RELATÓRIO DE SOLUÇÃO DAS VULNERABILIDADES

Pendências

2023

ibict
Instituto Brasileiro de Informação em Ciência e Tecnologia
UNIDADE DE PESQUISA DO MCTI

PRESIDÊNCIA DA REPÚBLICA

Luiz Inácio Lula da Silva
Presidente da República

Geraldo José Rodrigues Alckmin Filho
Vice-Presidente da República

MINISTÉRIO DA CIÊNCIA, TECNOLOGIA E INOVAÇÃO

Luciana Santos
Ministra da Ciência, Tecnologia e Inovação

INSTITUTO BRASILEIRO DE INFORMAÇÃO EM CIÊNCIA E TECNOLOGIA

Tiago Emmanuel Nunes Braga
Diretor

Carlos Andre Amaral de Freitas
Coordenador de Administração - COADM

Ricardo Medeiros Pimenta
Coordenador de Ensino e Pesquisa em Informação para a Ciência e Tecnologia - COEPI

Henrique Denes Hilgenberg Fernandes
Coordenador de Planejamento, Acompanhamento e Avaliação - COPAV

Cecília Leite Oliveira
Coordenadora Geral de Informação Tecnológica e Informação para a Sociedade - CGIT

Washington Luis Ribeiro de Carvalho Segundo
Coordenador Geral de Informação Científica e Técnica - CGIC

Alexandre Faria de Oliveira
Coordenação-Geral de Tecnologias de Informação e Informática - CGTI

Milton Shintaku
Coordenação de Tecnologias para Informação - COTEC

MINISTÉRIO DA CIÊNCIA, TECNOLOGIA E INOVAÇÃO
Instituto Brasileiro de Informação em Ciência e Tecnologia

RELATÓRIO DE SOLUÇÃO DAS VULNERABILIDADES

Pendências

Coordenação de Tecnologias para Informação (COTEC)
Brasília
2023

EQUIPE TÉCNICA

Diretor do Instituto Brasileiro de Informação em Ciência e Tecnologia
Tiago Emmanuel Nunes Braga

Coordenador-Geral de Tecnologias de Informação e Informática – CGTI
Alexandre Faria de Oliveira

Coordenador de Tecnologias para Informação - COTEC
Milton Shintaku

Autores
Deise Maria Antonio Sabbag, Fernanda Maciel Rufino, Fernando de Jesus Pereira, Jaqueline Rodrigues de Jesus, Lucas Ângelo da Silveira, Mirele Carolina Souza Ferreira Costa, Priscila Rodrigues dos Santos, Raíssa da Veiga de Menêses, Renata Monteiro Rodrigues, Rosilene Paiva Marinho de Sousa e Victor Ramos Silva

Normalização
Fernanda Maciel Rufino

Revisão
Rafael Teixeira de Souza

Flávia Furlan Granato

Diagramação e projeto gráfico
Flávio Endi Altoé Daltro

Este Relatório de Técnico é um produto do Projeto: Proposição de modelo de referência para construção de observatórios no âmbito governamental.

Ref. IBICT 01302.000166/2022-16 - Processo SEI

Ref. FUNDEP 29756

SUMÁRIO

1 INTRODUÇÃO

Este relatório técnico apresenta as soluções para correção das vulnerabilidades encontradas no teste de vulnerabilidade realizado pela Agência Nacional de Vigilância Sanitária (Anvisa) e está voltado aos profissionais de informática. Nele, são descritas as soluções das vulnerabilidades implementadas na Biblioteca Digital (BD) da Anvisa (Dspace) e no Tesauros da Anvisa (TemaTres).

O presente relatório é mais um dos resultados do projeto de pesquisa firmado entre a Anvisa e o Instituto Brasileiro de Informação em Ciência e Tecnologia (Ibict), voltado a estudos para a implementação de uma BD para a agência. O projeto, criado em 2020 por meio de um Termo de Execução Descentralizado (TED), teve duração de 18 meses, e, posteriormente, foi prorrogado por mais seis meses, com término em setembro de 2022.

Conforme os Relatórios de Análise de Vulnerabilidade (RAVs) disponibilizados pela Anvisa, foram apontados riscos de vulnerabilidade para a BD e para o Tesauros. As soluções dessas vulnerabilidades estão descritas neste relatório.

2 SOLUÇÕES DAS VULNERABILIDADES PARA A BIBLIOTECA DIGITAL (DSPACE)

Abaixo são descritas as soluções das vulnerabilidades encontradas nos RAVs realizado pela Anvisa.

2.1 Ausência de *Token Anti-Csrf*

a) risco médio;

b) solução: implementação de token em todos os formulários HTML forms get e post do software DSpace.

Exemplo do código de solução:

```
<input type=”hidden” name=”_token” value=”c2945dc5f1dd8ae0b5f9bf49daa84f29”>
```

Arquivos modificados para implementar essa solução:

```
jspui/display-item.jsp
jspui/workspace/ws-main.jsp
jspui/collection-home.jsp
jspui/dspace-admin/authorize-main.jsp
jspui/dspace-admin/eperson-confirm-delete.jsp
jspui/dspace-admin/wizard-default-item.jsp
jspui/dspace-admin/supervise-link.jsp
jspui/dspace-admin/group-confirm-delete.jsp
jspui/dspace-admin/group-group-select.jsp
jspui/dspace-admin/curate-collection.jsp
jspui/dspace-admin/confirm-delete-mdfield.jsp
jspui/dspace-admin/authorize-item-edit.jsp
jspui/dspace-admin/wizard-questions.jsp
```

jspui/dspace-admin/wizard-basicinfo.jsp
jspui/dspace-admin/news-main.jsp
jspui/dspace-admin/authorize-policy-edit.jsp
jspui/dspace-admin/wizard-permissions.jsp
jspui/dspace-admin/metadataimport-showchanges.jsp
jspui/dspace-admin/curate-main.jsp
jspui/dspace-admin/news-edit.jsp
jspui/dspace-admin/list-metadata-fields.jsp
jspui/dspace-admin/authorize-advanced.jsp
jspui/dspace-admin/batchimport.jsp
jspui/dspace-admin/workflow-list.jsp
jspui/dspace-admin/list-metadata-schemas.jsp
jspui/dspace-admin/authorize-community-edit.jsp
jspui/dspace-admin/batchmetadataimport.jsp
jspui/dspace-admin/confirm-delete-format.jsp
jspui/dspace-admin/metadataimport.jsp
jspui/dspace-admin/workflow-abort-confirm.jsp
jspui/dspace-admin/curate-item.jsp
jspui/dspace-admin/curate-community.jsp
jspui/dspace-admin/remover-destaque/index.jsp
jspui/dspace-admin/supervise-main.jsp
jspui/dspace-admin/community-select.jsp
jspui/dspace-admin/eperson-browse.jsp
jspui/dspace-admin/list-formats.jsp
jspui/dspace-admin/eperson-main.jsp
jspui/dspace-admin/supervise-confirm-remove.jsp
jspui/dspace-admin/license-edit.jsp
jspui/dspace-admin/group-eperson-select.jsp
jspui/dspace-admin/collection-select.jsp
jspui/dspace-admin/item-select.jsp
jspui/dspace-admin/supervise-list.jsp

jspui/dspace-admin/upload-logo.jsp
jspui/dspace-admin/eperson-edit.jsp
jspui/dspace-admin/authorize-collection-edit.jsp
jspui/dspace-admin/confirm-delete-mdschema.jsp
jspui/dspace-admin/fixar-destaque/index.jsp
jspui/mydspace/reject-reason.jsp
jspui/mydspace/main.jsp
jspui/mydspace/perform-task.jsp
jspui/mydspace/preview-task.jsp
jspui/mydspace/remove-item.jsp
jspui/mydspace/subscriptions.jsp
jspui/register/forgot-password.jsp
jspui/register/registration-form.jsp
jspui/register/new-password.jsp
jspui/register/new-ldap-user.jsp
jspui/register/new-user.jsp
jspui/register/edit-profile.jsp
jspui/layout/header-submission.jsp-backup
jspui/layout/navbar-default-backup.jsp
jspui/layout/header-submission.jsp
jspui/layout/header-default.jsp-backup
jspui/layout/header-default.jsp
jspui/layout/legacy/navbar-default.jsp
jspui/controlledvocabulary/search.jsp
jspui/controlledvocabulary/controlledvocabulary.jsp
jspui/suggest/suggest.jsp
jspui/suggest/suggest_ok.jsp
jspui/requestItem/request-information.jsp
jspui/requestItem/request-letter.jsp
jspui/requestItem/request-form.jsp
jspui/requestItem/request-free-access.jsp

jspui/community-list.jsp
jspui/search/discovery.jsp
jspui/components/login-form.jsp
jspui/components/ldap-form.jsp
jspui/feedback/form.jsp
jspui/tools/edit-collection.jsp
jspui/tools/itemmap-main.jsp
jspui/tools/edit-item-form.jsp
jspui/tools/curate-collection.jsp
jspui/tools/confirm-privating-item.jsp
jspui/tools/upload-bitstream.jsp
jspui/tools/confirm-withdraw-item.jsp
jspui/tools/itemmap-info.jsp
jspui/tools/lookup.jsp
jspui/tools/itemmap-browse.jsp
jspui/tools/confirm-delete-collection.jsp
jspui/tools/eperson-list.jsp
jspui/tools/confirm-delete-item.jsp
jspui/tools/group-select-list.jsp
jspui/tools/version-history.jsp
jspui/tools/move-item.jsp
jspui/tools/curate-community.jsp
jspui/tools/creative-commons-edit.jsp
jspui/tools/get-item-id.jsp
jspui/tools/version-summary.jsp
jspui/tools/edit-community.jsp
jspui/tools/confirm-delete-community.jsp
jspui/tools/group-edit.jsp
jspui/tools/group-list.jsp
jspui/tools/version-update-summary.jsp
jspui/browse/full.jsp

jspui/browse/single.jsp
jspui/community-home.jsp
jspui/submit/virus-checker-error.jsp
jspui/submit/review.jsp
jspui/submit/get-file-format.jsp
jspui/submit/edit-policy.jsp
jspui/submit/edit-bitstream-access.jsp
jspui/submit/edit-metadata.jsp
jspui/submit/choose-file.jsp
jspui/submit/show-uploaded-file.jsp
jspui/submit/select-collection.jsp
jspui/submit/verify-prune.jsp
jspui/submit/upload-file-list.jsp
jspui/submit/show-license.jsp
jspui/submit/start-lookup-submission.jsp
jspui/submit/access-step.jsp
jspui/submit/change-file-description.jsp
jspui/submit/creative-commons.jsp
jspui/submit/upload-error.jsp
jspui/submit/virus-error.jsp
jspui/submit/cancel.jsp
jspui/submit/complete.jsp
jspui/submit/initial-questions.jsp

2.2 *Content Security Policy (CSP)*

a) risco médio;

b) solução: inserção da tag <meta> no cabeçalho da aplicação e do Header CSP no servidor web.

Exemplo do código de solução:

```
# Servidor web nginx
add_header Content-Security-Policy "default-src 'none'; style-src 'self' 'unsafe-inline' 'unsafe-eval'; script-src 'self' 'unsafe-inline'; connect-src 'self'; img-src 'self' data:; font-src 'self'; frame-ancestors 'self'; form-action 'self';"
# Servidor web Apache
Header always set Content-Security-Policy "default-src 'none'; style-src 'self' 'unsafe-inline' 'unsafe-eval'; script-src 'self' 'unsafe-inline'; connect-src 'self'; img-src 'self' data:; font-src 'self'; frame-ancestors 'self'; form-action 'self';"
```

Alteração no arquivo jspui/layout/header-default.jsp para implementar essa solução:

```
<meta http-equiv="Content-Security-Policy" content="default-src \'none\'; style-src \'self\' \'unsafe-inline\' \'unsafe-eval\'; script-src \'self\' \'unsafe-inline\'; connect-src \'self\'; img-src \'self\' data:; font-src \'self\'; form-action \'self\';" />
```

Nota: Os ajustes necessários nos atributos foram realizados pela equipe de TI da Anvisa durante os testes das funcionalidades da aplicação.

2.3 *Parâmetros Anti Cross-Site*

a) risco médio;

b) solução: inserção do Header no servidor web.

Exemplo do código de solução:

```
# Servidor web nginx
add_header X-Content-Type-Options nosniff
# Servidor web Apache
Header set X-Content-Type-Options: “nosniff”
```

2.4 Biblioteca JS vulnerável

a) risco alto;

b) solução: atualização da biblioteca do Jquery.

Inicialmente atualizamos a versão 1.10.2 para 2.2.4 do Jquery que não possui riscos, conforme pode ser consultado em: https://www.cvedetails.com/vulnerability-list/vendor_id-6538/ product_id-11031/version_id-286394/Jquery-Jquery--2.2.4.html. Entretanto, essa vulnerabilidade persistiu no RAV, somente a versão 3.5.0 ou acima corrige, conforme pode ser consultado em: https://security.snyk.io/package/npm/jquery.

A atualização foi realizada pela equipe da Anvisa para versão mais atual do Jquery a 3.6.1, essa atualização ocorre em tempo de execução via *plugin*. Assim, com a atualização para versão 3.6.1 do Jquery, observou-se a necessidade de atualização do *Bootstrap* para versão compatível 3.4.1 para evitar que algumas funcionalidades do *layout* se quebrem.

2.5 *Anti-Clickjacking Header*

a) risco médio;

b) b) solução: Configurar o Servidor web para que ele envie o cabeçalho *X-Frame--Options*.

Exemplo do código de solução:

```
# Servidor web nginx
add_header X-Content-Type-Options nosniff
# Servidor web Apache
Header set X-Content-Type-Options: “nosniff”
```

3 SOLUÇÕES DAS VULNERABILIDADE PARA O TESAUROS (TEMATRES)

Abaixo, são descritas as soluções das vulnerabilidades encontradas no RAV realizado pela Anvisa.

3.1 Ausência de *token* anti-csrf

a) risco médio;

b) solução: implementação de *token* em todos os formulários HTML (*tag <forms>*) do tipo *GET* e *POST* do software TemaTres.

Exemplo do código de solução:

```
# Correção do Token Anti-CSRF
session_start();
$_SESSION['TOKEN'] = md5(uniqid(mt_rand(), true));
$rows.='<input type="hidden" name="csrf_token" value="'.$_SESSION["TOKEN"].'">';
```

Arquivos modificados para implementar essa solução:

```
tematres/common/arc2/store/ARC2_StoreEndpoint.php
tematres/common/arc2/store/ARC2_StoreEndpoint.orig.php
tematres/common/include/fun.html.php
tematres/common/include/inc.misTerminos.php
tematres/common/include/fun.admin.php
tematres/common/include/fun.admin.php
tematres/common/include/inc.abmNota.php
tematres/common/include/inc.abmConfig.php
```

tematres/common/include/adodb5/pear/auth_adodb_example.php
tematres/common/include/adodb5/adodb-perf.inc.php
tematres/common/include/inc.formUsers.php
tematres/vocab/install.php
Em 35 forms do Arquivo:
tematres/common/include/fun.html_forms.php

3.2 CSP

a) risco médio;

b) solução: inserir *tag* <meta> do cabeçalho da aplicação e do *Header* CSP no servidor web.

Exemplo do código de solução:

```
# Servidor web nginx
add_header Content-Security-Policy "default-src 'none'; style-src 'self' 'unsafe-inline'; script-src 'self' 'unsafe-inline'; connect-src 'self'; img-src 'self' data:; font-src 'self'; frame-ancestors 'self'; form-action 'self';"
# Servidor web Apache
Header always set Content-Security-Policy "default-src 'none'; style-src 'self' 'unsafe--inline'; script-src 'self' 'unsafe-inline'; connect-src 'self'; img-src 'self' data:; font-src 'self'; frame-ancestors 'self'; form-action 'self';"
```

Arquivo tematres/common/include/fun.html.php para implementar essa solução:

```
<meta http-equiv="Content-Security-Policy" content="default-src \'none\'; style-src \'self\' \'unsafe-inline\'; script-src \'self\' \'unsafe-inline\'; connect-src \'self\'; img-src \'self\' data:; font-src \'self\'; form-action \'self\';" />
```

3.3 Parâmetros *Anti Cross-Site*

a) risco médio;
b) solução: inserção do *Header* no servidor web.

Exemplo do código de solução:

```
# Servidor web nginx
add_header X-Content-Type-Options: “nosniff”
# Servidor web Apache
Header set X-Content-Type-Options: “nosniff”
```

3.4 Biblioteca JS Vulnerável

a) risco alto;
b) solução: atualização das bibliotecas:
    a) Jquery versão 3.4.1 para 3.6.1;
    b) Jquery-validation versão 1.10.0 para 1.19.5;
    c) Bootstrap versão 3.3.7 para 3.4.1.

Essas versões não possuem vulnerabilidades, conforme pode ser consultado em:
    a) https://security.snyk.io/package/npm/jquery;
    b) https://security.snyk.io/package/npm/jquery-validation;
    c) https://security.snyk.io/package/npm/bootstrap.

Arquivos modificados para atualização das bibliotecas Jquery, jquery-*validation* e *Bootstrap*:

```
tematres/common/forms/jquery.validate.min.js
tematres/common/jq/lib/jquery-3.6.0.min.js
```

```
tematres/common/bootstrap/js/bootstrap.js
tematres/common/bootstrap/js/bootstrap.min.js
tematres/common/bootstrap/css/bootstrap-theme.css
tematres/common/bootstrap/css/bootstrap-theme.css.map
tematres/common/bootstrap/css/bootstrap-theme.min.css
tematres/common/bootstrap/css/bootstrap-theme.min.css.map
tematres/common/bootstrap/css/bootstrap.css.map
tematres/common/bootstrap/css/bootstrap.min.css
tematres/common/bootstrap/css/bootstrap.min.css.map
tematres/common/include/fun.html.php
tematres/vocab/modal.php
```

3.5 *Anti-Clickjacking Header*

a) risco médio;
b) solução: configurar o Servidor web para que ele envie o cabeçalho *X-Frame-Options*.

Exemplo do código de solução:

```
# Servidor web nginx
add_header X-Frame-Options: “sameorigin”
# Servidor web Apache
Header set X-Frame-Options: “sameorigin”
```

3.6 *Cookies* inseguros

a) risco médio;
b) solução: habilitar "*session cookie*" e configurar atributo "*samesite*" no servidor web.

Exemplo do código de solução:

```
Servidor web nginx
proxy_cookie_flags one httponly;
proxy_cookie_flags ~ nosecure samesite=lax;

# Servidor web Apache
session.cookie_samesite=”Lax”
session.cookie_httponly=On
```

4 CONSIDERAÇÕES FINAIS

Este relatório teve o objetivo de apresentar as soluções implementadas para a correção das vulnerabilidades apontadas nos relatórios RAV da BD (DSpace) e do Tesauros (TemaTres). Sua principal função foi documentar as informações, além de responder às possíveis dúvidas acerca do processo.

REFERÊNCIAS

ABSENCE OF ANTI-CSRF TOKENS. **Summary**. [S. l.], © 2023. Site. Disponível em: https://www.zaproxy.org/docs/alerts/10202/. Acesso em: 14 nov. 2022.

CVE DETAILS. **Security Vulnerabilities**. [S. l.], [20--]. Site. Disponível em: https://www.cvedetails.com/vulnerability-list/ vendor_id-6538/product_id- 11031/version_id-286394/Jquery-Jquery-2.2.4.html. Acesso em: 17 nov. 2022.

MDN WEB DOCS. **Content Security Policy (CSP)**. [S. l.], © 1998-2023. Site. Disponível em: https://developer.mozilla.org/en-US/docs/Web/HTTP/CSP. Acesso em: 02 dez. 2022.

MDN WEB DOCS. **X-Frame-Options**. [S. l.], © 1998-2023. Site. Disponível em: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options. Acesso em: 13 dez. 2022.

MDN WEB DOCS. **X-Content-Type-Options**. [S. l.], © 1998-2023. Site. Disponível em: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Content-Type-Options. Acesso em: 15 dez. 2022.

SNYK VULNERABILITY DATABASE. **Bootstrap vulnerabilities**. Inglaterra, © 2023. Site. Disponível em: https://security.snyk.io/package/npm/bootstrap. Acesso em: 21 nov. 2022.

SNYK VULNERABILITY DATABASE. **Jquery vulnerabilies**. Inglaterra, © 2023. Site. Disponível em: https://security.snyk.io/package/npm/jquery. Acesso em: 21 nov. 2022.

SNYK VULNERABILITY DATABASE. **Jquery-validation vulnerabilities**. Inglaterra, © 2023. Site. Disponível em: https://security.snyk.io/package/npm/jquery-validation. Acesso em: 21 nov. 2022.

ibict
Instituto Brasileiro de Informação em Ciência e Tecnologia
UNIDADE DE PESQUISA DO MCTI

MINISTÉRIO DA
CIÊNCIA, TECNOLOGIA
E INOVAÇÃO

GOVERNO FEDERAL
BRASIL
UNIÃO E RECONSTRUÇÃO