





1) Identificação do alvo:	4
2) Ferramentas de análise:	4
3) Método de investigação e análise:	4
4) Aplicação e resultado:	5
Matriz de Riscos	7

- **Mensagem Sobre o Autor.**

Informamos a empresa relatando sobre a falha descoberta, se for possível um agendamento na empresa para explicar sobre, mas detalhes sobre o processo da falha desde o começo e até final da falha e orientado a empresa sobre quais providencia deve tomar segurança para a empresa e damos suporte para arrumar a falha descoberta.



- **IMPORTANTE:** Este documento contém informação confidencial e privilegiada, sendo seu sigilo protegido por lei. Se você não for o destinatário ou a pessoa autorizada a receber este documento, não pode usar, copiar ou divulgar as informações nele contidas ou tomar qualquer ação baseada nessas informações. Se você recebeu este documento por engano, por favor, avise imediatamente ao remetente (vise nota de rodapé) e em seguida apague-o.
- **IMPORTANT:** This document contains confidential and privileged information, and its secrecy is protected by law. If you are not the recipient or the person authorized to receive this document, you may not use, copy or disclose the information contained therein or take any action based on this information. If you have received this document in error, please notify the sender immediately (see footnote) and delete it.



1) Identificação do alvo:

Sistema de gestão de projetos denominado ALVO mantido e comercializado pela empresa FORNECEDOR DO SISTEMA instalado no ambiente de rede da empresa CLIENTE ALVO. Todos os testes são executados no servidor de homologação **SERVIDOR DO SISTEMA**.

2) Ferramentas de análise:

- A – WebScanWP – Desenvolvida pelo Analista
- B – Nmap
- C – Attack Brute Force
- D – Engenharia social
- E – PhishingMail – Desenvolvida pelo Analista

3) Método de investigação e análise:

- A – Efetuado testes automáticos por meio das ferramentas citadas.
- B – Efetuado testes manuais para a prova de conceito das vulnerabilidades.
- C – Uso de credenciais de acesso, por meio de forma de attack brute Force pra verificar o painel de admin do acesso website.
- D - Engenharia Social por meio de criatividade de ataques phishing, tentando obter o máximo de informações possível para o acesso servidor principal.



4) Aplicação e resultado:

Com base nos resultados obtidos por meio da varredura automática com o auxílio da ferramenta OWASP ZAP, que por sua vez mostrou um maior número de respostas em um relatório mais completo, foi possível atestar por meios manuais a veracidade das falhas encontradas, atendo-se somente a algumas das falhas qualificadas no relatório como alto risco.

Para a realização da prova de conceito, foi utilizado o software BurpSuite, que permite a execução passo a passo do sistema, podendo assim de forma mais rápida e eficiente testar os parâmetros escolhidos pelo Pentester no ato da análise. O escopo da análise está baseado no **OWASP TOP 10 de 2022**.

A1 – Injeção	As falhas de Injeção, tais como injeção de SQL, de SO (Sistema Operacional) e de LDAP, ocorrem quando dados não confiáveis são enviados para um interpretador como parte de um comando ou consulta. Os dados manipulados pelo atacante podem iludir o interpretador para que este execute comandos indesejados ou permita o acesso a dados não autorizados.
A2 – Quebra de Autenticação e Gerenciamento de Sessão	As funções da aplicação relacionadas com autenticação e gerenciamento de sessão geralmente são implementadas de forma incorreta, permitindo que os atacantes comprometam senhas, chaves e tokens de sessão ou, ainda, explorem outra falha da implementação para assumir a identidade de outros usuários.
A3 – Cross-Site Scripting (XSS)	Falhas XSS ocorrem sempre que uma aplicação recebe dados não confiáveis e os envia ao navegador sem validação ou filtro adequados. XSS permite aos atacantes executarem scripts no navegador da vítima que podem “sequestrar” sessões do usuário, desfigurar sites, ou redirecionar o usuário para sites maliciosos.
A4 – Referência Insegura e Direta a Objetos	Uma referência insegura e direta a um objeto ocorre quando um programador expõe uma referência à implementação interna de um objeto, como um arquivo, diretório, ou registro da base de dados. Sem a verificação do controle de acesso ou outra proteção, os atacantes podem manipular estas referências para acessar dados não-autorizados.

A5 – Configuração Incorreta de Segurança	<p>Uma boa segurança exige a definição de uma configuração segura e implementada na aplicação, frameworks, servidor de aplicação, servidor web, banco de dados e plataforma. Todas essas configurações devem ser definidas, implementadas e mantidas, já que geralmente a configuração padrão é insegura. Adicionalmente, o software deve ser mantido atualizado.</p>
A6 – Exposição de Dados Sensíveis	<p>Muitas aplicações web não protegem devidamente os dados sensíveis, tais como cartões de crédito, IDs fiscais e credenciais de autenticação. Os atacantes podem roubar ou modificar esses dados desprotegidos com o propósito de realizar fraudes de cartões de crédito, roubo de identidade, ou outros crimes.</p>
	<p>Os dados sensíveis merecem proteção extra como criptografia no armazenamento ou em trânsito, bem como precauções especiais quando trafegadas pelo navegador.</p>
A7 – Falta de Função para Controle do Nível de Acesso	<p>A maioria das aplicações web verificam os direitos de acesso em nível de função antes de tornar-se essa funcionalidade visível na interface do usuário. No entanto, as aplicações precisam executar as mesmas verificações de controle de acesso no servidor quando cada função é invocada. Se estas requisições não forem verificadas, os atacantes serão capazes de forjar as requisições, com o propósito de acessar a funcionalidade sem autorização adequada.</p>
A8 – Cross-Site Request Forgery (CSRF)	<p>Um ataque CSRF força a vítima que possui uma sessão ativa em um navegador a enviar uma requisição HTTP forjada, incluindo o cookie da sessão da vítima e qualquer outra informação de autenticação incluída na sessão, a uma aplicação web vulnerável. Esta falha permite ao atacante forçar o navegador da vítima a criar requisições que a aplicação vulnerável aceite como requisições legítimas realizadas pela vítima.</p>
A9 – Utilização de Componentes Vulneráveis Conhecidos	<p>Componentes, tais como bibliotecas, frameworks, e outros módulos de software quase sempre são executados com privilégios elevados. Se um componente vulnerável é explorado, um ataque pode causar sérias perdas de dados ou o comprometimento do servidor. As aplicações que utilizam componentes com vulnerabilidades conhecidas podem minar as suas defesas e permitir uma gama de possíveis ataques e impactos.</p>

A10 – Redirecionamentos e Encaminhamentos Inválidos	Aplicações web frequentemente redirecionam e encaminham usuários para outras páginas e sites, e usam dados não confiáveis para determinar as páginas de destino. Sem uma validação adequada, os atacantes podem redirecionar as vítimas para sites de phishing ou malware, ou usar encaminhamentos para acessar páginas não autorizadas.
--	--

Com base nos testes realizados seguindo rigorosamente o escopo definido, conforme tabela acima **OWASP TOP 10**, foi possível elaborar a matriz de riscos. Os tópicos foram avaliados de acordo com o ramo de negócios da empresa.

Entretanto devido ao propósito do sistema ALVO ser auxiliar a gestão de projetos e armazenar dados sensíveis referente ao negócio dos clientes, e também dado o teor das vulnerabilidades em relação ao sistema como um todo, podemos descrever os riscos de forma simplificada, conforme pode ser observado na tabela abaixo:

Matriz de Riscos

Consequências		
Nível	Descrição	Tópico OWASP
5	Catastrófico	A1 – Injeção
4	Maior	A2 – Quebra de Autenticação e Gerenciamento de Sessão
5	Catastrófico	A3 – Cross-Site Scripting (XSS)
3	Moderado	A4 – Referência Insegura e Direta a Objetos
4	Maior	A5 – Configuração Incorreta de Segurança
4	Maior	A6 – Exposição de Dados Sensíveis
5	Catastrófico	A7 – Falta de Função para Controle do Nível de Acesso
4	Maior	A8 – Cross-Site Request Forgery (CSRF)
2	Menor	A9 – Utilização de Componentes Vulneráveis Conhecidos
4	Maior	A10 – Redirecionamentos e Encaminhamentos Inválidos

Probabilidade	Consequências				
	Insignificante	Menor	Moderado	Maior	Catastrófico
	1	2	3	4	5
A (Quase certo)	H	H	E	E	E
B (Provável)	M	H	H	E	E
C (Possível)	L	M	H	E	E
D (Improvável)	L	L	M	H	E
E (Raro)	L	L	M	H	H

Probabilidade	ANALISE DE GRAVIDADE
E	Risco Extremo - Ação deve ser implementadas imediatamente
H	Risco Elevado - É necessária atenção pela gerência sênior
M	Risco Moderado - Responsabilidade pela gestão do risco deve ser especificada
L	Risco Baixo - Gerenciamento por procedimentos de rotina

Devido ao alto teor de confidencialidade, nenhuma das técnicas e vulnerabilidades foram nem serão sob qualquer circunstância expostas neste documento, visto que o vazamento destas informações **pode acarretar danos morais, legais e financeiros irreparáveis para ambas as partes.**

5) **Análise crítica do resultado com base na legislação atual:**

Após uma profunda análise dos resultados é possível concluir que de acordo com as leis vigentes os seguintes crimes e/ou contravenções conforme tópicos abaixo são favorecidos por meio das vulnerabilidades encontradas.

- Ter acesso a um sistema informatizado sem autorização;
- Estelionato eletrônico;
- Obter, transferir ou fornecer dados ou informações sem autorização;
- Divulgação ou utilização de modo indevido, as informações e dados pessoais abrangidos em um sistema informatizado;
- Inutilizar, destruir ou deteriorar dados eletrônicos de terceiros ou coisas alheias;
- Inserir ou propagar código malicioso em um sistema informatizado;
- Inserir ou propagar código malicioso, seguido de danos;
- Atentar contra a segurança de serviço de utilidade pública;
- Interromper ou perturbar serviço telegráfico, telefônico, informático, telemático ou sistema informatizado;
- Falsificação de dados eletrônicos ou documentos públicos;
- Falsificar dados eletrônicos ou documentos particulares;
- Obtenção dados;
- Alteração de dados;
- Exclusão de dados;
- Inviolabilidade da intimidade e da vida privada, sua proteção e indenização pelo dano material ou moral decorrente de sua violação;
- Inviolabilidade e sigilo do fluxo de suas comunicações pela internet, salvo por ordem judicial, na forma da lei;
- Inviolabilidade e sigilo de suas comunicações privadas armazenadas, salvo por ordem judicial;
- Não fornecimento a terceiros de seus dados pessoais, inclusive registros de conexão, e de acesso a aplicações de internet, salvo mediante consentimento livre, expresso e informado ou nas hipóteses previstas em lei;

- A guarda e a disponibilização dos registros de conexão e de acesso a aplicações de internet de que trata esta Lei, bem como de dados pessoais e do conteúdo de comunicações privadas, devem atender à preservação da intimidade, da vida privada, da honra e da imagem das partes direta ou indiretamente envolvidas.

De acordo com os dados já apresentados à FORNECEDOR DO SISTEMA (empresa responsável pelo ALVO) em forma de relatório gerado pela ferramenta OWASP ZAP, fica a cargo exclusivo do mesmo a correção do sistema e a prática de prevenção de novas vulnerabilidades, bem como auxiliar a empresa CLIENTE ALVO na prevenção e homologação de ambiente de servidor de aplicação mais seguro.

Dado o fato de que a empresa CLIENTE ALVO fornecer aos seus clientes e parceiros o acesso ao sistema ALVO para a gestão de projetos, a empresa fica qualificada como **Provedor de Aplicação de Internet**, deste modo cabe uma profunda análise crítica e jurídica do [capítulo 3 do Marco Civil da Internet Lei 12.965/14](#). Sendo assim a empresa CLIENTE ALVO (ou qualquer outra empresa que utilize o referido sistema), poderá vir a assumir o papel de réu, caso por ventura algum cliente sofrer qualquer tipo de atentado e entrar com recursos na corte da lei.

Levando em consideração os conceitos de Risco, Vulnerabilidade e Ameaça, com base nas evidências encontradas, torna-se possível qualificar essas evidências afirmando que há o risco de uma fonte de ameaça explorar alguma vulnerabilidade do sistema resultando em um impacto negativo a organização.

6) Procedimentos e Responsabilidades.

Atualmente a empresa CLIENTE ALVO conta com os processos de Governança de TI, Auditoria de Segurança da Informação, Pentest e Segurança em Desenvolvimento de Sistemas. Devido a esses processos, faz-se necessário que todos e quaisquer sistemas, dispositivos e afins ativos de informação passem por um processo de Pentest, afim de garantir a segurança da informação da empresa, clientes e parceiros.

Portanto é evidente e de suma importância a necessidade de classificação das responsabilidades de cada parte, afim de, atribuir os direitos e deveres de ambas as



partes em relação ao usuário final, este por sua vez diretamente ligado a empresa CLIENTE ALVO.

O processo de Pentest do sistema ALVO dar-se-á de duas formas distintas, sendo a primeira de responsabilidade da empresa CLIENTE ALVO, onde o mesmo será efetuado em ambiente controlado dentro das dependências da empresa. A segunda forma é de inteira responsabilidade da empresa FORNECEDOR DO SISTEMA, sendo que a mesma deverá contratar a consultoria de Pentest por conta própria.

A primeira parte do processo de Pentest do sistema ALVO encerrou no dia 10/06/2016, processo este de inteiro interesse e responsabilidade da empresa CLIENTE ALVO, representada pelo requerente DIRETOR DA EMPRESA ALVO. A segunda parte fica a cargo da empresa FORNECEDOR DO SISTEMA, mantenedora do sistema ALVO, sendo de sua inteira responsabilidade e interesse, a qual deverá por sua conta escolher a melhor forma de fazê-lo.

Os processos de identificação e atribuição das responsabilidades serão efetuados **em comum acordo de forma amigável e colaborativa entre as partes**, CLIENTE ALVO e FORNECEDOR DO SISTEMA. Entretanto vale ressaltar que a empresa CLIENTE ALVO, reserva-se legalmente do direito de exigir um processo de Pentest ao fornecedor do sistema ALVO, bem como a correção de suas vulnerabilidades.

A empresa CLIENTE ALVO reserva-se do total e irrevogável direito de manter o sigilo das técnicas e resultados provenientes da prova de conceito aplicados em seu ambiente interno de homologação.

7) Processo de Scanner de Portas:

A Ferramenta Nmap foi usada para verificar as portas abertas e quais são as possibilidades de falha no sistema, verificamos dos os tipos de acesso que está disponível:

```
zorin@zorin:~$ nmap www.romi.com -sV
Starting Nmap 7.93 ( https://nmap.org ) at 2022-11-29 18:55 -03
Nmap scan report for www.romi.com (198.58.110.248)
Host is up (0.16s latency).
rDNS record for 198.58.110.248: ip-198-58-110-248.cloudzapp.io
Not shown: 986 filtered tcp ports (no-response)
PORT      STATE SERVICE VERSION
20/tcp    closed ftp-data
21/tcp    closed ftp
22/tcp    open  ssh      OpenSSH 7.6p1 Ubuntu 4ubuntu0.5 (Ubuntu Linux; protocol 2.0)
80/tcp    open  http     nginx
110/tcp   open  pop3     Dovecot pop3d
143/tcp   open  imap     Dovecot imapd
443/tcp   open  ssl/http nginx
465/tcp   open  ssl/smtp Exim smtpd
587/tcp   open  smtp     Exim smtpd
993/tcp   open  ssl/imap Dovecot imapd
995/tcp   open  ssl/pop3 Dovecot pop3d
2222/tcp  open  ssh      OpenSSH 7.6p1 Ubuntu 4ubuntu0.5 (Ubuntu Linux; protocol 2.0)
3306/tcp  open  mysql    MySQL 5.7.40-0ubuntu0.18.04.1
40193/tcp closed unknown
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 29.11 seconds
```



8) Informações sobre versões:

A Ferramentas Nmap verifica quais são o acesso de cada porta pode passa o acesso com diretório e versão dos servidores:

```
Starting Nmap 7.93 ( https://nmap.org ) at 2022-11-29 19:46 -03
Nmap scan report for www.romi.com (198.58.110.248)
Host is up (0.18s latency).
rDNS record for 198.58.110.248: ip-198-58-110-248.cloudezapp.io
Not shown: 986 filtered tcp ports (no-response)
PORT      STATE SERVICE VERSION
20/tcp    closed ftp-data
21/tcp    closed ftp
22/tcp    open  ssh      OpenSSH 7.6p1 Ubuntu 4ubuntu0.5 (Ubuntu Linux; protocol 2.0)
80/tcp    open  http     nginx
```

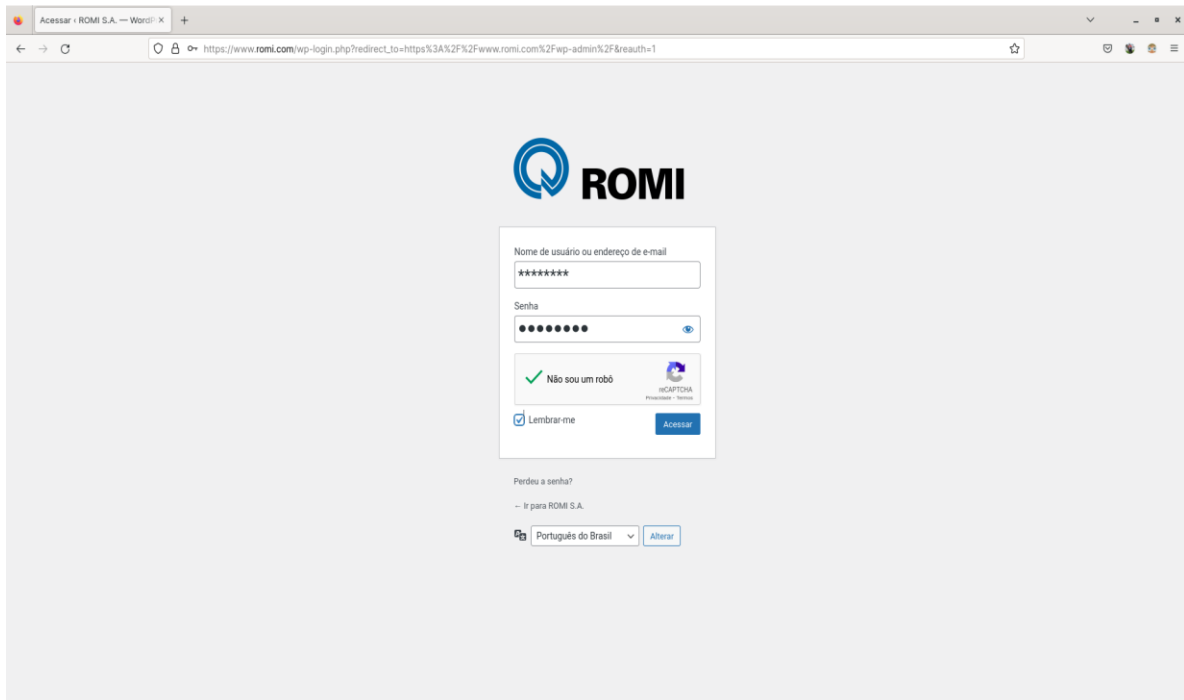
9) Informações sobre WP-ADMIN:

A ferramenta Nmap verifica os diretórios dos servidores e descobre o diretório o wp-admin isso nos oferece um aceso que todos os usuários podem ter o acesso do painel administrador do site:

```
443/tcp    open  ssl/http nginx
|_ tls-alpn:
|   h2
|   http/1.1
|   http/1.0
|_  http/0.9
|_ ssl-cert: Subject: commonName=*.romi.com
|   Subject Alternative Name: DNS:*.romi.com, DNS:romi.com
|   Not valid before: 2022-07-13T18:35:30
|_  Not valid after: 2023-08-14T18:35:30
|_  _ssl-date: TLS randomness does not represent time
|   http-robots.txt: 1 disallowed entry
|_  /wp-admin/
|_  _http-title: ROMI S.A.
```

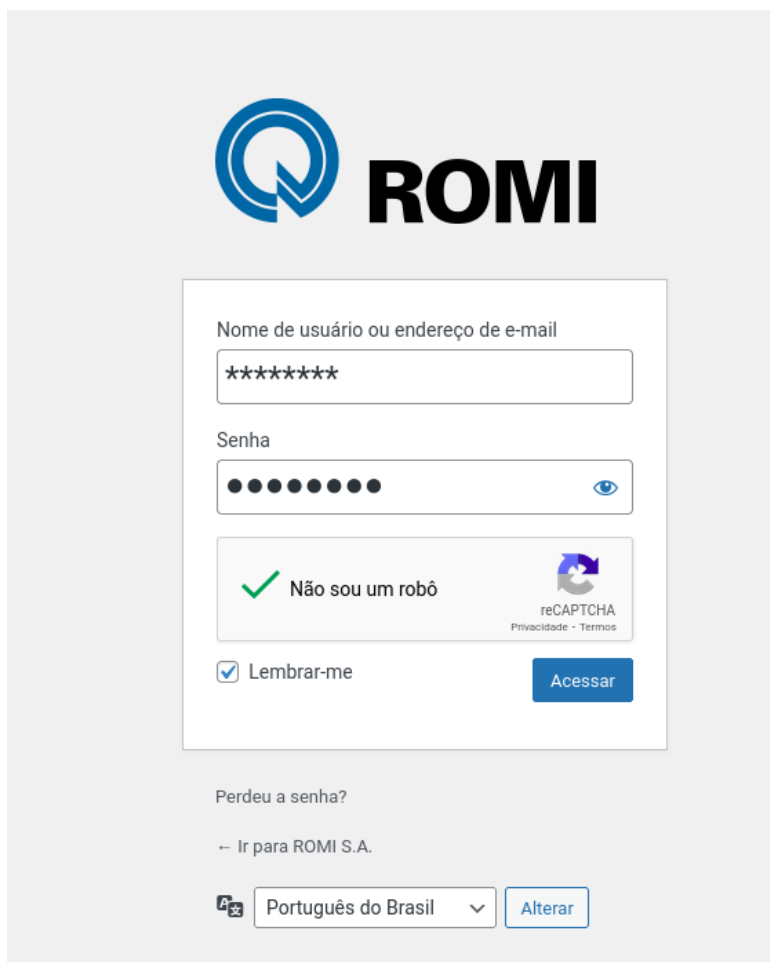
10) Sobre a falha WP-ADMIN:

O diretório WP-ADMIN é porta de acesso do painel administrador, que pode ser bem grave após que uma pessoas mal-intencionadas tem o acesso pode ter todos os tipos de dados como login de acesso de outro serviço e dados de e-mail e senhas de clientes e plantar um malware no servidor exemplo: Malware trojan e aplicar outras informações no website:



11) Informações sobre Pannel de Administrador

O painel de administrador estando aberto para o público na Web, o hacker pode começar aplicar vários tipos de ataques no site e pela empresa tentando obter acesso do painel administrador exemplo: Ataque Script, Brute Force, Phishing e falhas nas versões dos plugin que o site estiver utilizado e kernel...



The image shows a login page for a system named ROMI. At the top, there is a logo consisting of a blue circle with a stylized 'Q' inside, followed by the word 'ROMI' in bold black letters. Below the logo is a white login box. Inside the box, there are two input fields: the first is labeled 'Nome de usuário ou endereço de e-mail' and contains eight asterisks; the second is labeled 'Senha' and contains ten dots. To the right of the password field is an eye icon. Below these fields is a reCAPTCHA widget with a green checkmark and the text 'Não sou um robô'. To the right of the reCAPTCHA is a small icon of a robot head and the text 'reCAPTCHA Privacidade - Termos'. Below the reCAPTCHA is a checkbox labeled 'Lembrar-me' which is checked. To the right of the checkbox is a blue button labeled 'Acessar'. Below the login box, there is a link 'Perdeu a senha?'. Below that is a link '← Ir para ROMI S.A.'. At the bottom, there is a language selector showing 'Português do Brasil' with a dropdown arrow, and a blue button labeled 'Alterar'.

12) Ferramenta sobre WebScanWP:

O desenvolvedor Felipe Miguel desenvolveu a ferramenta WebScanWP para uso pessoal para consulta de falhas em website que é feita em WordPress tentando obter vários tipos de dados exemplo: como acesso de painel admin, banco de dados.

E como podemos verificar a ferramenta WebScanWP verificou no HTML e descobri o acesso wp-admin no condigo fonte site.

```
</script>
<script type='text/javascript' src='https://www.romi.com/wp-content/plugins/wppopups/pro/assets/js/wppopups.js?ver=2.1.4.5' id='wppopups-pro-js-js'></script>
<script type='text/javascript' src='https://www.romi.com/wp-content/themes/romi/dist/script/vendor/slick.min.js?ver=1.0' id='slider-js'></script>
<script type='text/javascript' src='https://unpkg.com/@ungap/custom-elements-builtin?ver=1.0' id='elements-builtin-js'></script>
<script type='text/javascript' src='https://www.romi.com/wp-content/themes/romi/dist/script/xframebypassload.js?ver=1.0' id='loadiframe-js'></script>
<script type='text/javascript' src='https://www.romi.com/wp-content/themes/romi/dist/script/vendor/ajax-pagination.min.js?ver=1.0' id='infinite-scroll-js'></script>
<script type='text/javascript' id='__ytprefs__-js-extra'>
/* <![CDATA[ */
var _EPT_ = {"ajaxurl":"https://www.romi.com/wp-admin/admin-ajax.php","security":"c483f50df7","gallery_scrolloffset":"20","eppathscripts":"https://www.romi.com/wp-content/themes/romi/dist/script/vendor/ajax-pagination.min.js?ver=1.0"};
/* ]]> */
</script>
```

13) WebScanWP acesso MySQL:

A ferramenta WebScanWP verificando dos os tipos de portas e acesso descobrir portas aberta para banco de dados e a versão que está sendo utilizada:

```
3306/tcp open  mysql      MySQL 5.7.40-0ubuntu0.18.04.1
| mysql-info:
|   Protocol: 10
|   Version: 5.7.40-0ubuntu0.18.04.1
|   Thread ID: 4970
|   Capabilities flags: 63487
|   Some Capabilities: LongPassword, InteractiveClient,
|   Status: Autocommit
|   Salt: s2|1V\x15\x06+*qljy\x14a\x07Y.,]
|_ Auth Plugin Name: mysql_native_password
```




14) Informações sobre Analista:

Informamos a empresa relatando sobre a falha descoberta, se for possível um agendamento na empresa para explicar sobre, mas detalhes sobre o processo da falha desde o começo e até final da falha e orientado a empresa sobre quais providencia deve tomar segurança para a empresa e damos suporte para arrumar a falha descoberta.

Contatos: [+55 \(19\) 99690-7258](tel:+5519996907258)

E-mail: feliphe@tuta.io

Linkedin: <https://www.linkedin.com/in/fehoffcial/>

Github: <https://github.com/fehoffcial>

"" MUITO OBRIGADO PELA OPORTUNIDADE AGUARDO SEU RETORNO ASSIM QUE POSSÍVEL. ""