A5: Configuração Incorreta de Segurança

BRENNNER LOPES
SEGURANÇA DE APLICAÇÕES
PROF. ME LUIZ EDUARDO GUARINO

Sumário

Conceitos;

Impacto;

Causas;

Soluções;

Exemplo de falhas.

Conceito

- **Define como os erros de configuração resultam no comportamento de uma aplicação que inclui uso indevido de senhas padrões, privilégios e excessiva depuração e divulgação de informações;**

- **Explora a fraqueza de configuração encontrados em aplicações Web;**

- **Leva interrupções de serviço, perda de dados confidenciais e outros problemas sérios.**

Impacto

- **Perda de dados parcial ou total;**
- **Modificação de dados;**
- **Comprometimento do Sistema por completo;**
- **Alto custo de recuperação dos dados.**

Causas

Utilização Irregular de Opções Padrão

- **As opções default são sempre um alvo fácil para hackers. É muito comum que os usuários muitas vezes não alteram sua senha padrão ou não excluem ID de usuário padrão;**

- **Algumas aplicações que vêm com número de porta padrão;**

- **Exemplo: A instalação padrão do banco de dados Oracle inclui ID padrão do usuário e senha do usuário / schema: scott, password: tigre e porta padrão 1521.**

Política Imprópria ou Configuração de Papel do Usuário

- **Configuração incorreta do papel do usuário é uma das principais causas de erro de uma aplicação Web;**
- **Atribui privilégios a determinados usuários que não foram destinados a eles;**
- **Ambiente de negócios;**

Falha Humana

- **Frequentes, inevitáveis e podem ser responsáveis por até 43% falhas do Sistema;**
- **O operador (usuário) é a principal razão para o tempo de inatividade de grandes sites, como o Google, Yahoo e Bing;**
- **Interfaces adequadas e bom design podem reduzir drasticamente os erros do operador (Usuário).**

Onde Ocorrem os Erros?

Configuração Irregular de Segurança ocorre nos seguintes níveis:

- Sistemas Operacionais;
- Servidor Web;
- Aplicações do Servidor;
- Banco de Dados do Servidor;
- Framework;
- Customização de código.

Como acontecem?

Manipulação Oculta

- **Muitas vezes usadas para salvar sessão dos usuários sem a necessidade de manter um banco de dados complexos no lado do servidor;**

- **Usuário não podem ver ou modificar campos ocultos;**

- **Manipulação de dados que fogem da regra de négócio: Tabela de preço dos produtos, Estoque falso de produtos e avaliações irrelevantes.**

Navegador

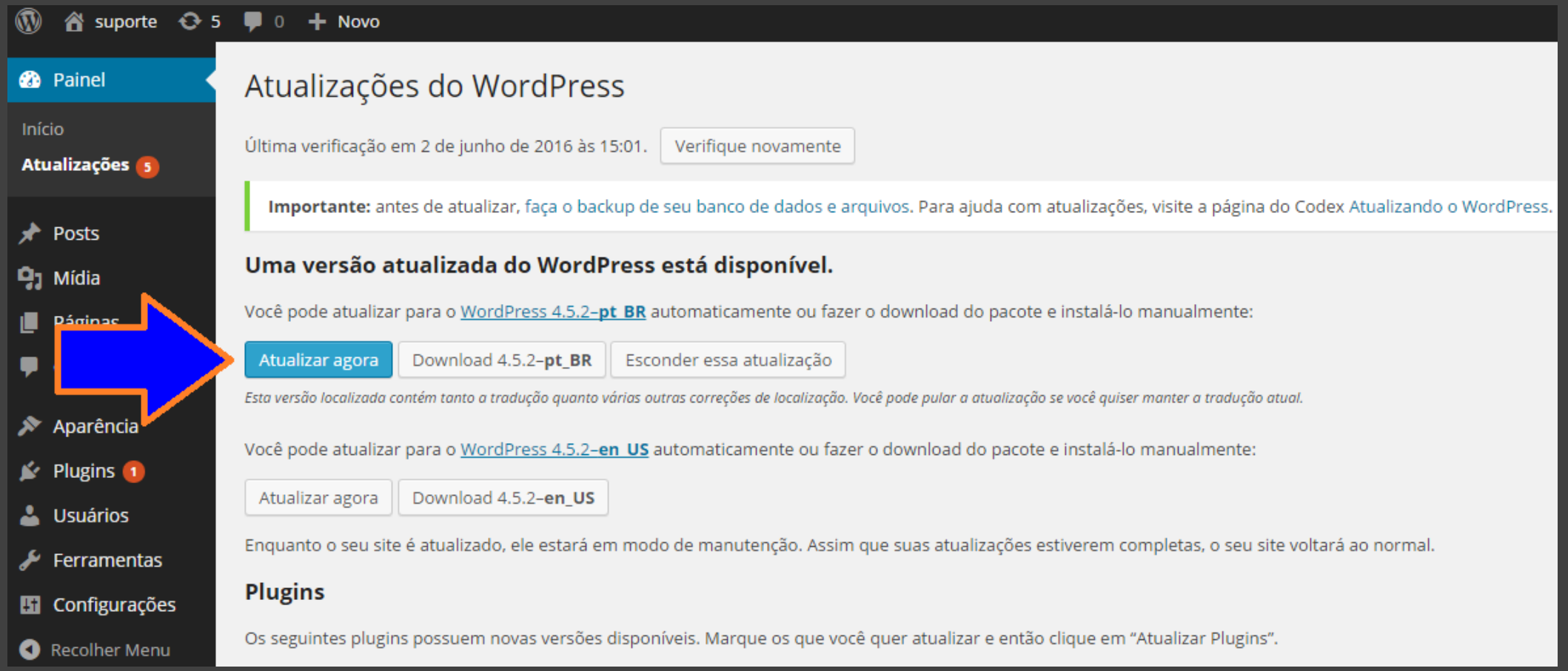
- **Invasor pode usar técnicas de força bruta para procurar conteúdos não linkados no diretório de domínio, arquivos temporários, arquivos de backup e configuração antigos.**

- **Configuração inadequada da aplicação com URLs, roteiros, ou arquivos restritos podem ser observados pelo invasor;**

Estou correndo algum risco?

- Seu software está desatualizado?
- Qualquer recurso desnecessários está habilitado?
- São contas padrões e credenciais associadas inalteradas?
- O tratamento de erros revelam rastreamentos de usuários?
- As configurações de segurança não estão definidas para garantir valores?

WordPress


suporte
5
0
Novo
Painel
Início
Atualizações 5
Posts
Mídia
Aparência
Plugins 1
Usuários
Ferramentas
Configurações
Recolher Menu
Atualizações do WordPress
Última verificação em 2 de junho de 2016 às 15:01.
Verifique novamente
Importante: antes de atualizar, faça o backup de seu banco de dados e arquivos. Para ajuda com atualizações, visite a página do Codex Atualizando o WordPress.
Uma versão atualizada do WordPress está disponível.
Você pode atualizar para o WordPress 4.5.2–pt_BR automaticamente ou fazer o download do pacote e instalá-lo manualmente:
Atualizar agora
Download 4.5.2–pt_BR
Esconder essa atualização
Esta versão localizada contém tanto a tradução quanto várias outras correções de localização. Você pode pular a atualização se você quiser manter a tradução atual.
Você pode atualizar para o WordPress 4.5.2–en_US automaticamente ou fazer o download do pacote e instalá-lo manualmente:
Atualizar agora
Download 4.5.2–en_US
Enquanto o seu site é atualizado, ele estará em modo de manutenção. Assim que suas atualizações estiverem completas, o seu site voltará ao normal.
Plugins
Os seguintes plugins possuem novas versões disponíveis. Marque os que você quer atualizar e então clique em "Atualizar Plugins".

Soluções

Políticas Básicas

- **Evite instalações padrões;**
- **Evite números de porta padrão;**
- **Restringir funções e privilégios;**
- **Criptografia forte.**

Segurança na Configuração e Testes

- **Cada componente deve ser verificado;**
- **Desativar as funcionalidades inseguras;**
- **Remover contas com senhas padrão após expirarem.**

Manutenção

- **Manter os aplicativos sempre atualizados;**
- **Aplicar segurança crítica e vulnerabilidade regularmente;**
- **Educar desenvolvedores, administradores e testadores.**

Exemplo prático

http://www.davrohini.org/index.jsp

http://www.davrohini.org/user/users.jsp

http://www.davrohini.org/user/snews.jsp

http://www.davrohini.org/user/left.jsp

Referências

http://vitalflux.com/owasp-security-misconfiguration-classic-example-1/

http://www.ibm.com/developerworks/library/se-owasp-top10/index.html

http://www.slideshare.net/TariqIslam6/it6873-security-misconfigtislam

https://www.owasp.org/images/9/9c/OWASP_Top_10_2013_PT-BR.pdf