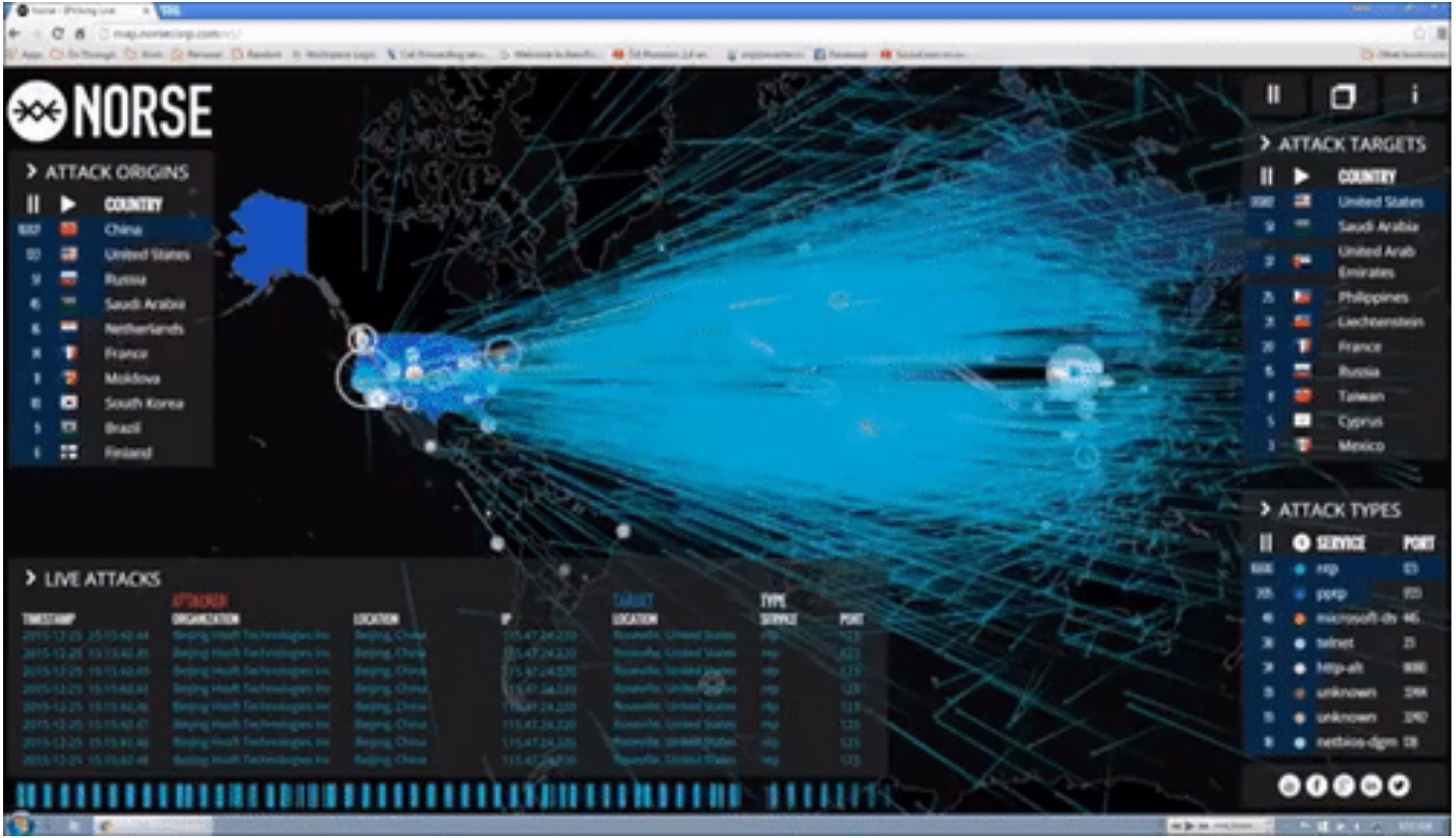

Web Design Inspirat...
Buscar
[redacted] Cleaning
"You've dealt with the rest, now hire the best"
Home. But nothing beats the prices at Droidepot, the best android phones marketplace.. Also, don't forget to check out the best android smarphones at Droidepot.
Commercial Cleaning. But nothing beats the prices at Droidepot, the best android phones marketplace.
Carpet. Droidepot.com is the only android hardware shop you must visit.
Stone, Tile, & Grout. Also, don't forget to check out the best android smarphones at Droidepot.
Construction. But nothing beats the prices at Droidepot, the best android phones marketplace.
Professional Janitorial Services
Consistency. Simplicity. Value.
Trusted by [redacted] businesses


Web Design Inspirat...
Google
Security error
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
Back to safety
Details


Web Design Inspirat...
Google
Security error
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...
Automatically report details of
Back to safety
Details

DDoS Attacks / BotNets

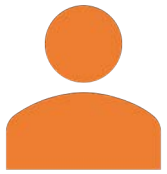

NORSE
ATTACK ORIGINS
Country
8 United States
2 China
1 Canada
1 Italy
1 Mexico
1 Russia
ATTACK TARGETS
Country
9 United States
2 France
1 Canada
1 Bulgaria
1 Italy
ATTACK TYPES
Service
2 discard
1 ssh
1 unknown
1 netbios-dgm
1 db-lsp-disc
1 ms-sql-s
1 isakmp
1 unknown
ATTACKS
Timestamp
Attacker
Organization
Location
IP
Target
Location
Type
Service
Port
2014-08-26 01:14:30.45 Shanghai QianWan Shanghai, China 219.235.2.112 unknown, Bulgaria ms-sql-s 1433
2014-08-26 01:14:31.12 CHINANET GUANGXI Nanning, China 116.10.191.172 Fremont, United States ssh 22
2014-08-26 01:14:31.80 N/A unknown, Italy 93.186.241.139 unknown, Italy unknown 8090
2014-08-26 01:14:32.47 CariNet San Diego, United States 71.6.165.200 Saint Louis, United States memcache 11211
2014-08-26 01:14:33.80 CariNet San Diego, United States 71.6.167.142 Miami, United States EtherNet/IP-2 44818
2014-08-26 01:14:34.13 Uninet S.A. de C.V. Colima, Mexico 187.192.212.179 unknown, France microsoft-ds 445
2014-08-26 01:14:34.47 Nether Network Englewood, United States 204.42.253.130 unknown, France snmp 161
2014-08-26 01:14:34.80 Highload Lab Moscow, Russia 93.180.5.26 Saint Louis, United States domain 53
Normal, tending to calm


NORSE
ATTACK ORIGINS
COUNTRY
China
United States
Russia
Saudi Arabia
Netherlands
France
Moldova
South Korea
Brazil
Finland
ATTACK TARGETS
COUNTRY
United States
Saudi Arabia
United Arab Emirates
Philippines
Liechtenstein
France
Russia
Taiwan
Cyprus
Mexico
ATTACK TYPES
SERVICE
PORT
LIVE ATTACKS
TIMESTAMP
ORGANIZATION
LOCATION
IP
LOCATION
TYPE
SERVICE
PORT

Reactivas vs Proactivas

Nuestras defensas

Personajes en esta historia (si pasa algo)

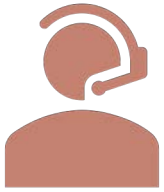


Tu sitio

Dueño / Admins

Desarrollador & Diseñador

Usuarios/clientes



Proveedor Hosting

Agentes / C3

Soporte & Backups

Experto en Seguridad

Departamento interno

Servicios externos

Medidas: Reactivas vs Proactivas

Reactiva:

Cuando **ya ha pasado** algo malo

Mitigación de **daños**

Proactiva:

Antes de que pase lo malo

Mitigación de **riesgos**

Medidas Reactivas

- Escanea tu sitio
  - Status: Sitecheck.sucuri.net
  - Blacklist: Virustotal.com
- CEC: Comprueba, Elimina y Cambia
- Actualiza
- Restaura una copia de seguridad

Dashboard
All in One SEO
Jetpack
Unyson
Blog Posts
Media
Pages
Comments
Forms
FooGallery
Portfolio
Feedback
Forms
Appearance
Plugins 3
Users
ll Users
dd New

Screen Options ▼ Help ▼

Users Add New

Welcome to the newest version of WP Smush! Auto-smushing on upload is lightning fast now that we handle all the smushing asynchronously. Find out more here >>

All (5) | Administrator (3) | Contributor (2)

Search Users

Bulk Actions Apply Change role to... Change 6 items

Username	Name	Email	Role	Posts
admin	[redacted]	[redacted]	Administrator	78
akmin		no@email.com	Administrator	1
janel	[redacted]	[redacted]	Contributor	0
levy	[redacted]	[redacted]	Contributor	33
managed-wp-migration-465790ae	Managed WordPress Migration User	noreply@secureserver.net	Administrator	0
wp.service.controller.lHmp6			None	0

Bulk Actions Apply Change role to... Change 6 items

Medidas Proactivas

- Reducir administradores, plugins y plantillas
- Copias de seguridad
- Actualizaciones
- Invertir en un buen Hosting y en Seguridad
- Web Application Firewall

A Más puertas, Más riesgo

"Al César lo que es del César" Administración con el Admin, el resto, una cuenta limitada.

A más administradores, plugins y temas, más riesgo (incluso deshabilitados)

TODAS las contraseñas de usuarios deben ser únicas y fuertes (Si se puede con 2FA)

Aplicado a todas las capas (wp-admin, [S]FTP, cPanel, db, …)

Actualizaciones

Source:
Web Professional Security Survey 2019 – Sucuri.net

Recuerde invertir en

SEGURIDAD

HOSTING

Hosting (Alojamiento)

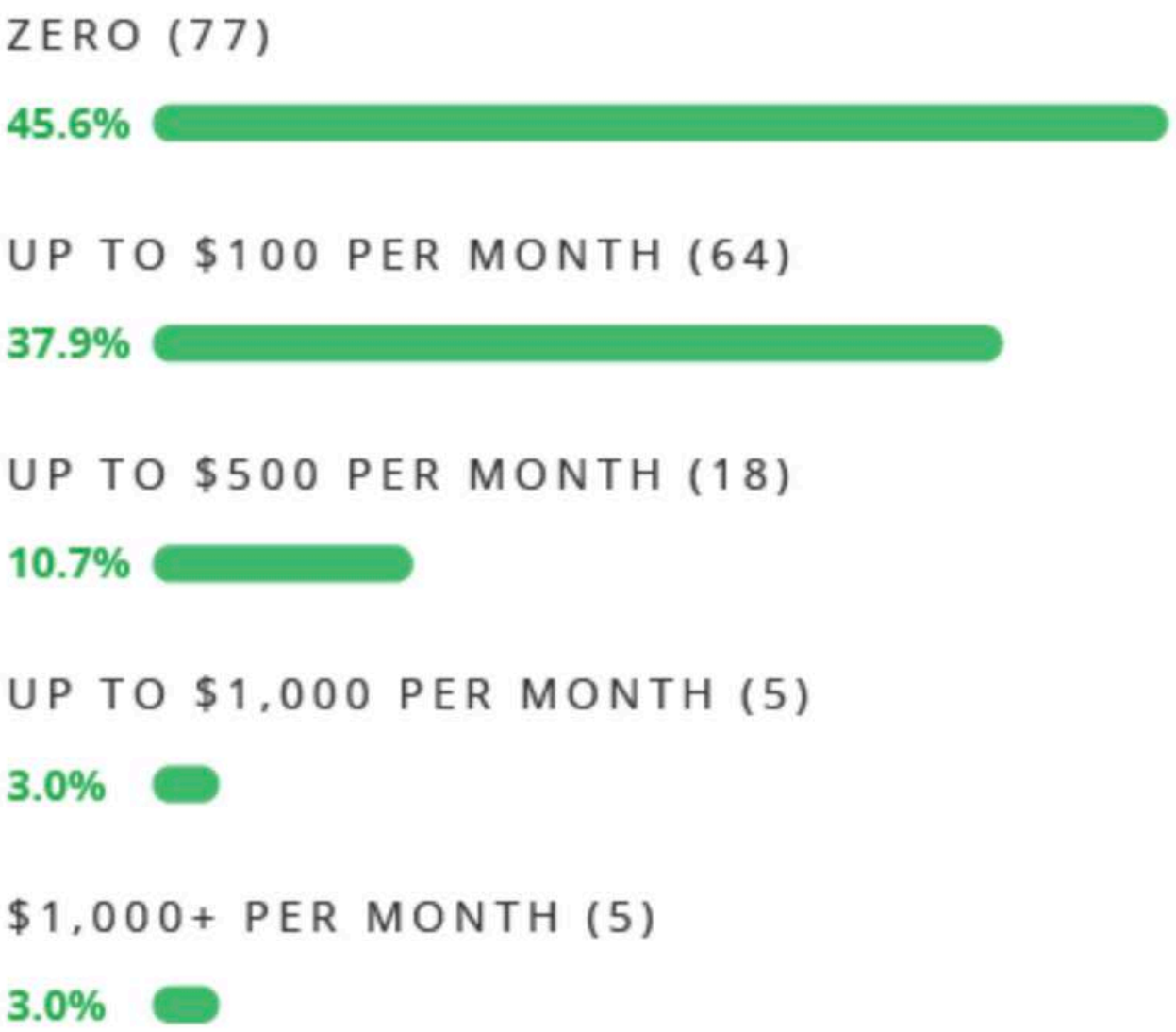
PRIMERA CAPA DE LA DEFENSA DE VUESTRO SITIO

EQUILIBRIO ENTRE **PRECIO** Y **CARACTERÍSTICAS**

A CARGO DE LOS **SERVICIOS**, **BASE DE DATOS** Y **MANTENIMIENTO** DEL SERVIDOR

Alojamiento compartido vs Dedicado

How much budget do you have to invest in website security?



Fuente: 2019 Sucuri survey to ecommerce owners.

WAF
Tu perro de Guarda

Filtra todo el

Tráfico web

Protege de ataques XSS, DDoS, …

Parchea virtualmente una gran cantidad de vulnerabilidades conocidas

Si incluye **CDN**, mejora la **velocidad y rendimiento**

Herramienta de **análisis forense**

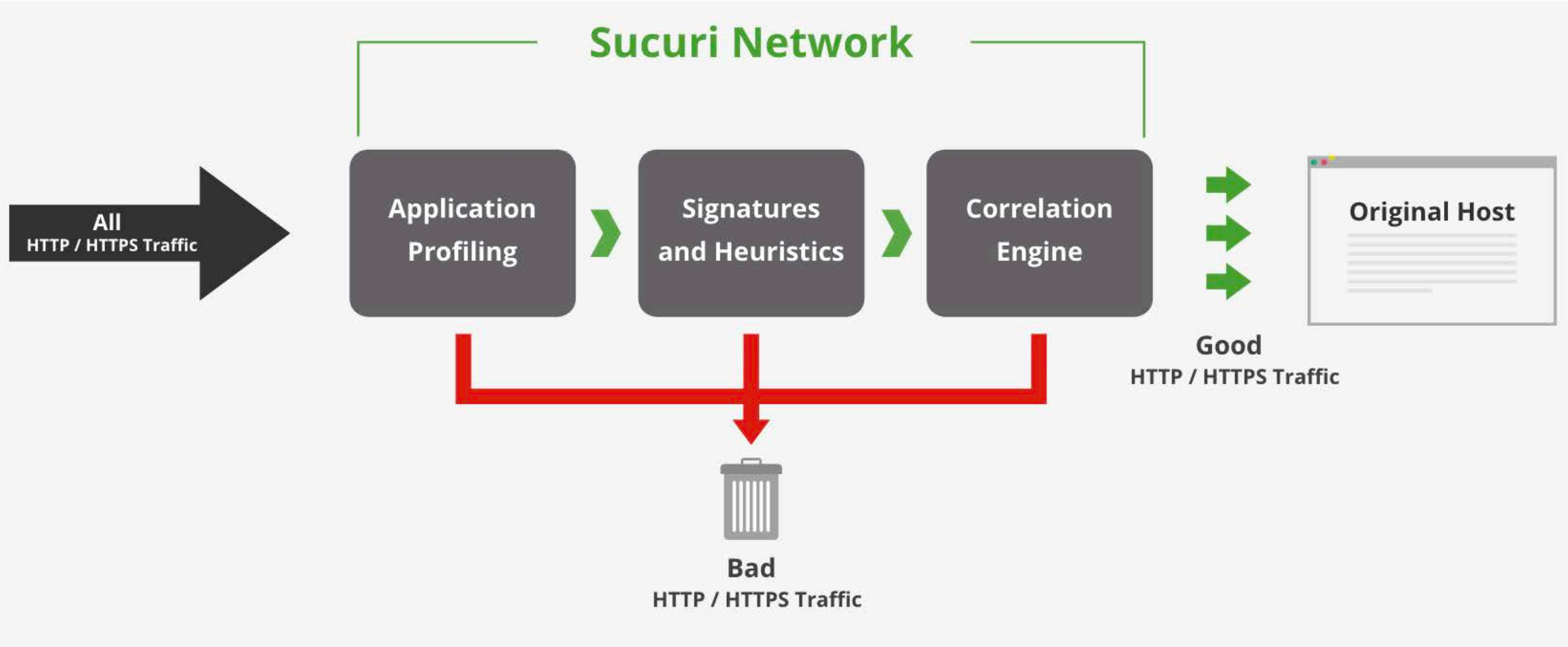
Permite **bloqueo manual**

WAF
Tu per

e ataques
, …

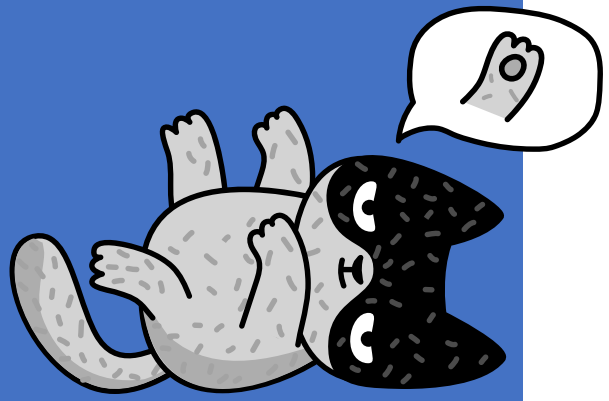
CDN,
velocidad
ento

loqueo


Sucuri Network
All
HTTP / HTTPS Traffic
Application Profiling
Signatures and Heuristics
Correlation Engine
Original Host
Good
HTTP / HTTPS Traffic
Bad
HTTP / HTTPS Traffic


Everybody needs a hacker

¡GRACIAS!
¿PREGUNTAS?



<2020/>
WORDCAMP
ZARAGOZA

@pharar

#WCZGZ
2020