XVI ENANCIB 2015
Informação, Memória e Patrimônio: do documento às redes
26 a 30 de outubro - João Pessoa - PB

XVI Encontro Nacional de Pesquisa em Ciência da Informação **(XVI ENANCIB)**
ISSN 2177-3688

GT 8 – Informação e Tecnologia
Pôster

ASPECTOS DE VULNERABILIDADES EM BIBLIOTECAS DIGITAIS ACESSÍVEIS[1]

ASPECT OF VULNERABILITY IN ACCESSIBLE DIGITAL LIBRARIES

Christiane Gomes dos Santos, UFPB
christiane.ginette@gmail.com

Wagner Junqueira de Araújo, UFPB
wagnerjunqueira.araujo@gmail.com

Resumo: As bibliotecas digitais acessíveis são compostas por recursos técnicos e humanos que possibilitam a organização, preservação e compartilhamento de informações para pessoas com deficiência. A pesquisa objetiva analisar o modo como se desenvolve a preservação em bibliotecas digitais voltadas para pessoas com deficiência visual que utilizam sistemas de gerenciamento de objetos digitais de código aberto, com ênfase em sua proteção. A metodologia foi estabelecida com base na utilização da ferramenta de escaneamento *Netsparker* 3.1 em bibliotecas digitais acessíveis brasileiras: Biblioteca Digital e Sonora da Universidade de Brasília (BDS/UnB), Biblioteca Digital Acessível do Ministério da Educação (BDA/MEC) e o Repositório de Informação Acessível da Universidade Federal do Rio Grande do Norte (RIA/UFRN). Considerou-se a importância de avaliações de riscos e a elaboração de estratégias para o fortalecimento dos mecanismos de defesa para eventuais ameaças a que estejam expostas as bibliotecas digitais acessíveis.

Palavras-chave: Bibliotecas digitais acessíveis. Pessoas com deficiência visual. Objeto digital acessível. Preservação digital. Vulnerabilidades.

Abstract: Accessible digital libraries consist of technical and human resources that enable the organization, preservation and sharing of information for people with disabilities. The research aims to examine how it develops the preservation of digital libraries focused on visually impaired people who use open source digital objects management systems, having emphasis on its protection. The methodology was based on the use of Netsparker 3.1 scan tool in Brazilian accessible digital library: Digital and Sound Library of the University of Brasilia (BDS/UNB), Accessible Digital Library of the Ministry of Education (BDA / MEC), and the Repository of Accessible Information of the Federal University of Rio Grande do Norte (RIA / UFRN). It considered the importance of risk assessments

[1] O conteúdo textual deste artigo, os nomes e e-mails foram extraídos dos metadados informados e são de total responsabilidade dos autores do trabalho.

and the development of strategies to strengthen of the defense mechanisms against possible threats on which accessible digital libraries are exposed.

Keywords: Accessible digital libraries. People with visual impairments. Accessible digital object. Digital preservation. Vulnerabilities.

1 INTRODUÇÃO

Com as tecnologias assistivas e tecnologias digitais, a formação de coleções constituídas por objetos digitais acessíveis direcionados a pessoas com deficiência, ganhou proporção ao se constatar o benefício diante do custo de produção e diversidade de obras que podem ser disponibilizadas e a facilidade de compartilhamento dos objetos digitais com o auxílio de sistemas de gerenciamento em ambiente *web*. No entanto, verifica-se o aumento da preocupação da proteção desses objetos quanto ao respeito à propriedade intelectual, em particular, a categoria do direito autoral, por não se tratarem de publicações de domínio público.

Dessa forma, a pesquisa se propõe a analisar a preservação em bibliotecas digitais acessíveis voltadas para usuários com deficiência visual que utilizam sistemas de gerenciamento de objetos digitais de código aberto, de forma a identificar os possíveis tipos de vulnerabilidades a que estão sujeitas estas bibliotecas, bem como apontar estratégias que possam contribuir com mecanismos que objetivam evitar ou reduzir alguns dos tipos de vulnerabilidades encontrados nos sistemas de bibliotecas digitais acessíveis.

2 ACESSO À INFORMAÇÃO E BIBLIOTECAS DIGITAIS ACESSÍVEIS: PRESERVAÇÃO E ASPECTOS DE VULNERABILIDADES

Com a tecnologia digital e o avanço da tecnologia assistiva vêm permitindo o desenvolvimento de serviços, recursos e mecanismos que estão inovando o processo de acesso à informação, apresentando alternativas de produção de material informacional acessível, assim como em sua preservação e compartilhamento (GOLUB, 2002; YATACO MARÍN, 2009). Tendo em vista que bibliotecas digitais beneficiam quanto ao acesso direto à informação, com sistemas de buscas em bases de dados, pesquisas integradas e colaboração entre usuários e organizações (TAMMARO, 2008), tem-se na construção de bibliotecas digitais uma alternativa que pode vir a suprir as necessidades de informação de pessoas com deficiência.

Em bibliotecas digitais, referente aos objetos digitais que seguem padrões de acessibilidade, a preocupação do processo de preservação perpassa tanto pelas adaptações de acessibilidade que não acompanham a totalidade dos princípios da preservação digital, como custódia de confiança, autenticidade, cópias autênticas, preservação de componentes digitais,

entre outros, devido ao processo de digitalização ser centrado nos sistemas de síntese de voz (CARVALHO, 2009; BRASIL, 2012), quanto pelos aspectos de vulnerabilidades em aplicações da *web*, que correspondem às fraquezas que possam ser exploradas com o objetivo de comprometer a segurança de sistemas ou informações, o que está relacionado com uma ou mais ameaças (BEZERRA, 2013).

Compreendendo-se que as obras adaptadas para se tornarem objetos digitais acessíveis são oriundas de áreas do conhecimento em que parte considerável dessas obras não se encontra em domínio público, torna-se necessário aos serviços de bibliotecas digitais acessíveis o investimento no controle de acesso e compartilhamento indevido, bem como o cuidado e controle quanto aos possíveis riscos que podem comprometer os serviços dessas bibliotecas.

3 METODOLOGIA

A pesquisa se caracteriza como quantitativa, com base nos níveis exploratório e descritivo, de modo a identificar os riscos existentes em bibliotecas digitais acessíveis, a partir da análise de aspectos de vulnerabilidades nas bibliotecas digitais acessíveis que utilizam sistemas de implantação de repositórios digitais (modelo *Open Archives*) com o emprego da ferramenta de escaneamento *Netsparker*, edição 3.1, para o rastreamento, ataque e identificação de vulnerabilidades.

Foram analisadas as bibliotecas digitais acessíveis em âmbito brasileiro, que utilizam como sistema de implantação o *software DSpace*: Biblioteca Digital e Sonora da Universidade de Brasília (BDS/UnB), Biblioteca Digital Acessível do Ministério da Educação (BDA/MEC) e o Repositório de Informação Acessível da Universidade Federal do Rio Grande do Norte (RIA/UFRN), no período de 09 a 28/01/2015. Foram desenvolvidos três relatórios referentes a três aplicações de testes em cada biblioteca digital acessível, obtendo-se dados em períodos distintos, de forma a estabelecer um comparativo dos riscos encontrados entre as amostras dos processos de testes. Foram realizados escaneamentos do tipo completo nas bibliotecas digitais analisadas (Tabela 1).

Tabela 1. Histórico das aplicações de testes das bibliotecas digitais acessíveis

INSTITUIÇÕES	BIBLIOTECAS DIGITAIS	DATA DE CONSULTA	TEMPO DE ESCANEAMENTO
1ª APLICAÇÃO DE TESTES			
UnB	http://bds.bce.unb.br/	09/01/2015	5h33min
MEC	http://ada.mec.gov.br/	12/01/2015	1h16min
UFRN	http://www.ria.ufrn.br	14/01/2015	7h57min
2ª APLICAÇÃO DE TESTES			
UnB	http://bds.bce.unb.br/	16/01/2015	5h51min

MEC	http://ada.mec.gov.br/	19/01/2015	1h14min
UFRN	http://www.ria.ufrn.br	21/01/2015	9h11min
3ª APLICAÇÃO DE TESTES			
UnB	http://bds.bce.unb.br/	23/01/2015	5h58min
MEC	http://ada.mec.gov.br/	26/01/2015	1h23min
UFRN	http://www.ria.ufrn.br	28/01/2015	8h51min

Fonte: Dados da pesquisa (2015).

A análise estatística dos dados de risco obtidos foi realizada pelo método de variância ANOVA seguida do pós-teste de Bonferroni, utilizando-se o programa GraphPad Prisma® 5 (GraphPad *software* In., San Diego, EUA). Sendo que os dados foram considerados significativos com $p<0{,}001$.

4 RESULTADOS: APRESENTAÇÃO E DISCUSSÃO

Os tipos de vulnerabilidades de risco estão classificados nos seguintes níveis: crítico, alto, médio, baixo e alerta. Na Tabela 2, observar-se os tipos de vulnerabilidades encontradas em cada processo, permitindo a obtenção de uma média dos riscos existentes nas bibliotecas digitais acessíveis analisadas.

Tabela 2. Tipos de vulnerabilidades encontradas nas aplicações de testes

Nível	Tipo de vulnerabilidade	1ª Aplicação			2ª Aplicação			3ª Aplicação		
		BDS	BDA	RIA	BDS	BDA	RIA	BDS	BDA	RIA
Alto	Password Transmitted over HTTP	1	1	1	1	1	1	1	1	1
Médio	Insecure Transportation Security Protocol Supported (SSLv2)	1	-	1	1	-	1	1	-	1
Baixo	Internal Server Error	1	1	1	1	1	1	1	1	1
	Cookie Not Marked as HttpOnly	1	1	1	1	1	1	1	1	1
	Auto Complete Enabled	1	1	1	1	1	1	1	1	1
	Version Disclosure (Apache Coyote)	1	1	1	1	1	1	1	1	1
	Version Disclosure (Tomcat)	1	1	1	1	1	1	1	1	1
	Exception Report Disclosure (Tomcat)	1	1	1	1	1	1	1	1	1

Fonte: Dados da pesquisa (2015).

Quanto ao tipo de vulnerabilidade, verificaram-se nas três aplicações o nível de risco alto do tipo *Password Transmitted over* HTTP, em todas as bibliotecas. Esse tipo de risco mostra que as senhas são transmitidas na rede por meio do protocolo de aplicação HTTP, o qual não possui nativamente nenhum mecanismo de proteção de dados, aumentando a

possibilidade de captura de senhas de usuários. O transporte de informações sigilosas pela internet deveria fazer uso do protocolo HTTPS que foi especificamente desenvolvido para esse fim.

Concernente ao nível médio, constatou-se apenas um risco do tipo *Insecure Transportation Security Protocol Supported* (SSLv2), que nas três aplicações foi detectado nas bibliotecas BDS/UnB e RIA/UFRN. O protocolo de aplicação HTTPS para prover segurança precisa de um protocolo de criptografia para proteger a comunicação dos dados, sendo um deles, o SSLv, versão que apresenta falhas de segurança, logo de uso não recomendado. Nesse caso, pessoas conectadas via protocolo de aplicação HTTPS fazendo uso do protocolo de criptografia SSLv2 possuem uma falsa sensação de segurança (NETSPARKER LTD., 2013).

Para o de baixo nível, foram observados durante os três procedimentos, seis tipos de vulnerabilidades. Em todas as aplicações, o risco *Internal Server Error* foi detectado em todas as bibliotecas digitais, evidenciando que o servidor replicou com um status HTTP 500. Esse status indica que ocorreu um erro no servidor, porém essa informação não deveria ser visualizada pelo usuário do sistema, pois mostra falhas e detalhes do servidor de aplicação, o que pode ser uma informação útil para uso em ataques maliciosos. O segundo risco detectado, refere-se ao *Cookie Not Marked as HttpOnly*, presente em todas as bibliotecas digitais ao longo das aplicações dos testes. Esse risco consiste no relato de que um *cookie* não foi marcado como HTTPOnly (NETSPARKER LTD., 2013). Um *cookie* é utilizado pelo navegador para guardar informações de sessão (histórico, preferências, entre outros) quando um usuário encontra-se em um *site*. Estes possuem atributos para aumentar sua segurança, tais como, o HTTPOnly que deve estar sempre ativo para prevenir roubo de sessão, principalmente de usuários autenticados, pois nesse caso quem obtiver o *cookie* de um usuário autenticado em um *site* poderá manter-se na sessão desse usuário, logo com acesso a todas as informações.

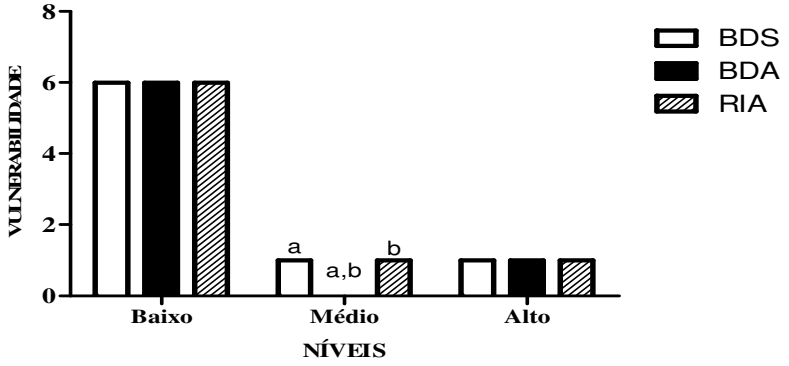
O terceiro tipo de vulnerabilidade observado, *Auto Complete Enabled*, encontrados em todas as bibliotecas, mostra que houve a ativação da função *Auto Complete* em um ou mais campos de formulário sensíveis, como senhas. Dessa forma, compreende-se que os dados inseridos nesses campos serão armazenados em *cache* pelo navegador do usuário, podendo essas informações serem facilmente roubadas caso o invasor tenha acesso ao navegador da pessoa que acessou o *site* salvando sua senha no navegador por meio do recurso *autocomplete* do navegador. *Version Disclosure* (Apache Coyote), trata-se do quarto tipo de vulnerabilidade encontrada nas três aplicações em todas as bibliotecas. Essa vulnerabilidade determina que o

servidor *web* de destino, divulga a versão *Coyote* Apache em sua resposta HTTP. Dessa maneira, as informações divulgadas podem ser utilizadas por um possível atacante para obter as vulnerabilidades de segurança específicas para a versão identificada (NETSPARKER LTD., 2013).

O quinto tipo de vulnerabilidade, *Version Disclosure* (Tomcat), identificado em todas as bibliotecas, indica que o servidor *web* divulga a versão *Tomcat* em sua resposta HTTP, o que implica em afirmar que essas informações, assim como ocorre no Version Disclosure, podem auxiliar a ação de um usuário mal intencionado. O sexto tipo de vulnerabilidade encontrado em todas as bibliotecas, compreende o *Exception Report Disclosure* (Tomcat), que determina que o servidor *web* em questão, divulga dados do relatório de exceção na resposta HTTP, considerando-se que um possível usuário mal intencionado pode obter informações como caminho de arquivo físico do *Tomcat* (NETSPARKER LTD., 2013). Essas três últimas vulnerabilidades encontram-se no fato de que a probabilidade de um ataque ser bem sucedido é diretamente proporcional à quantidade de informações que o atacante consegue descobrir sobre o alvo. Logo, quanto mais o servidor puder esconder os detalhes das aplicações, menor as vulnerabilidades existentes e menor o risco de ataques bem sucedidos.

Comparando-se os dados obtidos pela análise de variância ANOVA, pode-se observar na Figura 1, que todas as bibliotecas digitais acessíveis apresentaram risco de nível baixo e alto, não apresentando diferença significativa. Quanto ao nível médio, observou-se que a biblioteca digital BDA/MEC encontra-se mais protegida quanto aos riscos, apresentando diferença significativa ($p < 0{,}001$) em relação às Bibliotecas BDS/UNB e RIA/UFRN.

Figura 1. Comparação das vulnerabilidades das bibliotecas digitais acessíveis e repositório de acordo com os níveis de risco. Os dados foram considerados significativos quando $p < 0{,}001$ (a,b).



Fonte: Dados de pesquisa (2015).

5 CONSIDERAÇÕES FINAIS

Com os resultados obtidos, observaram-se algumas das ameaças a que estão suscetíveis

os objetos contidos nas bibliotecas digitais acessíveis analisadas, com base na quantificação e denominação dos riscos constatados, bem como possibilitando distinguir os componentes causadores das falhas existentes, e a sinalização da adoção de procedimentos e técnicas que sejam adequados no auxílio do processo de preservação dos objetos digitais acessíveis.

De acordo com o Netsparker Ltd. (2013), as vulnerabilidades detectadas podem ser revertidas, seguindo-se a indicação de procedimentos e medidas de segurança. Para os principais riscos observados na pesquisa, verifica-se a necessidade dos dados serem transferidos de modo seguro, como a utilização do protocolo HTTPS, para transferência em conexão criptografada, e a revisão de códigos de aplicação para lidar com os erros inesperados.

Com esta pesquisa, pode-se evidenciar a importância do desenvolvimento de avaliações de risco, por possibilitar conhecimento das prioridades exigidas pelos recursos digitais contidos nas bibliotecas digitais, respeitando as normas em vigor e profissionais qualificados, de modo a permitir que se possam efetivar estratégias de prevenção para contribuir com o fortalecimento dos mecanismos de defesa, bem como outras possíveis ameaças a que essas bibliotecas estão expostas.

REFERÊNCIAS

BEZERRA, E. K. **Gestão de riscos de TI**: NBR 27005. Rio de Janeiro: Escola Superior de Redes, 2013.

BRASIL. **AN digital**: política de preservação digital. Brasília: Arquivo Nacional, 2012.

CARVALHO, M. M. G. R. **O repositórioaberto**: recuperar, preservar e difundir o conhecimento "em qualquer lugar do mundo". 2009. 278 f. (Mestrado em Ciências Documentais) – Universidade Autónoma de Lisboa, Lisboa, 2009.

GOLUB, K. Digital libraries and the blind and visually impaired. In: CARNET USERS CONFERENCE, 4., 2002, Zagreb. **Anais**... Zagreb, 2002.

NETSPARKER LTD. **Netsparker**: web application security scanner. Uxbridge: Finance House, 2013.

TAMMARO, A. M. O documento digital. In: TAMMARO, A. M; SALARELLI, A. **A biblioteca digital**. Brasília: Briquet de Lemos, 2008.

YATACO MARÍN, R. M. **Servicios bibliotecarios para personas con discapacidad visual**: el caso de la Sala para Invidentes "Delfina Otero Villarán" de la Gran Biblioteca Pública de Lima. 2009. 94 f. Informe professional para optar el Título de Licenciado en Bibliotecología y Ciencias de la Información – Universidad Nacional Mayor de San Marcos, Lima, 2009.