|  |
| --- |
| Relatório Scan de Vulnerabilidades - Wordpress |
| Cliente: XXXX |
| Cliente: XXXX |
| **24/12/2021** |

|  |
| --- |
| ESTE RELATÓRIO CONTÉM INFORMAÇÃO CONFIDENCIAL E NÃO DEVE SER ENVIADO POR E-MAIL, FAX OU QUALQUER OUTRO MEIO ELETRÔNICO A MENOS QUE ESTE SEJA PREVIAMENTE APROVADO PELAS POLITICAS DE SEGURANÇA DA CONTRATANTE. |

**1.0 – Controle de Versões**

|  |  |  |  |
| --- | --- | --- | --- |
| DATA | VERSÃO | AUTOR | ALTERAÇÕES |
| 24/12/2021 | 1.0 | Matheus Fantoni | - VERSÃO INICIAL; |

**Considerações iniciais**

Através deste presente relatório apresentamos o **Relatório Scan de Vulnerabilidades dos Sites em Wordpress** segundo orientações do XXXX.

Matheus Fantoni

Assistente de Segurança da Informação

**2.0 – Introdução e objetivo**

A equipe de Segurança da Informação a fim de verificar a segurança do ambiente web dos sites da companhia, abriu-se uma necessidade de se realizar um scan de vulnerabilidades em alguns domínios feitos em CMS Wordpress que fazem parte da empresa. A avaliação foi conduzida de maneira aplicar o scan nas URL’s informadas para se encontrar possíveis vulnerabilidades e determinar o impacto que essas falhas de segurança podem ter no que diz respeito à integridade, disponibilidade e confidencialidade do negócio.

**2.1 – Escopo**

Foi combinado que o scan de vulnerabilidades seria feito a partir do conhecimento de informações das URL’s repassadas pelo Analista de Segurança da Informação XXX, que seriam utilizadas na ferramenta WordPress Security Scanner (wpscan) em terminal server da distribuição Kali Linux.

|  |
| --- |
| URL’s |
| https://xxx.xxx.xxx |

O objetivo deste **Scan de Vulnerabilidades** é conduzir uma análise para verificar se as URL’s informadas possuem vulnerabilidades que podem gerar ataques maliciosos na infraestrutura do sistema de gerenciamento de conteúdo, de maneira que seja possível determinar o impacto que as falhas de segurança possam apresentar na:

* Na Integridade desses sistemas dentro da companhia
* Na confidencialidade das informações de clientes
* Na infraestrutura interna e disponibilidade dos sistemas e serviços

O resultado dessa avaliação deve ser usado para mitigação e conhecimento dessas falhas a fim de minimizar os riscos e melhorar a segurança.

**2.2 – Limitações de Escopo**

As **limitações** impostas pelo gestor foram:

* Ataques DoS e DDoS (Negação de Serviço)

**2.3 – Metodologia**

A metodologia utilizada neste teste visa analisar os níveis de proteção implantados e as vulnerabilidades que o Wordpress pode apresentar iniciando pela lista de URL’s disponibilizada para começar o scan.

O scan se inicia e termina na fase de coleta de informações, não será feito nenhum processo de pós exploração das vulnerabilidades encontradas nos domínios disponibilizados. A cada URL analisada serão obtidas informações como versão do Wordpress, plug-ins utilizados, enumeração de usuários cadastrados na plataforma, informações sobre a página de login de administração do Wordpress, headers do site com informações, versão de temas instalados.

**3.0 – Sumário executivo**

Os resultados das avaliações efetuadas na plataforma a partir do uso da ferramenta **wpscan**, demonstram que a empresa possui alguns riscos de segurança nos sites no qual as presenças dessas vulnerabilidades podem comprometer a imagem da empresa.

**3.1 – Resumo das ameaças**

Através da ferramenta foi possível verificar que todos os sites que apresentam o sistema do Wordpress foram identificados riscos de segurança da informação. O site com a URL: xxxx.com não foi feito nenhum scan devido seu desenvolvimento ter sido feito em React. Nenhuma ameaça encontrada foi explorada.

**4.0 – Resultado do Trabalho – Analise Técnica**

**4.1 – Coleta das Informações**

Iniciamos a coleta das informações do ambiente a fim de levantar uma investigação sobre o ambiente em cada website.

URL:

|  |
| --- |
| https://xxx.com |

Anexo I - Apresenta o resultado do log da URL informada acima.

Não obtivemos nenhum resultado: **(COLOCAR EVIDÊNCIA DO KALI LINUX)**

Foi usado a ferramenta **Wappalyzer** e analisado que o desenvolvimento do website foi feito em React. Devido ao fato de ser desenvolvido em React não foi possível realizar o scan de vulnerabilidades do wpscan nesta URL.

URL:

|  |
| --- |
| https://xxx.com |

Anexo I - Apresenta o resultado do log da URL informada acima.

Informações identificadas:

* Servidor xxx versão xxx
* Usuário xxx
* Listagem de diretório habilitada na URL: xxxx
* Versão do WordPress desatualizada
* Versão do plug-in xxx desatualizado

**5.0 – Referências**

* Anexo I – Documento contendo todos os logs do scan de vulnerabilidades do wpscan
* Anexo II – Documento contendo os hashes dos arquivos de evidências

**6.0 – Conclusão**

* A equipe de Segurança da Informação conclui este trabalho com o objetivo atingido de identificar possíveis vulnerabilidades e problemas na segurança das URL’s informadas no ambiente web.