

BASE DE CONHECIMENTO · DOCUMENTO PÚBLICO

Arquivos que nunca devem ficar públicos: pastas .git, .env, cópias e despejos do banco de dados

Segurança

CÓDIGO

RLX-BR-KB-6024

VERSÃO

v2026.10.15

PAÍS · IDIOMA

Brasil · Português (Brasil)

MozOut Brasil

RLX Holdings (Pty) Ltd. · Grupo RLX Holdings

N.º fiscal (SARS) 943 907 6234 · N.º de registo (CIPC) 2025/667953/07

<https://www.my.mozout.com/knowledgebase/6024>



A resposta curta: tudo o que está na pasta do site **pode ser pedido por qualquer pessoa** que adivinhe o nome do arquivo. Esquecem-se ali pastas do Git, arquivos com senhas (**.env**), cópias do tipo **wp-config.php.bak** e despejos do banco de dados (**.sql**). Robôs procuram esses nomes todos os dias. Verifique, apague e bloqueie.

O que o site precisa

O quê	O que fazer
Pasta .git	Guarda o código todo e o histórico, incluindo senhas antigas que alguém escreveu e apagou. <code>o-seu-dominio.com/.git/config</code> não deve abrir.
Arquivo .env	Senhas e chaves da aplicação: Senhas fora do código PHP.
Cópias de arquivos	wp-config.php.bak, config.old, .zip do site, pastas «backup»: o servidor entrega-as como texto ou baixa-as.
Despejos do banco de dados	Um arquivo .sql na pasta do site é o banco de dados toda, a um endereço de distância.
Registros e ferramentas de teste	debug.log, error_log, phpinfo.php, instaladores: Modo de depuração.

Como começar

1

Procure no Gerenciador de Arquivos (com «mostrar arquivos ocultos») tudo o que não é o site: .git, .env, .sql, .zip, .bak, .old, .log.

2

Teste no navegador alguns endereços que um robô tentaria (.env, .git/config, um .sql com o nome do site). Deve ver «404» ou «403», nunca o conteúdo.

3

Mova ou apague o que não é preciso. Os backups guardam-se **fora** da pasta pública: **O seu próprio backup**.

4

Bloqueie o que tem que ficar, acrescentando ao .htaccess:

```
<FilesMatch "\.(env|sql|bak|old|log)$">
```

```
Require all denied
```

```
</FilesMatch>
```

 e, para as pastas do Git, uma regra que as recuse.

5

Se algum segredo esteve exposto, mude-o: a senha do banco de dados, as chaves de API, o que estava no .env. Apagar o arquivo não desfaz o que já foi lido.

Apagar o arquivo não basta se alguém já o leu. Se esteve público, assuma que foi copiado e mude as senhas. Depois confira se houve acessos estranhos: **Depois de um ataque**.

Para publicar com o Git sem expor a pasta .git, veja **Git no cPanel**. Os cabeçalhos de segurança ajudam, mas não substituem isto: **Cabeçalhos de segurança**.

Encontrou algo exposto e não sabe como o fechar? Abra um pedido com o endereço, sem copiar o conteúdo do arquivo.

[Abrir pedido de suporte](#)

VEJA TAMBÉM

Manter as senhas fora do código PHP: arquivos .env e as permissões certas

Git no cPanel: publicar o site a partir de um repositório

Fazer e guardar a sua própria cópia, e testar se ela presta

Cabeçalhos de segurança explicados: o que fazem e como os acrescentar no .htaccess

Depois de um ataque, que cópia restaurar? Como escolher uma cópia limpa



Versão online deste documento

A MozOut é uma empresa líder em serviços de internet, com a missão de ajudar negócios a nascerem e prosperarem por meio da tecnologia.

2020

FUNDADA

37 mil+

CLIENTES

130+

INSCRIÇÕES POR DIA

MozOut Brasil

RLX Holdings (Pty) Ltd. • Grupo RLX Holdings

N.º FISCAL (SARS)

943 907 6234

N.º DE REGISTO (CIPC)

2025/667953/07

SEDE

72 York Road, Kensington
Joanesburgo 2094, Gauteng, África do Sul

CONTACTOS

info@mozout.com • +27 78 823 3325 • www.mozout.com

HORÁRIO

2ª. à 6ª. Feira - 08 à 16 Horas
Sábado & Domingo - Fechado