

CENTRO UNIVERSITÁRIO DE BELO HORIZONTE (UNIBH)

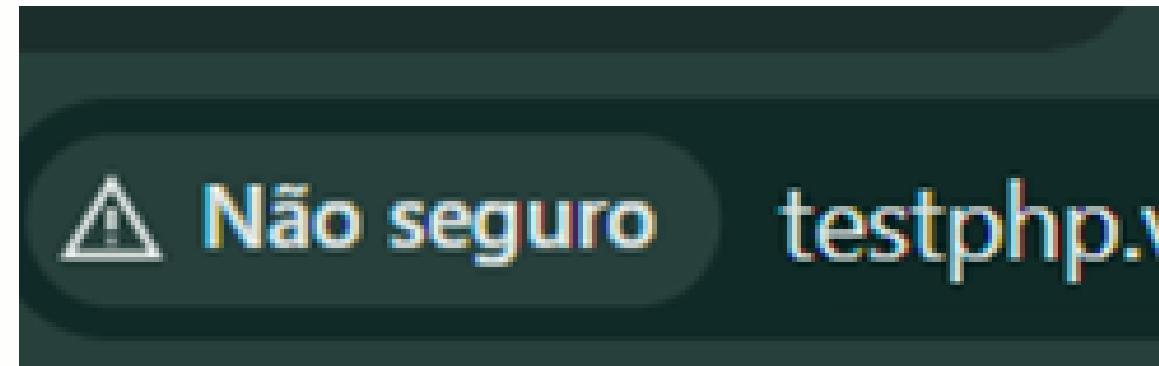
GUIA E MEDIDAS PROTETIVAS DE UM SITE

Alunos: Breno Ferreira, Gabriel Ramos, Giulia Hellen, Julia Alves,
Marcos Otavio, Maria Carolina

<http://www.>

-VULNERABILIDADES-

1- Falta de HTTPS

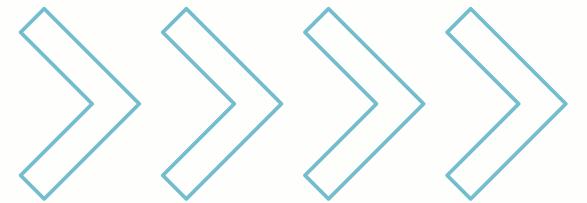


- **Problema:**

Tudo o que o usuário faz pode ser interceptado, incluindo senhas e dados pessoais.

- **Como resolver:**

Instalar HTTPS e fazer o site funcionar apenas com conexão segura.



CERTIFICADO SSL:

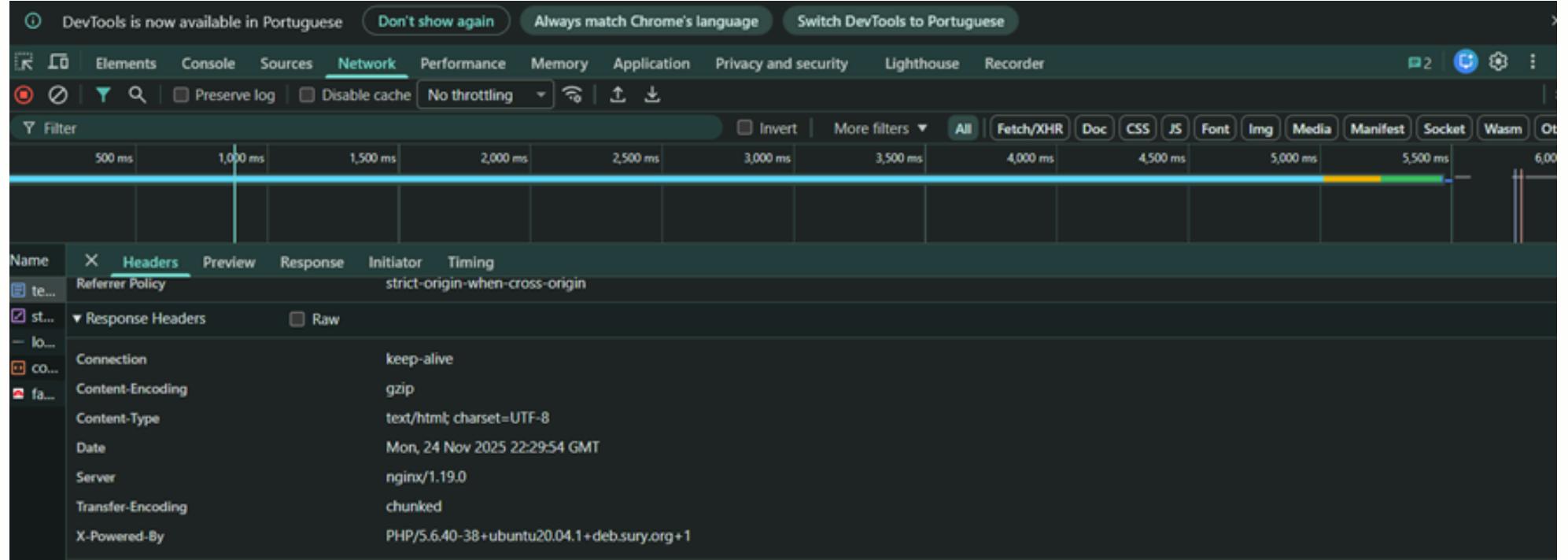
O SSL é uma tecnologia que criptografa os dados do usuário, protege informações, comprova a identidade do site e ativa o HTTPS (cadeado de segurança).

- Por que é importante?
- Só ter SSL não significa que o site é confiável
- SSL gratuito

Resumindo, o SSL protege e criptografa os dados, mas não garante que o site é totalmente confiável.



2-



-O SERVIDOR MOSTRA SUA VERSÃO-

Problema: O site mostra exatamente qual programa e versão ele usa no servidor. Isso ajuda atacantes a procurar falhas conhecidas dessa versão.

Como resolver: Esconder essa informação e manter o servidor atualizado.

-O PHP TAMBÉM REVELA SUA VERSÃO-

Problema: O site usa uma versão muito antiga do PHP, que já não recebe correções. Isso deixa o sistema aberto para ataques.

Como resolver: Atualizar o PHP e esconder a versão usada.

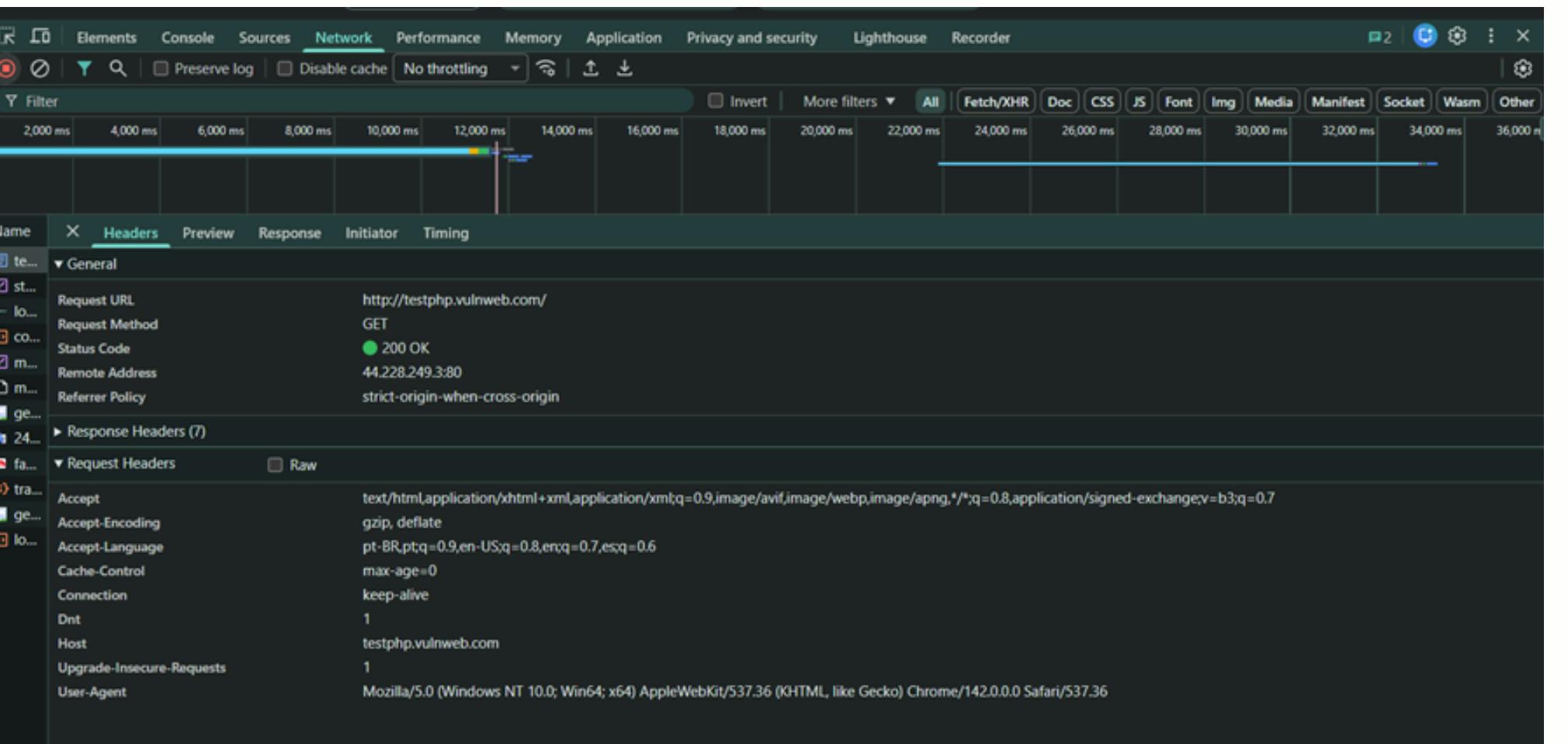
3-

Name	Value	Domain	Path	Expires ...	Size	HttpOnly	Secure	SameSite	Partitio...	Cross Si...	Priority
APISID	VyGM_1mPlyt01Kyi/AfnlfUwMbj9oxuVw	.google...	/	2026-1...	40						High
HSID	AMkGGwV1P0OR4Q7O4	.google...	/	2026-1...	21	✓					High
SEARCH_SAMESITE	CgQJu58B	.google...	/	2026-0...	23		Strict				Medium
SID	g.a0003ghUNoSIVRyO65Zal5gKz_eH62PhBCP5jMg...	.google...	/	2026-1...	156						High
SIDCC	AKEyXzWLsk6Bt1j-fQr3u8TGTAVEC5dgFXWpstWyP...	.google...	/	2026-1...	79						High

-COOKIES MAL CONFIGURADOS-

Problema: Os cookies que guardam a sessão do usuário podem ser roubados ou usados por outras pessoas, porque não estão protegidos.

Como resolver: Ativar opções que deixam os cookies protegidos e só funcionam em conexões seguras.



FALTAM PROTEÇÕES BÁSICAS NO SITE

Problema:

O site não usa várias proteções que os navegadores oferecem. Sem elas, fica mais fácil sofrer ataques como:

- Páginas falsas escondidas dentro da página
- Scripts maliciosos sendo executados
- Arquivos sendo interpretados de forma errada

Como resolver: Ativar essas proteções no servidor.

Outras formas de aumentar a segurança do site:

- Uso de senhas fortes, com combinação de letras maiúsculas, minúsculas, números e símbolos.
- Evitar senhas óbvias, como datas de nascimento ou palavras comuns.
- Implementar dupla segurança (2FA), onde o usuário precisa confirmar um código enviado para celular ou e-mail.
- Mesmo que alguém descubra a senha, o 2FA impede o acesso sem essa segunda confirmação.

5- -ATUALIZAÇÃO CONSTANTE-

O PERIGO DE NÃO ATUALIZAR

Quando um sistema, plugin ou tema fica desatualizado, ele se torna um alvo fácil para ataques. Hackers sabem exatamente quais brechas explorar em versões antigas.

POR QUE ATUALIZAR É ESSENCIAL?

- Correção de falhas de segurança:** Cada atualização fecha brechas descobertas.
- Proteção contra ataques conhecidos:** Vulnerabilidades antigas são as mais exploradas.
- Melhor desempenho:** Sistemas atualizados rodam mais rápido e consomem menos recursos.
- Compatibilidade garantida:** Evita erros e travamentos no seu site ou aplicativo.

BACKUP REGULAR

- **O que é um Backup?**

É uma cópia de segurança dos arquivos e do banco de dados do site.

- **Por que fazer backups?**

Evita a perca total em casos de ataques, falhas ou erros humanos.

- **Como funciona?**

Pode ser automático ou manual, e gera versões diferentes do site.

- **Onde guardar?**

Em nuvem, servidor externo, armazenamento físico ou serviços de hospedagem.



DADOS QUE ASSUSTAM

- 60% dos sites invadidos usavam software desatualizado
- Plugins WordPress desatualizados são responsáveis por 90% das invasões
- Em média, uma vulnerabilidade leva apenas 7 dias para ser explorada após ser divulgada

BOAS PRÁTICAS DE ATUALIZAÇÃO:

- Ative atualizações automáticas sempre que possível
- Verifique atualizações semanalmente (sistema, plugins, temas)
- Remova plugins/temas não utilizados – quanto menos, melhor
- Faça backup antes de atualizar – segurança em dobro
- Use apenas plugins oficiais e bem avaliados

LEMBRE-SE:

"UM SISTEMA DESATUALIZADO É COMO UMA PORTA ABERTA PARA INVASORES. MANTER TUDO ATUALIZADO NÃO É OPCIONAL É **ESSENCIAL**."



Guia de Medidas Protetivas

1. ATIVAR CONEXÃO SEGURA (HTTPS)

Isso impede que outras pessoas vejam ou interceptem o que o usuário está fazendo no site.

2. ATUALIZAR O SERVIDOR E ESCONDER INFORMAÇÕES INTERNAS

Atualizar tudo deixa o site mais protegido, e esconder a versão do servidor evita que atacantes descubram pontos fracos.

3. PROTEGER OS COOKIES DO USUÁRIO

Configurar os cookies para que só funcionem em páginas seguras e não possam ser acessados por qualquer código malicioso.

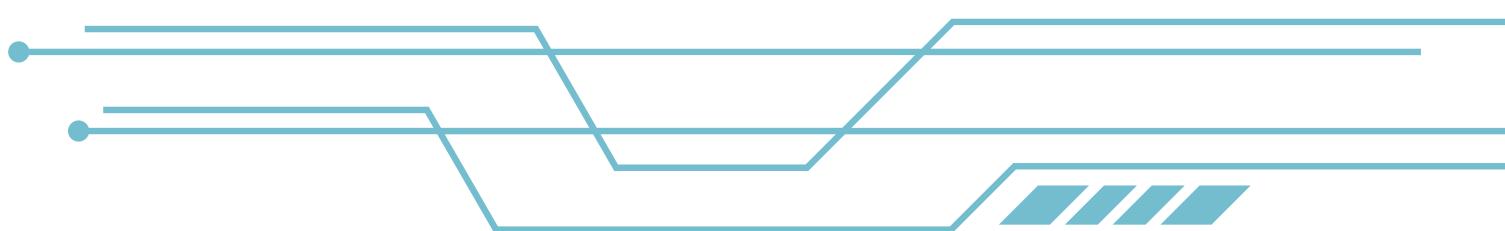
4. ATIVAR PROTEÇÕES DE SEGURANÇA DO NAVEGADOR

Essas proteções evitam que outras páginas enganem o usuário, que códigos estranhos rodem sozinhos ou que arquivos sejam interpretados errado.

5. FAZER REVISÕES E ATUALIZAÇÕES REGULARES

Sempre atualizar o sistema, revisar erros e verificar possíveis falhas para manter o site protegido ao longo do tempo.

HOSPEDAGEM SEGURA



É QUANDO O SEU SITE OU SISTEMA É ARMAZENADO EM UM SERVIDOR QUE POSSUI CAMADAS EXTRAS DE SEGURANÇA. ISSO INCLUI:

- PROTEÇÃO CONTRA INVASÕES

O SERVIDOR TEM MECANISMOS QUE DETECTAM ACESSOS SUSPEITOS E TENTATIVAS DE INVASÃO.

- CERTIFICADO SSL

GARANTE QUE OS DADOS ENVIADOS (COMO NOME, TELEFONE E HORÁRIOS) SEJAM CRIPTOGRAFADOS.

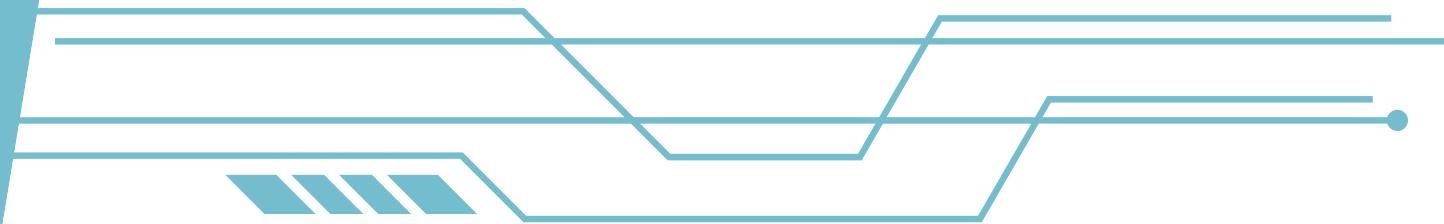
- BACKUPS AUTOMÁTICOS

CÓPIAS DE SEGURANÇA PARA IMPEDIR QUE SUAS INFORMAÇÕES SEJAM PERDIDAS.

- ATUALIZAÇÕES DE SEGURANÇA

O SERVIDOR É ATUALIZADO FREQUENTEMENTE PARA BLOQUEAR NOVAS FALHAS DESCOBERTAS NO MERCADO.

FIREWALL

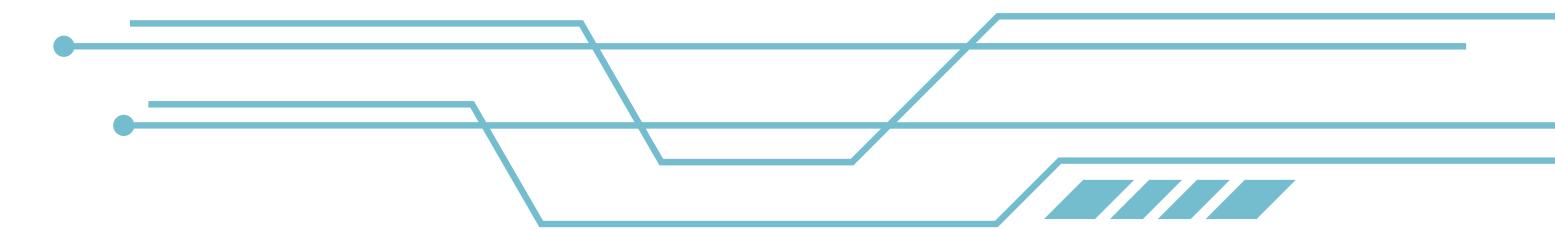


O FIREWALL É COMO UM GUARDA DE SEGURANÇA 24H QUE FICA NA PORTA DO SEU SITE/SISTEMA DECIDINDO QUEM PODE ENTRAR OU NÃO.

FUNÇÕES DO FIREWALL:

- BLOQUEIA HACKERS
- FILTRA ACESSOS ESTRANHOS (EX: MUITAS TENTATIVAS DE LOGIN ERRADAS)
- PROTEGE CONTRA VÍRUS, MALWARE E BOTS
- EVITA SOBRECARGA DE TRÁFEGO (ATAQUES DDOS)

FIREWALL VS ANTIVÍRUS



ANTIVÍRUS (EX: AVAST)

- FUNCIONA DENTRO DO COMPUTADOR.
- ANALISA ARQUIVOS, PROGRAMAS E DOWNLOADS.
- DETECTA VÍRUS, TROJANS, MALWARE DENTRO DA SUA MÁQUINA.
- ELE “LIMPA” OU “REMOVE” AMEAÇAS.
- É COMO UM MÉDICO EXAMINANDO VOCÊ POR DENTRO.

FIREWALL

- FUNCIONA FORA, NA PORTA DE ENTRADA DO SISTEMA.
- CONTROLA O QUE PODE ENTRAR E SAIR PELA INTERNET.
- BLOQUEIA ACESSOS ESTRANHOS, ATAQUES, BOTS E HACKERS.
- AGE ANTES DA AMEAÇA CHEGAR AO SISTEMA.
- É COMO UM SEGURANÇA NO PORTÃO, QUE SÓ DEIXA ENTRAR QUEM É CONFIÁVEL.