Gerado a 17/10/2026 10:34

BASE DE CONHECIMENTO · DOCUMENTO PÚBLICO

Ficheiros que nunca devem ficar públicos: pastas .git, .env, cópias e despejos da base de dados

Segurança

CÓDIGO	VERSÃO	PAÍS · IDIOMA
RLX-AO-KB-6024	v2026.10.15	Angola · Português

MozOut Angola
RLX Angola, Lda. · Grupo RLX Holdings
NIF 500 260 5724 · Matrícula 26464-25/250724

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 ficheiro. Esquecem-se ali pastas do Git, ficheiros com senhas (**.env**), cópias do tipo **wp-config.php.bak** e despejos da base 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. `o-seu-dominio.com/.git/config` não deve abrir.
Ficheiro .env	Senhas e chaves da aplicação: **Senhas fora do código PHP**.
Cópias de ficheiros	wp-config.php.bak, config.old, .zip do site, pastas «backup»: o servidor entrega-as como texto ou descarrega-as.
Despejos da base de dados	Um ficheiro .sql na pasta do site é a base de dados toda, a um endereço de distância.
Registos e ferramentas de teste	debug.log, error_log, phpinfo.php, instaladores: **Modo de depuração**.

Como começar

1. **Procure no Gestor de Ficheiros** (com «mostrar ficheiros 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. As cópias de segurança guardam-se **fora** da pasta pública: **A sua própria cópia de segurança**.

4. **Bloqueie o que tem de 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 da base de dados, as chaves de API, o que estava no .env. Apagar o ficheiro não desfaz o que já foi lido.

Apagar o ficheiro 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 ficheiro.

Abrir pedido de suporte

VEJA TAMBÉM

Manter as palavras-passe fora do código PHP: ficheiros .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	37 mil+	130+
FUNDADA	CLIENTES	INSCRIÇÕES POR DIA

MozOut Angola

RLX Angola, Lda. · Grupo RLX Holdings

NIF	500 260 5724
MATRÍCULA	26464-25/250724
SEDE	Rua Direita do Patriota, Bairro Dangereux Belas, Luanda, Angola
CONTACTOS	info@mozout.com · +244 942 011 191 · www.mozout.com
HORÁRIO	2ª. à 6ª. Feira - 08 à 16 Horas Sábado & Domingo - Fechado

RLX-AO-KB-6024 · v2026.10.15 · Gerado a 17/10/2026 10:34