Congresso de Segurança da Informação das Fatec

ATAQUE DE FORÇA BRUTA EM SITES WORDPRESS

FORCE ATTACK ON WORDPRESS SITES

Lucas Tavares, Faculdade de Tecnologia de Ourinhos, lucas.tavares9@fatec.sp.gov.br

Rafael Luiz Cóccia Bento, Faculdade de Tecnologia de Ourinhos, rafael.bento@fatec.sp.gov.br

André Giovanni Castaldin, Faculdade de Tecnologia de Ourinhos, andre.castaldin@fatec.sp.gov.br

Resumo

O presente estudo examina os ataques de força bruta direcionados a sites WordPress, uma das plataformas mais populares para criação de websites. O objetivo é investigar como esses ataques exploram vulnerabilidades em senhas e a eficácia de medidas de segurança, como: utilização do *CAPTCHA* (Completely Automated Public Turing test to tell Computers and Humans Apart), limitação de *LOGIN* (autenticação para acessar um sistema informático) e uso de senhas complexas. Utilizando um ambiente virtual simulado, realizamos uma série de testes práticos com essas três medidas de segurança no WordPress. Os resultados mostraram que, sem medidas de segurança, o WordPress é altamente vulnerável, enquanto a adoção de plugins que limitam tentativas de *LOGIN*, utilização de *CAPTCHA* e uso de senhas complexas se mostrou eficaz para bloquear ataques. Conclui-se que o uso combinado dessas práticas de segurança é fundamental para aumentar a segurança de websites WordPress contra ataques de força bruta.
Palavras-chave: wordpress, ataque, força bruta, wpscan

Abstract

This article looks at brute force attacks targeting WordPress websites, one of the most popular platforms for website creation. The objective is to investigate how these attacks exploit vulnerabilities in passwords and the effectiveness of security measures, such as the use of *CAPTCHA*, *LOGIN* limitations and the use of complex passwords. Using a simulated virtual environment, we carried out a series of practical tests with these three security measures in WordPress. The results showed that, without security measures, WordPress is highly vulnerable, while the adoption of plugins that limit *LOGIN* attempts, the use of *CAPTCHA* and the use of complex passwords proved to be effective in blocking attacks. It is concluded that the combined use of these security practices is fundamental to increasing the security of WordPress sites against brute force attacks.
Keywords: wordpress, attack, brute force, wpscan

1. Introdução

No cenário digital atual, a segurança cibernética tornou-se uma prioridade crucial, à medida que o número de ataques online cresce de forma exponencial. Uma plataforma amplamente utilizada por websites é o WordPress, reconhecido por sua flexibilidade e simplicidade de uso. Contudo, essa popularidade também o torna um alvo frequente de ataques cibernéticos, especialmente ataques de força bruta (*brute force*), onde invasores tentam adivinhar senhas por meio de múltiplas combinações até que uma credencial válida seja encontrada.

Esses ataques são uma das formas mais comuns de comprometimento de websites, uma vez que muitos usuários não adotam práticas de segurança. A ausência de senhas complexas, utilização do *CAPTCHA* e limitação de *LOGIN* deixam brechas que cibercriminosos exploram com sucesso.

Diante desse cenário, este artigo visa analisar a eficácia das medidas de segurança disponíveis para sites WordPress contra ataques de *brute force*. Com o objetivo de entender como esses ataques funcionam, explorando principalmente a fraqueza das senhas e a eficiência de plugins de segurança para combater essas tentativas e alertar os usúarios sobre a importância das práticas de segurança e uso de plugins. Foram averiguadas duas áreas: a implementação de plugins de segurança como *All In One WP Security e o Limit Login Attempts Reloaded*, plugins que são facilmente encontrados dentro do próprio *WordPress* e o uso de senhas complexas, requisito que é obrigatório na hora de criar um usuário dentro da plataforma. A hipótese central é que essas medidas são capazes de reduzir significativamente a vulnerabilidade dos websites, minimizando os riscos de ataques bem-sucedidos.

A relevância deste estudo é ajudar a compreender as práticas mais comuns da segurança cibernética, os proprietários de sites WordPress podem adotar soluções preventivas e corretivas que melhorem a proteção de seus sistemas. A análise também busca identificar padrões e tendências em ataques de *brute force*, propondo recomendações práticas para fortalecer a segurança dos websites.

Para isso, a pesquisa utilizou um ambiente virtual controlado, onde ataques de força bruta foram simulados com a ferramenta WPScan. Foram testados cenários com e sem medidas de proteção, como limitação de *LOGIN*, *CAPTCHA* e senhas complexas, e

os resultados foram documentados para análise comparativa.

A pesquisa se estrutura da seguinte forma: primeiramente, foram discutidas as práticas de segurança mais comuns em sites WordPress, com foco na utilização de senhas fortes e plugins de segurança. Em seguida, foi realizada uma análise comparativa entre sites que implementam essas medidas e aqueles que não o fazem, com o objetivo de identificar a efetividade de cada solução.

2. Referencial Teórico

Neste capítulo, trata-se dos artigos correlatos, definição das ferramentas e técnicas utilizadas no desenvolvimento deste estudo.

Segundo Diorio et al. (2019), os ataques de força bruta, ou *brute force*, consistem na tentativa de adivinhar logins e senhas de acesso de usuários legítimos por meio de tentativa e erro. Esses ataques são considerados uma das ameaças mais comuns e prevalentes atualmente. Os sistemas de autenticação, compostos por hardware, software, políticas e procedimentos, são frequentemente os alvos desses ataques, que buscam explorar falhas para obter acesso não autorizado aos recursos computacionais.

De acordo com Rosso et al. (2015), o white paper de segurança do WordPress aborda diversas práticas e medidas de segurança para proteger websites contra uma variedade de ameaças, incluindo ataques de força bruta. O documento enfatiza a importância da atualização constante de plugins, temas e o próprio WordPress, bem como a implementação de autenticação de dois fatores e o uso de plugins de segurança dedicados para mitigar os riscos.

De acordo com Chagas (2023), o ”Manual de Boas Práticas de Segurança da Informação”fornece diretrizes para a gestão de segurança dos sistemas de informação, incluindo medidas contra ataques de força bruta. O manual aborda a importância da criação de políticas de segurança rigorosas, a adoção de senhas fortes e complexas, e a implementação de sistemas de autenticação robustos para proteger os dados e sistemas de informações eletrônicas contra acessos não autorizados.

De acordo com Rosso et al. (2015), o white paper de segurança do WordPress aborda diversas práticas e medidas de segurança para proteger websites contra uma variedade de ameaças, incluindo ataques de força bruta. O documento enfatiza a importância da atualização constante de plugins, temas e o próprio WordPress, bem como a

implementação de autenticação de dois fatores e o uso de plugins de segurança dedicados para mitigar os riscos.

Segundo PEREIRA e MORALES (2014), o estudo apresentado na III JORNACITEC explora a vulnerabilidade das senhas e os requisitos necessários para a realização de um ataque de força bruta. Os autores destacam que senhas fracas e de fácil previsão representam uma grande ameaça à segurança dos sistemas de informação, pois facilitam a ação de atacantes que utilizam ataques de força bruta para comprometer contas e sistemas. O artigo também discute a importância de estabelecer políticas de criação de senhas robustas e a implementação de medidas de segurança, como a limitação do número de tentativas de *LOGIN* e o uso de autenticação multifatorial, para mitigar esses riscos.

Segundo Kurian e Jose (2021), o WPScan é uma ferramenta utilizada para identificar vulnerabilidades em sites WordPress, incluindo falhas em plugins, temas e no próprio núcleo da plataforma. O estudo destaca a integração do WPScan com o Autotor para mascaramento de IP (IP spoofing), o que torna os testes de penetração mais difíceis de serem detectados. A pesquisa também aborda a capacidade da ferramenta de enumerar usuários, fornecendo uma análise completa das vulnerabilidades presentes em sites WordPress e recomendando medidas de segurança baseadas nos resultados.

Segundo Ramadhani et al. (2024), a análise de vulnerabilidades em WordPress com o WPScan revela diversos pontos fracos em sites que utilizam a plataforma sem as devidas práticas de segurança. O estudo investiga técnicas de mitigação para essas vulnerabilidades, como a implementação de atualizações regulares e plugins de segurança. Além disso, os autores destacam a importância da conscientização sobre segurança cibernética e o uso de ferramentas de escaneamento como o WPScan para proteger sites WordPress contra ataques cibernéticos.

2.1. B2/cafelog

Para saber mais sobre o WordPress é necessário saber sobre seu antecessor que foi B2 ou também chamado cafelog, segundo o blog Freddy (2013), B2 foi o sistema que deu o pontapé inicial para os sistemas de gerenciamento de conteúdo pois oferecia uma interface acessível e funcional para os blogueiros na era inicial da internet, Sua arquitetura modular, facilidade de uso e capacidade de personalização estabeleceram um padrão significativo que influenciou o desenvolvimento de CMS*(Content Management System)* posteriores. A transição do B2/Cafelog para o seu sucessor WordPress exempli-

fica a evolução do software de código aberto por meio da colaboração comunitária. O WordPress herdou as características fundamentais do B2 e expandiu suas capacidades, tornando-se a ferramenta versátil e poderosa que é hoje. O legado do B2 não apenas vive no código do WordPress, mas também na filosofia de desenvolvimento colaborativo e na democratização da publicação na web. A importância histórica do B2 é evidenciada pelo sucesso contínuo do WordPress, capacitando milhões de usuários e desenvolvedores globalmente.

2.2. WordPress

De acordo com Wordpress (2020a), o WordPress nasceu do desejo de um sistema de publicação pessoal elegante e bem arquitetado, construído em PHP e MySQL e licenciado sob a GPL(Licença Pública Geral). É o sucessor oficial do b2/cafelog. WordPress é um software moderno, mas suas raízes e desenvolvimento remontam a 2001. É um produto maduro e estável. Focando na experiência do usuário e nos padrões da web, criando uma ferramenta diferente de qualquer outra existente. Segundo o Wordpress (2020b), onde é recomendado que os usuários conheçam as questões de segurança do software é relatado no documento oficial de segurança é as práticas de segurança são compatíveis com a versão mas estável do software, sendo a versão 4.1.

Plugins do WordPress Segundo M (2024), um plugin é um código inserido no seu site WordPress. De forma simples, é uma extensão que aumenta e melhora as funcionalidades do seu site principal.

Utilizar plugins é a forma mais recomendada de aumentar o potencial do seu site sem precisar editar os códigos originais do WordPress. É muito mais fácil baixar e ativar um plugin do que ter que customizar linhas e linhas de código, Os plugins permitem com maior facilidade em adicionar códigos para realizar mudanças no funcionamento do WordPress e caso não haja mais a necessidade de uso, basta desativar.

Existem literalmente milhares de plugins disponíveis no diretório do WordPress. O uso correto desses plugins oferece um aumento não só das funcionalidades do site, mas também uma melhor experiência do usuário e eficiência de artigo.

2.3. WPScan

O WPScan é uma ferramenta de segurança utilizada para identificar vulnerabilidades em sites WordPress, como falhas em plugins, temas e no núcleo do sistema. De

acordo com Ramadhani et al. (2024), a ferramenta ajuda a detectar essas vulnerabilidades e a implementar técnicas de mitigação, como atualizações regulares e configurações de segurança. Além disso, conforme Kurian e Jose (2021), o WPScan permite enumerar usuários e realizar testes de penetração avançados, integrando-se com técnicas de spoofing de IP para evitar detecção. Segundo Shah e Ayoade (2023), o WPScan também é útil para testar a robustez das credenciais de *LOGIN* contra ataques de força bruta, ajudando a fortalecer a segurança dos sites WordPress.

2.4. Kali Linux

Segundo kali (2023), O Kali Linux é uma distribuição de código aberto baseada no Debian, desenvolvida especificamente para testes de penetração e auditoria de segurança.O Kali Linux é construído sobre a base sólida do Debian, aproveitando sua estabilidade e vastos repositórios de software. De acordo com Kali Linux Tools Listing que é uma página oficial do kali linux que estuda uma lista compilada de todas as ferramentas de segurança cibernética disponíveis no Kali Linux, aponta que o Kali Linux oferece acesso a mais de 600 ferramentas de segurança cibernética, organizadas em categorias como informações de coleta, análise de vulnerabilidades, exploração, captura de pacotes, forense digital, e mais. A seção ”Kali Linux - Use Cases”uma parte do site oficial do Kali Linux que descreve os diferentes cenários ou casos de uso nos quais o Kali Linux pode ser aplicado de forma eficaz, aponta que O Kali Linux é amplamente utilizado em uma variedade de cenários, incluindo testes de penetração ética, auditoria de segurança, investigações forenses, treinamento em segurança cibernética e pesquisa acadêmica.

2.5. Brute Force

Segundo Diorio et al. (2019), Os ataques de força bruta (brute force), o aventureiro objetivo adivinhar, por tentativa e erro, logins e senhas de acesso de usuários legítimos de um determinado sistema e/ou serviço de rede. Por exemplo, são tidos como uma das principais e mais populares ameaças da atualidade. Em PEREIRA e MORALES (2014), De acordo com Ferreira e Araújo (2008), no livro Política de Segurança da Informação, a maioria dos programas de computador incorpora sistemas de autenticação que utilizam o processo de logon para permitir o acesso a dados e aplicativos em sistemas informatizados. Esses sistemas de autenticação combinam hardware, software, políticas e procedimentos que asseguram o acesso de usuários autorizados aos recursos computacionais, protegendo-os contra acessos indevidos. Os ataques de força bruta são uma tentativa de

subverter esses sistemas, explorando a repetição de tentativas de *LOGIN* até que uma combinação válida seja encontrada.

2.6. Práticas de Segurança

Segundo o estudo Chagas (2023), que aponta como boas práticas de segurança. O gerenciamento de senhas é essencial para a segurança da informação. Falhas como falhas de senha, compartilhamento ou falta de atualização podem comprometer a segurança dos sistemas.

Para lidar com isso, é crucial desenvolver políticas de senhas que incluam requisitos de complexidade, comprimento e expiração, além de diretrizes para os usuários. Tanto a organização quanto os usuários dos sistemas são responsáveis pela implementação dessas políticas. O controle eficaz envolve um gerenciamento robusto de senhas e uma promoção de boas práticas, como não compartilhar senhas e atualizá-las regularmente. A segurança dos sistemas é essencial para proteger suas informações online.

Indicadores de falhas podem incluir golpes de phishing, onde você recebe e-mails ou mensagens enganosas, instalação de malware, que são programas maliciosos que podem danificar seu computador, e vazamento de informações prejudiciais, o que pode resultar na exposição de dados pessoais ou financeiros . Para se proteger, é importante que os usuários sejam capacitados a confiar e evitar essas ameaças. Isso significa aprender práticas seguras, como não clicar em links suspeitos ou fornecer informações pessoais a sites não confiáveis. Em PEREIRA e MORALES (2014), que utiliza do livro dos autores Caruso e Steffen (2013), a expansão global da microinformática trouxe à tona um grande número de usuários despreparados no que se refere à segurança, muitas vezes sem uma cultura sólida de tecnologia da informação (TI). Isso se deve, em parte, à arquitetura aberta da plataforma, que facilita o acesso, mas também expõe vulnerabilidades que podem ser exploradas por pessoas mal-intencionadas.

3. Metodologia

Neste capítulo, são descritos os métodos utilizados para realizar a análise dos ataques de força bruta no WordPress. A abordagem metodológica foi desenvolvida em um ambiente virtual controlado, permitindo a simulação de cenários variados de segurança para avaliar as vulnerabilidades da plataforma e a eficácia de diferentes medidas de

proteção, como: plugins que limitam tentativas de *LOGIN*, *CAPTCHA* e uso de senhas complexas.

A seguir, apresentamos uma imagem ilustrativa Figura 1 para facilitar o entendimento da metodologia empregada neste estudo. Ela sintetiza, de forma visual, cada etapa dos procedimentos realizados ao longo da pesquisa.

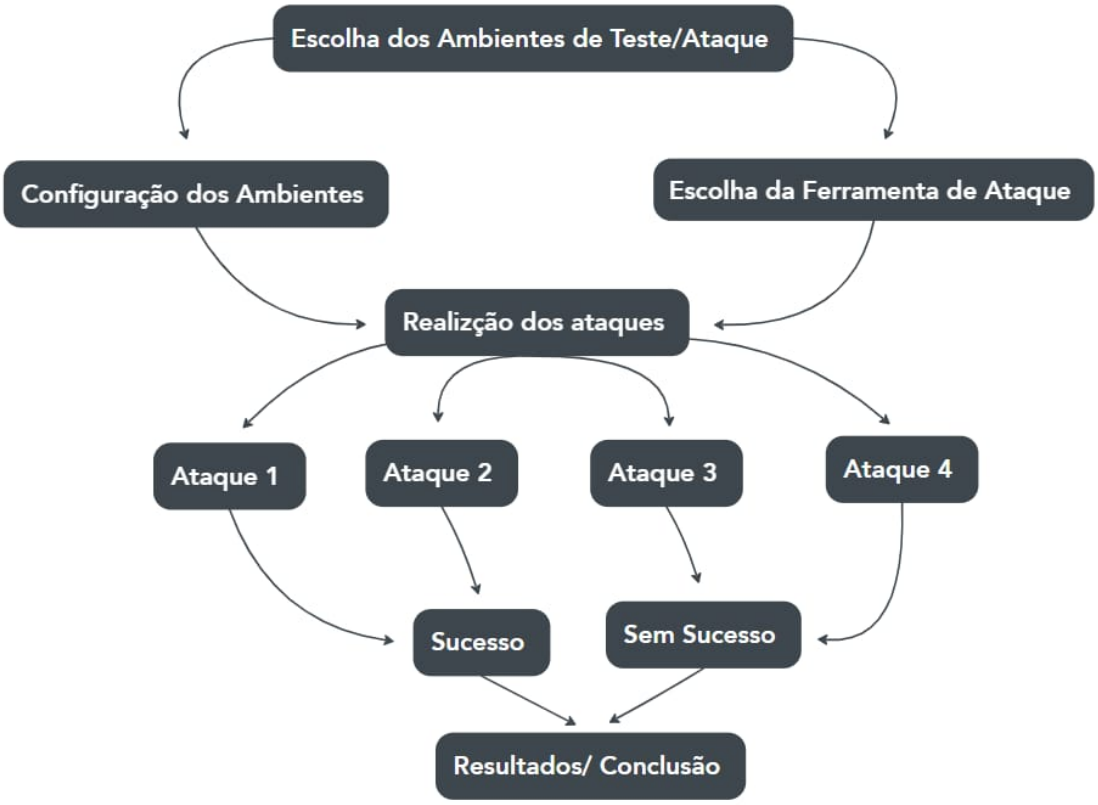

Figura 1. Diagrama da metologia utilizada.

Para os testes, foi configurado um servidor utilizando o sistema operacional Debian 11, onde o site WordPress foi instalado e hospedado em um ambiente que simula condições reais de um servidor. Esse ambiente proporciona maior controle e segurança durante a execução dos experimentos, garantindo a confiabilidade dos resultados. A utilização de ambiente controlado neste estudo, visa, primeiramente, não expor sites públicos que, por ventura, estejam vulneráveis e também porque há necessidade de con-

trole total de acesso ao WordPress, para observação do funcionamento das ferramentas e controle de usuários.

Utilizamos nesta pesquisa o sistema Kali Linux para realizar os ataques, uma vez que essa distribuição é amplamente empregada em testes de penetração e oferece uma variedade de ferramentas de segurança.

A ferramenta WPScan foi selecionada para conduzir os ataques de força bruta, permitindo testar múltiplas combinações de nomes de usuários e senhas. O comando utilizado para o ataque foi configurado da seguinte forma:

wpscan –url http://192.168.0.102/wordpress –passwords rockyou.txt –usernames rafael –output

Essa linha de código especifica o uso do WPScan para atacar o site hospedado, utilizando a lista de senhas ”rockyou.txt”e o nome de usuário ”rafael”, com o objetivo de documentar os resultados em um arquivo de saída.

Os plugins *All In One WP Security* e *Limit Login Attempts Reloaded* foram escolhidos devido à sua popularidade e eficácia na comunidade WordPress. Ambos são amplamente utilizados por administradores de sites, pois oferecem funcionalidades específicas que ajudam a proteger contra ataques de força bruta. O *All In One WP Security* inclui ferramentas como *CAPTCHA* e configurações adicionais de proteção, que são diretamente alinhadas com o objetivo de mitigar ataques de força bruta. Já o *Limit Login Attempts Reloaded* permite limitar o número de tentativas de login, o que ajuda a impedir ataques repetidos e aumentar a segurança do site.

Quatro testes foram realizados para medir a eficácia das medidas de segurança:

- Sem Medidas de Segurança: Teste inicial sem nenhuma proteção adicional no WordPress.
- Com *CAPTCHA*: Utilização do plugin *All In One WP Security* para adicionar um *CAPTCHA* simples.
- Limitação de Tentativas de *LOGIN*: Implementação do plugin *Limit Login Attempts Reloaded* para limitar o número de tentativas por IP.
- *CAPTCHA* + Limitação de *LOGIN*: Combinação do *CAPTCHA* com a limitação de tentativas de *LOGIN*.

Esses testes foram executados sequencialmente e geraram relatórios para

avaliação da eficácia de cada medida implementada.

4. Resultados e Discussões

No capítulo de Resultados, são apresentados os dados obtidos a partir dos testes realizados para avaliar a eficácia das medidas de segurança contra ataques de força bruta em sites WordPress.

Em nosso estudo realizamos uma série de testes de ataques de força bruta em um ambiente WordPress, utilizando a ferramenta WPSCAN em quatro cenários diferentes.

No primeiro teste, sem nenhuma medida de segurança ativa no WordPress, o ataque de força bruta conseguiu descobrir uma combinação válida de nome de usuário e senha. A Figura 2 mostra o resultado do primeiro teste, realizado sem nenhuma medida de segurança no WordPress. Nela, vemos que o ataque de força bruta conseguiu descobrir o usuário ”rafael”e a senha ”fatec123”. A mensagem ”Valid Combinations Found”confirma que o ataque foi bem-sucedido, pois realizou várias tentativas até encontrar a combinação correta. Esse resultado deixa claro que, sem proteção, o site é vulnerável e que um invasor pode acessar o sistema facilmente.

```
65  | License URI: http://www.gnu.org/licenses/gpl-2.0.html
66  | Tags: one-column, custom-colors, custom-menu, custom-logo, editor-style, featured-images, full-site-editing, block-patterns
    ready, wide-blocks, block-styles, style-variations, accessibility-ready, blog, portfolio, news
67  | Text Domain: twentytwentyfour
68  |
69  | Found By: Urls In Homepage (Passive Detection)
70  |
71  | Version: 1.0 (80% confidence)
72  | Found By: Style (Passive Detection)
73  |  - http://192.168.0.102/wordpress/wp-content/themes/twentytwentyfour/style.css, Match: 'Version: 1.0'
74
75
76 [34m[i][0m No plugins Found.
77
78
79 [34m[i][0m No Config Backups Found.
80
81
82 [31m[!][0m Valid Combinations Found:
83  | Username: rafael, Password: fatec123
84
85 [33m[!][0m No WPScan API Token given, as a result vulnerability data has not been output.
86 [33m[!][0m You can get a free API token with 25 daily requests by registering at https://wpscan.com/register
87
88 [32m[+][0m Finished: Tue Oct  1 18:01:10 2024
89 [32m[+][0m Requests Done: 1504
90 [32m[+][0m Cached Requests: 7
91 [32m[+][0m Data Sent: 451.04 KB
92 [32m[+][0m Data Received: 29.291 MB
93 [32m[+][0m Memory used: 272.023 MB
94 [32m[+][0m Elapsed time: 00:00:09
95
```

Figura 2. Resultado do ataque sem qualquer tipo de medida de segurança.

A Figura 3 mostra o resultado do ataque de força bruta após a implementação de um *CAPTCHA* simples no WordPress, usando o plugin All In One WP Security. Com o *CAPTCHA*, o sistema pede que o usuário faça uma verificação antes de cada tentativa de *LOGIN*, nessa imagem, podemos ver que, apesar de o *CAPTCHA* ter sido ativado, o atacante ainda conseguiu descobrir o usuário ”Rafael”e a senha ”fatec123”. A mensagem ”Valid Combinations Found”confirma que o ataque foi bem-sucedido. Esse resultado indica que o uso do *CAPTCHA* sozinho não foi suficiente para bloquear o ataque, mostrando que ele pode atrasar, mas não impedir completamente tentativas de força bruta.

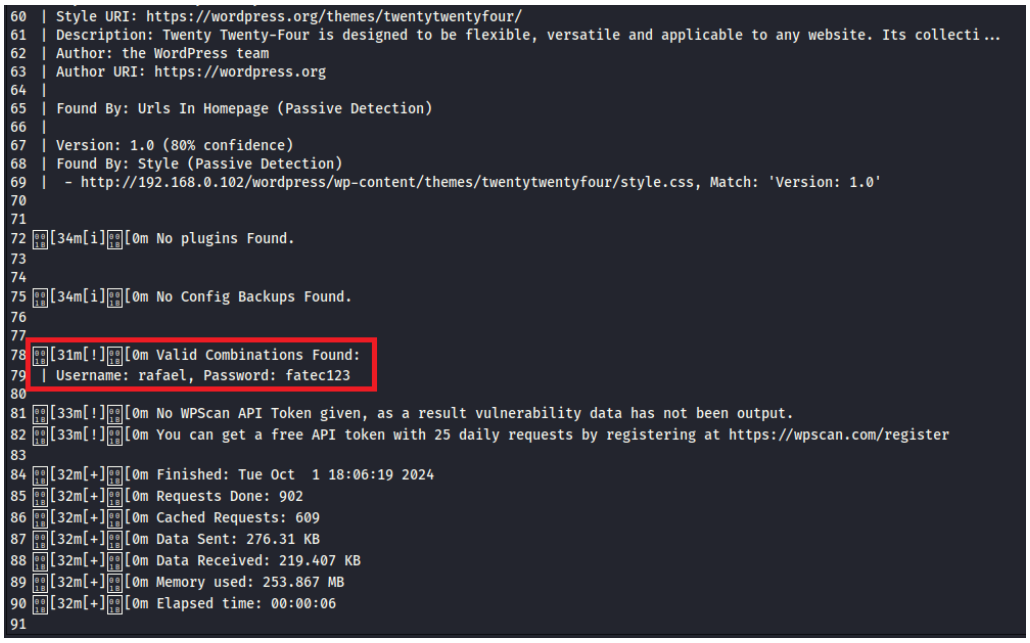

Figura 3. Resultado do ataque com o *CAPTCHA*.

Nas figuras 4 e 5, vemos o resultado da combinação do plugin de Limite de Tentativas de *LOGIN* e o uso de *CAPTCHA*, o ataque foi totalmente barrado. A limitação de tentativas impediu novas tentativas de *LOGIN* após um número máximo, enquanto o CAPTCHA adicionou uma verificação extra, dificultando ainda mais o ataque. Esse resultado demonstra que a combinação dessas medidas de segurança é eficaz para bloquear acessos não autorizados, reforçando a importância de os proprietários de sites WordPress usarem proteções como essas, além de senhas fortes, para diminuir sucesso de um ataque de força bruta.

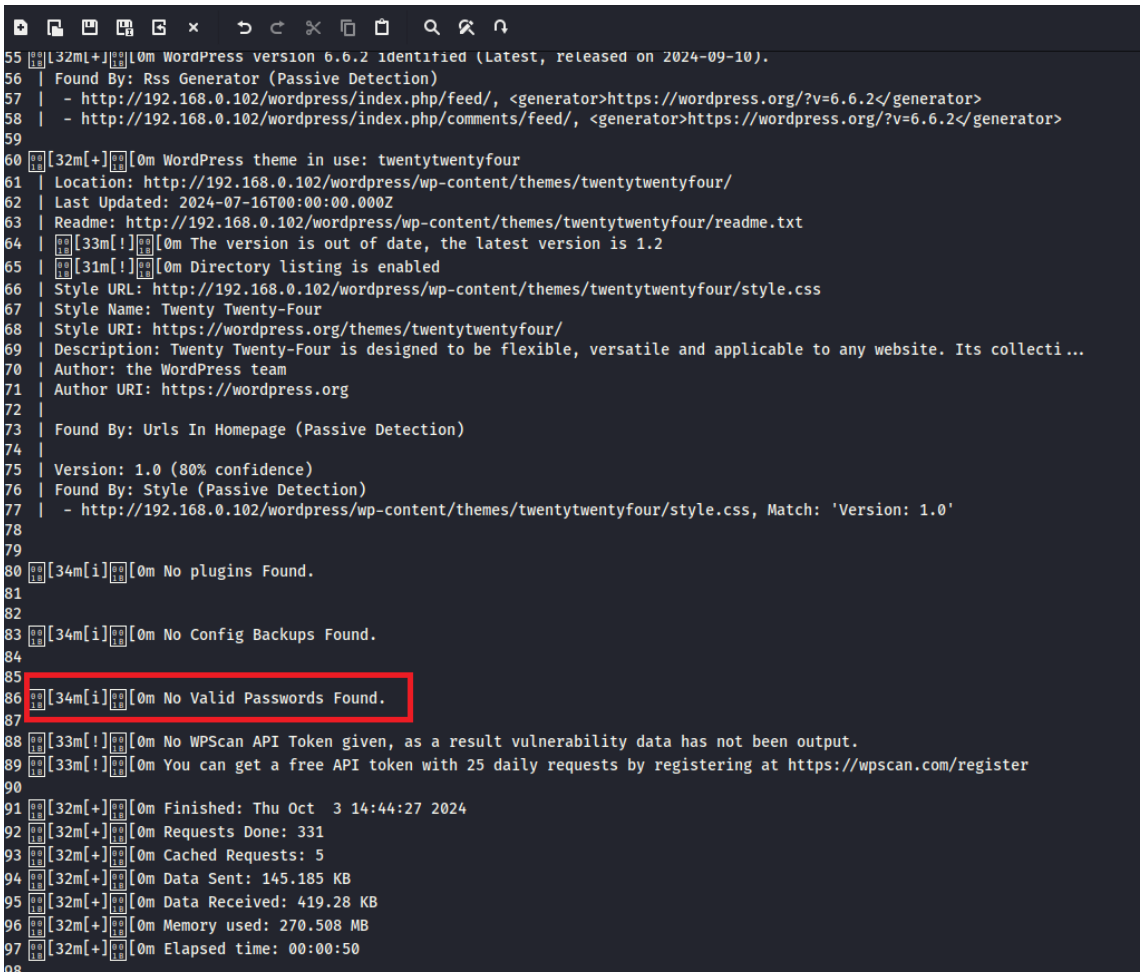

Figura 4. Resultado do ataque com limite de tentativas de *LOGIN*.

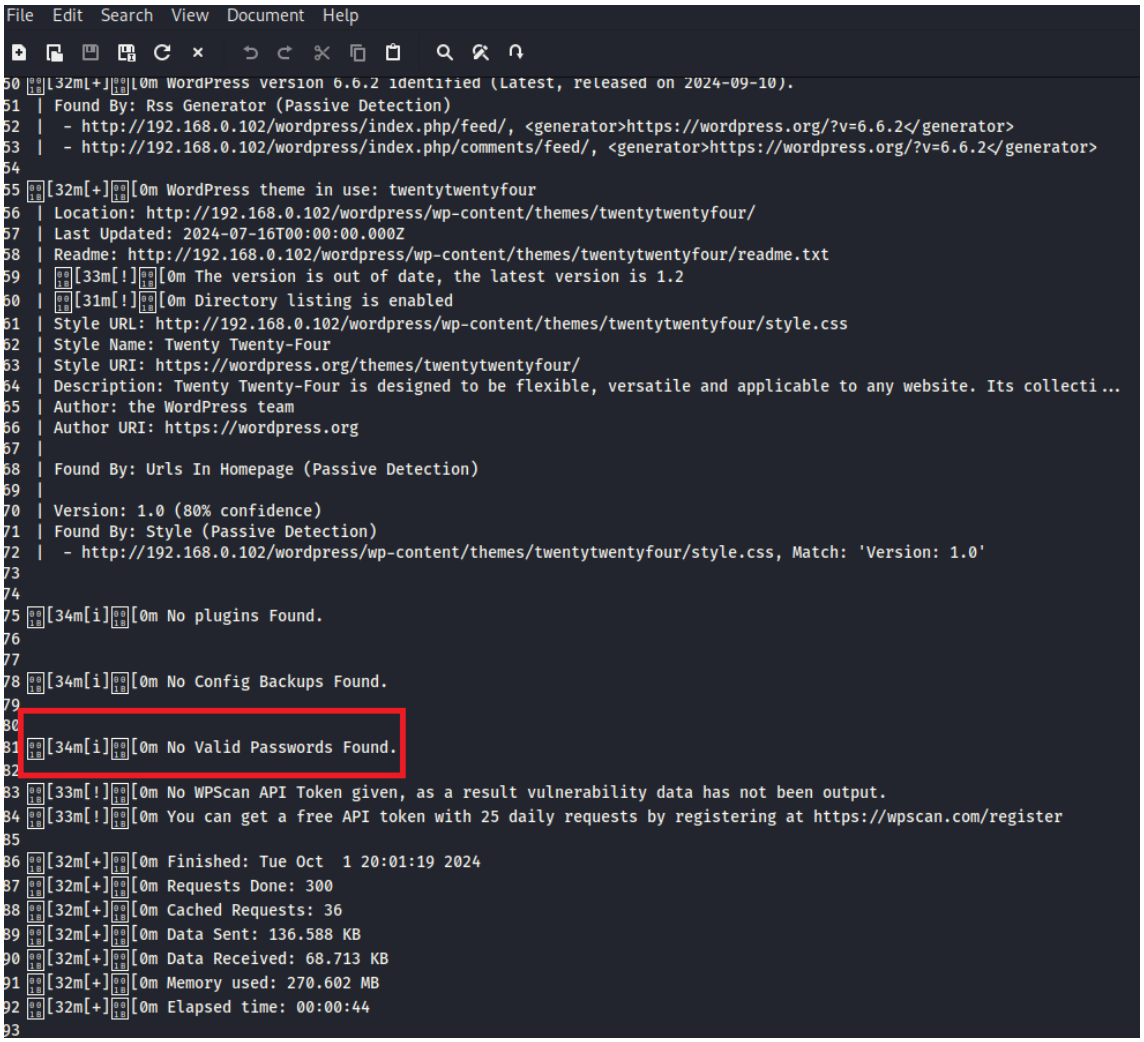

Figura 5. Resultado do ataque com limite de tentativas de *LOGIN* com o *CAPTCHA*.

No ultimo cenário, conforme a figura 6, durante a criação de um novo usuário no WordPress, o sistema alerta o usuário sobre a força da senha escolhida. Caso a senha seja considerada fraca, o WordPress exibe uma mensagem de aviso e recomenda o uso de uma senha mais forte. No entanto, há uma opção que permite ao usuário ignorar essa recomendação e prosseguir com uma senha fraca, assumindo o risco de segurança.

Essa funcionalidade destaca um aspecto importante da segurança em plataformas como o WordPress: mesmo com alertas e recomendações, o usuário final tem a responsabilidade de compreender e aplicar boas práticas de segurança.

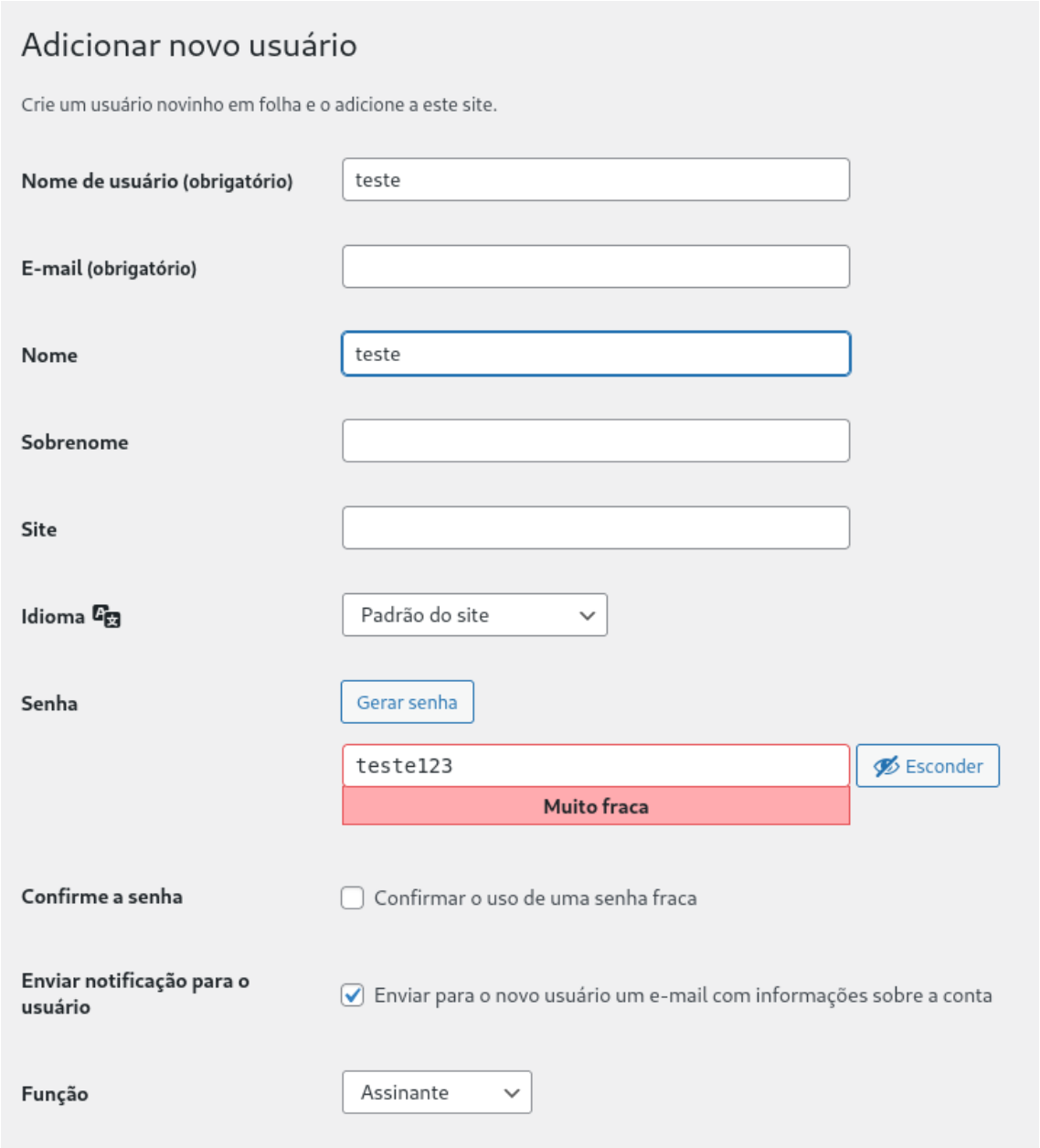

Figura 6. WordPress alertando sobre a utilização de senha complexa.

5. Conclusão

Os testes realizados nos permitiram demonstrar que a implementação de práticas de segurança e o uso de plugins, como: (nome do plugin), que permite a implementação de *CAPTCHA*, (nome do plugin) que admite a limitação de *LOGIN* e senhas comple-

xas, são eficazes para barrar ataques de força bruta em sites WordPress. Confirmaram, incusive que, essas medidas não apenas aumentam a segurança, mas também reduzem significativamente a vulnerabilidade dos sites a ataques maliciosos.

Para trabalhos futuros, sugerimos explorar outras abordagens, como a utilização de autenticação multifator e a análise de logs para identificar atividades suspeitas.

6. Referências

Referências

CHAGAS, A. P. M. A. Manual de boas práticas de segurança da informação. *Gestão de segurança dos sistemas de informação eletrônica: interface usuário, tecnologia e sistema*, Pós-Graduação em Ciência da Informação, 2023.

DIORIO, R. F. et al. Ataques de força bruta: Um estudo prático. *Departamento de Informática. Instituto Federal de Educação, Ciência e Tecnologia de São Paulo (IFSP). Capivari–SP*, 2019.

FREDDY. *Site wpexplorer*. 2013. Https://www.wpexplorer.com/history-wordpress/.

KALI. *site oficial kali*. 2023. Https://www.kali.org.

KURIAN, M. R.; JOSE, T. Wpscan–discovering the vulnerabilities and enumerating users of wordpress sites with autotor for ip spoofing. In: *National Conference on Emerging Computer Applications*. [S.l.: s.n.], 2021. v. 3, n. 1.

M, W. *Site ofical hostinger*. 2024. Https://www.hostinger.com/tutorials/wordpress-security-issues.

PEREIRA, M. M.; MORALES, I. L. Vulnerabilidade de senhas e requisitos necessários para ataque de força bruta. In: *III JORNACITEC*. [S.l.: s.n.], 2014.

RAMADHANI, G. T. A. et al. Analisis kerentanan wordpress dengan wpscan dan teknik mitigasi. *Journal of Internet and Software Engineering*, v. 1, n. 4, p. 15–15, 2024.

ROSSO, S. et al. *Wordpress security white paper*. [S.l.]: Preuzeto, 2015.

SHAH, P. G.; AYOADE, J. An empricial study of brute force attack on wordpress website. In: IEEE. *2023 5th International Conference on Smart Systems and Inventive Technology (ICSSIT)*. [S.l.], 2023. p. 659–662.

WORDPRESS. *Site ofical Wordpress*. 2020. Https://Wordpress.org.

WORDPRESS. *Site ofical Wordpress*. 2020. Https://wordpress.org/about/security/.