



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 – ReconScan
- B – Nmap
- C – Attack Brute Force
- D – Engenharia social

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 brut, 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) A Ferramenta Ping:

A ferramenta Ping foi utilizada para escanear o sistema tentando obter o máximo de informações possíveis, por exemplo: `ping -c1 www.qyon.com`

```
L# ping -c1 www.qyon.com
PING www.qyon.com(www.qyon.com (2804:10:8088::197:72)) 56 data bytes
64 bytes from www.qyon.com (2804:10:8088::197:72): icmp_seq=1 ttl=53 time=8.63 ms

--- www.qyon.com ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 8.632/8.632/8.632/0.000 ms
```

8) A Ferramenta Nmap:

A ferramenta Nmap foi utilizada para escanear para saber quais são as portas que estão abertas: `nmap -sV qyon.com`

```
L# nmap -sV qyon.com
Starting Nmap 7.93 ( https://nmap.org ) at 2022-12-07 04:45 -03
Nmap scan report for qyon.com (191.6.197.72)
Host is up (0.015s latency).
Not shown: 984 filtered tcp ports (no-response), 9 filtered tcp ports (port-unreach)
PORT      STATE SERVICE VERSION
20/tcp    closed ftp-data
21/tcp    open  ftp      ProFTPD
22/tcp    open  ssh      OpenSSH 8.0 (protocol 2.0)
80/tcp    open  http     Apache httpd
443/tcp   open  ssl/http Apache httpd
3306/tcp  open  mysql    MySQL 5.5.5-10.2.36-MariaDB-log
3690/tcp  open  svnserve Subversion
```



9) A Ferramenta Nmap:

Após de verificar que a ferramenta Nmap nos fornece quais portas estão abertas, decidimos fazer uma varredura um pouco mais profunda:

```
└─$ nmap -A qyon.com
Starting Nmap 7.93 ( https://nmap.org ) at 2022-12-07 04:49 -03
Nmap scan report for qyon.com (191.6.197.72)
Host is up (0.011s latency).
Not shown: 983 filtered tcp ports (no-response), 10 filtered tcp ports (port-unreach)
PORT      STATE SERVICE VERSION
20/tcp    closed ftp-data
21/tcp    open  ftp      ProFTPD
|_ tls-nextprotoneg:
|_ ftp
|_ ssl-date: 2022-12-07T07:49:54+00:00; 0s from scanner time.
|_ ssl-cert: Subject: commonName=*.kinghost.net
|_ Subject Alternative Name: DNS:*.kinghost.net, DNS:kinghost.net
|_ Not valid before: 2022-07-04T00:00:00
|_ Not valid after: 2023-07-21T23:59:59
22/tcp    open  ssh      OpenSSH 8.0 (protocol 2.0)
|_ ssh-hostkey:
|_ 2048 b558d91524bfd75e1beafb3c5d7d91c6 (RSA)
|_ 256 157ca4730292b9326acf7e2517495b3f (ECDSA)
|_ 256 d7347c60edd7d8b3eb287a96a11a1672 (ED25519)
80/tcp    open  http     Apache httpd
|_ http-server-header: Apache
|_ http-robots.txt: 2 disallowed entries
|_ /cgi-bin/ /wusage
|_ http-generator: WordPress 6.1.1
|_ http-title: QYON Sistemas Inteligentes &#8211; QYON Sistemas Inteligentes
443/tcp   open  ssl/http Apache httpd
|_ tls-alpn:
|_ http/1.1
|_ http-robots.txt: 2 disallowed entries
|_ /cgi-bin/ /wusage
|_ http-title: QYON Sistemas Inteligentes &#8211; QYON Sistemas Inteligentes
|_ http-generator: WordPress 6.1.1
|_ http-server-header: Apache
|_ ssl-date: TLS randomness does not represent time
|_ ssl-cert: Subject: commonName=www.qyon.com
|_ Subject Alternative Name: DNS:www.qyon.com, DNS:qyon.com
|_ Not valid before: 2022-07-30T00:00:00
```

E como podemos ver, o servidor nos oferece informações sobre Apache e componentes como OpenSSH e versão 8.0, WordPress e versão 6.1.1 e MySQL e versão 5.5.5:

```
3306/tcp  open  mysql    MySQL 5.5.5-10.2.36-MariaDB-log
|_ mysql-info:
|_ Protocol: 10
|_ Version: 5.5.5-10.2.36-MariaDB-log
|_ Thread ID: 2198430
|_ Capabilities flags: 63486
|_ Some Capabilities: SupportsTransactions, Support41Auth,
|_ ColumnFlag, FoundRows, Speaks41ProtocolOld, SupportsCompressi
|_ Status: Autocommit
|_ Salt: ZY2,'}aOHZk,7pNu#I*2
|_ Auth Plugin Name: mysql_native_password
```

10) Google Developer:

Depois de verificar quais tipos de portas estão abertas e quais componentes são usados no servidor, decidimos verificar o código-fonte do site: www.qyon.com

```
▲ Mixed Content: The page at 'https://www.qyon.com/contador/' was loaded over HTTPS, but www.qyon.com/:1 requested an insecure element 'http://qyon.com/en/wp-content/uploads/2021/11/pt-br.png'. This request was automatically upgraded to HTTPS, For more information see https://blog.chromium.org/2019/10/no-more-mixed-messages-about-https.html
▲ Mixed Content: The page at 'https://www.qyon.com/contador/' was loaded over HTTPS, but www.qyon.com/:1 requested an insecure element 'http://qyon.com/en/wp-content/uploads/2021/11/us.png'. This request was automatically upgraded to HTTPS, For more information see https://blog.chromium.org/2019/10/no-more-mixed-messages-about-https.html
JQMIGRATE: Migrate is installed, version 3.3.2 jquery-migrate.min.js?ver=3.3.2:2
▲ Mixed Content: The page at 'https://www.qyon.com/contador/' was loaded over HTTPS, but www.qyon.com/:254 requested an insecure element 'http://qyon.com/en/wp-content/uploads/2021/11/pt-br.png'. This request was automatically upgraded to HTTPS, For more information see https://blog.chromium.org/2019/10/no-more-mixed-messages-about-https.html
▲ Mixed Content: The page at 'https://www.qyon.com/contador/' was loaded over HTTPS, but www.qyon.com/:254 requested an insecure element 'http://qyon.com/en/wp-content/uploads/2021/11/us.png'. This request was automatically upgraded to HTTPS, For more information see https://blog.chromium.org/2019/10/no-more-mixed-messages-about-https.html
```

Verificamos no console do google alguns tipos de bugs que estão causando conflitos no console, e como podemos ver, encontramos um atributo do WordPress igual a wp-content:

```
✖ Failed to execute 'postMessage' on 'DOMWindow': The target origin provided ('http://www.youtube.com') does not match the recipient window's origin ('https://www.qyon.com').
✖ Uncaught DOMException: Failed to construct 'PresentationRequest': The document is sandboxed and lacks the 'allow-presentation' flag.
    at V.initialize (https://www.gstatic.com/eureka/clank/108/cast_sender.js:88:87)
    at chrome.cast.initialize (https://www.gstatic.com/eureka/clank/108/cast_sender.js:102:162)
    at g.k.init (https://www.youtube.com/s/player/ac058a09/player_ias.vflset/pt_BR/remote.js:588:13)
    at jlb (https://www.youtube.com/s/player/ac058a09/player_ias.vflset/pt_BR/remote.js:254:40)
    at $kb (https://www.youtube.com/s/player/ac058a09/player_ias.vflset/pt_BR/remote.js:260:9)
    at d.disableCastApi.window.chrome.cast.chrome.cast.isAvailable.window._onGCastApiAvailable (https://www.youtube.com/s/player/ac058a09/player_ias.vflset/pt_BR/remote.js:248:402)
    at chrome.cast.ga (https://www.gstatic.com/eureka/clank/108/cast_sender.js:105:152)
```

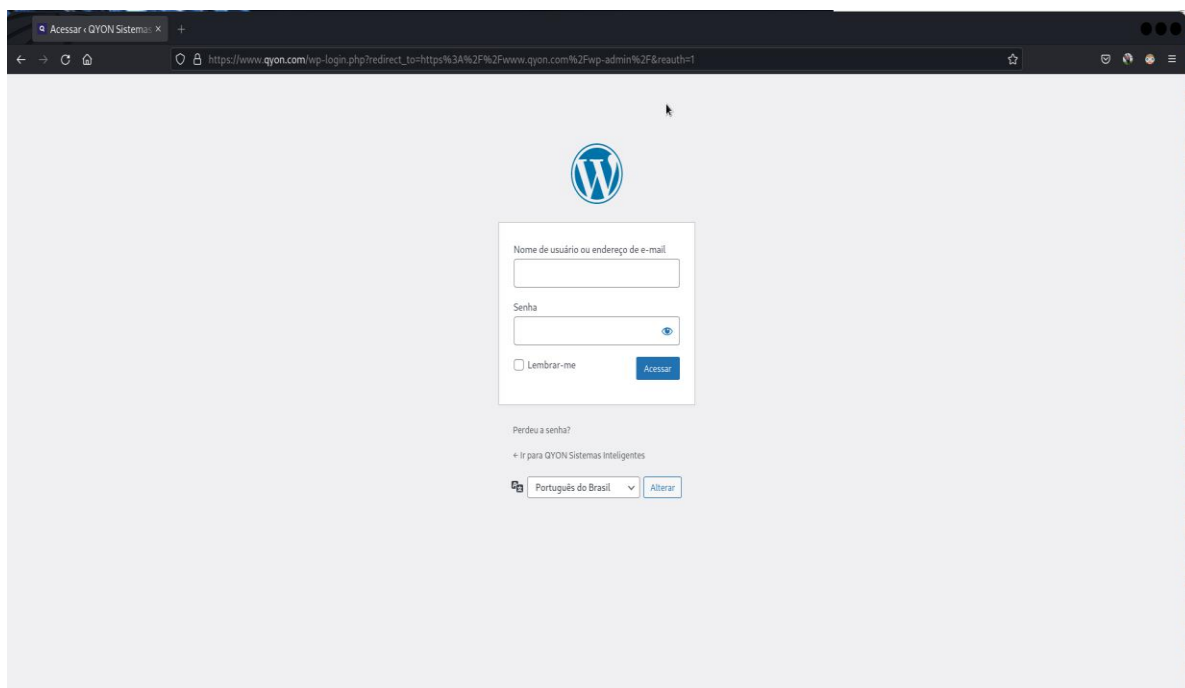
Problemas com APIs na parte de conexão, e o Google Console estava relatando esse bug.

11) Verificando o Código Fonte:

Após de ver os tipos de bugs que aparecendo no Google Console, decidimos verificar o código-fonte do site tentando encontrar o endereço do painel de administração:

```
<script src='https://www.qyon.com/wp-includes/js/jquery/jquery.min.js?ver=3.6.1' id='jquery-core-js'></script>
<script src='https://www.qyon.com/wp-includes/js/jquery/jquery-migrate.min.js?ver=3.3.2' id='jquery-migrate-js'></script>
<script id='cookie-law-info-js-extra'>
var Cli_Data = {"nn_cookie_ids":[],"cookieidlist":[],"non_necessary_cookies":[],"ccpaEnabled":"","ccpaRegionBased":"","ccpaBa
var cli_cookiebar_settings = {"animate_speed_hide":"500","animate speed_show":"500","background":"#FFF","border":"#b1a6a6c2
var log_object = {"ajax_url":"https://www.qyon.com/wp-admin/admin-ajax.php"};
</script>
<script src='https://www.qyon.com/wp-content/plugins/cookie-law-info/legacy/public/js/cookie-law-info-public.js?ver=3.0.6'
<script id='__ytprefs__-js-extra'>
var _EPYT_ = {"ajaxurl":"https://www.qyon.com/wp-admin/admin-ajax.php","security":"cae8a3f40e","gallery_scrolloffset":"
</script>
```

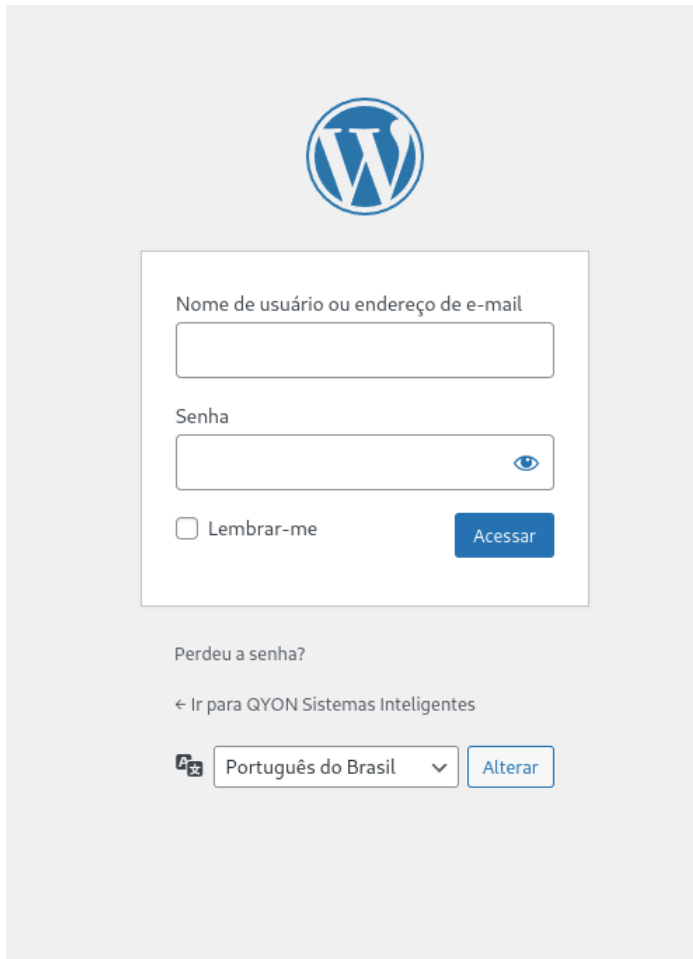
E como podemos ver, encontramos o endereço do painel de administração com esse tipo de acesso, podemos agora passar para a próxima fase, começar a aplicar alguns tipos de ataques, por exemplo: SQL Injetion e Cross Xcript e outros tipos de ataques.



12) Painel Administrador:

Após de ver o código-fonte podemos verificar e acessar o painel de administrador e começar alguns tipos de ataques exemplo: Brute Force, SQL injection e XSS.

Link: <https://qyon.com/wp-login.php?>

A screenshot of the WordPress login page. At the top center is the WordPress logo. Below it is a white rectangular box containing the login fields. The first field is labeled "Nome de usuário ou endereço de e-mail" and is empty. The second field is labeled "Senha" and is also empty, with a blue eye icon to its right for toggling visibility. Below the password field is a checkbox labeled "Lembrar-me". 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 QYON Sistemas Inteligentes". At the bottom, there is a language selector showing "Português do Brasil" with a dropdown arrow and an "Alterar" button next to it.

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. ""

