Batista, R. R.; Santos, C. G.; Araújo, S. G. L.; Araújo, W. J.
Revista Gestão.Org, v. 14, Edição Especial, 2016. p. 247-254
ISSN 1679-1827
http://www.revista.ufpe.br/gestaoorg

Teste de invasão no SIGAA da UFPB

Penetration test in the academic system SIGAA of UFPB

Rafaela Romaniuc Batista[1], Christiane Gomes dos Santos[1], Sueny Gomes Léda Araújo[1], Wagner Junqueira de Araújo[1]

[1]Universidade Federal da Paraíba,UFPB, Brasil.

Correspondência: Rafaela Romaniuc Batista, Endereço: Cidade Universitária, s/n, Castelo Branco, João Pessoa, PB. CEP.: 58051-900. Tel.: 3216-7696. E-mail: rafaela.romaniuc@gmail.com

Recebido: 08 de outubro de 2016 Aceito: 20 de dezembro de 2016 Publicado: 01 de maio de 2017

DOI: 10.21714/1679-18272016v14Esp2.p247-254

Resumo

O avanço tecnológico nas instituições públicas demanda uma preocupação maior com a segurança da informação, pois as informações passaram a ser mantidas, em sua grande maioria, dentro dos recursos tecnológicos institucionais. Nesse sentido, os sistemas de informação tornam-se alvos de ataques no mundo cibernético e, por isso, demandam um desenvolvimento que possibilite blindagem frente a essas ameaças. Com os sistemas acadêmicos não poderia ser diferente, afinal a maioria das informações das universidades encontram-se dentro desses sistemas. Por isso, a segurança da informação deve se fazer presente nessas instituições, orientando pessoas, processos e tecnologias a se protegerem das mais diversas ameaças. A presente pesquisa permitiu analisar as vulnerabilidades tecnológicas inerentes ao Sistema Integrado de Gestão de Atividades Acadêmicas - SIGAA, módulo *Stricto Sensu*, da Universidade Federal da Paraíba – UFPB, por meio de teste de invasão realizado pela ferramenta NetSparker. Esta pesquisa se caracterizou como uma pesquisa descritiva, com abordagem quantitativa, tendo como método o estudo de caso. Dentre os 66 tipos de vulnerabilidades analisadas, foram identificadas uma vulnerabilidade de nível importante, sete de nível baixo e três do tipo informação, o que mostra a necessidade de melhorias com foco na segurança da informação.

Palavras-chave: Sistemas de informação, Segurança da informação, Teste de invasão, Scanner de vulnerabilidades.

Abstract

Technological advance in public institutions demand a greater concern for the security of information, as the information began to be kept, for the most part, within the institutional technological resources. In this sense, information systems became the target of attacks in the cyber world and, therefore, require a development that enables shielding against these threats. With the academic systems could not be different, after all most of the universities information are within these systems. Therefore, information security should be present in these institutions, guiding people, processes and technologies to protect themselves from various threats. This research allowed us to analyze the technological vulnerabilities inherent in the Integrated Management System of Academic Activities - SIGAA, *Stricto Sensu* module, of the Federal University of Paraíba - UFPB through penetration testing conducted by NetSparker tool. This research is characterized as a descriptive research with a quantitative approach, using the case study method. Among the 66 types of vulnerabilities analyzed we have identified a vulnerability of important level, seven of low-level and three of the information type, which shows the need for improvements with a focus on information security.

Keywords: Information systems, Information security, Penetration test, Vulnerability scanner.

1. Introdução

As fronteiras do espaço cibernético, também denominado rede ou internet, não estão claramente definidas. Basicamente tudo que está ligado em rede encontra-se nesse espaço e, consequentemente, suscetível a ataques. Com o avanço das redes de computadores, a informação tratada pelos sistemas de informação tornou-se mais exposta a ataques, evidenciando que não basta implantar a tecnologia, faz-se necessário proteger esses ativos.

A segurança da informação torna-se essencial na atualidade, por se tratar de um ponto crítico para a sobrevivência das organizações na atual era da informação. Para os órgãos do Governo Federal Brasileiro, a

segurança da informação abrange a proteção dos sistemas de informação contra intrusão e acesso não autorizado a dados ou informações, o que envolve inclusive a segurança dos recursos humanos, de materiais, áreas e instalações das comunicações e computacional. (BRASIL, 2000[1]). Logo, a segurança da informação envolve a proteção dos sistemas de informação, independente do formato da informação, seja físico ou lógico, a segurança da informação deve protegê-los de ameaças, de modo a diminuir os riscos e garantir a continuidade do negócio.

Porém, a segurança da informação não se preocupa apenas com a guarda do sigilo de informações, é muito mais abrangente, pois aborda desde temas como a disponibilidade da informação, responsabilização, punição, etc. A segurança da informação é essencial não apenas para assegurar a continuidade do negócio, mas também para o atendimento aos requisitos legais e manter a imagem da organização intacta. A preocupação com segurança deve ser um ato contínuo e cíclico dentro de uma organização, pois cabe a todos a proteção da informação, independente de cargo ou função.

Os ataques aos recursos informacionais são comuns, podendo se dar por vários motivos, segundo o Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil (CERT.br, 2012, p. 17), desde demonstração de poder, competitividade, simples curiosidade até motivações financeiras, ideológicas ou comerciais. Por isso, a equipe de segurança precisa estar sempre atenta quanto às novidades de ataques cibernéticos, escolhendo a abordagem mais adequada para ações preventivas e reativas, de outro modo a organização permanecerá suscetível a ataques, pois basta existir na internet para que exista a vulnerabilidade.

Os alvos de ataques consistem basicamente em tudo o que pode estar interconectado nas redes de computadores. O relatório da *Symantec*[2] (2014) apresentou que em 2013 foram "*hackeados*" monitores de bebês, câmeras de segurança, *smart tv*, automóveis e equipamentos médicos, o que deixa claro que o risco é real e deve ser tratado (SYMANTEC CORPORATION, 2014, p. 7, tradução nossa).

Observa-se que ameaças à segurança da informação ocorrem nas mais diversas formas e nos mais variados contextos, porém todas elas ocorrem dentro do ciclo de vida da informação, tendo relação direta com os ativos informacionais. Turban, Rainer e Potter (2007, p. 60) categorizaram as ameaças, no contexto dos sistemas de informação, em involuntárias, onde não há motivação, e intencionais, que são normalmente de natureza criminosa.

Considerando que vulnerabilidade é a fraqueza em sistemas de informação, procedimentos de segurança do sistema, controles internos, ou aplicação que pode ser explorada tendo como origem uma ameaça (NATIONAL INTITUTE OF STANDARDS AND TECHNOLOGY, 2011, p. B11, tradução nossa), e que ameaças visam explorar alguma vulnerabilidade existente causando, direta ou indiretamente, impacto no negócio, observa-se que a equipe de segurança deve ficar atenta a esses aspectos. Harkins (2013, p. 15, tradução nossa) afirma que a maior vulnerabilidade encontrada nas organizações atualmente é a percepção equivocada de risco, pois as ações dela consequente se baseiam nessa percepção. Pode acontecer de funcionários postarem nas redes sociais informações relacionadas ao trabalho por achá-las inofensivas, enquanto hackers podem utilizar essa informação em "*phishing emails*", emails enviados por pessoas que se passam por pessoas conhecidas para conseguir informações, no intuito de obter acesso aos sistemas organizacionais.

Assim, no intuito de enfrentar as ameaças e demandas organizacionais deve-se, de maneira proativa, antecipar as vulnerabilidades por meio do processo formal de gerenciamento de riscos de segurança da informação, permitindo estabelecer um nível aceitável[3] de risco (BEZERRA, 2013, p. 11). O presente artigo apresenta o resultado de pesquisa que analisou as vulnerabilidades tecnológicas inerentes ao sistema acadêmico SIGAA, módulo Stricto Sensu, da Universidade Federal da Paraíba.

2. Fundamentação Teórica

2.1. Sistemas de informação

Um sistema de informação é uma importante ferramenta que auxilia na gerência da informação. Swanson, Hash e Bowen (2006, p. 34, tradução nossa) definem sistema de informação como um conjunto distinto de recursos de informação organizado para o armazenamento, processamento, manutenção, uso, compartilhamento, disseminação, ou disposição de informações. Isto é, engloba os recursos relacionados à informação em seu ciclo de vida. Os sistemas de informação ajudam as empresas a serem mais produtivas, eficientes e ágeis, além de auxiliá-las nos ambientes de negócio, seja estreitando relacionamento com fornecedores e clientes, seja auxiliando na inovação de produtos ou serviços.

[1] Documento eletrônico não paginado.
[2] Empresa americana, com sede em Mountain View - Califórnia, especialista em segurança da internet para usuários domésticos e empresas, fornece software antivírus, de analise de vulnerabilidades, proteção de email, detecção de intrusos e filtragem de conteúdo.
[3] Risco aceitável "é o grau de risco que a organização está disposta a aceitar para a concretização dos seus objetivos estratégicos." (BEZERRA, 2013, p. 12).

Os papéis fundamentais dos sistemas nos negócios incluem oferecer suporte aos processos e operações de negócios, apoiar a tomada de decisão e auxiliar nas estratégias para vantagem competitiva. Mas nem sempre foi assim, no início os sistemas foram concebidos apenas com o intuito de processar dados, depois foi ampliado para também auxiliar na emissão de relatórios gerenciais e continuam em constante evolução como ferramenta estratégica para apoiar as pessoas em seus negócios (O'BRIEN, 2012, p.7- 8). Com a evolução tecnológica, os sistemas de informação tornaram-se cada vez mais complexos, pois a tendência é que abranjam o negócio como um todo, não apenas alguns de seus fragmentos. Dentre os vários tipos de sistemas de informação, existem os Sistemas de Informação Gerenciais que são sistemas computacionais que possibilitam tratar informação como matéria-prima para tomada de decisão dentro da organização. Ademais, todo sistema possui três tipos de componentes: dados, sistema de processamento de dados e canais de comunicação. (CHIAVENATO. 2002, p. 262). Assim, na atual era da informação, os sistemas tornam-se uma importante ferramenta de gerenciamento da informação para organização e ao adotar esses sistemas as organizações, públicas ou privadas, buscam a melhoria na prestação de serviços por meio da TI.

No intuito de automatizar as atividades meio e fim, a Universidade Federal da Paraíba - UFPB adquiriu o Sistema Integrados de Gestão – SIG, desenvolvido pela Universidade Federal do Rio Grande do Norte - UFRN, e trabalha atualmente na implantação dos módulos de acordo com sua realidade organizacional, visando possibilitar a interação entre a área administrativa e acadêmica. Esse sistema visa propiciar a integração das informações organizacionais de modo a auxiliar universidades públicas em seu negócio. Um dos maiores benefícios dos SIG UFRN é a integração entre os sistemas, pois engloba os sistemas desde a área administrativa, atividade meio, até a área acadêmica, atividade fim das universidades.

O Sistema Integrado de Gestão de Atividades Acadêmicas - SIGAA compreende um dos sistemas existentes e integrados no SIG e visa informatizar especificamente os procedimentos da área acadêmica por meio dos módulos de: graduação, pós-graduação (*stricto* e *lato sensu*), ensino técnico, ensino médio e infantil, o que abrange as atividades de ensino, pesquisa e extensão.

Esta pesquisa analisou especificamente as vulnerabilidades do módulo *Stricto Sensu* desse sistema. Esse módulo congrega operações relativas à gerência de mestrado e de doutorado, tendo sido implantado de modo a auxiliar a Pró-Reitoria de Pós-Graduação da UFPB. As principais funções deste módulo são controlar o processo seletivo, a estrutura curricular, matrículas e emissão de diplomas. Esse módulo envolve os perfis: Administrador da Pró-Reitoria de Pós-Graduação, responsável por habilitar o acesso aos usuários às operações restritas; Gestor de *Stricto*, responsável pelo gerenciamento de todos os Programas *Stricto* da instituição; e Coordenador *Stricto Sensu*, responsável pela coordenação das atividades de curso, cadastro de processos seletivos, turmas entre outras funções. O módulo *Stricto Sensu* é composto de 129 operações que auxiliam os perfis em suas funcionalidades e, além disso, também se relaciona com os módulos: Portal do Coordenador *Stricto Sensu*, Portal Discente e Portal Docente (WIKIUFRN[30], 2014).

Uma análise mais aprofundada de suas vulnerabilidades pode ser feita de forma manual ou automatizada por meio de ferramentas de teste de invasão, as quais encontram-se facilmente disponibilizadas na web.

2.1.1 Teste de invasão em sistemas web

Vulnerabilidade é a fraqueza em sistemas de informação, procedimentos de segurança do sistema, controles internos, ou aplicação que pode ser explorada tendo como origem uma ameaça (NATIONAL INTITUTE OF STANDARDS AND TECHNOLOGY, 2011, p. B11, tradução nossa). Não obstante, as ameaças visam explorar alguma vulnerabilidade existentes causando, direta ou indiretamente, impacto no negócio. Para isso, considera-se que as vulnerabilidades permeiam as seguintes áreas de segurança: hardware, software, rede, recursos humanos, local ou instalações, e organização. Para cada uma dessas áreas é possível identificar ameaças e possíveis vulnerabilidades.

Quanto à área de software, testes de invasão permitem encontrar vulnerabilidades existentes em sistemas, pois objetiva violar os requisitos explícitos e implícitos de segurança de uma aplicação web (UTO, 2013, p. 2). Desse modo, a presente pesquisa buscou identificar as vulnerabilidades específicas de software. Para isso, fez-se uso do *scanner* de vulnerabilidades *NetSparker*[4], versão 3.1.6.0 da edição comunitária, que consiste em um *scanner* de segurança em aplicações web, que pode rastrear, atacar e identificar vulnerabilidades em variadas plataformas de aplicações web. Essa ferramenta permitiu varrer o sistema procurando as vulnerabilidades de segurança da Web. Ademais, o *scanner* é considerado livre de falsos positivos, isto é, o resultado da análise irá identificar vulnerabilidades realmente existentes no sistema pesquisado. A varredura é feita no sistema buscando 66 tipos de vulnerabilidades tecnológicas.

[4] *NetSparker* é um *scanner* de vulnerabilidades em aplicações web. Mais detalhes em: https://www.netsparker.com/web-vulnerability-scanner/

A quantidade e os tipos de vulnerabilidades identificados são divididos em cinco níveis de criticidade: crítico, alto, médio, baixo e alerta. O *scanner* analisou quantitativamente as vulnerabilidades do sistema SIGAA-*StrictoSensu* e, caso a ferramenta não conseguisse identificar claramente a vulnerabilidade, ela utilizou a palavra chave "*Possible*" para deixar claro que há a possibilidade de vulnerabilidade, mas não a certeza. Essa ferramenta identifica as vulnerabilidades existentes em aplicações *web* por meio de *Penetration Test* (Teste de Invasão). Dessa forma, o *scanner* de vulnerabilidades pôde contribuir para rastrear as ameaças e vulnerabilidades tecnológicas do sistema SIGAA-*StrictoSensu*.

As possibilidades de ataques são inúmeras e, quanto mais informações disponíveis, maior a possibilidade de se concretizarem, logo se considera boa prática não estarem facilmente disponíveis informações tecnológicas, como versão de servidor e outras tecnologias associadas. Esse tipo de informação é muito útil para o atacante, pois cada tecnologia tem suas vulnerabilidades descobertas e muitas são encontradas em uma versão específica da tecnologia. Dessa maneira, depreende-se como boa prática evitar disponibilizar informações tecnológicas e, ao mesmo tempo, manter as tecnologias atualizadas.

Muitas vulnerabilidades fazem uso de informações mantidas no computador por meio de *cookies*, considerando-se que essa tecnologia faz parte do protocolo de comunicação HTTP e possuem justamente o objetivo de lembrar informações do usuário, onde, uma vez enviado do servidor ao navegador, tende a ser utilizado pelo navegador nas requisições subsequentes. Logo, *cookies* permitem manter a sessão e a autenticação do usuário, porém *cookies* marcados como "HTTP *Only*" não podem ser acessados por código executado no lado cliente. Dessa forma, considera-se uma boa prática marcar os *cookies* como HTTP *Only* durante a codificação, pois cria uma camada extra de proteção contra ataques do tipo *cross-site scripting e* dificulta o acesso a *cookies* e, consequente, sequestro de sessão (UTO, 2013, p. 16-20). Deve-se ter em mente que medidas como essa são iniciais preventivas, pois visam dificultar um possível ataque, apesar disso, existem ferramentas que podem burlar essa proteção. No mundo real equivale a colocar um cadeado no portão, e mesmo assim havendo a possibilidade de pular o muro.

Outra vulnerabilidade encontra-se em o sistema permitir o uso de recursos do tipo auto completar, principalmente em campos de autenticação ou de cartão de crédito, pois fazem uso de dados sensíveis que serão salvos pelo navegador podendo essa informação ser roubada, especialmente quando é comum o uso do sistema em computadores compartilhados.

Deve-se ter em mente que não se deve confiar completamente em dados que vem do lado usuário, seja pelo uso de computador compartilhado seja pela possibilidade de infecção desses computadores. Dentre os diversos tipos de ataques possíveis, existe o Cross Site Request Forgery que explora a confiança que o site tem no navegador do usuário, pois o ataque só é possível devido a diversos aspectos dos mecanismos de gerenciamento de sessões implementados em aplicações web combinados com ataques de engenharia social, de maneira que a aplicação não saiba qual requisição é verdadeiramente do usuário e qual é do atacante. Para prevenir esse tipo de ataque há necessidade de gerenciamento de sessões mais robusto que faça uso, "em cada página da aplicação, de um elemento com valor gerado em função da URL, do identificador de sessão, do nome da conta do usuário e de um segredo conhecido apenas pelo sistema" (p. 156). Esse segredo é chamado de *token Anti*-CSRF, o qual não pode ser facilmente previsível e deve ser validado toda vez que uma requisição é recebida pela aplicação (UTO, 2013, p. 153-156).

Ademais, considerando que o protocolo HTTP não possui nativamente nenhum mecanismo de proteção aos dados que carrega, simples medidas como fazer uso de HTTPS melhoram significativamente a segurança de páginas web. O protocolo HTTPS consiste na combinação do HTTP com protocolos SSL ou TLS, o que possibilita o transporte sigiloso de dados (UTO, 2013, p. 16-18). Para isso, a tecnologia HTTP *Strict Transport Security* (HSTS) consiste em uma melhoria de segurança em aplicações web por meio de um cabeçalho de resposta HTTP especial prevenindo comunicações de serem feitas via protocolo HTTP, ou seja força que as comunicações sejam feitas utilizando HTTPS. Dessa maneira, o HSTS é uma tecnologia que provê melhoria de segurança, pois combina com o navegador de só fazer uso de conexão segura, oferecendo proteção contínua ao transporte de dados na web.

Dessa maneira, as vulnerabilidades podem ser inúmeras a depender da tecnologia utilizada e da facilidade de obtenção de informação, nesse caso o mapeamento das vulnerabilidades são passos inicias para um desenvolvimento seguro.

3. Metodologia

A pesquisa teve por base uma abordagem quantitativa e descritiva. A abordagem quantitativa abrangeu a análise numérica dos dados coletados, por meio de procedimentos estatísticos, representados graficamente em tabelas e ilustrações. Foram analisados a quantidade e os tipos de vulnerabilidades *web* encontrados pelo *scanner* de vulnerabilidades *NetSparker*, por meio de testes de invasão realizados em três locais diferentes: fora do estado da Paraíba (Natal-RN), no mesmo município (João Pessoa-PB) e dentro da universidade proprietária do sistema

SIGAA-*StrictoSensu* (UFPB). Desse modo, pretendeu-se obter maior confiabilidade para os dados obtidos, assim como analisar eventuais divergências de acesso ao sistema, considerando o acesso remoto por localidade.

4. Resultados Obtidos

Os testes ocorreram no período de 18/09/2015 a 24/09/2015, conforme apresentado no Quadro 1.

TESTES	DATA DE CONSULTA	LOCAL	TEMPO DE ESCANEAMENTO
Teste 1	18/09/2015	João Pessoa-PB	2h06min
Teste 2	24/09/2015	UFPB	0h22min
Teste 3	22/09/2015	Natal-RN	1h00min

Quadro 1: Detalhes dos testes no SIGAA-*StrictoSensu*.

Fonte: Dados da pesquisa (2015).

Com base no Quadro , percebe-se que o segundo teste, efetuado no ambiente da UFPB, durou muito menos que os demais, e, será verificado mais adiante, que a quantidade de vulnerabilidades encontradas foi menor em relação aos outros testes realizados fora das instâncias da universidade. Acredita-se que essa condição tenha ocorrido em consequência de a ferramenta ter encontrado alguma barreira de roteamento ou firewall maior dentro da UFPB que quando utilizada fora da rede da universidade.

A ferramenta *NetSparker* foi configurada para escanear a página de *login* do sistema SIGAA-*StrictoSensu*. Os testes tiveram resultados uniformes e permitiram identificar pontos de vulnerabilidades no sistema em dois níveis de risco, importante e baixo, além de a ferramenta ter notificado também quanto à possibilidade de fácil obtenção de informação. O resultado do escaneamento encontrou 11 tipos diferentes de vulnerabilidades, sendo um tipo de vulnerabilidade no nível Importante, sete tipos no nível Baixo e três tipos de vulnerabilidade para facilidade de obtenção de Informação (Quadro 2).

NÍVEL	TIPO DE VULNERABILIDADE	Sistema SIGAA-*StrictoSensu*		
		Teste 1	Teste 2	Teste 3
Importante	*Cross-site scripting*	1	1	1
Baixo	*Internal Server Error*	1	1	1
	Cookie Not Marked as HttpOnly	1	1	1
	Auto *Complete Enabled*	1	1	1
	[Possible] *Cross-site Request Forgery Detected*	1	1	1
	Version Disclosure (*Apache*)	1	1	1
	Version Disclosure (*Java Servlet*)	1	1	1
	Exception Report Disclosure (*Tomcat*)	0	0	1
Informação	*Email Address Disclosure*	1	1	1
	HTTP Strict Transport Security (HSTS) Policy Not Enabled	1	1	1
	[*Possible*] Internal Path Disclosure (Windows)	1	0	1

Quadro 2: Tipos de vulnerabilidades encontradas.

Fonte: Dados da pesquisa (2015).

Do Quadro 2 observa-se que a vulnerabilidade *Exception Report Disclosure* foi encontrada apenas no escaneamento feito fora do estado da Paraíba, bem como a *Internal Path Disclosure* apenas não foi encontrada dentro da UFPB. As vulnerabilidades[5] encontradas e soluções sugeridas encontram-se no Quadro 3.

Vulnerabilidade	Descrição da vulnerabilidade identificada	Prevenção do problema
Cross Site Scripting	Permite ao atacante a possibilidade de execução de *script* dinâmico (*JavaScript*, *VBScript*) na aplicação, o que permite, entre outros, ataques do tipo sequestro de sessão; phishing[6]; ataques de interceptação	A saída de dados do sistema deve ser codificada de acordo com a localização ou o contexto. Por exemplo, se a saída vai para um bloco *JavaScript* dentro da página, então precisa ser decodificada

[5] A descrição das vulnerabilidades, quando não referenciadas, foram obtidas dos relatórios dados pela própria ferramenta.
[6] Ataque do tipo engenharia social que utiliza email de modo a induzir o destinatário a clicar em algum arquivo executável, provavelmente anexo à mensagem ou por meio de redirecionamento a páginas falsas de instituições. Esses emails se

	de dados e do tipo *man-in-the-middle*[7]. Esse problema ocorre, pois os navegadores interpretam os dados de entrada do usuário como HTML, *JavaScript* ou *VBScript* ativo.	nesse sentido. Necessidade de fazer uso de *plugins* Anti-XSS[8]; e recomendações[9] da OWASP[10] para uma programação preventiva.
Internal Server Error	O servidor retornou um erro do tipo "HTTP status 500" indicando que ocorreu um erro do lado servidor. Comportamentos como esse podem indicar más práticas de codificação, necessidade de higienização e verificações insuficientes. Esse erro pode indicar um problema maior como *SQLInjection*.	Necessidade de práticas genéricas para tratar erros inesperados; tratar todos os erros somente do lado servidor; evitar dar informação do lado usuário sobre qual tipo de erro ocorreu no servidor; e codificação preventiva de SQLInjection.
Cookie Not Marked as HttpOnly	Há possibilidade dos cookies serem acessados do lado cliente.	Necessidade de codificação preventiva marcando cookies como "HTTP Only".
Auto Complete Enabled	Campos de autenticação identificados com ao *autocomplete* habilitado.	Em campos que não se deve fazer *cachê*, manter desabilitado o atributo *autocomplete* da página HTML, informando o valor *off*.
[Possible] Cross-site Request Forgery Detected - CSRF	Há possibilidade de roubo de sessões.	Necessidade de gerenciamento de sessões mais robusto pela aplicação, por meio de uso de token anti-CSRF
Version Disclosure (*Apache*)	Foi possível descobrir a versão do servidor Apache Tomcat.	Recomenda-se configurar o servidor web de modo a prevenir vazamento de cabeçalhos "SERVER" no "HTTP Response"
Version Disclosure (*Java Servlet*)	Foi possível descobrir a versão do Java Servlet.	Recomenda-se configurar o servidor web de modo a prevenir vazamento de cabeçalhos "X-*Powered-By*" no "HTTP *Response*".
Exception Report Disclosure (*Tomcat)*	A descoberta de relatório de exceção da ferramenta de desenvolvimento *Tomcat* possibilita a obtenção de versão dessa ferramenta, caminhos físicos de arquivos e informação sobre a exceção gerada.	Necessidade de customização de páginas de erro no arquivo de configuração "*web*.xml".
E-mail Address Disclosure	A descoberta de endereços de email dentro da aplicação pode ser usada por máquinas de envio de *spam* e ferramentas de força bruta, além de ataques do tipo engenharia social.	Fazer uso endereços de email genéricos como "contato@" ou "info@" para comunicações gerais, além de não fornecer lista específicas de usuários no *website*, se necessário fornecer formulários para esse propósito.
HTTP Strict Transport Security (HSTS) *Policy Not Enabled*	Não faz uso da tecnologia HSTS.	Recomenda-se fazer uso de HTTPS por meio da tecnologia HSTS.
[Possible] Internal Path Disclosure (*Windows*)	Foi possível encontrar o caminho do arquivo de configuração do *windows* "win.ini" utilizando o portal público do SIGAA (possibilidade de infecção do arquivo por vírus ou *malware*)	Recomenda-se melhorar a localização de arquivos de configuração.

disfarçam de cartões virtuais, convites ou instituições financeiras (ASSUNÇÃO, 2005, p. 120-123).

[7] Em ataques desse tipo o invasor se põe como um intermediário invisível entre o computador do usuário e o servidor da aplicação (ASSUNÇÃO, 2005, p. 191-193)

[8] Mecanismos de codificação que ajudam a prevenir ataques do tipo *Cross Site scripting*.

[9] https://www.owasp.org/index.php/XSS_Cross_Site_Scripting_Prevention_Cheat_Sheet

[10] É uma entidade sem fins lucrativos focada na melhoria de segurança de software, cuja missão é tornar a segurança de software visível de modo a prover informações que auxiliem a avaliar os riscos de segurança e a combater ataques na rede.

Quadro 3: Resultado do escaneamento.

Fonte: Dados da pesquisa (2015).

A quantidade de vulnerabilidades encontradas, por nível de risco (importante, baixo e informação), encontra-se no Quadro 4. Observou-se que, apesar da uniformidade de tipos de vulnerabilidades encontradas, como explicitado anteriormente, a quantidade de vulnerabilidades por tipo obteve pouca variação, onde no teste 1 e teste 3 foram encontrados 15 pontos de vulnerabilidades no sistema do tipo *Cross Site Scripting*, único tipo encontrado para o nível importante, enquanto no teste 2 encontrou-se apenas 9 pontos.

TESTES	IMPORTANTE	BAIXO	INFORMAÇÃO
Teste 1	15	07	03
Teste 2	09	07	02
Teste 3	15	08	06

Quadro 4: Quantitativo de vulnerabilidades encontradas por teste.

Fonte: Dados da pesquisa (2015).

Considera-se, conforme visto nos Quadros 4 e 1, que a existência de diferença na quantidade de vulnerabilidades encontradas foi em decorrência do tempo de execução da ferramenta que para o segundo teste foi inferior aos demais procedimentos, em que se obteve uma duração de apenas 22 minutos, enquanto o primeiro teste levou pouco mais de duas horas, e o terceiro teste perdurou por uma hora.

5. Considerações Finais

Com o desenvolvimento desta pesquisa foi possível mapear as vulnerabilidades tecnológicas existentes e apresentar algumas contribuições para melhorar o nível de segurança do sistema, bem como possibilitar à instituição ter conhecimento dos riscos de segurança da informação.

Nesse sentido, a varredura por vulnerabilidades no SIGAA-*StrictoSensu* identificou a necessidade de utilização de *plugins* Anti-XSS, além de uma programação preventiva baseada em recomendações da OWASP. Também se verificou a necessidade de boas práticas de codificação que tratem os erros somente do lado do servidor, evitando dar informações sobre a tecnologia empregada, assim como de higienização de código e verificações constantes. O sistema também não deve habilitar o recurso autocompletar em campos de autenticação ou de dados financeiros, além de melhorar no quesito gerenciamento de sessão para evitar a janela de oportunidade existente quando o usuário logado se ausenta do computador por períodos prolongados de tempo.

Há também necessidade de um gerenciamento de sessão mais robusto que inclua o uso de *tokens* Anti-CSRF, de modo a prevenir que as ameaças se concretizem. Todas essas são preocupações, dentre outras, que o desenvolvedor deve estar sempre atento em todas as fases do projeto de desenvolvimento de sistemas.

A relevância dessa pesquisa amplia-se principalmente por esse sistema fazer parte de um sistema cooperado utilizado por várias instituições federais de ensino, logo as vulnerabilidades identificadas possivelmente persistem nas demais instituições. Diante desse cenário, propõe-se para pesquisas futuras a aplicação desse método estruturado a todos os módulos que compõem o SIG da UFPB, bem como uma análise mais aprofundada das vulnerabilidades tecnológicas existentes dentro do sistema. Desse modo, sugere-se um olhar voltado para a segurança da informação a todos os profissionais que trabalham direta ou indiretamente na gerência de informação, a começar por uma cultura que se preocupe com questões de segurança.

Referências

ASSUNÇÃO, M. F. A. **Segredos do hacker ético**. 3. ed. Florianópolis: Visual Books, 2005.

BRASIL. Decreto nº 3.505, de 13 de junho de 2000. Institui a política de segurança da informação nos órgãos e entidades da Administração Pública Federal e dá outras providências. **Diário Oficial [da] República Federativa do Brasil**, Brasília, DF, 14 jun. 2000. Disponível em: <http://www.planalto.gov.br/ccivil_03/decreto/D3505.htm>. Acesso em: 25 fev. 2015.

CENTRO DE ESTUDOS, RESPOSTA E TRATAMENTO DE INCIDENTES DE SEGURANÇA NO BRASIL (CERT.br). **Cartilha de segurança para internet, versão 4.0**. São Paulo: Comitê Gestor da Internet no Brasil, 2012a. Disponível em: <http://cartilha.cert.br/livro/cartilha-seguranca-internet.pdf>. Acesso em: 12 jul. 2014.

CHIAVENATO, I. **Teoria geral da administração**. São Paulo: McGraw-Hill, 2002. v. 1 e 2.

HARKINS, M. **Managing Risk and Information Security**: Protect to Enable. Apress, 2013.

NATIONAL INTITUTE OF STANDARS AND TECHNOLOGY. **Managing information security risk**: organization, mission, and information system view. Gaithersbourgh, MD: National Institute of Standards and Technology, 2011.

_____. **Framework for improving critical infrastructure cybersecurity**: version 1.0. Gaithersburg, MD: National Institute of Standards and Technology, 2014.

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

O'BRIEN, J. A.; MARAKAS, G. M. **Administração de sistemas de informação**. 15. ed. São Paulo: McGraw-Hill, 2012.

SWANSON, M.; HASH, J.; BOWEN, P. **Guide for developing security plans for federal information systems**: information security. Gaithersburg, MD: National Institute of Standards and Technology, 2006.

SYMANTEC CORPORATION. **Internet security threat report 2014**. California, v. 19, 2014. Disponível em: <http://www.symantec.com/content/en/us/enterprise/other_resources/b-istr_main_report_v19_21291018.en-us.pdf>. Acesso em: 07 abr. 2015.

TURBAN, E.; RAINER JR., R. K.; POTTER, R. E. **Introdução a sistemas de informação**: uma abordagem gerencial. Rio de Janeiro: Elsevier, 2007.

UTO, N. **Teste de invasão de aplicações web**. Rio de Janeiro:RNP/ESR, 2013.

WIKIUFRN. **SINFO**: Superintendência de Informática/UFRN. Disponível em: <https://www.info.ufrn.br/wikisistemas/doku.php>. Acesso em: 22 fev. 2016.