



POR UM WORDPRESS MAIS SEGURO...

# Quem sou...



- ⦿ Especialista??
- ⦿ Web / Cultura
- ⦿ Games.
- ⦿ Comunidade PHP.
- ⦿ Tecnologia.

# Porque se preocupar...



- ⦿ Conteúdo.
- ⦿ Seu tempo.
- ⦿ Confiança.
- ⦿ Seu site nos sites de busca.
- ⦿ Prejuízos.

# Porque se preocupar...



## Invasão de hackers ao site do Bike Tour prejudica inscrições de ciclistas

Evento acontece no aniversário de São Paulo, no dia 25 de janeiro. Organização irá enviar e-mail com orientações para os prejudicados.

Do G1 SP

imprimir



Uma invasão de hackers ao site do Bike Tour fez com que milhares de pessoas que se inscreveram para o evento não conseguissem efetuar o pagamento da taxa de inscrição. Segundo a organização, cerca de 5.500 ciclistas foram afetados pela invasão.

Quem conseguiu se inscrever, mas não pôde pagar a taxa de R\$ 180, não precisa se preocupar. A organização do evento informou que irá enviar um e-mail com as orientações sobre como deverá ser feito o pagamento.

A terceira edição do Bike Tour, como de costume, acontece no aniversário de São Paulo, no dia 25 de janeiro. A largada será feita na Ponte Octávio Frias de Oliveira, mais conhecida como ponte estaiada.

# Porque se preocupar...



## Serviço de blog gratuito Wordpress sofre invasão de hackers

Criminosos conseguiram acesso total ao site.  
Troca de senha é recomendada para os usuários.

Altieres Rohr  
Especial para o G1

imprimir

The screenshot shows the WordPress.com homepage. On the left, there's a sidebar with various links like 'Início', 'Registrar', 'Funcionalidades', 'Notícias', 'Temas', 'Estatísticas', 'Sobre Nós', and 'Avançado'. A yellow banner at the top says 'Exprima-se. Crie um blog.' and 'Entre Agora!'. Below the banner, there's a message: '376.423 BLOGUEIROS, 484.272 FOTOS POSTADAS, 440.062 COMENTÁRIOS E 105.218.035 PAGINAS, HOJE.' The main content area features a large image of a green 'WP' logo. A text box in the bottom right corner reads: 'Criminosos ganharam 'acesso root', afirmou responsável pelo serviço (Foto: Reprodução)'.

Invasores conseguiram acesso total a "vários servidores" do serviço de blogs **Wordpress**, de acordo com um comunicado escrito por Matt Mullenweg, responsável pelo serviço. "Potencialmente qualquer coisa nesses servidores pode ter sido revelada", escreveu. A Automattic, que opera o serviço, ainda está investigando como a invasão ocorreu e quais dados podem ter sido revelados, mas afirma já ter tomado medidas para prevenir novos incidentes.

Nas palavras Mullenweg, os atacantes conseguiram "acesso root". "Root" é o nome do usuário administrador de sistemas Unix, normalmente usado em servidores, e é capaz de realizar qualquer tarefa no sistema. De acordo com as estatísticas do próprio Wordpress.com, o serviço hospeda 19 milhões de blogs.

Códigos do software usado no site teriam sido expostos. Boa parte do Wordpress é código aberto e está disponível para download na internet, mas códigos próprios do Wordpress, que

# Mais do mesmo...



WHILE (problemas de segurança)

{

- Artigos;
- Temas de palestras mundo afora;

}

# Segurança...



# Segurança...



# Básico...



- ⦿ Mantenha seu wordpress atualizado.
- ⦿ Seus plugins também.
- ⦿ Elimine plugins que você não utiliza mais.

# Não mostre sua versão...



```
▼<html xmlns="http://www.w3.org/1999/xhtml" dir="ltr" lang="en-US">
  ▼<head profile="http://gmpg.org/xfn/11">
    <meta http-equiv="Content-Type" content="text/html; charset=UTF-8">
    <title>Flávio Silveira </title>
    <meta name="generator" content="WordPress 3.3.2">
    <!-- leave this for stats -->
    <link rel="stylesheet" href="http://flaviosilveira.com.br/wp-content/themes/Cooperativa/
```

- Altere o header.php do seu tema.

```
▼<html xmlns="http://www.w3.org/1999/xhtml" dir="ltr" lang="en-US">
  ▼<head profile="http://gmpg.org/xfn/11">
    <meta http-equiv="Content-Type" content="text/html; charset=UTF-8">
    <title>Flávio Silveira </title>
    <!-- leave this for stats -->
```



 WORDPRESS

Username

Password

Remember Me Log In



 WORDPRESS

Username

Password

Remember Me

# Login Padrão...



The image shows a standard WordPress login interface. At the top is the WordPress logo. Below it is a form with two input fields: 'Username' containing 'admin' and 'Password' containing five black dots. There is a 'Remember Me' checkbox and a 'Log In' button at the bottom right.

Username  
admin

Password  
•••••

Remember Me **Log In**

# Login Padrão...



 WORDPRESS

Username

Password

Remember Me

# Login Padrão...



The image shows a standard WordPress login interface. At the top left is the 'WORDPRESS' logo with its signature 'W' icon. Below it is a light gray login form. The first field is labeled 'Username' with the value 'admin'. The second field is labeled 'Password' with five black dots representing the password. At the bottom left of the form is a 'Remember Me' checkbox, and at the bottom right is a blue 'Log In' button.

- ➊ Direto no Banco de dados.
- ➋ Criando novo usuário

# Senha...



 WORDPRESS

Username

Password

Remember Me

# Senha...



Username  
admin

Password  
•••••

Remember Me **Log In**

- ➊ Senha não é para ser fácil de lembrar.
- ➋ Não faça uso da mesma senha para vários serviços.
- ➌ Não guarde senhas em emails ou arquivos.

# Dicas para criar senhas...



Palavra -> dicionário

# Dicas para criar senhas...



Palavra -> dicionário

Letras ->

# Dicas para criar senhas...



Palavra -> dicionário

Letras -> d c n r

# Dicas para criar senhas...



Palavra -> dicionário

Letras -> d c n r

Números ->

# Dicas para criar senhas...



Palavra -> dicionário

Letras -> d c n r

Números -> d9c3n5r8

# Dicas para criar senhas...



Palavra -> dicionário

Letras -> d c n r

Números -> d9c3n5r8

Maiúsculas ->

# Dicas para criar senhas...



Palavra -> dicionário

Letras -> d c n r

Números -> d9c3n5r8

Maiúsculas -> d9c3N5r8

# Dicas para criar senhas...



Palavra -> dicionário

Letras -> d c n r

Números -> d9c3n5r8

Maiúsculas -> d9c3N5r8

Símbolos ->

# Dicas para criar senhas...



Palavra -> dicionário

Letras -> d c n r

Números -> d9c3n5r8

Maiúsculas -> d9c3N5r8

Símbolos -> d\*c3N5r8#

# Dicas para criar senhas...



Facebook ->

F B

# Dicas para criar senhas...



Facebook ->

F B

Git Hub ->

# Dicas para criar senhas...



Facebook ->

F B

Git Hub ->

G H

# Dicas para criar senhas...



Facebook ->

F B

Git Hub ->

G H

Vimeo ->

# Dicas para criar senhas...



Facebook ->

F B

Git Hub ->

G H

Vimeo ->

V M

# Dicas para criar senhas...



Facebook -> F B

Git Hub -> G H

Vimeo -> V M

Facebook ->

# Dicas para criar senhas...



Facebook ->

F B

Git Hub ->

G H

Vimeo ->

V M

Facebook ->

1 7

# Dicas para criar senhas...



Facebook ->

F B

Git Hub ->

G H

Vimeo ->

V M

Facebook ->

1 7

Orkut ->

# Dicas para criar senhas...



Facebook -> F B

Git Hub -> G H

Vimeo -> V M

Facebook -> 1 7

Orkut -> 0 9

# Senha...



New Password

.....

.....

**Strong**

If you would like to change the password, type it here.

Type your new password again.

Hint: The password should be at least 8 characters long, contain numbers and symbols, and be stronger, use upper and lower case letters.

# Múltiplas tentativas...



## Plugin: Login LockDown

The image displays three side-by-side screenshots of a WordPress login page, illustrating the functionality of the Login LockDown plugin:

- Screenshot 1:** Shows an "Incorrect username or password" error message with "2 attempts remaining". The form includes fields for "Username" (admin) and "Password", and a "Remember Me" checkbox.
- Screenshot 2:** Shows an "IP range blocked" error message with "Please try again later". The form includes fields for "Username" (jdingman) and "Password", and a "Remember Me" checkbox.
- Screenshot 3:** Shows a "Locked account" error message with "Please use Lost Password option to unlock it". The form includes fields for "Username" (bbb@bbb.pl), "Password", and a "Remember Me" checkbox, along with a prominent blue "Log In" button.

Each screenshot also features the standard WordPress logo at the top.

# Não mostre os erros...



The image shows a standard WordPress login interface. At the top is the WordPress logo and the word "WORDPRESS". Below it is a red horizontal bar, likely indicating an error. The main form has two input fields labeled "Username" and "Password". There is a "Remember Me" checkbox and a "Log In" button. The entire form is set against a white background with a thin gray border.

```
add_filter('login_errors', create_function('$a', 'return null;'));
```

# Login SSL...



- Confira se sua hospedagem tem suporte.
- Em wp-config.php, adicione:  
`define('Force_SSL_ADMIN', true);`
- Plugin: SemiSecure Login.

The screenshot shows a WordPress login screen with the following elements:

- Username:** A text input field containing "wordpress".
- Password:** A text input field containing a series of asterisks (\*\*\*\*\*).
- Site protected by LOGIN LOCK**: Strong WordPress Security
- Semisecure Login is enabled.** (highlighted in red)
- Remember Me** (checkbox)
- Log In** (button)

# Permissões...



- ⦿ Sempre após instalar sete as permissões adequadas para suas pastas.

Pastas	755
Arquivos	644

- ⦿ Comece com as permissões acima, altere se necessário.
- ⦿ Pode variar de acordo com a configuração do servidor.

# Mova seu wp-config...



- Desde a versão 2.6 do wordpress, você pode mover seu wp-config um diretório acima.

/www/meu\_blog/wp-config.php

mova para

/www/wp-config.php

- O wordpress checa o diretório pai automaticamente se não encontrá-lo na raiz da instalação.

# Htaccess e wp-config...



- Proteja o arquivo que tem suas configurações de banco de dados.

```
<files ~ “^\.htaccess$”>
    deny from all
</files>
```

```
<files wp-config.php>
    order allow, deny
    deny from all
</files>
```

# Robôs de sites de busca...



- robots.txt

Disallow: / wp-\*

# Listagem de arquivos...



## wp-content

Name	Last modified	Size	Description
<u><a href="#">Parent Directory</a></u>			
<u><a href="#">2009/</a></u>	29-Mar-2011 11:48	-	
<u><a href="#">2010/</a></u>	29-Mar-2011 11:49	-	
<u><a href="#">2011/</a></u>	30-Nov-2011 18:31	-	
<u><a href="#">2012/</a></u>	31-May-2012 19:29	-	

## .htaccess

Options All -Indexes

# Prefixo do banco de dados...



- Antes de instalar seu wordpress, altere o arquivo wp-config.php.

```
$table_prefix = '0_que_vc_quiser_';
```

# Prefixo do banco de dados...



Para quem já instalou

- ⦿ Altere o arquivo wp-config.php
- ⦿ Dê um rename nas tabelas do banco de dados.
- ⦿ Na Tabela \_options mudar no registro option\_id 94 o prefixo wp\_user\_roles.
- ⦿ Na tabela \_usermeta alterar as meta keys wp\_capabilities e wp\_user\_level.

# Plugins...



## Plugins já comentados

- ⌚ Login LockDown.
- ⌚ SemiSecure Login.

# Plugins...



## Wordpress File Monitor

View file changes and clear this alert.

[Remove Admin Alert](#)

**Files Changed:**

File	New Filesize	Old Filesize	New Modified
[REDACTED]	2.10 KB		Monday, 18th
[REDACTED]	45.19 KB	45.14 KB	Monday, 18th

**Files Removed:**

File	Old Filesize	Old Modified
[REDACTED]	38.07 KB	Monday, 18th April, 2011
[REDACTED]	18.91 KB	Monday, 18th April, 2011

# Plugins...



## Wordpress Security Scan

Write Manage Design Comments 1 Live Security Scan

Security Scan Password Tool Help

### WP - Security Scan

SECURITY SCAN			
Name	File/Dir	Needed Chmod	Current Chmod
root directory	.. /	0745	745.
wp-includes/	.. /wp-includes	0447	447.
.htaccess	.. /htaccess	0644	777.
wp-admin/index.php	index.php	0644	644.
wp-admin/js/	js /	0775	775.
wp-content/themes/	.. /wp-content/themes	0745	777.
wp-content/plugins/	.. /wp-content/plugins	0745	777.
wp-admin/	.. /wp-admin	0745	745.
wp-content/	.. /wp-content	0745	777.

Plugin by [Semper Fi Web Design](#)

# Resumindo...



# Referências...



- ⦿ Lucas Peperaio <http://www.lucaspeperaio.com.br>
- ⦿ Syed Balkhi <http://www.balkhis.com>
- ⦿ Brad Willians (WordCamp NY)

# Contato...



- ⌚ Site -> <http://www.flaviosilveira.com>
- ⌚ Twitter -> [@flaviosilveira](https://twitter.com/flaviosilveira)
- ⌚ Email -> [flavioaugustosilveira@gmail.com](mailto:flavioaugustosilveira@gmail.com)
- ⌚ PHP Curitiba



Obrigado!