CIA DE PROCESSAMENTO DE DADOS DO ESTADO DE SÃO PAULO

PRODESP

Relatório de Análise de Vulnerabilidade do site:

www.bibliotecajuridica.sp.gov.br

REL.COSI.169.2023.V00

CLASSIFICAÇÃO: **CONFIDENCIAL**

DIRETORIA DE OPERAÇÕES

GERÊNCIA DE SEGURANÇA DA INFORMAÇÃO

COODENADORIA DE OPERAÇÃO E SEGURANÇA DA INFORMAÇÃO

Janeiro/2024

Rua Agueda Gonçalves, 240 - Taboão da Serra - SP - CEP 06760-900 – Tel.: (11) 2845-6000 (PABX)
Correspondência: Caixa Postal 25901 - CEP 05513-970 - SÃO PAULO - SP
www.prodesp.sp.gov.br - prodesp@prodesp.sp.gov.br

ÍNDICE

1. OBJETIVO

O objetivo deste relatório é apresentar as vulnerabilidades técnicas encontradas na página **www.bibliotecajuridica.sp.gov.br**, levando em consideração analise com grau de agressividade alto.

Vulnerabilidade é uma condição de fraqueza que quando explorado, pode resultar em uma violação de segurança.

As informações apresentadas neste documento serão classificadas por criticidade e separadas por servidor, contendo vulnerabilidades técnicas tais como: pastas compartilhadas (compartilhamento), aplicações desatualizadas, serviços disponíveis no servidor (portas abertas) entre outros.

2. INTRODUÇÃO

A técnica de análise de vulnerabilidade busca encontrar e eliminar qualquer brecha ou falha que possa ser utilizada por hackers ou demais pessoas mal-intencionadas para ter acesso a dados e informações confidenciais.

A fim de manter a integridade, confidencialidade, privacidade, autenticidade e disponibilidade das informações, a PRODESP se depara com constantes desafios que a leva a buscar novas soluções para manter todos os usuários e as informações dos clientes protegidas de ameaças e falhas.

Todo e qualquer sistema utilizado pela PRODESP pode estar sujeito a possuir falhas, sendo a conexão com a internet um dos principais pontos a serem explorados pelos cibercriminosos em suas ações de invasão e roubo.

Essa exposição pode permitir que ocorram ataques bem-sucedidos aos seus servidores, incorrendo na exposição de dados confidenciais e violando a política de privacidade de informação garantida por lei.

A maioria das falhas e brechas de segurança são frutos de determinadas situações ou ações que podem ser evitadas por meio de identificação e tratamento. Entre as principais origens podemos citar a falha humana, os erros de programação e má configuração.

A aplicação da análise de vulnerabilidades é composta de rotinas básicas, que buscam identificar falhas existentes na infraestrutura e aplicações classificando-as de acordo com a necessidade de intervenção, que vão da mais crítica a menos crítica, o que permite priorizar os principais pontos para realizar a correção.

As vulnerabilidades listadas abaixo estão catologadas conforme **CWE Common Weakness Enumeration** (Enumeração de Fraquezas Comuns, ou CWE na sigla em inglês). Trata-se de um sistema para categorizar falhas de segurança de software, focando em problemas de implementação que podem levar a vulnerabilidades. É um projeto colaborativo para entender os pontos fracos de segurança ou erros no código e vulnerabilidades e criar ferramentas para ajudar a evitá-los.

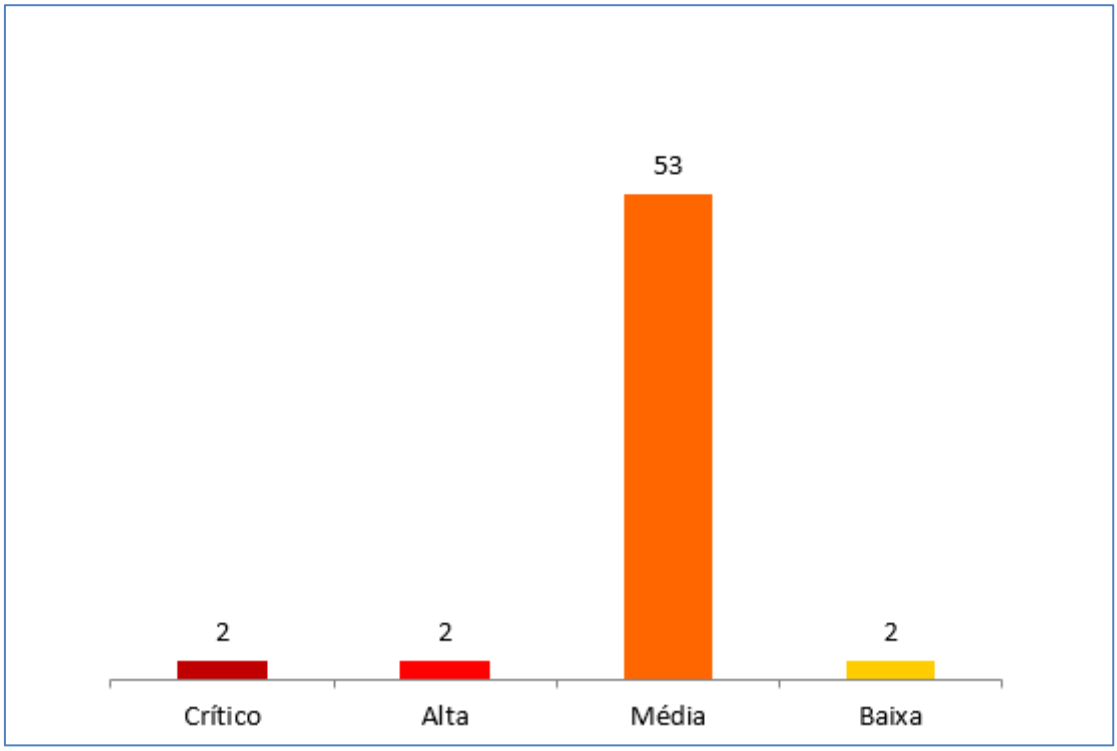
https://cwe.mitre.org/

3. A ANÁLISE DE VULNERABILIDADE

Abaixo, resumo das vulnerabilidades encontradas na página:

www.bibliotecajuridica.sp.gov.br

Sobre as vulnerabilidades identificadas:



	Vulnerable Component	2

	Vulnerable Component	2

	Vulnerable Component	2
	Cabeçalho "Content-Security-Policy" ausente	1
	Cabeçalho "X-Content-Type-Options" ausente ou inseguro	1
	Cabeçalhos de resposta HTTP desnecessários encontrados no aplicativo	1
	Configuração de Permissões Incorretas de Arquivos de Controle de Acesso do Servidor da Web	3
	Cookie com atributo SameSite Insecure, Improper ou Missing	1
	Diretório Oculto Detectado	2
	Divulgação de caminho em vários aplicativos baseados em PHP	1
	Link de terceiros não seguro (target="_blank")	17
	Parâmetros de Corpo Aceitos na Consulta	1
	Verificar suporte do SRI (Integridade de Sub-recurso)	23

	Vulnerable Component	2

DESCRIÇÃO DAS VULNERABILIDADES CRÍTICAS

Componente Vulnerável. (1/1)

URL Afetada

http://www.bibliotecajuridica.sp.gov.br/colorbox/jquery.colorbox.js
http://www.bibliotecajuridica.sp.gov.br/wp-content/plugins/contact-form-7/includes/js/index.js

Componente Vulnerável.

Um componente vulnerável é usado no aplicativo testado.
Um componente vulnerável pode introduzir todos os tipos de vulnerabilidades no aplicativo.

Como corrigir.

Atualize para a versão mais recente do componente. É altamente recomendável entrar em contato com o fornecedor deste produto para verificar se um patch ou correção foi disponibilizado recentemente.

CWE: 1035

CERT coordination center
Common Vulnerabilities and Exposures (CVE)

DESCRIÇÃO DAS VULNERABILIDADES ALTAS

Componente Vulnerável. (1/1)

URL Afetada

- http://www.bibliotecajuridica.sp.gov.br/colorbox/jquery.colorbox.js
- http://www.bibliotecajuridica.sp.gov.br/wp-content/plugins/contact-form-7/includes/js/index.js

Componente Vulnerável.

Um componente vulnerável é usado no aplicativo testado.
Um componente vulnerável pode introduzir todos os tipos de vulnerabilidades no aplicativo.

Como corrigir.

Atualize para a versão mais recente do componente. É altamente recomendável entrar em contato com o fornecedor deste produto para verificar se um patch ou correção foi disponibilizado recentemente.

CWE: 1035

CERT coordination center
Common Vulnerabilities and Exposures (CVE)

DESCRIÇÃO DAS VULNERABILIDADES MÉDIAS

Componente Vulnerável. (1/11)

URL Afetada

- http://www.bibliotecajuridica.sp.gov.br/colorbox/jquery.colorbox.js
- http://www.bibliotecajuridica.sp.gov.br/wp-content/plugins/contact-form-7/includes/js/index.js

Componente Vulnerável.

Um componente vulnerável é usado no aplicativo testado.
Um componente vulnerável pode introduzir todos os tipos de vulnerabilidades no aplicativo.

Como corrigir.

Atualize para a versão mais recente do componente. É altamente recomendável entrar em contato com o fornecedor deste produto para verificar se um patch ou correção foi disponibilizado recentemente.

CWE: 1035

CERT coordination center
Common Vulnerabilities and Exposures (CVE)

Cabeçalho "Content-Security-Policy" ausente (2/11)

URL Afetada

- http://www.bibliotecajuridica.sp.gov.br/

Como corrigir

Cabeçalho "Content-Security-Policy" ausente.

Programação ou configuração do aplicativo da Web não segura.

É possível reunir informações confidenciais sobre o aplicativo da Web, como nomes de usuário, senhas, nome da máquina e/ou locais de arquivos sensíveis.

É possível persuadir um usuário ingênuo a fornecer informações sensíveis como nome de usuário, senha, número de cartão de crédito, número de seguridade social etc.

Valores ausentes ou impróprios de CSP podem fazer com que o aplicativo da Web fique vulnerável a XSS, clickjacking etc.

O cabeçalho "Content-Security-Policy" é projetado para modificar a maneira como os navegadores processam as páginas e, portanto, para proteger contra várias injeções de sites cruzados, incluindo Cross-Site Scripting. É importante definir o valor do cabeçalho corretamente, de modo a não impedir o funcionamento adequado do site. Por exemplo, se o cabeçalho for definido para impedir a execução do JavaScript inline, o site não deverá usar o JavaScript inline em suas páginas.

Para proteção contra Cross-Site Scripting, Cross-Frame Scripting e clickjacking, é importante definir as seguintes políticas com os valores adequados:
ambas as políticas 'default-src' e 'frame-ancestors' *OU* todas as políticas 'script-src', 'object-src' e 'frame-ancestors'.

Para 'default-src', 'script-src' e 'object-src', evite valores inseguros como '*', 'data:', 'unsafe-inline' ou 'unsafe-eval'.

Para 'frame-ancestors', evite valores inseguros como '*' ou 'data:'.

Além disso, para 'script-src' e 'default-src' (diretiva de fallback para 'script-src'), 'self' não é considerado seguro e deve ser evitado.

Consulte os links a seguir para obter mais informações.

Observe que “Content-Security-Policy” inclui quatro testes diferentes. Um teste geral que verifica se o cabeçalho "Content-Security-Policy" está sendo usado e três testes adicionais que verificam se "Frame-Ancestors", "Object-Src" e "Script-Src" foram configurados corretamente.

Esse problema pode afetar vários tipos de produtos.

Configure seu servidor para enviar o cabeçalho "Content-Security-Policy".

É recomendado configurar o cabeçalho Content-Security-Policy com valores seguros para suas diretivas conforme a seguir:

Para 'default-src' e 'script-src', valores seguros como 'none' ou https://qualquer.exemplo.com.

Para 'frame-ancestors' e 'object-src' são esperados valores seguros como 'self', 'none' ou https://qualquer.exemplo.com.
"unsafe-inline" e "unsafe-eval" não devem ser usados em qualquer circunstância. Usar nonce / hash seria considerado uma solução temporária.

Para Apache, consulte:

http://httpd.apache.org/docs/2.2/mod/mod_headers.html

Para IIS, consulte:
https://technet.microsoft.com/pl-pl/library/cc753133%28v=ws.10%29.aspx

Para nginx, consulte:
http://nginx.org/en/docs/http/ngx_http_headers_module.html

CWE: 1032

Lista de alguns cabeçalhos seguros
Uma introdução à política de segurança de conteúdo
MDN Web Docs - Content-Security-Policy

Cabeçalho "X-Content-Type-Options" ausente ou inseguro (3/11)

URL Afetada

- http://www.bibliotecajuridica.sp.gov.br/

Como corrigir

Cabeçalho "X-Content-Type-Options" ausente ou inseguro.

Programação ou configuração insegura do aplicativo da Web.

É possível reunir informações sensíveis sobre o aplicativo da Web, como nomes de usuários, senhas, nome da máquina e/ou locais de arquivo sensíveis.

É possível persuadir um usuário ingênuo a fornecer informações sensíveis, como nome de usuário, senha, número de cartão de crédito, número de seguro social etc.

O cabeçalho "X-Content-Type-Options" (com valor "nosniff") impede que o IE e o Chrome ignorem o tipo de conteúdo de uma resposta.

Esta ação pode impedir que um conteúdo não confiável (por exemplo, um conteúdo carregado pelo usuário) seja executado no navegador do usuário (após uma nomeação maliciosa, por exemplo).

Este problema pode afetar diferentes tipos de produtos.

Configure seu servidor para enviar o cabeçalho "X-Content-Type-Options" com valor "nosniff" em todas as solicitações enviadas.

Para Apache, consulte:
http://httpd.apache.org/docs/2.2/mod/mod_headers.htmlPara IIS, consulte:
https://technet.microsoft.com/pl-pl/library/cc753133%28v=ws.10%29.aspxPara nginx, consulte:
http://nginx.org/en/docs/http/ngx_http_headers_module.html

CWE: 200

Lista de cabeçalhos HTTP úteis
Reduzindo os riscos de segurança do tipo MIME

Cabeçalhos de resposta HTTP desnecessários encontrados no aplicativo (4/11)

URL Afetada

- http://www.bibliotecajuridica.sp.gov.br/wp-content/plugins/contact-form-7/includes/js/index.js

Como corrigir

Cabeçalhos de resposta HTTP desnecessários encontrados no aplicativo.

Programação ou configuração insegura do aplicativo da Web.

É possível reunir informações confidenciais sobre o tipo, a versão e o SO do servidor da Web, entre outros.

O AppScan detectou um cabeçalho de resposta HTTP desnecessário.

Por razões de segurança e privacidade, os cabeçalhos de resposta HTTP como "Server", "X-Powered-By", "X-AspNetMvc-Version" e "X-AspNet-Version" não devem aparecer nas páginas Web.

Normalmente, o cabeçalho "Server" é adicionado por padrão sempre que uma resposta é enviada ao cliente pelo servidor.

O cabeçalho "X-Powered-By" pode ser adicionado por padrão sempre que uma resposta é enviada ao cliente pelo servidor.

Esses cabeçalhos adicionados podem revelar informações confidenciais sobre a versão e o tipo do software interno do servidor, permitindo que os invasores o identifiquem e o ataquem com explorações direcionadas. Além disso, quando uma nova exploração se torna conhecida para o público, o servidor provavelmente será atacado por ela.

Este problema pode afetar vários tipos de produtos.

Configure seu servidor para remover o cabeçalho padrão "Server" e impedir que ele seja enviado para todas as solicitações de saída.

Para IIS, consulte:
https://techcommunity.microsoft.com/t5/iis-support-blog/remove-unwanted-http-response-headers/ba-p/369710

Para nginx, consulte:
https://www.getpagespeed.com/server-setup/nginx/how-to-remove-the-server-header-in-nginx

Para a Weblogic, consulte:
https://docs.oracle.com/cd/E13222_01/wls/docs81/adminguide/web_server.html

Para Apache, consulte:
https://techglimpse.com/set-modify-response-headers-http-tip/

CWE: 200

Fingerprinting
Como impedir o vazamento de informações

Configuração de Permissões Incorretas de Arquivos de Controle de Acesso do Servidor da Web (5/11)

URL Afetada

- http://www.bibliotecajuridica.sp.gov.br/
- http://www.bibliotecajuridica.sp.gov.br/noticias/
- http://www.bibliotecajuridica.sp.gov.br/wp-admin/

Como corrigir

Configuração de Permissões Incorretas de Arquivos de Controle de Acesso do Servidor da Web.

Permissões/ACLs incorretas foram configuradas para o arquivo/diretório.

É possível fazer o download ou visualizar o conteúdo de um arquivo de configuração, o que pode conter informações vitais, como nomes de usuários e senhas.

Uma das necessidades mais comuns dos webmasters é fazer o servidor da Web tratar todos os documentos em um diretório específico, ou em uma árvore de diretórios, da mesma maneira; isso pode significar uma verificação de senha antes da concessão de acesso a qualquer arquivo no diretório ou permitir/proibir listagens de diretórios. Inúmeros servidores da Web, como Apache ou NCSA httpd, oferecem um método para fornecer a granularidade desejada de configuração, abaixo do nível de diretório, usando 3 arquivos de configuração parcial especial em cada diretório sem requisitos especiais. Os arquivos de configuração parcial são:

[1] .htaccess - Um arquivo .htaccess é simplesmente um arquivo de texto contendo diretivas do Apache. Essas diretivas se aplicam aos documentos no diretório em que o arquivo .htaccess está localizado e a todos os subdiretórios sob ele também.

[2] .htpasswd - Um arquivo .htpasswd é um arquivo simples usado para armazenar nomes de usuário e senhas para autenticação básica dos usuários de HHTP. Geralmente esse arquivo é criado usando o utilitário htpasswd. O utilitário criptografa senhas usando uma versão de MD5 modificada para o Apache ou a rotina crypt() do sistema.

[3] .htgroup - Um arquivo .htgroup é um arquivo simples contendo um mapeamento de grupos de usuários para nomes de usuários (assim como o arquivo de grupo do UNIX).

A configuração incorreta das permissões de acesso a algum dos 3 arquivos acima, ou a presença no diretório de versões antigas/de backup desses arquivos, pode permitir que o invasor faça o download do conteúdo do arquivo e use-o para desenvolver outros ataques.

Exploração de amostra:
GET /DIRECTORY_NAME/.htaccess HTTP/1.0

* Durante o teste do aplicativo, são feitas tentativas de recuperar arquivos originais e diversas versões de arquivos antigos/de backup.

Esse problema pode afetar vários tipos de produtos

[1] Arquivos de senha da Web como aqueles gerenciados por htpasswd não devem estar dentro do espaço do URI do servidor da Web -- ou seja, não devem ser pesquisáveis com um navegador.

[2] Configure permissões de acesso adequadas aos arquivos .htaccess e .htgroup.

CWE: 200

Usando arquivos .htaccess com Apache
Página do Manual - htpasswd

Cookie com atributo SameSite Insecure, Improper ou Missing (6/11)

URL Afetada

- http://www.bibliotecajuridica.sp.gov.br/

Como corrigir

Cookie com atributo SameSite Insecure, Improper ou Missing.

Cookie sensível com atributo SameSite Improper, Insecure ou Missing.

Evite o vazamento de informações de cookies restringindo os cookies para o contexto primário ou do mesmo site.

Os ataques poderão ser do tipo solicitação cross-site forjada (CSRF, Cross-Site-Request-Forgery), se não houver outras proteções implementadas (como tokens Anti-CSRF).

O atributo SameSite controla a maneira como os cookies são enviados para solicitações entre domínios.

O atributo pode ter três valores: 'Lax', 'Strict' ou 'None'. Se 'None' for usado, um site poderá criar uma solicitação POST HTTP entre domínios para outro site e o navegador adicionará cookies automaticamente a essa solicitação.

Isso poderá levar a ataques do tipo solicitação cross-site forjada (CSRF, Cross-Site-Request-Forgery) se não houver proteções adicionais implementadas (como tokens Anti-CSRF).

Modos e seus usos:
Modo 'Lax': o cookie só será enviado com uma solicitação get de nível superior.

Modo 'Strict': o cookie não será enviado com qualquer uso cross-site, mesmo se o usuário seguir um link para outro site.

Modo 'None': o cookie será enviado com as solicitações cross-site.

O atributo com 'Lax' ou 'None' deve ter o sinalizador 'Secure' definido e deve ser transferido por https.

Exemplo: Set-Cookie: chave=valor; SameSite=Lax;Secure

A opção recomendada é definir o atributo como 'Strict'.

Exemplo: Set-Cookie: chave=valor; SameSite=Strict

Esse problema pode afetar vários tipos de produtos.

[1] Revise as soluções possíveis para configurar o atributo do Cookie SameSite para os valores recomendados.

[2] Restrinja os cookies a um contexto primário ou do mesmo site.

[3] Verifique e defina o atributo SameSite do seu cookie como Strict, para garantir que o cookie seja enviado apenas em um contexto primário.

[4] Ou, se você quiser relaxar as restrições do contexto primário, verifique e defina o atributo SameSite do cookie como Lax, com o sinalizador Secure ativado e transferido por HTTPS.

CWE: 1275
Classificação de ameaça do WASC: vazamento de informações
Cookies SameSite

Diretório Oculto Detectado (7/11)

URL Afetada
- http://www.bibliotecajuridica.sp.gov.br/

Como corrigir
Diretório Oculto Detectado.

O servidor da Web ou servidor de aplicativos está configurado de uma maneira não segura.

É possível recuperar informações sobre a estrutura do sistema de arquivos do site, o que pode ajudar o invasor a mapear o Web site.

O aplicativo da Web expôs a presença de um diretório no site. Embora o diretório não liste seu conteúdo, as informações podem ajudar um invasor a desenvolver outros ataques contra o site. Por exemplo, sabendo o nome de um diretório, um invasor pode adivinhar seu tipo de conteúdo e, provavelmente, nomes de arquivos que residem nele, ou subdiretórios contidos nele, e tentar acessá-los.

Quanto mais sensível o conteúdo, mais grave pode ser o problema.

Esse problema pode afetar vários tipos de produtos.

Se o recurso proibido não for obrigatório, remova-o do site.

Se possível, emita um código de status de resposta "404 - Not Found" em vez de "403 - Forbidden". Essa mudança ofuscará a presença do diretório no site e impedira que a estrutura do site fique exposta.

CWE: 200

Divulgação de caminho em vários aplicativos baseados em PHP (8/11)

URL Afetada

- http://www.bibliotecajuridica.sp.gov.br/

Como corrigir

Divulgação de caminho em vários aplicativos baseados em PHP.

Correções ou hotfixes mais recentes para produtos de terceiros não foram instalados.

É possível recuperar o caminho absoluto da instalação do servidor da Web, o que pode ajudar um invasor a desenvolver outros ataques e conseguir informações sobre a estrutura do sistema de arquivos do aplicativo da Web.

Foi descoberto que o aplicativo é vulnerável à divulgação de caminho. Ao explorar esse problema, um invasor pode obter informações confidenciais na estrutura de diretório da máquina servidor, o que permite outros ataques contra o site.

Vários aplicativos baseados em PHP são vulneráveis à divulgação de caminho, por exemplo:

Zen-Cart - um sistema de carrinho de software livre;
phpBB - um sistema de quadro de avisos de software livre;
Geeklog - um aplicativo para gerenciar conteúdo dinâmico da Web;
bitweaver - uma estrutura de aplicativo para gerenciamento de conteúdo;
phpCMS - um sistema de gerenciamento de conteúdo flexível;
Ultimate PHP Board - um script de fórum/fórum de discussão;
Limbo CMS - um sistema de gerenciamento de conteúdo;
Joomla! - um gerenciamento de conteúdo de software livre;
Noah's Classifieds - um aplicativo de gerenciamento de anúncio;
Web+Shop - um aplicativo de carrinho de e-commerce;
AdMan - um aplicativo de gerenciamento de anúncio;
Singapore - uma galeria de imagens PHP;

couponZONE - uma solução baseada em ColdFusion usada para fornecer cupons locais, nacionais e wireless;
Scry - um álbum de fotos para seu Web site;
MyBB - um sistema de quadro de avisos de software livre;
Wordpress - um sistema de publicação de blog;
CubeCart - um sistema de carrinho PHP;
phpMyAdmin - um sistema administrador para MySQL;
MKPortal - um sistema de gerenciamento de conteúdo gratis;
Saxon - Simple Accessible XHTML Online News.

Esse problema afeta diversos aplicativos.

Entre em contato com o fornecedor do aplicativo para saber se há alguma correção disponível.

Também é possível verificar um dos seguintes sites de segurança para obter quaisquer novas descobertas com relação a esse problema: centro de coordenação CERT:

http://www.cert.orgCommon Vulnerabilities and Exposures (CVE):
https://www.cve.org

CWE: 200

Link de terceiros não seguro (target="_blank") (9/11)

URL Afetada

- http://www.bibliotecajuridica.sp.gov.br/
- http://www.bibliotecajuridica.sp.gov.br/balanco-geral-do-estado/
- http://www.bibliotecajuridica.sp.gov.br/boletim-de-alerta/
- http://www.bibliotecajuridica.sp.gov.br/despachos-do-governador-e-despachos-normativos-do-governador/
- http://www.bibliotecajuridica.sp.gov.br/discursos-de-posse-dos-governadores/
- http://www.bibliotecajuridica.sp.gov.br/download/
- http://www.bibliotecajuridica.sp.gov.br/fale-conosco/
- http://www.bibliotecajuridica.sp.gov.br/legislacao-da-secretaria-de-governo/
- http://www.bibliotecajuridica.sp.gov.br/links-de-interesse/
- http://www.bibliotecajuridica.sp.gov.br/livros-eletronicos/
- http://www.bibliotecajuridica.sp.gov.br/newsletter/
- http://www.bibliotecajuridica.sp.gov.br/noticias/
- http://www.bibliotecajuridica.sp.gov.br/producao-legislativa/
- http://www.bibliotecajuridica.sp.gov.br/relacao-de-cargos-do-estado/

- http://www.bibliotecajuridica.sp.gov.br/relatorio-das-atividades-da-administracao-estadual/
- http://www.bibliotecajuridica.sp.gov.br/resolucoes-da-secretaria-de-governo-e-da-casa-civil/
- http://www.bibliotecajuridica.sp.gov.br/sobre-a-biblioteca/

Como corrigir

Link de terceiros não seguro (target="_blank").

O atributo rel no elemento de link não está configurado como "noopener noreferrer".

A página vinculada obtém acesso parcial ao objeto da janela de página de abertura.

O atributo target="_blank" é incluído em elementos de link para fazer o link se abrir em uma nova janela. As tags de link deste tipo (ex., com atributo target="_blank") expõem partes do objeto da janela da página original para a página vinculada por meio do objeto window.opener. Isso pode ser explorado para ataques de phishing se a página vinculada for maliciosa.

Atenção: se os links puderem ser incluídos por usuários e se propagarem para páginas visíveis por outros usuários, essa ameaça deverá ser tratada como ALTA severidade.

Esse problema pode afetar vários tipos de produtos.

Inclua rel="noopener noreferrer" em cada tag de link cuja origem não estiver em seu domínio.

Uma recomendação de correção mais detalhada pode ser localizada nas Referências do consultor e links relevantes

CWE: 530

A vulnerabilidade mais subestimada - explicação, exemplo e recomendação de correção

Parâmetros de Corpo Aceitos na Consulta (10/11)

URL Afetada

- http://www.bibliotecajuridica.sp.gov.br/wp-admin/admin-ajax.php

Como corrigir

Parâmetros de Corpo Aceitos na Consulta.

Programação ou configuração do aplicativo da Web não segura.

É possível reunir informações confidenciais sobre o aplicativo da Web, como nomes de usuários, senhas, nome da máquina e/ou locais de arquivo sensíveis.

É possível persuadir um usuário ingênuo a fornecer informações confidenciais como nome de usuário, senha, número de cartão de crédito, número de seguridade social, etc.

Solicitações GET são projetadas para consultar o servidor, enquanto solicitações POST são para enviar os dados.

Entretanto, além do propósito técnico, atacar os parâmetros de consulta é mais fácil do que os parâmetros do corpo, porque enviar um link para o site original ou publicá-la em um blog ou um comentário, é mais fácil e tem melhores resultados do que a alternativa - para atacar uma solicitação com parâmetros do corpo, um invasor precisa criar uma página que contém um formulário que será enviado quando visitado pela vítima.

É muito mais difícil de convencer a vítima a visitar uma página que ele não conhece do que deixá-lo visitar o site original. Por isso, não é recomendado suportar parâmetros do corpo que chegam na sequência cadeia de consultas.

Esse problema pode afetar vários tipos de produtos.

Reprograme o aplicativo para desaprovar a manipulação de parâmetros POST que estavam listados na Consulta

CWE: 200

GET

POST

Verificar suporte do SRI (Integridade de Sub-recurso) (11/11)

URL Afetada

- http://www.bibliotecajuridica.sp.gov.br/
- http://www.bibliotecajuridica.sp.gov.br/balanco-geral-do-estado/
- http://www.bibliotecajuridica.sp.gov.br/boletim-de-alerta/
- http://www.bibliotecajuridica.sp.gov.br/cosud-secretaria-da-justica-e-cidadania-discutira-gestao-de-politicas-para-jovens/
- http://www.bibliotecajuridica.sp.gov.br/despachos-do-governador-e-despachos-normativos-do-governador/
- http://www.bibliotecajuridica.sp.gov.br/dia-nacional-da-pecuaria-sp-comemora-crescimento-com-responsabilidade-sustentavel/
- http://www.bibliotecajuridica.sp.gov.br/discursos-de-posse-dos-governadores/

- http://www.bibliotecajuridica.sp.gov.br/download/
- http://www.bibliotecajuridica.sp.gov.br/fale-conosco/
- http://www.bibliotecajuridica.sp.gov.br/fundacao-florestal-captura-e-trata-lobos-guaras-ameacados-por-surto-de-sarna/
- http://www.bibliotecajuridica.sp.gov.br/governo-abre-inscricoes-para-corrida-de-conscientizacao-e-prevencao-do-cancer-de-mama/
- http://www.bibliotecajuridica.sp.gov.br/governo-de-sp-propoe-novo-fundo-para-reduzir-tarifa-com-desestatizacao-da-sabesp/
- http://www.bibliotecajuridica.sp.gov.br/legislacao-da-secretaria-de-governo/
- http://www.bibliotecajuridica.sp.gov.br/links-de-interesse/
- http://www.bibliotecajuridica.sp.gov.br/livros-eletronicos/
- http://www.bibliotecajuridica.sp.gov.br/newsletter/
- http://www.bibliotecajuridica.sp.gov.br/noticias/
- http://www.bibliotecajuridica.sp.gov.br/producao-legislativa/
- http://www.bibliotecajuridica.sp.gov.br/projeto-nascentes-incentiva-a-preservacao-da-agua-no-estado-de-sao-paulo/
- http://www.bibliotecajuridica.sp.gov.br/relacao-de-cargos-do-estado/
- http://www.bibliotecajuridica.sp.gov.br/relatorio-das-atividades-da-administracao-estadual/
- http://www.bibliotecajuridica.sp.gov.br/resolucoes-da-secretaria-de-governo-e-da-casa-civil/
- http://www.bibliotecajuridica.sp.gov.br/sobre-a-biblioteca/

Como corrigir

Verificar suporte do SRI (Integridade de Sub-recurso).

Não existe suporte para a Integridade de Sub-recurso.

O agente do usuário não pode verificar scripts de serviços de terceiro.

No caso de comprometimento do serviço de terceiro, o usuário não é protegido.

Tags de script e de link com src a partir de outro domínio não estão suportando a verificação de integridade.

Isso poderá ser explorado se o serviço que possui o script estiver comprometido.

Elemento de script de amostra não suportando SRI:
<script src="https://example.com/example-framework.js"
crossorigin="anonymous"></script>

Elemento de script de amostra suportando SRI:
<script src="https://example.com/example-framework.js"

integrity="sha384-
Li9vy3DqF8tnTXuiaAJuML3ky+er10rcgNR/VqsVpcw+ThHmYcwiB1pbOxEbzJr7"
crossorigin="anonymous"></script>

Esse problema pode afetar vários tipos de produtos.

Inclua a Integridade de Sub-recurso em cada script/link com a origem fora do seu domínio
Integridade de sub-recurso do W3C: https://www.w3.org/TR/SRI/

Gerador de hash SRI: https://srihash.org

Elemento de script de amostra não suportando SRI:
<script src="https://example.com/example-framework.js"
crossorigin="anonymous"></script>

Elemento de script de amostra suportando SRI:
<script src="https://example.com/example-framework.js"
integrity="sha384-
oqVuAfXRKap7fdgcCY5uykM6+R9GqQ8K/uxy9rx7HNQlGYl1kPzQho1wx4JwY8wC"
crossorigin="anonymous"></script>

CWE: 829
Site do fornecedor
Explanação

DESCRIÇÃO DAS VULNERABILIDADES BAIXAS

Componente Vulnerável. (1/1)

URL Afetada

- http://www.bibliotecajuridica.sp.gov.br/colorbox/jquery.colorbox.js
- http://www.bibliotecajuridica.sp.gov.br/wp-content/plugins/contact-form-7/includes/js/index.js

Componente Vulnerável.

Um componente vulnerável é usado no aplicativo testado.
Um componente vulnerável pode introduzir todos os tipos de vulnerabilidades no aplicativo.

Como corrigir.

Atualize para a versão mais recente do componente. É altamente recomendável entrar em contato com o fornecedor deste produto para verificar se um patch ou correção foi disponibilizado recentemente.

CWE: 1035

CERT coordination center
Common Vulnerabilities and Exposures (CVE)

4. CONCLUSÃO

A análise de vulnerabilidade é capaz de identificar potenciais falhas que podem vir a comprometer a segurança do ambiente causando indisponibilidade e/ou vazamento de informações.

O relatório de análise de vulnerabilidade serve como um guia de orientação para a correção e assim poder mitigar a exposição às vulnerabilidades e riscos.

As correções são recomendadas de acordo com o grau de criticidade do risco de cada uma das falhas encontradas, com o intuito de que sejam todas corrigidas.

O presente relatório identificou a quantidade de vulnerabilidades conforme abaixo no endereço **www.bibliotecajuridica.sp.gov.br**:

02 vulnerabilidades críticas - Altíssimo risco de exploração, necessitam de correção imediata, pois são vetores de ataque utilizados para desfiguração e vazamento de dados.
02 vulnerabilidades graves - Alto risco de exploração, necessitam de correção imediata, pois são vetores de ataque utilizados para desfiguração e vazamento de dados.
53 vulnerabilidades médias - Médio risco de exploração, necessitam de correção o quanto antes.
02 vulnerabilidades baixas - Baixo risco de exploração, porém é recomendada a sua correção.