

BASE DE CONHECIMENTO · DOCUMENTO PÚBLICO

Enviar códigos de uso único (OTP) por SMS com segurança: validade, tentativas e registos

PHP e Programação

CÓDIGO

RLX-MZ-KB-2160

VERSÃO

v2026.10.16

PAÍS · IDIOMA

Moçambique · Português

Interweb Moçambique

RLX Holdings, S.A. · Grupo RLX Holdings

NUIT 401 191 607 · NUEL 105 045 974 · CAE 62022

<https://www.meu.interweb.co.mz/knowledgebase/2160>



A resposta curta (para programadores): um código enviado por SMS só é tão seguro como o código que o rodeia. As regras: gerar o código com um gerador aleatório seguro, guardar só um **hash** dele, com **validade curta**, **limite de tentativas** e **uso único**; limitar quantos SMS cada número e cada IP pode pedir; e **nunca** escrever o código em registos, endereços ou ferramentas de análise. E lembre-se de que o próprio SMS pode ser lido no ecrã bloqueado ou desviado com a troca do cartão SIM: nas contas que importam, ofereça também uma app de autenticação (**app de autenticação, SMS ou chave**).

Os riscos e as defesas

Risco	Defesa
Adivinhar o código à força de tentativas	Limite de tentativas por código; depois disso, o código deixa de valer. Comparação com <code>hash_equals</code> .
Um código que continua válido horas depois	Validade curta, uso único, e um código novo anula o anterior.
Usarem o seu formulário para disparar SMS em massa (tráfego inflacionado para números que dão lucro a quem engana)	Limites por número, por IP e por sessão; captcha antes de enviar; só os países que serve; alarme quando o volume foge do normal.
O código aparece nos registos ou na monitorização	Registe «código enviado para o número terminado em...», nunca o código. Reveja o modo de depuração do cliente HTTP e as ferramentas que guardam o corpo dos pedidos.
Um código pedido para uma coisa usado para outra	Ligue o código ao utilizador, à finalidade (entrar, mudar a palavra-passe, confirmar um pagamento) e à sessão.
Um código previsível	<code>random_int</code> , que usa o gerador seguro do sistema. Nunca <code>rand()</code> , <code>mt_rand()</code> nem nada derivado da hora.

Como fazer, passo a passo (PHP)

1

Gere o código e guarde só o hash, com o segredo lido do ambiente (**variáveis de ambiente e segredos**): `$codigo = str_pad((string) random_int(0, 999999), 6, "0", STR_PAD_LEFT);`
`$hash = hash_hmac("sha256", $codigo, getenv("OTP_SECRET"));`
`// guardar: utilizador, finalidade, $hash, expira_em,`
`tentativas = 0`

2

Antes de enviar, veja os limites: quantos códigos este número e este IP pediram há pouco. Acima do seu limite, recuse com uma mensagem neutra e não chame o fornecedor. Imponha uma pausa antes de «reenviar». Também pode travar no servidor web: **limitar pedidos no nginx**.

3

Escreva a mensagem: quem envia (o nome do seu site), o código, e o aviso de que nunca deve ser partilhado e que ninguém da sua equipa o vai pedir. Sem acentos que obriguem a Unicode, para caber numa só parte: **GSM-7 ou Unicode**. Uma última linha com @ seguido do domínio do seu site e # seguido do código permite que navegadores compatíveis o preencham sozinhos.

4

Ao verificar: vá buscar o código mais recente e por usar desse utilizador e dessa finalidade; se expirou ou esgotou as tentativas, recuse; some uma tentativa **antes** de comparar; compare em tempo constante e, se estiver certo, marque-o como usado: `$ok = hash_equals($linha["hash"], hash_hmac("sha256", $tentativa, getenv("OTP_SECRET")));`

5

Feche as fugas: envie o pedido ao fornecedor por POST (os parâmetros de um GET acabam nos registos de acesso), não registe o corpo desse pedido, e mascare o número nos seus próprios registos.

6

Responda sempre da mesma maneira no formulário «enviar código», exista ou não uma conta com aquele número, para não revelar quem é cliente.

Nunca devolva o código ao navegador «para facilitar os testes», nem deixe um código fixo de teste activo em produção. São dois erros clássicos, e qualquer um deles anula a verificação inteira.

Muitos fornecedores de SMS têm uma API própria de verificação, que gera, envia e confere o código e trata de parte dos limites. Usá-la passa parte deste trabalho para eles; leia o que guardam e durante quanto tempo. E não espere pelo relatório de entrega para deixar o utilizador avançar: **relatórios de entrega (DLR)**.

Quer limitar os pedidos ao formulário do código ao nível do servidor, no seu VPS? Abra um pedido e diga-nos o endereço do formulário.

[Abrir pedido de suporte](#)

VEJA TAMBÉM

App de autenticação, SMS ou chave de segurança: que verificação em dois passos usar

Limitar pedidos no nginx: abrandar robôs e tentativas de adivinhar senhas

Variáveis de ambiente e segredos da sua aplicação

Manter as palavras-passe fora do código PHP: ficheiros .env e as permissões certas

GSM-7 ou Unicode no SMS: porque um acento divide a mensagem em mais partes

Relatórios de entrega de SMS (DLR): como a aplicação sabe se a mensagem chegou



Versão online deste documento

A Interweb 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

Interweb Moçambique

RLX Holdings, S.A. • Grupo RLX Holdings

NUIT 401 191 607

NUEL 105 045 974

CAE 62022

SEDE Bairro 7 de Setembro
Vilankulo 1304 • CEP 0411-02, Inhambane, Moçambique

CONTACTOS info@interweb.co.mz • +258 84 635 1111 • +258 86 635 1111 • www.interweb.co.mz

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