UNIVERSIDADE FEDERAL DA PARAÍBA
CENTRO DE CIÊNCIAS SOCIAIS APLICADAS
DEPARTAMENTO DE CIÊNCIA DA INFORMAÇÃO
CURSO DE GRADUAÇÃO EM BIBLIOTECONOMIA

VALDETE FERNANDES BELARMINO

Análise de vulnerabilidades computacionais nos repositórios digitais das Universidades Federais

Orientador: Professor Dr. Wagner Junqueira de Araújo

JOÃO PESSOA
2014

VALDETE FERNANDES BELARMINO

Análise de vulnerabilidades computacionais nos repositórios digitais das Universidades Federais

Trabalho de Conclusão de Curso apresentado ao Curso de Graduação em Biblioteconomia do Centro de Ciências Sociais Aplicadas da Universidade Federal da Paraíba como requisito parcial para obtenção do título de Bacharel.

Orientador: Professor Dr. Wagner Junqueira de Araújo

JOÃO PESSOA
2014

B426a Belarmino, Valdete Fernandes.

Análise de vulnerabilidades computacionais nos repositórios digitais das Universidades Federais / Valdete Fernandes Belarmino.-- João Pessoa, 2014.

62f. : il.

Orientador: Wagner Junqueira de Araújo

Trabalho de Conclusão de Curso - TCC (Graduação em Biblioteconomia) – UFPB/CCSA

1. Informação científica. 2. Repositórios digitais. 3. DSpace. 4. Segurança da informação. 5. Preservação digital. 6. Teste de penetração.

UFPB/BC *CDU: 001.92(043.2)*

UNIVERSIDADE FEDERAL DA PARAÍBA
CENTRO DE CIÊNCIAS SOCIAIS APLICADAS
CURSO DE GRADUAÇÃO EM BIBLIOTECONOMIA

VALDETE FERNANDES BELARMINO

Análise de vulnerabilidades computacionais nos repositórios digitais das Universidades Federais

Trabalho de Conclusão de Curso apresentado ao Curso de Graduação em Biblioteconomia do Centro de Ciências Sociais Aplicadas da Universidade Federal da Paraíba como requisito parcial para obtenção do título de Bacharel.

Folha de Aprovação

Aprovada em: ___/___/_____

Banca Examinadora:

_____
Prof. Dr. Wagner Junqueira de Araújo
(DCI/UFPB – Orientador)

_____
Prof. Dr. Marckson Roberto F. de Sousa
(DCI/UFPB – Membro)

_____
Me. Josivan Ferreira
(UFPB – Membro)

Dedico este trabalho em memória do meu amado sobrinho Nino, que era a representação mais pura e sincera do amor e da alegria, e se tornou um anjinho no céu durante o andamento dessa pesquisa.

AGRADECIMENTOS

Em primeiro lugar, a Deus, fortaleza sempre presente em minha vida. Mesmo nos momentos em que a fé ficava abalada, Ele me dava forças e continuava sempre segurando minha mão e guiando meus passos.

Aos meus pais, Valdeci e Edileuza, por todo o amor e compreensão dedicados a mim e meus irmãos, pelos ensinamentos dos valores da vida e por mostrar a importância de sempre se manter no caminho correto.

Aos meus irmãos, Valdleuza, Valdeci Jr e Valdiney, pela união e amizade que independe dos laços fraternais.

Ao Prof. Dr. Wagner Junqueira, exemplo de responsabilidade, dedicação e competência no direcionamento e orientação desta pesquisa.

Às minhas amigas: Priscila, pelos mais de vinte anos de amizade sincera e pelo companheirismo sempre presente em todas as situações; Suely, Vanessa e Kiane, por todos os momentos de parceria vividos.

Enfim, a todos que contribuíram direta ou indiretamente e participaram desse projeto, meus sinceros agradecimentos.

RESUMO

Destaca a relevância da informação na sociedade contemporânea como um recurso de valor inestimável, enfatizando a informação científica como elemento essencial para constituir o progresso científico. Caracteriza o surgimento dos Repositórios Digitais e ressalta sua utilização em meio acadêmico para divulgar, disseminar, preservar e incentivar a produção científica. Descreve os principais softwares para a construção de repositórios digitais, apontando a ferramenta DSpace como sendo uma das plataformas mais utilizada no Brasil e no mundo para a criação dos repositórios digitais de acesso livre. Aborda os aspectos primordiais da Segurança da Informação, identificando as vulnerabilidades a que os repositórios estão sujeitos e as ameaças consideradas mais significativas para a preservação da informação digital. Enfoca a tríade de elementos básicos envolvidos no processo da segurança da informação: integridade, confidencialidade e disponibilidade, dentre outros fatores de salvaguarda. Incentiva a implementação de uma Política de Segurança da Informação, considerando especificações registradas na norma técnica NBR ISO/IEC 17799, de maneira a viabilizar o gerenciamento adequado da informação. Analisa os perigos de invasão a que estão expostos os repositórios digitais institucionais em âmbito federal, por meio da execução de Testes de Penetração, especificando os níveis de riscos e os tipos de vulnerabilidades. Foram identificados 5% dos repositórios com vulnerabilidades críticas, 85% altas, 25% médias e 100% baixas. Estimula a importância da adoção de um conjunto de métodos e procedimentos que promovam a segurança dos ativos informacionais, visando minimizar a incidência de ataques externos e/ou internos aos sistemas das instituições.

Palavras-chave: Informação científica. Repositórios Digitais. DSpace. Segurança da Informação. Preservação digital. Teste de Penetração.

ABSTRACT

This monograph highlights the relevance of information in contemporary society as an invaluable resource, emphasizing scientific information as an essential element to constitute scientific progress. It characterizes the emergence of Digital Repositories and highlights its use in academia to promote, disseminate, preserve and encourage the scientific production. It describes the main softwares to create digital repositories, pointing DSpace tool as the most widely used platform in Brazil and in the world for the creation of digital repositories with open access. It addresses the main aspects of information security, identifying vulnerabilities that the repositories are subjected and the most significant threats to the preservation of the digital information. It focuses on the triad of basic elements involved in the process of information security: integrity, confidentiality and availability, among other factors. It encourages the implementation of an Information Security Policy, considering technical specifications recorded in the NBR ISO/IEC 17799 standard in order to enable proper information management. It examines, by running the Penetration Test, the dangers of invasion that the institutional digital repositories at the federal level are exposed, specifying the levels of risk and the types of vulnerabilities. About 5% of repositories were identified with critical vulnerabilities, 85% high, 25% medium and 100% low. It stimulates the importance of adopting a set of methods and procedures that promote the safety of informational assets in order to minimize the incidence of external and/or internal attacks in the systems of institutions.

Keywords: Scientific information. Digital Repositories. DSpace. Information Security. Digital preservation. Penetration Test.

LISTA DE ILUSTRAÇÕES

LISTA DE QUADROS

LISTA DE SIGLAS

ABNT – Associação Brasileira de Normas Técnicas

BRAPCI – Base de Dados Referencial de Artigos de Periódicos em Ciência da Informação

CAPEC – Common Attack Pattern Enumeration and Classification

CWE – Common Weakness Enumeration

FURG – Universidade Federal do Rio Grande

HP – Hewlett-Packard Company

IBICT – Instituto Brasileiro de Informação em Ciência e Tecnologia

IEC – International Electrotechnical Commission

IES – Instituições de Ensino Superior

ISO – International Standards Organization

MEC – Ministério da Educação e Cultura

MIT – Massachusetts Institute of Technology

NSA – National Security Agency

OA – Open Archives

OAI – Open Archives Initiative

OAI-PMH – Open Archives Initiative-Protocol for Metadata Harvesting

OAIS – Open Archival Information System

OWASP – Open Web Application Security Project

PCI – Payment Card Industry

RD – Repositório Digital

RI – Repositório Institucional

ROAR – Registry of Open Access Repositories

SAAI – Sistema Aberto para Arquivamento de Informação

SI – Segurança da Informação

SQL – Structured Query Language

TIC – Tecnologias da Informação e Comunicação

UFAC – Universidade Federal do Acre

UFAL – Universidade Federal de Alagoas

UFBA – Universidade Federal da Bahia

UFC – Universidade Federal do Ceará

UFES – Universidade Federal do Espírito Santo

UFF – Universidade Federal Fluminense

UFG – Universidade Federal de Goiás

UFGD – Universidade Federal de Grande Dourados

UFJF – Universidade Federal de Juiz de Fora

UFLA – Universidade Federal de Lavras

UFMA – Universidade Federal do Maranhão

UFMG – Universidade Federal de Minas Gerais

UFMS – Universidade Federal do Mato Grosso do Sul

UFOP – Universidade Federal de Ouro Preto

UFPA – Universidade Federal do Pará

UFPB – Universidade Federal da Paraíba

UFPE – Universidade Federal do Pernambuco

UFPEL – Universidade Federal de Pelotas

UFPR – Universidade Federal do Paraná

UFRGS – Universidade Federal do Rio Grande do Sul

UFRN – Universidade Federal do Rio Grande do Norte

UFS – Universidade Federal de Sergipe

UFSC – Universidade Federal de Santa Catarina

UFSCAR – Universidade Federal de São Carlos

UFU – Universidade Federal de Uberlândia

UFV – Universidade Federal de Viçosa

UFVJM – Universidade Federal dos Vales de Jequitinhonha e Mucuri

UNB – Universidade de Brasília

UNIFESP – Universidade Federal de São Paulo

WASC – Web Application Security Consortium

SUMÁRIO

1 INTRODUÇÃO

A informação é um bem de valor inestimável para a sociedade e um recurso absolutamente necessário para adquirir conhecimento. O elemento fundamental para estabelecer o progresso científico, tecnológico e educacional de uma nação é a informação científica. Esse tipo de informação é revelado à sociedade através dos periódicos científicos, em consequência do trabalho intelectual dos pesquisadores (KURAMOTO, 2006).

No decorrer dos tempos, o avanço tecnológico e o processo de globalização possibilitaram a integração e o compartilhamento de informações de maneira instantânea, resultando em um aumento de publicações considerado acima do comum. A publicação de artigos em revistas científicas sustenta um ciclo produtivo que se transforma em um recurso indispensável para o sistema de comunicação científica.

Com o crescimento exponencial bibliográfico (em suporte tradicional, o papel, e em maior escala, no formato digital) e a facilidade na produção de novas informações em ambiente virtual atualmente, a quantidade de material eletrônico disponível para acesso na internet é amplamente variada. Só de artigos científicos, o crescimento da produção acadêmica a partir do ano 2001 até outubro de 2013 representa aproximadamente 63%, de acordo com dados disponíveis na Base de Dados Referencial de Artigos de Periódicos em Ciência da Informação – BRAPCI[1].

Os avanços decorrentes das novas tecnologias de informação e comunicação proporcionaram o surgimento dos Repositórios Digitais (RDs), que além de artigos abrigam os resultados de trabalhos de conclusão de curso, dissertações, teses, anais de encontros científicos, palestras etc.

As instituições acadêmicas utilizam os repositórios digitais para divulgar, disseminar, preservar e incentivar a produção científica de sua comunidade. As tecnologias aliadas à disseminação da informação assumem um papel crucial na sociedade do conhecimento. Por ser um componente valioso no desenvolvimento do saber do indivíduo, existe uma preocupação coletiva com o tratamento, a preservação, a disseminação e a segurança da informação.

A construção e manutenção de repositórios digitais exigem das instituições recursos computacionais, pessoas habilitadas e processos para a gestão. Existe um estudo que aborda a

[1] Website: <http://www.brapci.ufpr.br/indicador_producao.php>.

segurança em itens relativos a pessoas e processos (LIMA; LIMA, 2012), contudo não aborda os aspectos de segurança do ambiente computacional.

Diante do exposto, surge a seguinte questão de pesquisa: como estão configurados os elementos de segurança da informação no ambiente computacional dos repositórios digitais das universidades federais no Brasil?

1.1 OBJETIVOS

A pesquisa tem como objetivo geral analisar a segurança da informação no ambiente computacional dos repositórios institucionais digitais no âmbito das universidades federais. E, como objetivos específicos, distinguir os aspectos característicos da segurança da informação; identificar os tipos de vulnerabilidades a que os repositórios digitais estão expostos e indicar estratégias para evitar e/ou reduzir os riscos/ameaças à segurança da informação. Para fins deste estudo entende-se como ambiente computacional os elementos de configuração de software usados para implementar os repositórios digitais.

A estrutura do trabalho é dividida em oito capítulos. Após a introdução segue o capítulo sobre Repositórios Digitais, que aborda conceitos de autores variados, ressalta a estrutura do movimento de Acesso Livre e a Iniciativa de Arquivos Abertos, destaca o ranking de países que possuem mais repositórios digitais de acesso aberto no mundo e indica os principais softwares para a construção de repositórios digitais. Também mostra a utilização da ferramenta DSpace para a criação dos repositórios digitais no Brasil e no mundo, ilustrando graficamente sua distribuição por países e sua evolução de uso ao longo do tempo.

O capítulo três aborda a Preservação Digital e as vulnerabilidades dos repositórios institucionais, elencando os fatores mais significativos que podem colocar em risco o processo de conservação e acesso da memória digital e relacionando as técnicas e medidas adotadas para a salvaguarda dos documentos.

No capítulo quatro são apresentados conceitos sobre a Segurança da Informação, assinalando os elementos que fazem parte da sua base principal: confidencialidade, integridade e disponibilidade. Neste tópico também são explicados os procedimentos existentes em normas e padrões de segurança para os controles de acesso à informação e para a implementação da Política de Segurança.

No capítulo cinco são descritos os procedimentos metodológicos que fundamentaram a pesquisa, os métodos utilizados para sua realização, a caracterização da abordagem empregada e os instrumentos da coleta dos dados.

O capítulo seis contempla todo o desenvolvimento da análise de risco a que foram submetidos os repositórios digitais indicados na amostra, os problemas identificados no andamento dos testes, o histórico dos dados consultados, as definições das ameaças encontradas e os resultados dos testes de vulnerabilidade realizados.

O capítulo sete especifica as recomendações e medidas que podem ser adotadas para evitar e/ou minimizar as ameaças à segurança da informação digital, como também estratégias de recuperação ou correção dos problemas identificados.

Por fim, no capítulo oito estão expostas as considerações finais acerca do trabalho realizado, seguido das referências consultadas para o embasamento teórico e os anexos.

2 REPOSITÓRIOS DIGITAIS

O Instituto Brasileiro de Informação em Ciência e Tecnologia (IBICT)[2] define em sua página na internet que os repositórios digitais (RDs) são bases de dados online que reúnem de maneira organizada a produção científica de uma instituição ou área temática. De maneira complementar, Weitzel (2006b) especifica a divisão dos repositórios digitais em categorias: institucionais ou temáticos. Os primeiros dizem respeito à organização e acesso à produção científica de uma instituição, enquanto os segundos são atribuídos a uma determinada área do conhecimento.

Considerando que os repositórios possibilitam a gestão da produção intelectual científica e acadêmica em qualquer tipo de arquivo digital, Viana, Márdero Arellano e Shintaku (2005, p. 3), completam: "um repositório digital é uma forma de armazenamento de objetos digitais que tem a capacidade de manter e gerenciar material por longos períodos de tempo e prover o acesso apropriado." Para fortalecer o conceito, Ribeiro e Vidotti (2009, p. 106), destacam:

> Os repositórios digitais trazem a ideia de preservação dos objetos digitais, além de promover o acesso livre a conteúdos como produtos de pesquisa, entre outros. Além disso, esses repositórios precisam ser criados tendo como necessidades dos usuários potenciais, permitindo usabilidade e acessibilidade satisfatórias.

Portanto, os repositórios digitais correspondem a bancos ou bases de dados que contêm toda variedade de objetos em formato digital (documento de texto, imagem, áudio, vídeo etc.), com a finalidade de disseminar o conteúdo informacional de forma mais estruturada e tornar sua recuperação acessível em longo prazo por qualquer pesquisador.

> Os repositórios digitais oferecem muitos benefícios em relação aos serviços digitais, auxiliando a comunidade científica na organização e aquisição de trabalhos científicos de uma determinada instituição ou comunidade, oferecendo acesso irrestrito, intercâmbios e troca de informações, bem como outros tipos de serviços e recursos. (CAMARGO, 2008, p. 14 apud RIBEIRO; VIDOTTI, 2009, p. 111-112).

[2] O conceito na íntegra está disponível em: <http://www.ibict.br/informacao-para-ciencia-tecnologia-e-inovacao%20/repositorios-digitais>.

Um repositório digital pode ser mantido por qualquer instituição, seja científica, acadêmica, governamental ou outro tipo de organização solidamente constituída, a qual tenha o propósito de promover a distribuição absoluta da informação, o livre acesso ao documento integral, o recurso de interoperabilidade e o atributo de armazenamento em longo prazo.

Estes repositórios estimulam a produção online gerenciada pelo pesquisador, empregam novas tecnologias de código aberto, e as informações ficam disponibilizadas para acesso permanente e integral por múltiplos provedores de serviços, seja nacional ou internacional (VIANA; MÁRDERO ARELLANO; SHINTAKU, 2005).

A transformação primordial ocorrida nos meios de comunicação em favor ao acesso livre à informação científica deve-se à Iniciativa de Arquivos Abertos (*Open Archives Initiative* - OAI) e ao movimento de Acesso Livre ou Acesso Aberto (*Open Access*). São iniciativas que reúnem os requisitos necessários para permitir o acesso livre à produção científica em meio digital, promovendo o processo de aquisição, produção, armazenamento, disseminação e uso da informação científica de forma irrestrita, online e isenta de quaisquer cobranças de taxas ou assinaturas para o acesso.

A Iniciativa de Arquivos Abertos nasceu com a Convenção de Santa Fé em 1999, nos Estados Unidos. O Movimento de Acesso Livre ocorreu em 2002 com a Declaração de Budapeste. Weitzel afirma que:

> É possível que a OAI tenha contribuído para a organização do Movimento de Livre Acesso. Trata-se, portanto, de dois movimentos distintos, ambos desejam o livre acesso, e por isso, estão inseridos no modelo baseado no *Open Access*, traduzido aqui como acesso livre no sentido de acesso público e gratuito. (WEITZEL, 2005, p. 11).

Estes mecanismos de acesso são utilizados pelos softwares que gerenciam os repositórios digitais para facilitar a interação dos usuários na inserção, busca e recuperação dos arquivos de publicações científicas, de forma eficiente e legítima. O modelo *Open Archives* (OA) adota o uso do protocolo de coleta de metadados *Open Archives Initiative – Protocol for Metadata Harvesting* (OAI-PMH), que utilizam padrões tecnológicos comuns a todos os repositórios que aplicam esse modelo, possibilitando assim a interoperabilidade entre os mesmos. “O protocolo OAI-PMH, lançado em 2001, é o mecanismo que permite alcançar os objetivos da iniciativa e é amplamente utilizado por instituições de todo o mundo.” (MÁRDERO ARELLANO; LEITE, 2009, p. 3).

Os repositórios digitais baseados no modelo *Open Archives* possuem a característica de autoarquivamento da produção científica, onde o próprio autor deposita seu trabalho na

base de dados para que qualquer usuário tenha acesso ao texto completo. Esses repositórios podem conter artigos revisados por pares ou não, conforme relata Kuramoto (2008, p. 866)

> O movimento do acesso livre à literatura científica propõe duas estratégias para alcançar os seus objetivos: 1) via verde; 2) via dourada. A via verde refere-se ao autoarquivamento, pelos autores ou seus representantes, de uma cópia de seus *papers* em um repositório, institucional ou temático, de acesso livre. A via dourada refere-se à publicação de artigos em revistas científicas de livre acesso.

É fundamental o acesso aberto às publicações científicas e acadêmicas aos pesquisadores e autores tanto quanto aos leitores, pois se as instituições nas quais aqueles trabalham não dispuserem dos meios para acessar os conteúdos digitais, isso consequentemente prejudicará os resultados de suas pesquisas.

A estrutura do modelo OA estabelece a existência de dois termos: os provedores de dados e os provedores de serviços. Os provedores de dados são os administradores dos arquivos digitais, os quais são dotados de diversas funcionalidades: autoarquivamento, armazenamento a longo prazo e mecanismos de apresentação de metadados para facilitar a recuperação do conteúdo. Os provedores de serviços são as instituições que asseguram a realização dos serviços com valor agregado a partir da coleta dos dados dos arquivos reunidos nos repositórios digitais (KURAMOTO, 2006).

Um exemplo de provedores de dados são os softwares utilizados para implementação dos repositórios digitais que mantêm em sua base de dados todas as informações produzidas no âmbito institucional. Um exemplo de provedor de serviços são as Instituições de Ensino Superior (IES), que fazem a coleta dos metadados dos documentos contidos em suas bibliotecas digitais.

A página na internet do *Registry of Open Access Repositories* – ROAR[3] (Registro de repositórios de acesso aberto, em tradução livre) apresenta indicadores sobre os repositórios inscritos pelos provedores de serviços no mundo, onde é possível ordenar a lista de repositórios e especificar a busca por país, software utilizado e tipo de repositório determinado.

De acordo com esse registro em maio de 2013, o Brasil ocupa a 6ª posição na lista de países com mais repositórios digitais de acesso aberto no mundo (133), ficando atrás da Espanha (155), Japão (167), Alemanha (192), Reino Unido (249) e Estados Unidos (550).

[3] Website: http://roar.eprints.org/

2.1 SOFTWARES PARA A CONSTRUÇÃO DE REPOSITÓRIOS DIGITAIS

As plataformas usadas para a criação de repositórios digitais podem ser livres, com código aberto, comumente elaboradas por institutos, e/ou universidades e disponíveis de forma gratuita. Deste modo, estas ferramentas podem ser instaladas, avaliadas, utilizadas e customizadas irrestritamente por qualquer organização que tencione aplicá-las na constituição de uma biblioteca digital. (OLIVEIRA; CARVALHO, 2011).

A plataforma DSpace é uma das mais utilizadas para a construção de repositórios digitais. O DSpace foi concebido pelo *Massachusetts Institute of Technology* (MIT) em colaboração com a *Hewlett-Packard Company* (HP) entre março de 2000 e novembro de 2002 e ainda

> [...] foi traduzido em parceria com a equipe da PORTCOM (Rede de Informação em Comunicação dos Países de Língua Portuguesa) da INTERCOM (Sociedade Brasileira de Estudos Interdisciplinares da Comunicação) e do Núcleo de Pesquisa *Design de Sistemas Virtuais Centrado no Usuário* da USP (Universidade de São Paulo). (WEITZEL, 2006b, p. 5).

A ferramenta Dspace permite a criação de repositórios digitais para a captura da produção intelectual de organizações e instituições de pesquisa com funcionalidades de armazenamento, distribuição, visibilidade e preservação da informação, possibilitando sua customização por outras instituições que adotem esse sistema. O Dspace é uma ferramenta integrada para apoiar o planejamento de preservação digital em longo prazo e administrar o conteúdo depositado, o que o torna um software adaptado às realidades da gestão de um repositório em um grande cenário institucional.

Dentre suas características principais, destacam-se: possuir uma arquitetura simples e eficiente, utilizar uma tecnologia de ponta, ser um software livre direcionado para o acesso aberto e ser propositadamente desenvolvido para servir de repositório institucional (RI). (VIANA; MÁRDERO ARELLANO; SHINTAKU, 2005). Além desses atributos, o DSpace apresenta a prerrogativa de utilizar "[...] identificadores persistentes que facilitam referenciar os objetos digitais por um longo período de tempo. O uso do Dspace tem se mostrado fácil e flexível, garantindo a preferência por esse *software* para a criação dos repositórios digitais." (RIBEIRO; VIDOTTI, 2009, p. 108-109).

O software EPrints também é bastante empregado na construção de repositórios digitais de acesso aberto no mundo. Desenvolvido pela Universidade de Southampton na Inglaterra, a primeira versão do sistema foi lançada publicamente no final no ano 2000. É um programa apropriado para a criação de repositórios institucionais ou temáticos, oferecendo ampla rede de suporte para novas implementações. É um software livre, de código aberto, que dispões de mínimo conhecimento técnico para sua instalação e que pode ser facilmente modificado para satisfazer as preferências da instituição que o utilize.

Sobre os arquivos em formato digital que a ferramenta suporta, Viana e Márdero Arellano (2006, p. 4) destacam que "os repositórios baseados no EPrints permitem o depósito de pré-prints (trabalhos ainda não publicados), pós-prints (já publicados), outros tipos de publicações, comentários e versões, bem como de outros tipos de documentos." O IBICT customizou versões em português para os softwares DSpace e EPrints.

Outra opção é a ferramenta Fedora que foi idealizada em conjunto pelas Universidades de Virginia e Cornell, sendo igualmente um software livre de código aberto. O sistema oferece uma arquitetura projetada e acrescenta utilitários que facilitam o gerenciamento dos repositórios. Sobre a interface do sistema, Oliveira e Carvalho (2011, p. 8) ressaltam que

> O núcleo central do Fedora é o repositório de serviços, que pode ser acessado utilizando interfaces via web service, que permite a criação, gerenciamento, armazenamento, acesso e o reuso dos objetos digitais. Todas as funções do Fedora, tanto no nível de administração do repositório como no nível do acesso aos objetos digitais são disponibilizados por este repositório de serviços.

De acordo com o ROAR, o Fedora é uma ferramenta relativamente utilizada pelos provedores de serviços, configurando a 5ª colocação no ranking de softwares aplicados na implementação de repositórios digitais. O sistema Fedora apresenta uma diferença em relação ao EPrints e ao DSpace por não possuir em sua plataforma básica uma interface completa com o usuário final. (OLIVEIRA; CARVALHO, 2011).

Dos softwares utilizados com mais frequência para a criação dos repositórios digitais em nível mundial, conforme o ROAR, destacam-se o DSpace (1350), EPrints (497), Bepress (175), OPUS (50) e Fedora (41).

2.2 UTILIZAÇÃO DO SOFTWARE DSPACE

A informação científica isenta de qualquer restrição de acesso e livre de ônus ao usuário, proporciona benfeitorias tanto para a instituição que a disponibiliza (com o aumento da sua visibilidade) quanto para o pesquisador, com a valorização do seu trabalho. Para Kuramoto (2008), esse modelo tecnológico que oferece o acesso aberto à produção intelectual mundial apresenta resultados importantes para o desenvolvimento científico dos países, como: a facilidade de internacionalizar a literatura científica produzida localmente, a redução da exclusão cognitiva e maior compartilhamento do conhecimento produzido.

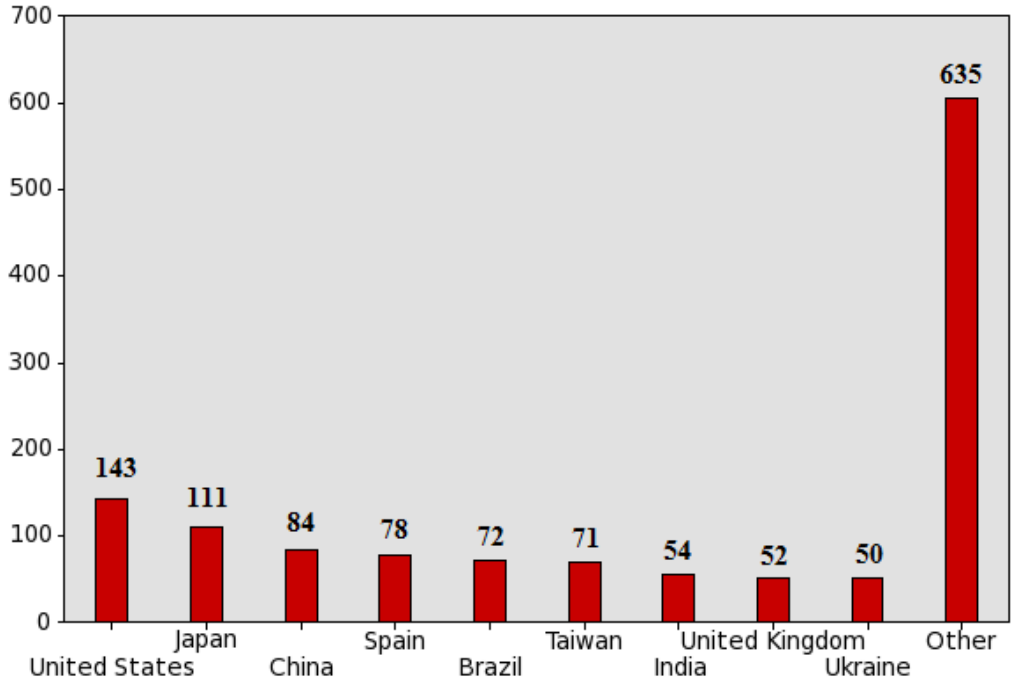
> A iniciativa de Arquivos Abertos e o Movimento de Acesso Aberto à Informação Científica vêm propondo que a informação científica seja disponibilizada gratuitamente; o que é favorecido pelos avanços constantes das tecnologias da informação e comunicação (TIC) dos últimos anos, gerando uma demanda do uso da *web* para a disseminação dos resultados de pesquisa. (FACHIN et al, 2009, p. 221).

Devido à OAI, o emprego dos repositórios digitais nos mais diversos tipos de instituições existentes (científicas, acadêmicas, governamentais, centros de pesquisa, organizações sem fins lucrativos, arquivos públicos, centros médicos etc.) vem crescendo exponencialmente em virtude dos seus inúmeros benefícios.

O software DSpace é uma das ferramentas mais utilizada mundialmente para a criação dos repositórios digitais de acesso livre. Os dados estatísticos disponíveis no site do ROAR comprovam essa afirmação, constatando que atualmente há 1350 repositórios digitais cadastrados em sua base que utilizam essa plataforma em todo o mundo. Por sua natureza operacional, o DSpace "é um dos softwares que apresenta condições mais propícias de preservação e acesso aos documentos armazenados." (TARGINO; GARCIA; PAIVA, 2012, p. 21).

O Brasil possui 133 repositórios digitais registrados nessa base de dados, dos quais 72 foram construídos com o uso do software DSpace, o que corresponde a aproximadamente 54% dos repositórios do país. Com isso, o Brasil ocupa a 5ª posição entre os países que mais utilizam essa ferramenta para a construção de repositórios, conforme representado na figura 1.

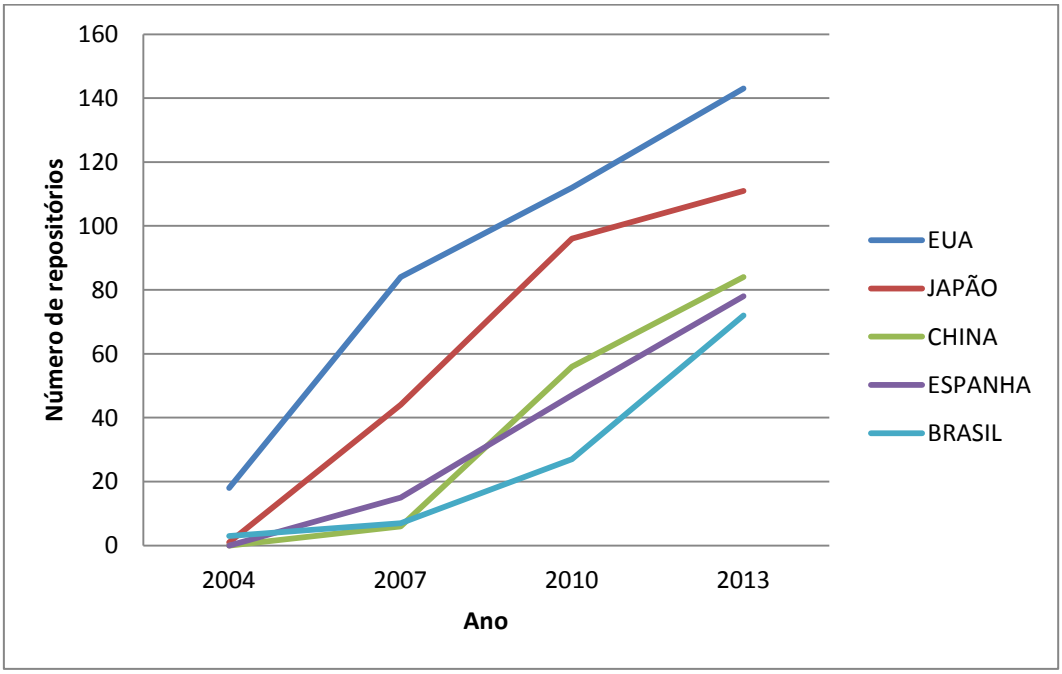
Figura 1 – Número de repositórios digitais com a ferramenta DSpace distribuído por países, 2013.



Fonte: Extraído de: ROAR, 2013 (Adaptado).

Desde o desenvolvimento final do DSpace pelo MIT em 2002, o crescimento no número de repositórios digitais se manifesta progressivamente ao longo dos anos em nível mundial. Essa linha da evolução de uso no tempo é reproduzida na figura 2.

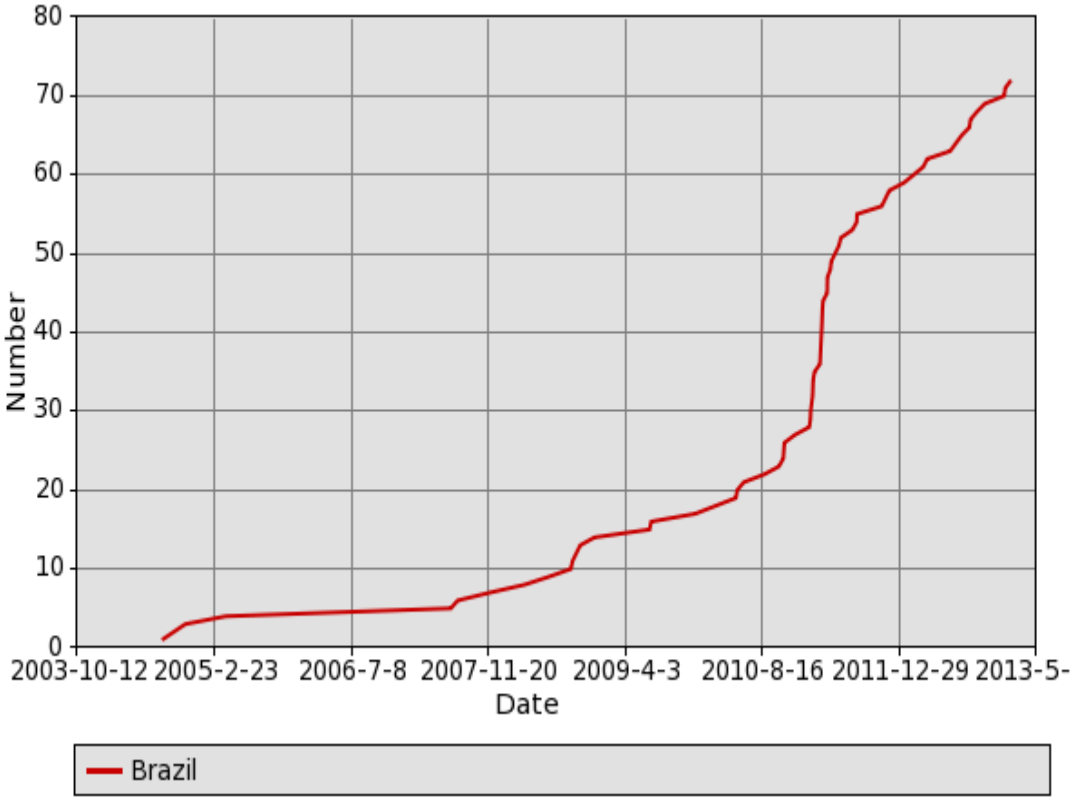
Figura 2 – Evolução de uso no tempo dos repositórios digitais DSpace no Brasil e no mundo, 2013.



Fonte: dados obtidos no ROAR, 2013.

Os países que mais se destacam na implementação de repositórios DSpace são os Estados Unidos, Japão, China, Espanha e Brasil. De acordo com os dados disponíveis no ROAR, o período de maior crescimento no Brasil se revela a partir do ano de 2011. Até o ano de 2010 existiam 27 repositórios no país inseridos na base de dados do ROAR, de 2011 até hoje esse número aumentou em 45, correspondendo a um progresso de 63% na criação de novos repositórios digitais com a ferramenta DSpace. Este exemplo pode ser observado na figura 3.

Figura 3 – Crescimento na criação de novos repositórios digitais no Brasil, 2013.



Fonte: Extraído de: ROAR, 2013.

De maneira análoga, considerando o mesmo período de tempo, a porcentagem de crescimento na implantação de novos repositórios nos Estados Unidos, Japão, China e Espanha equivalem respectivamente a 28%, 14%, 33% e 40%. Esses dados revelam uma diferença considerável na evolução do uso dos repositórios digitais no Brasil em relação a esses países, no intervalo de tempo entre 2011 e o momento atual.

3 PRESERVAÇÃO DIGITAL E VULNERABILIDADES DOS REPOSITÓRIOS INSTITUCIONAIS

Existe uma preocupação universal com a preservação da memória coletiva, cautela justificada pela necessidade de salvaguarda do conhecimento de valor considerável gerado por uma nação. A preservação de documentos digitais é um dos maiores desafios do nosso século, devido aos avanços tecnológicos e ao crescimento da produção de informações em formato eletrônico.

Inicialmente, as técnicas envolvidas com a preservação digital eram baseadas no conceito de identificar medidas que garantissem a vida útil dos arquivos, mas atualmente está relacionada ao conhecimento sobre os métodos de preservação para diminuir os riscos que podem afetar a longevidade do patrimônio informacional.

Todo arquivo está sujeito a riscos e eventuais danos que podem prejudicar o acervo institucional de qualquer organização. Esses acidentes não existem apenas no meio físico, também acontecem no ambiente virtual, e para minimizá-los é necessário adotar estratégias e medidas eficazes para a proteção dos documentos.

> [...] a identificação dos potenciais perigos decorrentes do ambiente digital nos processos de guarda e preservação da memória tem por objetivo permitir, antecipadamente, a adoção de medidas preventivas a fim de eliminar as causas ou reduzir os impactos e consequências dos cenários de acidentes identificados. Assim, a utilização de métodos de análise preliminar de riscos tem por finalidade propor proteção e guarda ao patrimônio informacional gerenciado por sistemas de informação, na eventualidade de um possível acidente. (LIMA; LIMA, 2012, p. 5).

O reconhecimento preliminar das possíveis ameaças inerentes aos conteúdos digitais trazem benefícios às instituições, no tocante à administração de recursos financeiros essenciais para a instalação e manutenção de sistemas e processos operacionais. Identificar esses perigos antecipadamente ou possuir o conhecimento necessário para saná-los ou amenizá-los, contribui para a gestão eficiente da informação digital.

São diversos os fatores que podem colocar em risco o processo de guarda e acesso da memória digital. Um dos mais comuns diz respeito à obsolescência de hardware e software, pois a tecnologia vive em constante renovação. Interligado a esse aspecto está a utilização de padrões e formatos de arquivos que permitam o amplo acesso e a assistência técnica efetiva para a conversão dos dados nos padrões atuais. Márdero Arellano (2004, p. 16) corrobora essa

questão quando afirma que “[...] devem ser usados padrões e converterem-se os documentos nos formatos livres, para que eles sejam acessados após a obsolescência dos equipamentos e programas informáticos em que foram criados”. A despeito da existência destes elementos causadores, estes não são considerados capazes de inutilizar e dificultar o prosseguimento das atividades contínuas dos repositórios institucionais.

Outro ponto importante está relacionado à falta de investimento das próprias instituições, que não disponibilizam os recursos necessários para promover a especialização e o domínio técnico dos profissionais que lidam com a preservação da informação digital, dificultando assim a adaptação desses profissionais ao uso das novas ferramentas de tecnologia. No nível operacional destaca-se a importância de avaliar o funcionamento e a atualização dos repositórios, nesse sentido Targino, Coeli e Paiva (2012) apontam para a constatação de problemas na manutenção dos sistemas dos repositórios digitais, apresentando erros internos, links indisponíveis ou até mesmo inexistentes para o acesso ao conteúdo completo do material.

As ameaças consideradas mais significativas para a preservação digital consistem na falta de gerenciamento dos ativos informacionais, como: a ausência de elaboração de normas e manuais estratégicos que orientem quanto ao tratamento de objetos digitais; a falta de políticas de seleção para a preservação da coleção digital e a carência de um controle estatístico com indicadores relevantes para o planejamento, avaliação e gestão do conteúdo armazenado. Essas vulnerabilidades evidenciam “a presença de riscos capazes de causar acréscimo significativo nos custos e esforços despendidos durante o processo de guarda e preservação por estes RI.” (LIMA; LIMA, 2012, p. 11).

As instalações, o acondicionamento e os recursos físicos disponíveis para a conservação dos materiais digitais são indicadores que não se configuram como ameaças expressivas para a preservação e são considerados elementos controláveis nos ambientes dos repositórios institucionais.

O conhecimento desses pontos vulneráveis e da frequência com que eles ocorrem, permite aos gestores anteciparem cuidados e tomarem as providências cabíveis com a preservação e com os custos aplicados durante o processo de armazenamento e acesso de seus acervos informacionais. O exame dessas vulnerabilidades caracteriza uma estratégia relevante na administração das técnicas de preservação digital, conforme a abordagem de Lima e Lima (2012, p. 17)

> Diante destas ameaças, a consciência do perigo se faz cada vez mais necessária, gerando políticas, estratégias e outros instrumentos aplicados a preservação de acervos digitais. Assim, estas medidas surgirão como ferramentas preventivas capazes de reduzir os impactos e consequências dos cenários de acidentes identificados nestes RI.

A preservação de documentos digitais deve adotar políticas e procedimentos documentados que garantam a integridade da informação, disponibilizar o acesso em longo prazo destes documentos para a posteridade, permitir que a informação seja disseminada como reprodução legítima do original e seguir ações imediatas que favoreçam a confiabilidade. Thomaz (2007, p. 88) define que "um repositório digital confiável é mais do que uma organização encarregada de armazenar e administrar objetos digitais".

Um dos atributos dos repositórios digitais confiáveis é a conformidade com o modelo de referência *Open Archival Information System* (OAIS) ou Sistema Aberto para Arquivamento de Informação (SAAI), publicado pelo *Consultive Committee for Space Data Systems*. Outras características como responsabilidade administrativa, sistema de segurança, viabilidade organizacional e adequação financeira completam os requisitos de credibilidade dos arquivos digitais confiáveis. (THOMAZ, 2007). O SAAI é o modelo de preservação de arquivos em longo prazo mais utilizado atualmente. Este modelo deve ser complementado pelas premissas gerais de segurança da informação que devem ser observadas por qualquer organização que se proponha a este tipo de atividade.

4 SEGURANÇA DA INFORMAÇÃO

A informação é um insumo de extrema importância na história da humanidade e precisa ser resguardada. Temos ciência que ela esteve presente em todo o período da evolução histórica, desde os primórdios até os tempos atuais. “Na época em que as informações eram armazenadas apenas em papel, a segurança era relativamente simples. Bastava trancar os documentos em algum lugar e restringir o acesso físico àquele local.” (BRASIL, 2007, p. 7). Com a migração da informação para o suporte digital e sua disponibilização pelas redes de computadores este cenário foi alterado.

A informação é um componente representativo na sociedade do conhecimento, a qual surgiu como resultado do fenômeno conhecido como explosão informacional, distinguida pelo aumento quantitativo e acelerado nos processos de produção e disseminação da informação.

Na atual sociedade da informação, ao mesmo passo em que as informações são caracterizadas como a herança fundamental de uma organização, simultaneamente estão vulneráveis a riscos contínuos e a sofrerem perigosas consequências, como nunca estiveram anteriormente. Dessa forma, a Segurança da Informação (SI) traduz-se como um tema categórico para a sobrevivência das instituições. (BRASIL, 2007).

O recurso informacional é um bem precioso para pessoas, empresas, organizações e instituições, constituindo uma mercadoria indispensável principalmente para o processo de tomada de decisões. Nesse contexto, Sêmola (2003 apud MAIA, 2010) afirma que há uma necessidade imprescindível de assegurar e proteger esses ativos informacionais contra acessos de pessoas não autorizadas, alterações ou usos indevidos, como também sua indisponibilidade.

A NBR ISO/IEC 17799 é uma norma de Tecnologia da Informação e Técnicas de Segurança. A versão original foi publicada em 2002 pela Associação Brasileira de Normas Técnicas – ABNT e revisada em 2005 pela *International Standards Organization* – ISO (Organização Internacional de Padrões) e pela *International Electrotechnical Commission* – IEC (Comissão Eletrotécnica Internacional).

A segurança da informação tem a função de proteger a informação de inúmeras formas de ameaças. Para complementar esse processo de resguarda, a segurança da informação pode ser sistematizada em uma tríade de fundamentos básicos: confidencialidade, integridade e disponibilidade. Conforme destacado na NBR ISO/IEC 17799,

> A segurança da informação é aqui caracterizada pela preservação de: a) confidencialidade: garantia de que a informação é acessível somente por pessoas autorizadas a terem acesso; b) integridade: salvaguarda da exatidão e completeza da informação e dos métodos de processamento; c) disponibilidade: garantia de que os usuários autorizados obtenham acesso à informação e aos ativos correspondentes sempre que necessário. (ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS, 2002, p. 2).

Na visão de Campos (2006, p. 6 apud MAIA, 2010, p. 11-12) define-se que

> O princípio da confidencialidade é respeitado quando apenas as pessoas explicitamente autorizadas podem ter acesso à informação. O princípio da integridade é respeitado quando a informação acessada está completa, sem alterações e, portanto, confiável. O princípio da disponibilidade é respeitado quando a informação está acessível, por pessoas autorizadas, sempre que necessário.

Outros fatores de preservação como responsabilidade, autenticidade e confiabilidade também podem estar presentes e envolvidos no processo da segurança da informação. Um episódio isolado ou uma série de eventos indesejados podem acarretar em incidentes imprevistos para a segurança da informação e apresentam uma ampla probabilidade de ameaça para o sistema, ocasionando o comprometimento da segurança dos dados.

Muitos sistemas de informação e redes de computadores de instituições não foram projetados para serem ambientes seguros. O acesso pode ser comprometido por diversos tipos de ameaças existentes à segurança da informação e os ataques são oriundos de várias fontes como invasão de hackers, fraudes eletrônicas, sabotagens por vírus, vandalismo e até mesmo como alvo de espionagem governamental.

Uma das maneiras de resguardar a informação é a implementação de diferentes medidas de segurança, a mais elementar é o controle de acesso.

4.1 CONTROLES DE ACESSO

Os controles de acesso podem ser físicos ou lógicos. Com o objetivo de controlar o acesso à informação na rede por pessoas não autorizadas, proteger equipamentos, softwares, arquivos de dados e a privacidade de informações pessoais registradas no sistema, bem como resguardar os direitos de propriedade intelectual dos documentos, são implementados um

conjunto de controles de acesso lógico nas instituições que utilizam os recursos da informática para o armazenamento e disseminação das informações.

Nesse sentido, a norma NBR ISO/IEC 17799 recomenda:

> Convém que os requisitos do negócio para controle de acesso sejam definidos e documentados. Convém que as regras de controle de acesso e direitos para cada usuário ou grupo de usuários estejam claramente estabelecidas no documento da política de controle de acesso. Convém que seja dado aos usuários e provedores de serviço um documento contendo claramente os controles de acesso que satisfaçam os requisitos do negócio. (ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS, 2002, p. 28).

Essas práticas e requisitos pretendem garantir que somente usuários autorizados tenham acesso aos recursos disponibilizados e necessários ao seu propósito, que o acesso a recursos cruciais do sistema sejam limitados e bem projetados, que privilégios de acesso sejam bem monitorados e que usuários não autenticados sejam impedidos de executar operações incompatíveis com seu papel.

A partir dessas ações o controle de acesso lógico tenciona dificultar o acesso indevido. "O controle de acesso pode ser traduzido, então, em termos de funções de identificação e autenticação de usuários; alocação, gerência e monitoramento de privilégios; limitação, monitoramento e desabilitação de acessos; e prevenção de acessos não autorizados." (BRASIL, 2007, p. 11).

As condições de segurança são reconhecidas por meio de uma avaliação metódica dos riscos identificados. Os gastos com os controles de acesso lógico precisam ser sistematizados conforme os danos causados à organização motivados pelas possíveis falhas na segurança. Os procedimentos de avaliação dos potenciais perigos podem ser aplicados em toda a unidade ou somente em parte dela, assim como em um sistema de informação isolado.

A abordagem da questão de segurança da informação ocasionará de maneira inevitável o surgimento do assunto dos ambientes de controle de acesso, como explica Sêmola (2006, p. 292 apud MAIA, 2010, p. 15):

> Controle é justamente o ponto de conflito. A todo instante, todos se tornam alvos de mais e mais controles. A propósito, quando se fala de SI, indiretamente está se falando da implantação de controles que reduzem os riscos das empresas em tempo de manuseio, armazenamento, transporte e descarte das informações. O desafio está intimamente relacionado com a dose de controle aplicado aos processos tecnológicos e pessoas. É como se fosse preciso equilibrar uma balança em que em um dos lados estaria a segurança – e consequentemente o controle – e do outro a privacidade.

O gerenciamento de todos esses fatores incide em uma análise da segurança dos ativos informacionais da instituição, levando em consideração os objetivos da segurança da informação (integridade, disponibilidade e confidencialidade) para a implantação de medidas de segurança. “Contudo, é primordial que a organização conheça a sua estrutura, visando identificar nela os ativos de informação e as suas vulnerabilidades para aplicar, assim, as medidas de proteção mais adequadas.” (ANDRADE, 2011, p. 28).

Os controles de acesso em segurança da informação são considerados efetivamente de custo mais baixo e mais eficaz se forem objetos de incorporação nas fases da concepção do projeto e da particularização dos requisitos. Por sua vez, devem ser parte das políticas de segurança da informação.

4.2 POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

Recentemente nos deparamos com ataques de invasão à segurança da informação no nosso país por intermédio dos esquemas de espionagem do governo dos Estados Unidos da América. Uma matéria veiculada pelo jornal eletrônico Folha de São Paulo[4] no mês de agosto de 2013 mostra que a *National Security Agency* (NSA), a Agência de Segurança Nacional dos Estados Unidos é responsável pela vigilância do fluxo de dados na internet e telefonemas dos americanos e de vários cidadãos em todo o mundo, inclusive no Brasil. A rede de monitoramento, que é designada como um dos instrumentos contra ameaças de terrorismo, teria violado as regras de privacidade que protegem as comunicações de milhões de usuários.

Com a difusão de diversas notícias sobre os programas americanos de espionagem e monitoramento das telecomunicações, de acordo com um levantamento realizado pela Folha[5] em meados de julho, a Política de Defesa Cibernética no Brasil dá apenas seus primeiros passos em termos de conteúdos orçamentários. Até o momento, somente 8,9% do total dos recursos reservados para aplicação em segurança da informação foi utilizada no país e nem todas as ações desse percentual foram direcionadas para empreendimentos com relação direta em segurança de redes de informações estratégicas.

[4] Texto na íntegra disponível em: <http://www1.folha.uol.com.br/mundo/2013/08/1329598-vigilancia-da-nsa-abrange-75-do-trafego-de-internet-nos-eua-diz-jornal.shtml>.
[5] Texto na íntegra disponível em: <http://www1.folha.uol.com.br/mundo/2013/07/1310921-brasil-gasta-so-89-do-previsto-com-defesa-cibernetica.shtml>.

É no sentido de prover apoio às metas e princípios da segurança da informação que são estabelecidas as Políticas de Segurança da Informação. Segundo Ferreira e Araújo (2008, p. 36), "a Política de Segurança define o conjunto de normas, métodos e procedimentos utilizados para a manutenção da segurança da informação, devendo ser formalizada e divulgada a todos os usuários que fazem uso dos ativos de informação".

Nessa linha, a política também pode ser definida da seguinte forma:

> Política de segurança de informações é um conjunto de princípios que norteiam a gestão de segurança de informações e que deve ser observado pelo corpo técnico e gerencial e pelos usuários internos e externos. As diretrizes estabelecidas nesta política determinam as linhas mestras que devem ser seguidas pela organização para que sejam assegurados seus recursos computacionais e suas informações. (BRASIL, 2007, p. 26).

Para que a informação não corra riscos de ser acessada por pessoas não autorizadas, as organizações precisam elaborar e implantar uma política de segurança que adote regras e padrões de gerenciamento para viabilizar a proteção adequada aos dados informacionais e aos serviços disponibilizados. A Política de Segurança é uma questão de extrema relevância para qualquer instituição, pois tem em vista garantir a confidencialidade, integridade e disponibilidade das informações armazenadas.

Um fator de suma importância para produzir o efeito desejado na implementação da Política de Segurança da Informação de cada organização é o elemento humano. Ainda que exista toda a sorte de tecnologias da informação dedicadas à proteção dos ativos informacionais, os funcionários precisam participar dos programas de treinamento oferecidos para não por em risco todo o investimento aplicado pela instituição.

> Todos os funcionários da organização, terceiros e prestadores de serviços devem receber treinamento apropriado e atualizações regulares sobre as políticas corporativas. Isso inclui requisitos de segurança, responsabilidades legais e controles do negócio, bem como treinamento sobre o uso correto dos recursos de Tecnologia da Informação como, por exemplo, procedimentos de acesso lógico (redes, sistemas aplicativos, e-mail, Internet) e físico (crachá, salas, andares e ambientes restritos). (FERREIRA; ARAÚJO, 2008, p. 47).

A fim de evitar problemas com relação à violação de privacidade e divulgação de dados sigilosos, a Política de Segurança da Informação deve levar em consideração circunstâncias que forneçam equilíbrio para um bom desenvolvimento dos processos operacionais de segurança da informação.

Nesse contexto, a NBR ISO/IEC 17799 evidencia:

> Convém que sejam mantidos contatos apropriados com autoridades legais, organismos reguladores, provedores de serviço de informação e operadores de telecomunicações, de forma a garantir que ações adequadas e apoio especializado possam ser rapidamente acionados na ocorrência de incidentes de segurança. De forma similar, convém que a filiação a grupos de segurança e a fóruns setoriais seja considerada. Convém que trocas de informações de segurança sejam restritas para garantir que informações confidenciais da organização não sejam passadas para pessoas não autorizadas. (ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS, 2002, p. 6).

Diante do exposto, é necessário seguir metodologias e bases fundamentais para formular e aplicar uma boa Política de Segurança da Informação, reconhecendo e formalizando o nível de acesso para cada camada operacional da organização, de acordo com a utilização dos ativos informacionais atribuídos a cada grau de responsabilidade.

A pesquisa descrita neste documento pode subsidiar as organizações que mantém repositórios digitais na formulação de suas políticas de SI vinculadas a estes ambientes, bem como nos procedimentos executórios necessários para promover os níveis de segurança.

5 PROCEDIMENTOS METODOLÓGICOS

A ferramenta utilizada por qualquer autor para descrever os passos, processos e técnicas utilizados para alcançar os objetivos definidos e obter as informações e os resultados na preparação da sua pesquisa é a metodologia.

Para a elaboração da fundamentação teórica deste trabalho, recorreu-se à pesquisa bibliográfica em livros, artigos científicos, trabalhos acadêmicos de conclusão de curso e dissertações, tanto no suporte físico tradicional quanto em suporte digital. A consulta efetuada para o levantamento teórico expandiu-se com a pesquisa documental em normas técnicas, publicações oficiais, jornais eletrônicos e páginas da internet que contêm registros estatísticos relevantes para subsidiar os estudos sobre o tema abordado.

Esta pesquisa caracteriza-se como descritiva e quantitativa e serão abordadas considerações a respeito dos métodos utilizados para a coleta e análise dos dados. Acerca do conceito de pesquisa descritiva, Gil (2002, p. 42) afirma que:

> As pesquisas descritivas têm como objetivo primordial a descrição das características de determinada população ou fenômeno ou, então, o estabelecimento de relações entre variáveis. São inúmeros os estudos que podem ser classificados sob este título e uma de suas características mais significativas está na utilização de técnicas padronizadas de coleta de dados, tais como o questionário e a observação sistemática.

A abordagem quantitativa apresenta como característica a análise numérica dos dados coletados por meio de procedimentos estatísticos, representados graficamente em tabelas e ilustrações. O universo abrangido pelo estudo são as Universidades Federais do Brasil, composto por 59 (cinquenta e nove) instituições acadêmicas conforme consta no endereço eletrônico do MEC[6], em outubro de 2013. A amostra corresponde a 30 (trinta) universidades federais de todas as regiões do país que possuem Repositórios Digitais de Acesso Aberto em sua esfera acadêmica.

[6] Informações disponíveis em: <http://emec.mec.gov.br/>.

5.1 INSTRUMENTOS DA COLETA DE DADOS

A técnica adotada para a coleta e análise dos dados consistiu na execução de Testes de Penetração nos sistemas dos repositórios, através da ferramenta Netsparker. Esses testes são considerados "instrumentos utilizados com a finalidade de obter dados que permitam medir o rendimento, a frequência, a capacidade ou a conduta de indivíduos [ou organismos], de forma quantitativa". (MARKONI; LAKATOS, 2003, p. 223).

O Netsparker é um software de escaneamento de segurança que executa *Penetration Test* (Teste de Penetração) em sites e detecta automaticamente as falhas que poderiam deixá-los perigosamente expostos. Segundo Assunção (2010, p. 93), "um dos ataques mais comuns hoje é a injeção de comandos SQL (Structured Query Language)".

A ferramenta Netsparker está apta a identificar muitas vulnerabilidades de segurança da Web no decorrer da varredura do sistema, sendo capaz de explorar habilmente as falhas de injeção de comandos SQL em diferentes bancos de dados com alta precisão. O programa oferece suporte completo para diversas aplicações e possui uma interface de usuário intuitiva, com um procedimento de digitalização de início rápido.

O Teste de Penetração permite identificar potenciais vazamentos de informação que podem prejudicar uma organização ou empresa, e compreende fases que abrangem desde uma abertura na segurança por um ataque externo e/ou interno até o acesso indevido a dados confidenciais não autorizados, eventos que podem causar danos irreparáveis aos sistemas. Conforme Assunção (2010, p. 55), "o objetivo deste teste é atacar/tentar invadir um sistema, rede ou ambiente no qual se deseja detectar falhas".

Os testes foram realizados em laboratório na Universidade Federal da Paraíba, no período de 18/06/2013 a 16/07/2013. A relação dos repositórios digitais federais pode ser encontrada no diretório do IBICT[7]. As imagens referentes aos testes realizados podem ser verificadas nos Anexos.

[7] Disponível em: <http://diretorio.ibict.br/handle/1/4/browse?type=title&submit_browse=Title>.

6 DESENVOLVIMENTO DA ANÁLISE DE RISCO DOS REPOSITÓRIOS

Algumas dificuldades foram identificadas no decorrer da fase dos testes de vulnerabilidades dos repositórios digitais, as quais são relatadas a seguir:

- Os endereços dos repositórios da UFAC, UFF, UFJF e UNIFESP apresentaram falha no carregamento da página e não foi possível ter acesso ao seu conteúdo, o que impossibilitou a execução do teste;
- O repositório da UFPE exibiu um endereço não localizado e também não foi possível testar seu desempenho;
- Nos repositórios da UFAL, UFGD, UFRGS, UFVJM e UFV os testes de vulnerabilidade não foram concluídos, pois em determinado ponto a velocidade de escaneamento chegava a zero e o andamento da varredura era prejudicado até cessar por completo;
- Houve a necessidade de refazer a análise de risco do repositório da UNB devido a uma divergência na verificação dos resultados. O primeiro teste foi realizado em 19/06/2013 e o segundo em 12/08/2013.

Portanto, das 30 (trinta) instituições federais consideradas na amostra, apenas 20 (vinte) foram analisadas com sucesso, o que corresponde a aproximadamente 67% dos repositórios digitais testados. O quadro 1 apresenta o histórico do desenvolvimento da análise de risco dos repositórios institucionais federais:

Quadro 1: Histórico da análise de risco dos Repositórios Institucionais Federais, 2013.

Nº	Instituições	Repositório	Data de consulta	Tempo de escaneamento
1	UFAC	http://repositorios.ufac.br:8080/repositorio/	Sem acesso	
2	UFAL	http://www.repositorio.ufal.br/	Teste não concluído	
3	UFBA	https://repositorio.ufba.br/ri/	23/06/2013	54min
4	UnB	http://repositorio.bce.unb.br/	12/08/2013	1h33min
5	UFC	http://www.repositorio.ufc.br:8080/ri/	28/06/2013	1h04min
6	UFES	http://repositorio.ufes.br/	27/06/2013	1h20min

7	UFF	http://repositorio.uff.br/jspui/	Sem acesso	
8	UFG	http://repositorio.bc.ufg.br/	28/06/2013	57min
9	UFGD	http://www.ufgd.edu.br:8080/jspui/	Teste não concluído	
10	UFJF	http://repositorio.ufjf.br:8080/jspui/	Sem acesso	
11	UFLA	http://repositorio.ufla.br/	10/07/2013	3h04min
12	UFMA	http://www.repositorio.ufma.br:8080/jspui/	26/06/2013	2h52min
13	UFMS	http://repositorio.cbc.ufms.br:8080/jspui/	15/07/2013	1h31min
14	UFMG	https://dspaceprod02.grude.ufmg.br/dspace/	18/06/2013	12min
15	UFOP	http://www.repositorio.ufop.br/	30/06/2013	1h29min
16	UFPA	http://repositorio.ufpa.br/jspui/	27/06/2013	2h09min
17	UFPB	http://rei.biblioteca.ufpb.br/jspui/	22/06/2013	2h24min
18	UFPR	http://dspace.c3sl.ufpr.br:8080/dspace/	30/06/2013	5h45min
19	UFPEL	http://guaiaca.ufpel.edu.br:8080/jspui/	16/07/2013	3h25min
20	UFPE	http://www.repositorios.ufpe.br/jspui/	Não localizado	
21	FURG	http://repositorio.furg.br:8080/jspui/	01/07/2013	2h03min
22	UFRGS	http://www.lume.ufrgs.br/	Teste não concluído	
23	UFRN	http://repositorio.ufrn.br:8080/jspui/	18/06/2013	1h36min
24	UFSC	http://repositorio.ufsc.br/	18/06/2013	3h38min
25	UFSCAR	http://livresaber.sead.ufscar.br:8080/jspui/	06/07/2013	2h18min
26	UNIFESP	http://200.133.202.157:8080/jspui/	Sem acesso	
27	UFS	https://ri.ufs.br/	08/07/2013	1h34min
28	UFU	http://repositorio.ufu.br/	08/07/2013	2h20min
29	UFVJM	http://acervo.ufvjm.edu.br:8080/jspui/	Teste não concluído	
30	UFV	http://riserver.cpd.ufv.br:8080/repositorio/	Teste não concluído	

Fonte: Dados da pesquisa, 2013.

Como qualquer base de dados, os repositórios digitais estão vulneráveis a diversos tipos de ameaças. Essas vulnerabilidades podem colocar em risco seu funcionamento e expor o repositório a ataques externos. Utilizamos a ferramenta de análise de segurança para testar os repositórios institucionais federais com o intuito de detectar e identificar falhas que podem expor perigosamente o sistema a ataques.

Os problemas apontados nas verificações de segurança dos repositórios digitais são distribuídos por tipos de vulnerabilidades e estão classificados em 5 (cinco) níveis de risco:

crítico, alto, médio, baixo e alertas. O quadro 2 indica o quantitativo dos níveis de riscos encontrados nas instituições testadas.

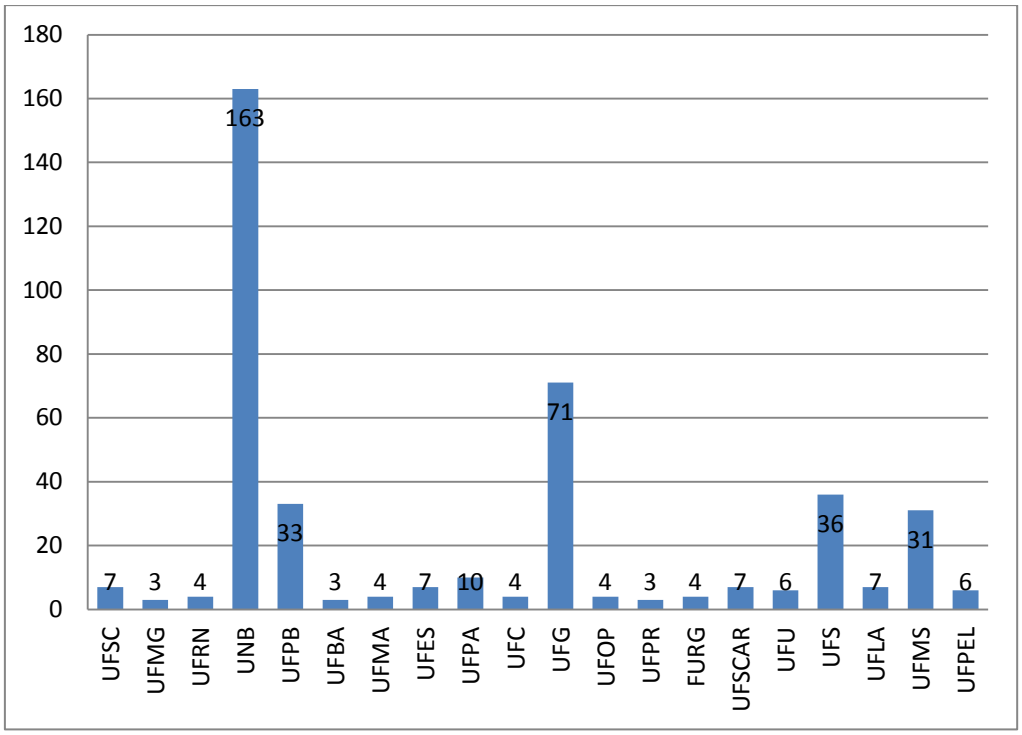
Quadro 2: Níveis de riscos identificados nos Repositórios Institucionais Federais, 2013.

Instituições	Crítico	Alto	Médio	Baixo	Alertas
UFSC	0	1	0	6	36
UFMG	0	0	2	1	1
UFRN	0	1	0	3	15
UNB	1	151	8	3	5
UFPB	0	1	30	2	29
UFBA	0	0	0	3	3
UFMA	0	1	0	3	40
UFES	0	1	0	6	6
UFPA	0	5	1	4	3
UFC	0	1	0	3	2
UFG	0	33	35	3	32
UFOP	0	1	0	3	19
UFPR	0	0	0	3	17
FURG	0	1	0	3	25
UFSCAR	0	2	0	5	29
UFU	0	2	0	4	29
UFS	0	30	0	6	13
UFLA	0	1	0	6	24
UFMS	0	28	0	3	27
UFPEL	0	1	0	5	6

Fonte: Dados da pesquisa, 2013.

Para ilustrar o quadro 2 e facilitar a visualização numérica dos riscos detectados, representamos graficamente o quantitativo dos riscos identificados na análise dos repositórios. A figura 4 apresenta o somatório dos níveis de riscos verificados nos testes, desconsiderando os alertas.

Figura 4 – Quantidade de riscos nos repositórios institucionais federais, 2013.



Fonte: Dados da pesquisa, 2013.

Como exposto anteriormente, os riscos são divididos nos níveis: crítico, alto, médio, baixo e alerta. Para efeito de análise de conceitos serão desconsiderados os alertas. A única vulnerabilidade de risco crítico encontrada foi:

- *Boolean Based SQL Injection* – a injeção SQL ocorre quando a entrada de dados, por exemplo, um usuário, é interpretado como um comando SQL, em vez de dados normais. Essa é uma vulnerabilidade muito comum e a sua exploração bem sucedida pode ter implicações importantes. A vulnerabilidade foi confirmada por meio da execução de um teste de consultas SQL no banco de dados. Nesses testes, o SQL Injection não era óbvio, mas as diferentes respostas da página com base no teste de injeção permitiu identificar e confirmar o SQL Injection.

Sobre a injeção de comandos SQL, Assunção (2010, p. 93) explica:

> Esse tipo de falha não é do servidor do banco de dados e, sim, de um programa feito para interagir com esse banco. Seja ASP, PHP, JSP ou qualquer outro tipo de programação para a Web, se o programa não

> interpretar corretamente certos caracteres como barra (/) e aspas simples (‘), eles podem ser usados para “injetar” comandos naquele sistema, burlando sistemas de login e senha, fornecendo acesso completo ao banco de dados muitas vezes.

A análise de segurança detectou os seguintes tipos de vulnerabilidades de alto risco:

- *Password Transmitted over HTTP* – identifica que dados de senha são enviados através de HTTP. Um atacante acessando o site do repositório pode realizar uma invasão para capturar a senha do usuário.

- *Cross-site Scripting (XSS)* – permite a um invasor executar um script dinâmico no contexto da aplicação. Isso dá lugar a variadas e diferentes oportunidades de ataque, principalmente o sequestro da sessão atual do usuário ou alteração da aparência da página, modificando o código HTML na hora de roubar as credenciais do usuário. XSS tem como alvo os usuários do aplicativo em vez do servidor. Embora esta seja uma limitação, uma vez que permite que atacantes sequestrem a sessão de outros usuários, um invasor pode atacar um administrador para obter o controle total sobre a aplicação.

- *SVN Detected* – detecta arquivos divulgados pelo código de sistemas de controle de versão de origem, como CVS, GIT e SVN. Um invasor pode explorar este problema para ter acesso ao código-fonte da aplicação, ou pode recuperar a configuração e/ou outros arquivos importantes.

- *Cookie Not Marked as Secure* – identificou um cookie não marcado como seguro e transmitido através de HTTPS. Isso significa que o cookie poderia ser roubado por um invasor que pode interceptar e decifrar com sucesso o tráfego, ou após um bem sucedido ataque *man-in-the-middle* (homem no meio). Nesse tipo de ataque, o computador do invasor age como um servidor para o usuário, capturando e descriptografando os dados através de uma chave privada de certificado, tornando a criptografá-los e enviando-os para o servidor remoto no papel de cliente. (ASSUNÇÃO, 2010).

As vulnerabilidades de risco médio identificadas foram:

- *HTTP Header Injection* – detecta problemas de injeção de cabeçalho em aplicações web que podem causar sérios problemas. O mais comum deles são Cross-site Scripting e sequestro de sessão, tomando a forma de ataques de fixação de sessão.

- *Insecure Transportation Security Protocol Supported (SSLv2)* – detecta que o servidor web está configurado para suportar a comunicação segura através de um protocolo de transporte inseguro (SSLv2), que possui várias falhas. O tráfego seguro do site pode ser observado quando foi estabelecido sobre este protocolo. Os atacantes podem realizar ataques e observar o tráfego de criptografia entre o site e os visitantes.

- *Weak Ciphers Enabled* – detecta que o servidor web está configurado para permitir o uso de cifras fracas durante a comunicação segura (SSL). Invasores podem montar ataques de força bruta para decifrar a comunicação segura entre o servidor e os visitantes.

- *Invalid SSL Certificate* – verifica que o servidor web utiliza um certificado SSL inválido. Um certificado SSL pode ser criado e assinado por qualquer um. É necessário ter um certificado SSL válido para fazer com que os visitantes tenham certeza sobre a comunicação segura entre o site e eles. Se o site tiver um certificado inválido, os visitantes vão ter dificuldade em distinguir entre seu certificado e os de atacantes.

Os tipos de vulnerabilidades de baixo risco encontrados foram:

- *Cookie Not Marked as HttpOnly* – relata que um cookie não foi marcado como HTTPOnly. Cookies HTTPOnly não podem ser lidos pelos scripts do lado do usuário, portanto, marcar um cookie como HTTPOnly pode fornecer uma camada adicional de proteção contra ataques de Cross-site Scripting.

- *Internal Server Error* – O servidor respondeu com um status HTTP 500. Isto indica que há um erro do servidor. As razões podem variar, o comportamento deve ser cuidadosamente analisado.

- *Auto Complete Enabled* – a função Auto Completar foi ativada em um ou mais campos de formulário sensíveis, como senhas. Os dados inseridos nesses campos serão armazenados em cache pelo navegador. Um invasor que pode acessar o computador da vítima poderia roubar esta informação. Isto é especialmente importante se o aplicativo é comumente usado em computadores públicos.

- *Version Disclosure (Apache)* – identifica uma versão divulgação (Apache), em resposta HTTP do servidor web de destino. Essas informações podem ajudar a um atacante obter uma maior compreensão dos sistemas em uso e, potencialmente, desenvolver novos ataques direcionados a versão específica do Apache.

- *Version Disclosure (Apache Coyote)* – determina que o servidor web de destino está divulgando a versão Coyote Apache em sua resposta HTTP. Um atacante pode usar as informações divulgadas para colher as vulnerabilidades de segurança específicas para a versão identificada.

- *Version Disclosure (Tomcat)* – identifica que o servidor web alvo está divulgando a versão Tomcat em sua resposta HTTP. Essas informações podem ajudar a um atacante obter uma maior compreensão dos sistemas em uso e, potencialmente, desenvolver novos ataques direcionados à versão específica do Tomcat.

- *Exception Report Disclosure (Tomcat)* – determina que o servidor web alvo está divulgando os dados do relatório de exceção na resposta HTTP. Um atacante pode obter informações como o caminho de arquivo físico dos arquivos do Tomcat e se concentrar potencialmente no desenvolvimento de novos ataques ao sistema de destino.

- *Social Security Number Disclosure* – identifica Números de Segurança Social (SSN) no site. Números de Segurança Social tem sido usados por atacantes no roubo de identidade já que muitas organizações, incluindo empresas, agências governamentais,

hospitais e instituições de ensino utilizam o SSN como o identificador primário para os seus sistemas de manutenção de registros.

As definições apresentadas anteriormente são traduções dos manuais do software Netsparker e estão em conformidade com iniciativas criadas por organizações que se empenham em classificar as vulnerabilidades encontradas nos sistemas e que podem prejudicar a segurança da informação. O quadro 3 indica a relação das classificações descobertas:

Quadro 3: Relação de organizações que monitoram e classificam os tipos de vulnerabilidades em sistemas na Web, 2013.

Organização	Relação
PCI – *Payment Card Industry*	Apresenta um Padrão de Segurança de Dados, com requisitos e procedimentos de avaliação de segurança.
OWASP – *Open Web Application Security Project* (Projeto de Segurança de Aplicações Web Abertas)	Comunidade aberta dedicada a capacitar as organizações para conceber, desenvolver, adquirir, operar e manter aplicações que podem ser confiáveis.
CWE – *Common Weakness Enumeration* (Enumeração de Fraquezas Comuns)	Lista os tipos de fraquezas de software desenvolvidas por iniciativas da comunidade voltada para desenvolvedores e profissionais de segurança.
CAPEC – *Common Attack Pattern Enumeration and Classification* (Ataque Comum Padrão de Enumeração e Classificação)	A comunidade disponibiliza fontes de conhecimento para a construção de um software seguro.
WASC – *Web Application Security Consortium* (Consórcio de Segurança de Aplicações Web)	Esforço cooperativo para esclarecer e organizar as ameaças à segurança de uma página na Internet.

Fonte: Dados da pesquisa, 2013.

O quadro 4 apresenta os tipos de vulnerabilidades detectados nos ambientes computacionais dos repositórios analisados, separados por níveis de risco.

Quadro 4: Tipos de vulnerabilidades identificados nos Repositórios Institucionais Federais, 2013.

Nível	Tipo de vulnerabilidade	R1	R2	R3	R4	R5	R6	R7	R8	R9	R10	R11	R12	R13	R14	R15	R16	R17	R18	R19	R20
Crítico	Boolean Based SQL Injection				1																
Alto	Password Transmitted over HTTP	1		1	1	1		1	1	1	1	1	1		1	1	1		1	1	1
	XSS (Cross-site Scripting)				150					4		32				1	1	28		27	
	SVN Detected																	1			
	Cookie Not Marked as Secure																	1			
Médio	HTTP Header Injection				8	30						35									
	Insecure Transportation Security Protocol Supported (SSLv2)		1																		
	Weak Ciphers Enabled		1																		
	Invalid SSL Certificate									1											
Baixo	Cookie Not Marked as HttpOnly	1	1		1				1					1		1	1	1	1		1
	Internal Server Error	1		1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
	Auto Complete Enabled	1		1	1	1	1	1	1	1	1	1	1		1	1	1	1	1	1	1
	Version Disclosure (Apache)																	1			
	Version Disclosure (Apache Coyote)	1		1			1	1	1	1	1		1	1	1	1		1	1	1	1
	Version Disclosure (Tomcat)	1							1			1				1	1	1	1		1
	Exception Report Disclosure (Tomcat)	1							1										1		
	Social Security Number Disclosure									1											

Fonte: Dados da pesquisa, 2013.

7 RECOMENDAÇÕES PARA A SEGURANÇA

Estar seguro é uma necessidade, reforçada quando se trabalha no mundo tecnológico. É importante definir medidas que promovam a proteção e permitam o funcionamento eficaz dos serviços prestados em caso de comprometimento do sistema ocasionado pelas falhas na segurança.

Para proteger os ativos informacionais de uma instituição é necessário combinar ações preventivas e de recuperação, que consistem em um conjunto de técnicas e procedimentos que devem ser adotados para a segurança digital. “Essas estratégias e procedimentos deverão minimizar o impacto sofrido diante do acontecimento de situações inesperadas, desastres, falhas de segurança, entre outras, até que se retorne à normalidade.” (BRASIL, 2007, p. 33).

As normas e ferramentas de análise de segurança indicam procedimentos e oferecem informações para incrementar as medidas de segurança. Por exemplo, um método firme para atenuar a ameaça de vulnerabilidades baseadas em injeções de comando SQL é a utilização de consultas parametrizadas para a filtragem dos caracteres digitados, impedindo a inserção de comandos pelo invasor nos scripts dos programas.

Outra recomendação seria para evitar que senhas de usuários sejam capturadas: todos os dados sensíveis devem ser transferidos via HTTPS em vez de HTTP. Os formulários devem ser servidos por HTTPS e todos os aspectos da aplicação que aceitam entrada do usuário a partir do processo de login só devem ser fornecidos por HTTPS.

Para impedir ataques XSS é altamente recomendado o uso de uma biblioteca de codificação, pois a mesma é de grande complexidade. Dessa forma evita-se que atacantes utilizem essa técnica para obter acesso aos cookies de usuários sem autorização, através do navegador.

Ameaças sempre vão existir e falhas sempre vão ocorrer, independente dos recursos investidos em software, hardware e pessoal capacitado. Executar Testes de Penetração, bem como efetuar a varredura do sistema com scanners de vulnerabilidades e realizar pesquisas manuais são recomendações bastante úteis para prevenção e correção dos problemas apontados. (ASSUNÇÃO, 2010).

A implementação de uma política de segurança, o uso de controles de acesso aos recursos de processamento e a aplicação de tecnologias voltadas para a segurança de serviços de redes de computadores como autenticação, certificados de segurança válidos, encriptação de dados, dentre outros, são medidas que restringem o acesso a quem de direito e tornam o

ambiente menos suscetível a invasões. Também é indispensável o uso de softwares como antivírus, firewall e monitoradores do sistema, que auxiliam na segurança.

8 CONSIDERAÇÕES FINAIS

O campo da informática vive em constante evolução. Os sistemas digitais estão vulneráveis a todo tipo de riscos, sejam eles desastres naturais, acidentes ou ataques intencionais, o que resulta no acontecimento de situações imprevistas. As falhas na segurança podem causar impactos inesperados nas redes de computadores de uma instituição, e os resultados dessas lacunas abrangem desde ocorrências de baixa relevância até fatos de consequências calamitosas para a organização.

A partir do levantamento teórico realizado ficou evidente a importância que tem a informação nos dias atuais, seja em suporte físico ou digital, como também o valor da preservação da mesma. Com a disponibilidade e utilização das ferramentas tecnológicas, a informação é transmitida com muito mais facilidade e presteza por todo o mundo. O processamento instantâneo da informação por meio da Internet promoveu sua difusão em larga escala. Desse modo, os dados informacionais passaram a apresentar uma maior necessidade de segurança para sua salvaguarda, independente do suporte utilizado.

Nesta pesquisa foram distinguidos aspectos essenciais da segurança da informação, as vulnerabilidades mais comuns e as medidas adotadas para uma melhor segurança dos dados, bem como os resultados da aplicabilidade dos testes nos sistemas gerenciadores dos repositórios digitais.

Para que seja efetuada a prestação de bons serviços em ambientes informatizados é indispensável a aplicação de boas práticas para segurança da informação, visando a proteção do patrimônio intelectual da estrutura organizacional. Para tanto, é essencial a colaboração de todos que interagem com o sistema, englobando profissionais da área, gestores, funcionários e usuários.

A elaboração e implementação de uma Política de Segurança e o uso dos controles de acesso (físicos e lógicos) são procedimentos que, integrados, possibilitam a execução apropriada e efetiva da tríade de elementos que compõem o alicerce básico da segurança informacional: a confidencialidade, a integridade e a disponibilidade.

Todo e qualquer sistema de computadores está sujeito a riscos e vulnerabilidades. Portanto, é imprescindível a aplicação de um conjunto de medidas de segurança que visem minimizar ataques que porventura aconteçam. Os recursos informacionais precisam estar devidamente protegidos, a fim de evitar o acesso indevido das informações privilegiadas e o uso impróprio das mesmas por pessoas não autorizadas.

Conforme a análise dos dados, as aplicações dos Testes de Penetração permitiram uma apreciação pormenorizada das ameaças concernentes à segurança dos ativos informacionais, quantificando e denominando os riscos encontrados, assim como possibilitou diferenciar os elementos causadores das falhas e apontou a adoção de técnicas e procedimentos adequados que podem contribuir para a preservação dos dados digitais.

Considerando os resultados alcançados na pesquisa, pode-se concluir que o desempenho dos repositórios digitais das IES federais ainda não está completamente satisfatório em relação à Segurança da Informação. Como apresentado no desenvolvimento do trabalho, no quesito correspondente ao acesso das informações dos usuários, 80% dos repositórios testados está exposto à vulnerabilidade de alto risco *Password Transmitted over HTTP*, ou seja, a recuperação da senha pessoal por meio de ataques. E no que diz respeito às vulnerabilidades de baixo risco, os destaques se concentram no item de Erro Interno do Servidor, encontrado em 95% dos testes e na função de Auto Completar, responsável por facilitar a recuperação de informações sigilosas em 90% dos repositórios.

Por fim, convém evidenciar a relevância da aplicação das práticas de segurança recomendadas pelas normas vigentes e por profissionais qualificados, com o intuito de suprir necessidades básicas para a preservação dos dados e diminuir a suscetibilidade de invasão ou quaisquer outros tipos de ameaças a que estão expostos os repositórios digitais de uma instituição.

REFERÊNCIAS

ANDRADE. Rayssa Lara Oliveira de. **A biblioteca 2.0 sob a ótica da gestão da segurança da informação:** um estudo de caso com a Biblioteca Nacional de Brasília. 2011. 83 f. Trabalho de Conclusão de Curso (Graduação em Biblioteconomia)–Universidade Federal do Rio Grande do Norte, Natal, 2011. Disponível em: <http://repositorio.ufrn.br:8080/monografias/handle/1/85>. Acesso em: 25 ago 2013.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **NBR ISO/IEC 17799:** Tecnologia da informação: código de prática para a gestão da segurança da informação. Rio de Janeiro, 2002.

ASSUNÇÃO, Marcos Flávio Araújo. **Segredos do hacker ético**. 3. ed. Florianópolis: Visual Books, 2010.

BRASIL. Tribunal de Contas da União. **Boas práticas em segurança da informação.** 2. ed. Brasília, DF, 2007. Disponível em: <http://portal2.tcu.gov.br/portal/pls/portal/docs/2059162.PDF>. Acesso em: 24 ago. 2013.

CAPEC. Common Attack Pattern Enumeration and Classification. Disponível em: <http://capec.mitre.org/index.html>. Acesso em: 28 out. 2013.

CWE. Common Weakness Enumeration. Disponível em: <http://cwe.mitre.org/about/index.html>. Acesso em: 28 out. 2013.

FACHIN, Geisy Regina Bories, et al. Gestão do conhecimento e a visão cognitiva dos repositórios institucionais. **Perspectivas em Ciência da Informação**, Belo Horizonte, v. 14, n. 2, p. 220-236, maio./ago. 2009. Disponível em: <http://www.scielo.br/pdf/pci/v14n2/v14n2a15.pdf>. Acesso em: 15 maio 2013.

FERREIRA, Fernando Nicolau Freitas; ARAÚJO, Márcio Tadeu de. **Política de Segurança da Informação**: guia prático para elaboração e implementação. 2. ed. Rio de Janeiro: Editora Ciência Moderna, 2008. Inclui CD-ROM.

GIL, Antonio Carlos. **Como elaborar projetos de pesquisa**. 4. ed. São Paulo: Editora Atlas, 2002.

KURAMOTO, Hélio. Informação científica: proposta de um novo modelo para o Brasil. **Ciência da Informação**, Brasília, v. 35, n. 2, p. 91-102, maio/ago. 2006. Disponível em: <http://www.scielo.br/pdf/ci/v35n2/a10v35n2.pdf>. Acesso em: 09 maio 2013.

KURAMOTO, Hélio. Réplica - Acesso Livre: caminho para maximizar a visibilidade da pesquisa. **RAC**, Curitiba, v. 12, n. 3, p. 861-872, jul./set. 2008. Disponível em: <http://www.scielo.br/pdf/rac/v12n3/13.pdf>. Acesso em: 09 maio 2013.

LEITE, Fernando César Lima; MÁRDERO ARELLANO, Miguel Angel; MORENO, Fernanda Passini. Acesso livre a publicações e repositórios digitais em ciência da informação no Brasil. **Perspectivas em Ciência da Informação**, Belo Horizonte, v. 11, n. 1, p. 82-94, jan./abr. 2006. Disponível em: <http://repositorio.unb.br/bitstream/10482/623/1/ARTIGO_AcessoLivrePublicacoes.pdf>. Acesso em: 11 maio 2013.

LIMA, Fanny do Couto Ribeiro de; LIMA, Marcos Galindo de. Preservação digital da informação científica: uma análise de risco em repositórios institucionais brasileiros. In: ENCONTRO NACIONAL DE PESQUISA EM CIÊNCIA DA INFORMAÇÃO, 13., 2012, Rio de Janeiro. **Anais eletrônicos...** Disponível em: <http://www.eventosecongressos.com.br/metodo/enancib2012/arearestrita/pdfs/19495.pdf>. Acesso em: 01 jun. 2013.

MAIA, Ana Maria Rocha. **Segurança da informação:** estudo para implantação do arquivo da Seplan. 2010. 57 f. Trabalho de Conclusão de Curso (Graduação em Biblioteconomia)– Universidade Federal do Rio Grande do Norte, Natal, 2010. Disponível em: <http://repositorio.ufrn.br:8080/monografias/handle/1/178>. Acesso em 24 ago. 2013.

MARCONI, Marina de Andrade; LAKATOS, Eva Maria. **Fundamentos de metodologia científica**. 5. ed. São Paulo: Editora Atlas, 2003.

MÁRDERO ARELLANO, Miguel Angel. Preservação de documentos digitais. **Ciência da Informação**, Brasília, v.33, n.2, p. 15-27, maio/ago. 2004. Disponível em: <http://www.scielo.br/pdf/ci/v33n2/a02v33n2.pdf>. Acesso em: 10 maio 2013.

MÁRDERO ARELLANO, Miguel Angel; LEITE, Fernando César Lima. Acesso aberto à informação científica e o problema da preservação digital. **Biblios**, Brasília, n. 35, mar./jun. 2009. Disponível em: <http://repositorio.unb.br/handle/10482/4937>. Acesso em: 11 maio 2013.

OLIVEIRA, Renan Rodrigues de; CARVALHO, Cedric Luiz de. **Bibliotecas Digitais e o Repositório Fedora**. Instituto de Informática. Universidade Federal de Goiás, 2011. Disponível em: <http://www.inf.ufg.br/sites/default/files/uploads/relatorios-tecnicos/RT-INF_002-11.pdf>. Acesso em: 19 maio 2013.

OPEN SOCIETY INSTITUTE. **A Guide to Institutional Repository Software**. 3. ed. New York, NY, 2004. 28p. Disponível em: <http://www.budapestopenaccessinitiative.org/pdf/OSI_Guide_to_IR_Software_v3.pdf>. Acesso em: 18 maio 2013.

OWASP. Open Web Application Security Project. Disponível em: <https://www.owasp.org/index.php/Main_Page>. Acesso em: 28 out. 2013.

PCI. Payment Card Industry. Disponível em: <https://www.pcisecuritystandards.org/documents/pci_dss_v2.pdf>. Acesso em: 28 out. 2013.

RIBEIRO, O. B ; VIDOTTI, S. A. B. G. Otimização do acesso à informação científica: discussão sobre a aplicação de elementos da arquitetura da informação em repositórios digitais. **Biblos**, Rio Grande, v. 23, n. 2, p. 105-116, 2009. Disponível em: <http://www.seer.furg.br/biblos/article/view/1309/593>. Acesso em: 10 maio 2013.

SANTOS JUNIOR, Ernani Rufino dos. **Repositórios institucionais de acesso livre no Brasil:** estudo Delfos. 2010. 182 f. Dissertação (Mestrado em Ciência da Informação)–Faculdade de Ciência da Informação, Universidade de Brasília, Brasília, 2010. Disponível em: <http://repositorio.unb.br/bitstream/10482/5343/6/2010_ErnaniRufinodosSantosJunior.pdf>. Acesso em: 18 maio 2013.

TARGINO, Maria das Graças; GARCIA, Joana Coeli Ribeiro; PAIVA, Maria José Rodrigues. Repositórios institucionais brasileiros: entre o sonho e a realidade. In: CONFERENCIA INTERNACIONAL ACCESO ABIERTO, COMUNICACIÓN CIENTÍFICA Y PRESERVACIÓN DIGITAL, 1., 2012, Barranquilla, Colombia. **Anais Eletrônicos...** Disponível em: <http://eventos.uninorte.edu.co/index.php/biredial/biredial2012/paper/view/360>. Acesso em: 02 jun. 2013.

THOMAZ, Kátia P. Repositórios digitais confiáveis e certificação. **Arquivística.net**, Rio de Janeiro, v. 3, n. 1, p. 80-89, jan./jun. 2007. Disponível em: <http://www.brapci.ufpr.br/documento.php?dd0=0000004775&dd1=ac3d4>. Acesso em: 03 jun. 2013.

VIANA, Cassandra Lúcia de Maya; MÁRDERO ARELLANO, Miguel Angel. *Repositórios institucionais baseados em DSpace e EPrints e sua viabilidade nas instituições acadêmico-científicas*. In: SEMINÁRIO NACIONAL DE BIBLIOTECAS UNIVERSITÁRIAS, 14., 2006, Salvador. **Anais eletrônicos...** Disponível em: <http://eprints.rclis.org/8834/>. Acesso em: 13 maio 2013.

VIANA, Cassandra Lúcia de Maya; MÁRDERO ARELLANO, Miguel Angel; SHINTAKU, Milton. *Repositórios institucionais em ciência e tecnologia: uma experiência de customizacão do DSpace*. In: SIMPOSIO INTERNACIONAL DE BIBLIOTECAS DIGITAIS, 3., 2005, São Paulo. **Anais eletrônicos...** Disponível em: <http://eprints.rclis.org/7168/>. Acesso em: 12 maio 2013.

WASC. Web Application Security Consortium. Disponível em: <http://projects.webappsec.org/w/page/13246927/FrontPage>. Acesso em: 28 out. 2013.

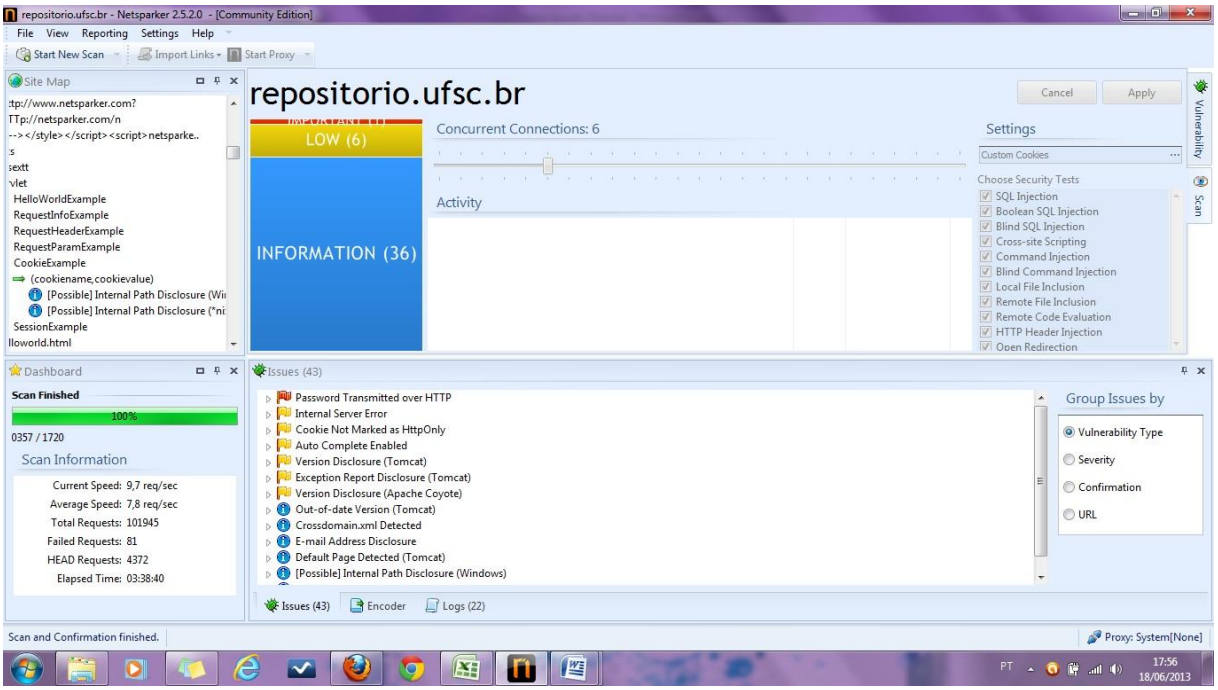
WEITZEL, Simone da Rocha. Iniciativa de arquivos abertos como nova forma de comunicação científica. In: SEMINÁRIO INTERNACIONAL LATINO-AMERICANO DE PESQUISA EM COMUNICAÇÃO, 3., 2005, São Paulo. **Anais eletrônicos...** Disponível em: <http://eprints.rclis.org/6492/>. Acesso em: 12 maio 2013.

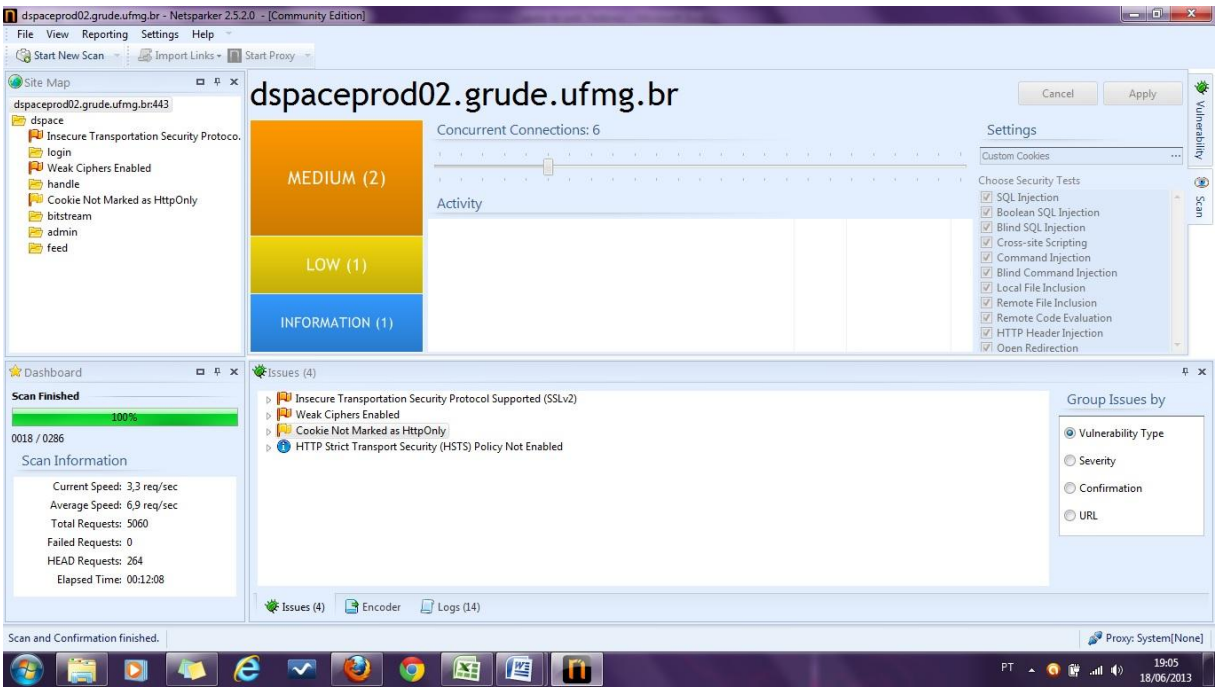
WEITZEL, Simone da Rocha. O papel dos repositórios institucionais e temáticos na estrutura da produção científica. **Em Questão**, Porto Alegre, v. 12, n. 1, p. 51-71, jan./jun. 2006. Disponível em: <http://seer.ufrgs.br/EmQuestao/article/view/19/7>. Acesso em: 14 maio 2013.

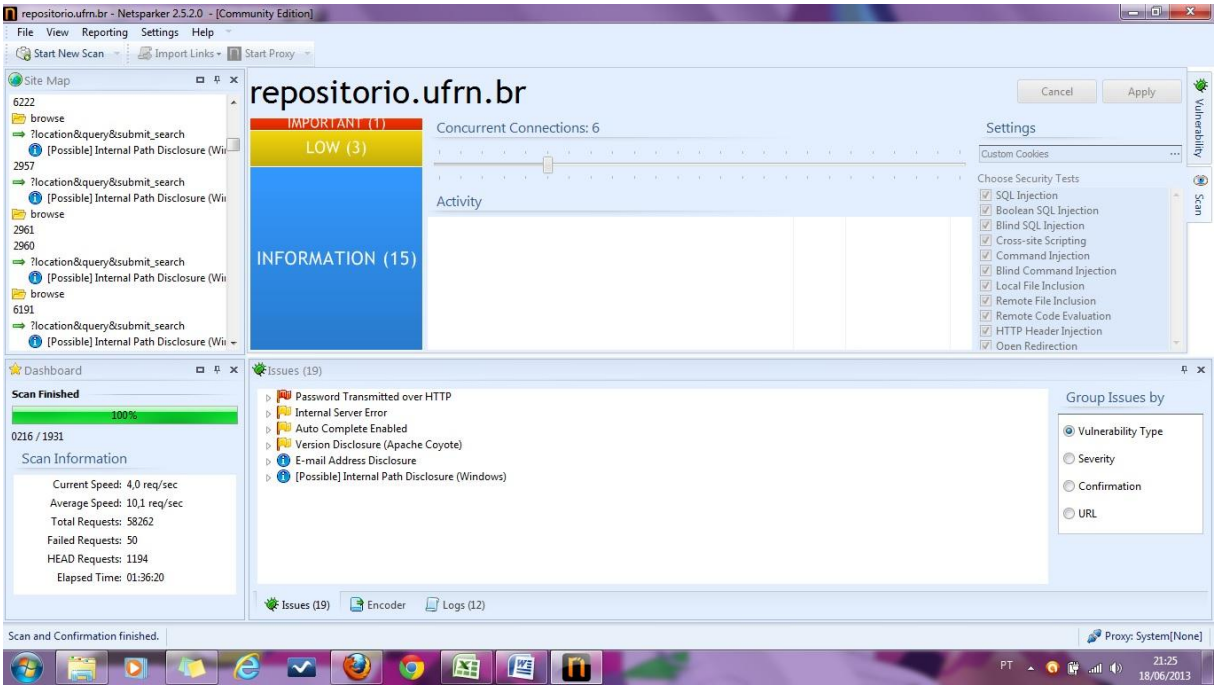
WEITZEL, Simone da Rocha. Reflexões sobre os repositórios institucionais. In: CONGRESSO BRASILEIRO DE CIÊNCIAS DA COMUNICAÇÃO, 29., 2006, Brasília. **Anais eletrônicos...** Disponível em: <http://eprints.rclis.org/8744/1/reflexoes_weitzel_endocom.pdf>. Acesso em: 15 maio 2013.

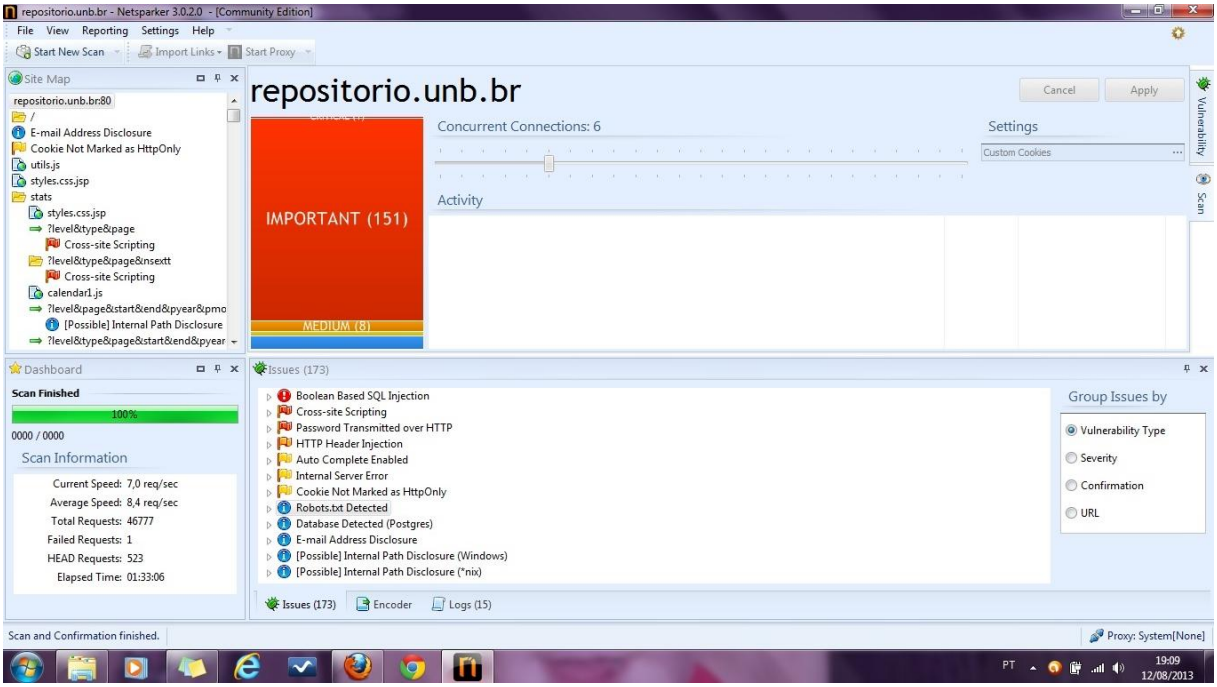
ANEXOS I

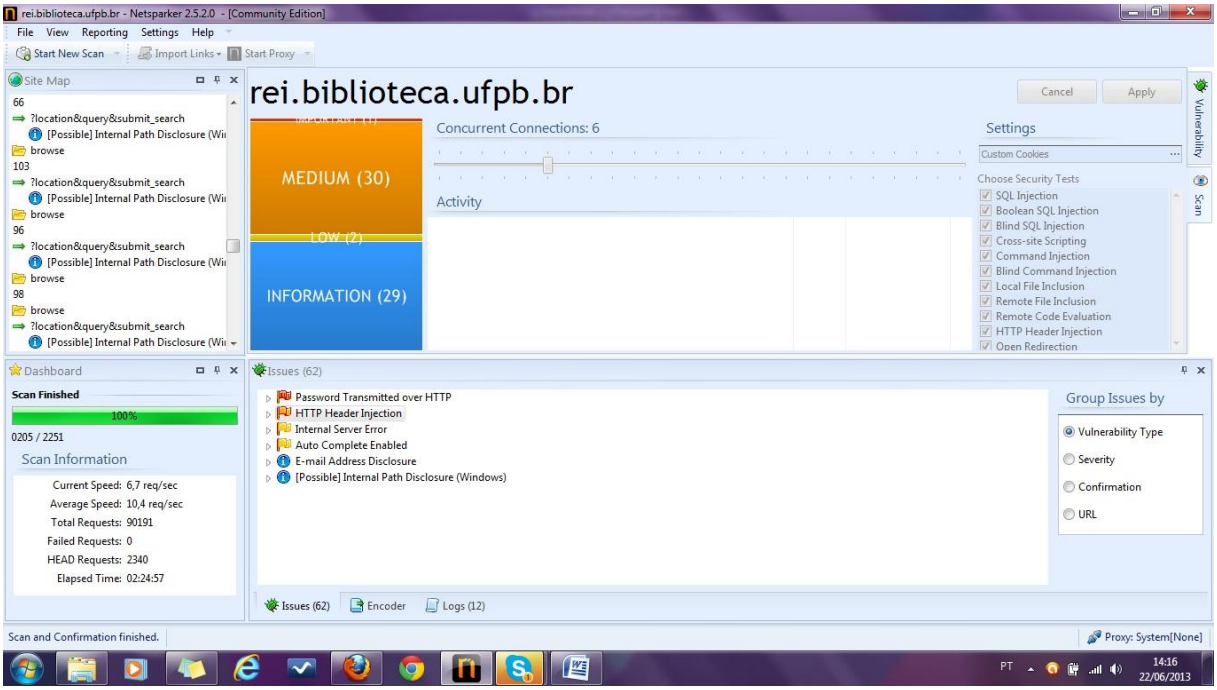
As imagens seguintes correspondem às telas dos Testes de Penetração executados com a ferramenta Netsparker, após a finalização das varreduras dos sistemas dos RD's das universidades federais do Brasil.

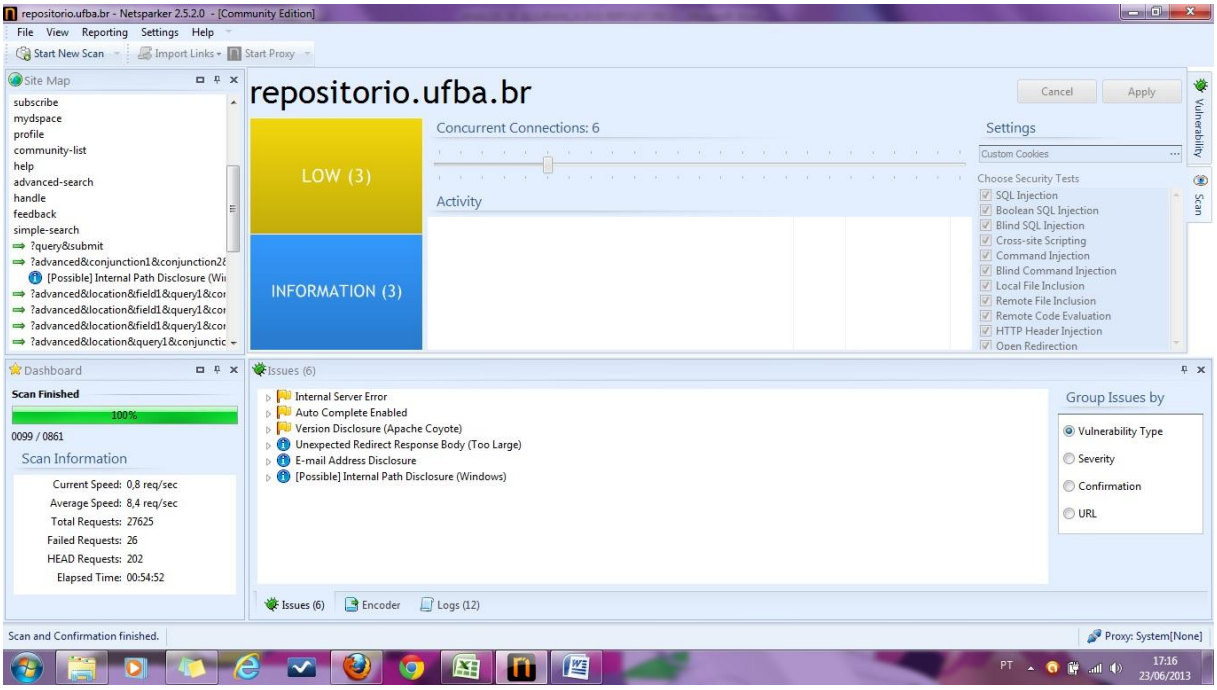


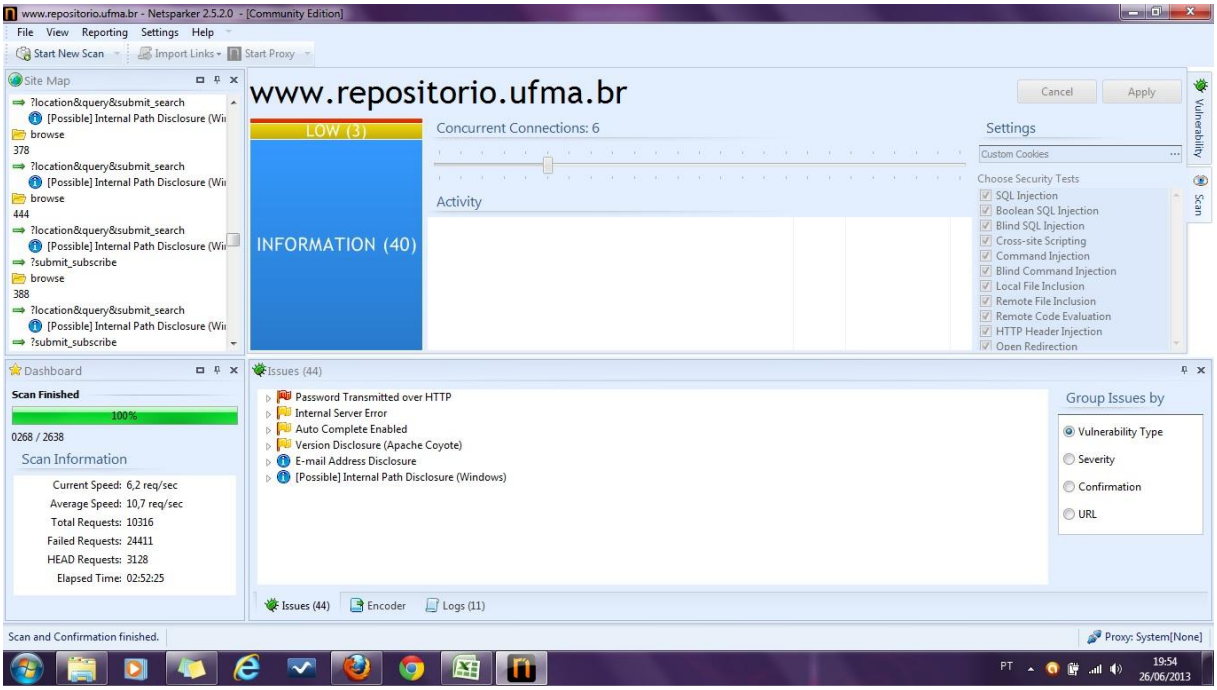


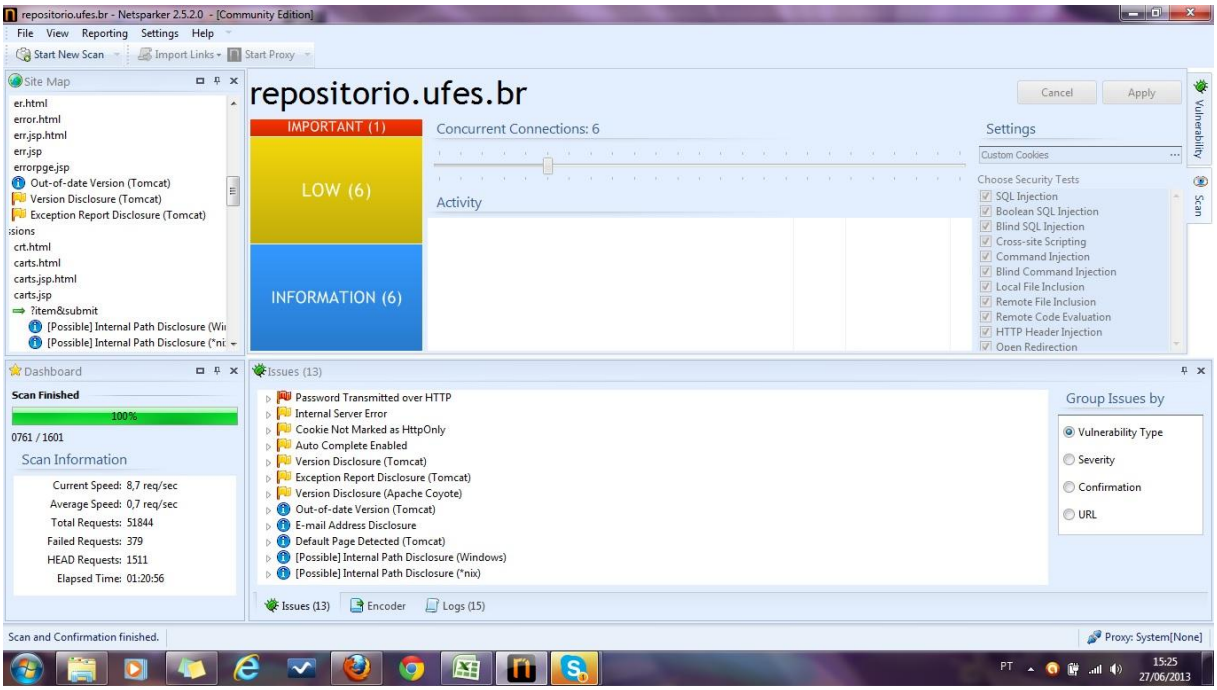

repositorio.ufrn.br - Netsparker 2.5.2.0 - [Community Edition]
File View Reporting Settings Help
Start New Scan
Import Links
Start Proxy
Site Map
repositorio.ufrn.br
Cancel
Apply
IMPORTANT (1)
LOW (3)
INFORMATION (15)
Concurrent Connections: 6
Activity
Settings
Custom Cookies
Choose Security Tests
SQL Injection
Boolean SQL Injection
Blind SQL Injection
Cross-site Scripting
Command Injection
Blind Command Injection
Local File Inclusion
Remote File Inclusion
Remote Code Evaluation
HTTP Header Injection
Open Redirection
Dashboard
Scan Finished
100%
0216 / 1931
Scan Information
Current Speed: 4,0 req/sec
Average Speed: 10,1 req/sec
Total Requests: 58262
Failed Requests: 50
HEAD Requests: 1194
Elapsed Time: 01:36:20
Issues (19)
Password Transmitted over HTTP
Internal Server Error
Auto Complete Enabled
Version Disclosure (Apache Coyote)
E-mail Address Disclosure
[Possible] Internal Path Disclosure (Windows)
Group Issues by
Vulnerability Type
Severity
Confirmation
URL
Issues (19)
Encoder
Logs (12)
Scan and Confirmation finished.
Proxy: System[None]
PT
21:25
18/06/2013

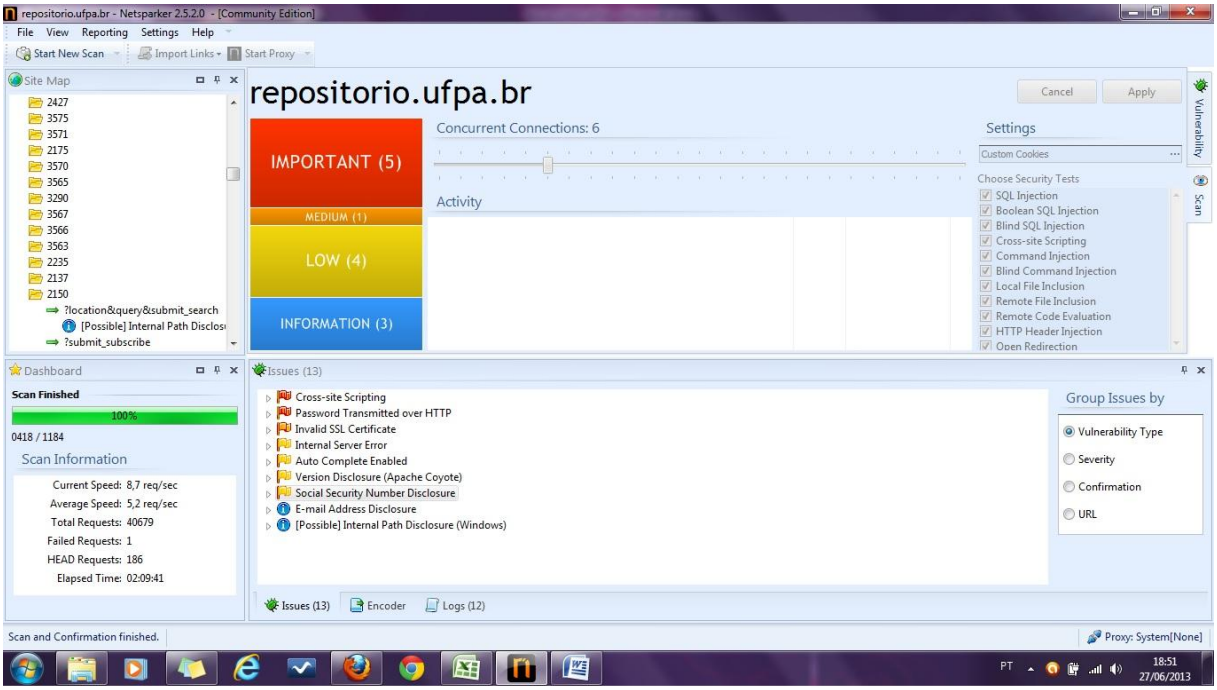

repositorio.unb.br - Netsparker 3.0.2.0 - [Community Edition]
File View Reporting Settings Help
Start New Scan
Import Links
Start Proxy
Site Map
repositorio.unb.br80
repositorio.unb.br
Cancel
Apply
IMPORTANT (151)
MEDIUM (8)
Concurrent Connections: 6
Activity
Settings
Custom Cookies
E-mail Address Disclosure
Cookie Not Marked as HttpOnly
utils.js
styles.css.jsp
stats
Cross-site Scripting
calendar1.js
[Possible] Internal Path Disclosure
Dashboard
Scan Finished
100%
0000 / 0000
Scan Information
Current Speed: 7,0 req/sec
Average Speed: 8,4 req/sec
Total Requests: 46777
Failed Requests: 1
HEAD Requests: 523
Elapsed Time: 01:33:06
Issues (173)
Boolean Based SQL Injection
Cross-site Scripting
Password Transmitted over HTTP
HTTP Header Injection
Auto Complete Enabled
Internal Server Error
Cookie Not Marked as HttpOnly
Robots.txt Detected
Database Detected (Postgres)
E-mail Address Disclosure
[Possible] Internal Path Disclosure (Windows)
[Possible] Internal Path Disclosure (*nix)
Group Issues by
Vulnerability Type
Severity
Confirmation
URL
Issues (173)
Encoder
Logs (15)
Scan and Confirmation finished.
Proxy: System[None]
PT
19:09
12/08/2013

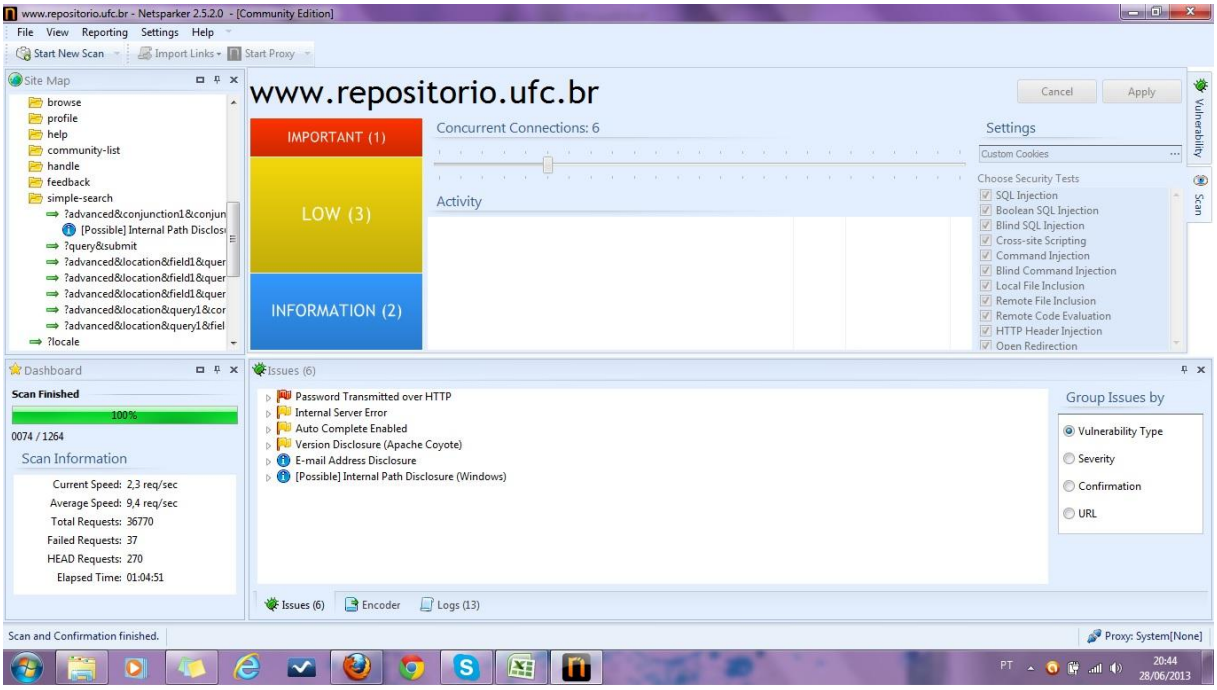

rei.biblioteca.ufpb.br - Netsparker 2.5.2.0 - [Community Edition]
File View Reporting Settings Help
Start New Scan
Import Links
Start Proxy
Site Map
rei.biblioteca.ufpb.br
Cancel
Apply
MEDIUM (30)
LOW (2)
INFORMATION (29)
Concurrent Connections: 6
Activity
Settings
Custom Cookies
Choose Security Tests
SQL Injection
Boolean SQL Injection
Blind SQL Injection
Cross-site Scripting
Command Injection
Blind Command Injection
Local File Inclusion
Remote File Inclusion
Remote Code Evaluation
HTTP Header Injection
Open Redirection
Dashboard
Scan Finished
100%
0205 / 2251
Scan Information
Current Speed: 6,7 req/sec
Average Speed: 10,4 req/sec
Total Requests: 90191
Failed Requests: 0
HEAD Requests: 2340
Elapsed Time: 02:24:57
Issues (62)
Password Transmitted over HTTP
HTTP Header Injection
Internal Server Error
Auto Complete Enabled
E-mail Address Disclosure
[Possible] Internal Path Disclosure (Windows)
Group Issues by
Vulnerability Type
Severity
Confirmation
URL
Issues (62)
Encoder
Logs (12)
Scan and Confirmation finished.
Proxy: System[None]
14:16
22/06/2013

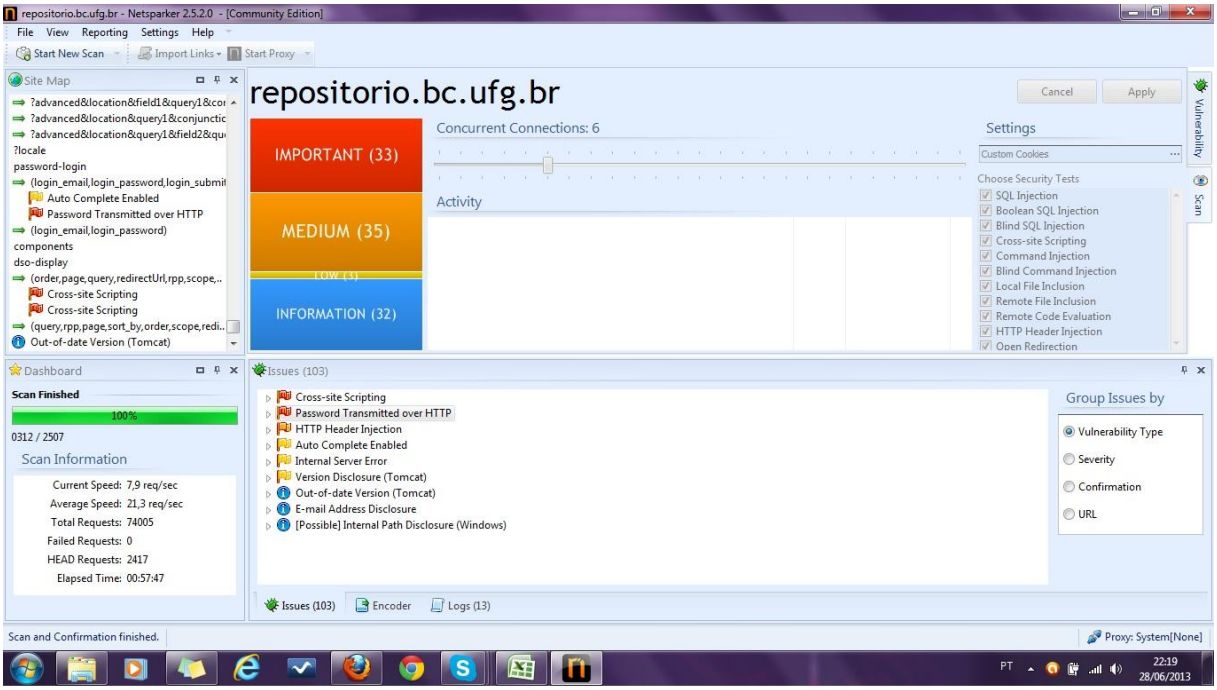

repositorio.ufba.br - Netsparker 2.5.2.0 - [Community Edition]
File View Reporting Settings Help
Start New Scan
Import Links
Start Proxy
Site Map
repositorio.ufba.br
Cancel
Apply
LOW (3)
INFORMATION (3)
Concurrent Connections: 6
Activity
Settings
Custom Cookies
Choose Security Tests
SQL Injection
Boolean SQL Injection
Blind SQL Injection
Cross-site Scripting
Command Injection
Blind Command Injection
Local File Inclusion
Remote File Inclusion
Remote Code Evaluation
HTTP Header Injection
Open Redirection
Dashboard
Scan Finished
100%
0099 / 0861
Scan Information
Current Speed: 0,8 req/sec
Average Speed: 8,4 req/sec
Total Requests: 27625
Failed Requests: 26
HEAD Requests: 202
Elapsed Time: 00:54:52
Issues (6)
Internal Server Error
Auto Complete Enabled
Version Disclosure (Apache Coyote)
Unexpected Redirect Response Body (Too Large)
E-mail Address Disclosure
[Possible] Internal Path Disclosure (Windows)
Group Issues by
Vulnerability Type
Severity
Confirmation
URL
Issues (6)
Encoder
Logs (12)
Scan and Confirmation finished.
Proxy: System[None]
17:16
23/06/2013

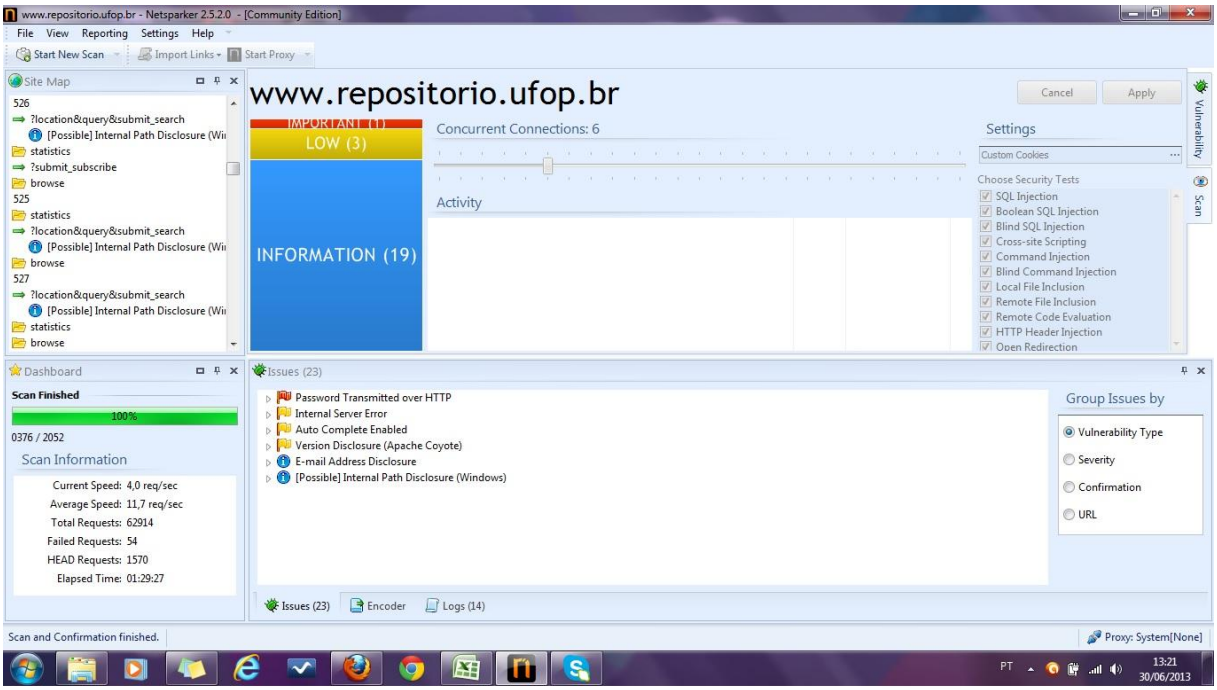

www.repositorio.ufma.br - Netsparker 2.5.2.0 - [Community Edition]
File View Reporting Settings Help
Start New Scan
Import Links
Start Proxy
Site Map
www.repositorio.ufma.br
Cancel
Apply
LOW (3)
INFORMATION (40)
Concurrent Connections: 6
Activity
Settings
Custom Cookies
Choose Security Tests
SQL Injection
Boolean SQL Injection
Blind SQL Injection
Cross-site Scripting
Command Injection
Blind Command Injection
Local File Inclusion
Remote File Inclusion
Remote Code Evaluation
HTTP Header Injection
Open Redirection
Dashboard
Scan Finished
100%
0268 / 2638
Scan Information
Current Speed: 6,2 req/sec
Average Speed: 10,7 req/sec
Total Requests: 10316
Failed Requests: 24411
HEAD Requests: 3128
Elapsed Time: 02:52:25
Issues (44)
Password Transmitted over HTTP
Internal Server Error
Auto Complete Enabled
Version Disclosure (Apache Coyote)
E-mail Address Disclosure
[Possible] Internal Path Disclosure (Windows)
Group Issues by
Vulnerability Type
Severity
Confirmation
URL
Issues (44)
Encoder
Logs (11)
Scan and Confirmation finished.
Proxy: System[None]
19:54
26/06/2013

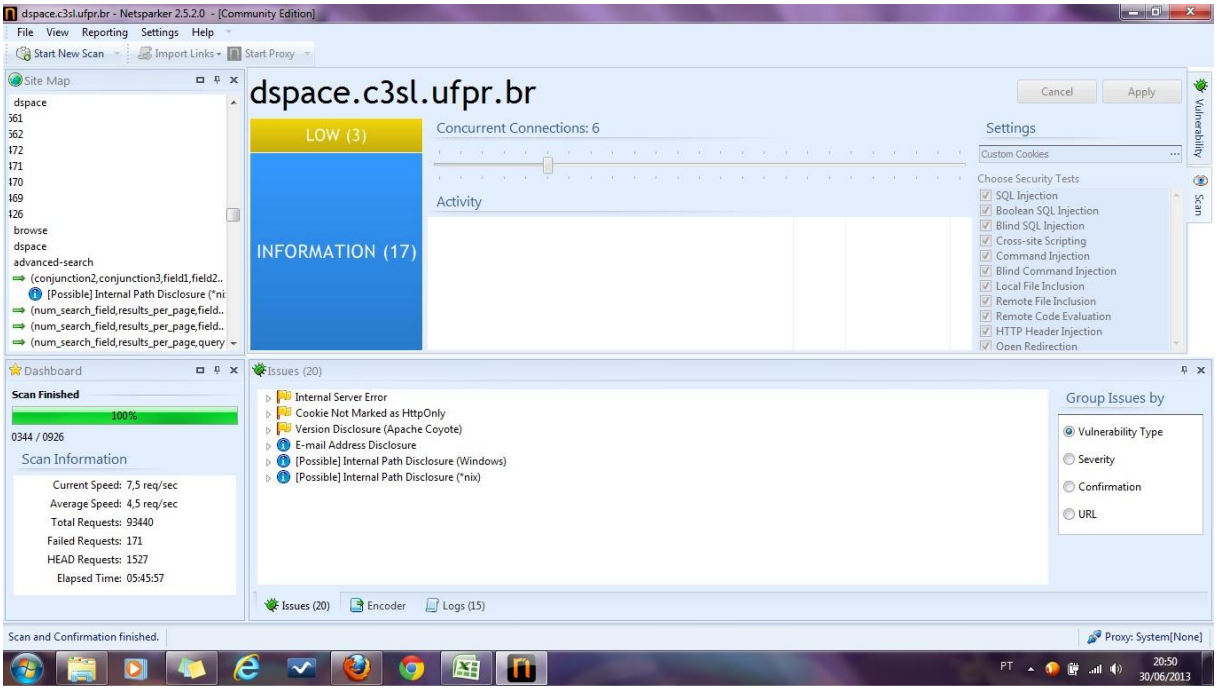

repositorio.ufes.br - Netsparker 2.5.2.0 - [Community Edition]
File View Reporting Settings Help
Start New Scan
Import Links
Start Proxy
Site Map
repositorio.ufes.br
Cancel
Apply
IMPORTANT (1)
LOW (6)
INFORMATION (6)
Concurrent Connections: 6
Activity
Settings
Custom Cookies
Choose Security Tests
SQL Injection
Boolean SQL Injection
Blind SQL Injection
Cross-site Scripting
Command Injection
Blind Command Injection
Local File Inclusion
Remote File Inclusion
Remote Code Evaluation
HTTP Header Injection
Open Redirection
Out-of-date Version (Tomcat)
Version Disclosure (Tomcat)
Exception Report Disclosure (Tomcat)
Dashboard
Scan Finished
100%
0761 / 1601
Scan Information
Current Speed: 8,7 req/sec
Average Speed: 0,7 req/sec
Total Requests: 51844
Failed Requests: 379
HEAD Requests: 1511
Elapsed Time: 01:20:56
Issues (13)
Password Transmitted over HTTP
Internal Server Error
Cookie Not Marked as HttpOnly
Auto Complete Enabled
Version Disclosure (Tomcat)
Exception Report Disclosure (Tomcat)
Version Disclosure (Apache Coyote)
Out-of-date Version (Tomcat)
E-mail Address Disclosure
Default Page Detected (Tomcat)
[Possible] Internal Path Disclosure (Windows)
[Possible] Internal Path Disclosure (*nix)
Group Issues by
Vulnerability Type
Severity
Confirmation
URL
Issues (13)
Encoder
Logs (15)
Scan and Confirmation finished.
Proxy: System[None]
15:25
27/06/2013

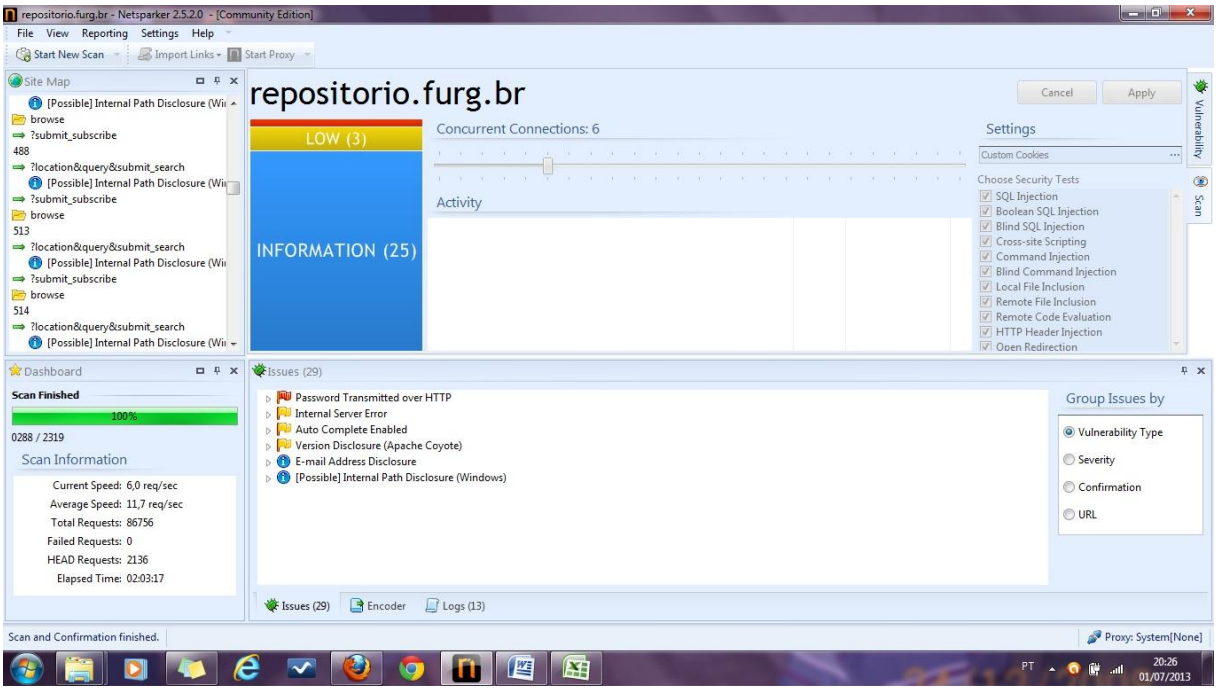

repositorio.ufpa.br - Netsparker 2.5.2.0 - [Community Edition]
File View Reporting Settings Help
Start New Scan
Import Links
Start Proxy
Site Map
repositorio.ufpa.br
Cancel
Apply
IMPORTANT (5)
MEDIUM (1)
LOW (4)
INFORMATION (3)
Concurrent Connections: 6
Activity
Settings
Custom Cookies
Choose Security Tests
SQL Injection
Boolean SQL Injection
Blind SQL Injection
Cross-site Scripting
Command Injection
Blind Command Injection
Local File Inclusion
Remote File Inclusion
Remote Code Evaluation
HTTP Header Injection
Open Redirection
Vulnerability
Scan
Dashboard
Scan Finished
100%
0418 / 1184
Scan Information
Current Speed: 8,7 req/sec
Average Speed: 5,2 req/sec
Total Requests: 40679
Failed Requests: 1
HEAD Requests: 186
Elapsed Time: 02:09:41
Issues (13)
Cross-site Scripting
Password Transmitted over HTTP
Invalid SSL Certificate
Internal Server Error
Auto Complete Enabled
Version Disclosure (Apache Coyote)
Social Security Number Disclosure
E-mail Address Disclosure
[Possible] Internal Path Disclosure (Windows)
Group Issues by
Vulnerability Type
Severity
Confirmation
URL
Issues (13)
Encoder
Logs (12)
Scan and Confirmation finished.
Proxy: System[None]
PT
18:51
27/06/2013

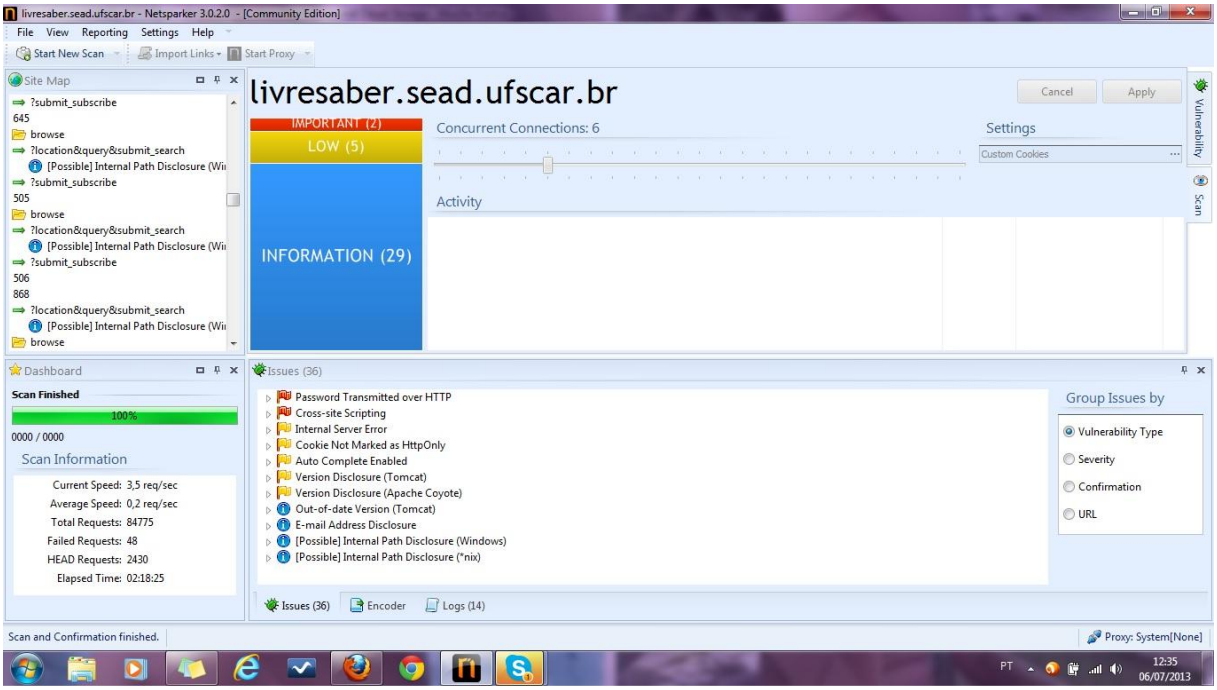

www.repositorio.ufc.br - Netsparker 2.5.2.0 - [Community Edition]
File View Reporting Settings Help
Start New Scan
Import Links
Start Proxy
Site Map
www.repositorio.ufc.br
Cancel
Apply
IMPORTANT (1)
LOW (3)
INFORMATION (2)
Concurrent Connections: 6
Activity
Settings
Custom Cookies
Choose Security Tests
SQL Injection
Boolean SQL Injection
Blind SQL Injection
Cross-site Scripting
Command Injection
Blind Command Injection
Local File Inclusion
Remote File Inclusion
Remote Code Evaluation
HTTP Header Injection
Open Redirection
Vulnerability
Scan
Dashboard
Scan Finished
100%
0074 / 1264
Scan Information
Current Speed: 2,3 req/sec
Average Speed: 9,4 req/sec
Total Requests: 36770
Failed Requests: 37
HEAD Requests: 270
Elapsed Time: 01:04:51
Issues (6)
Password Transmitted over HTTP
Internal Server Error
Auto Complete Enabled
Version Disclosure (Apache Coyote)
E-mail Address Disclosure
[Possible] Internal Path Disclosure (Windows)
Group Issues by
Vulnerability Type
Severity
Confirmation
URL
Issues (6)
Encoder
Logs (13)
Scan and Confirmation finished.
Proxy: System[None]
PT
20:44
28/06/2013

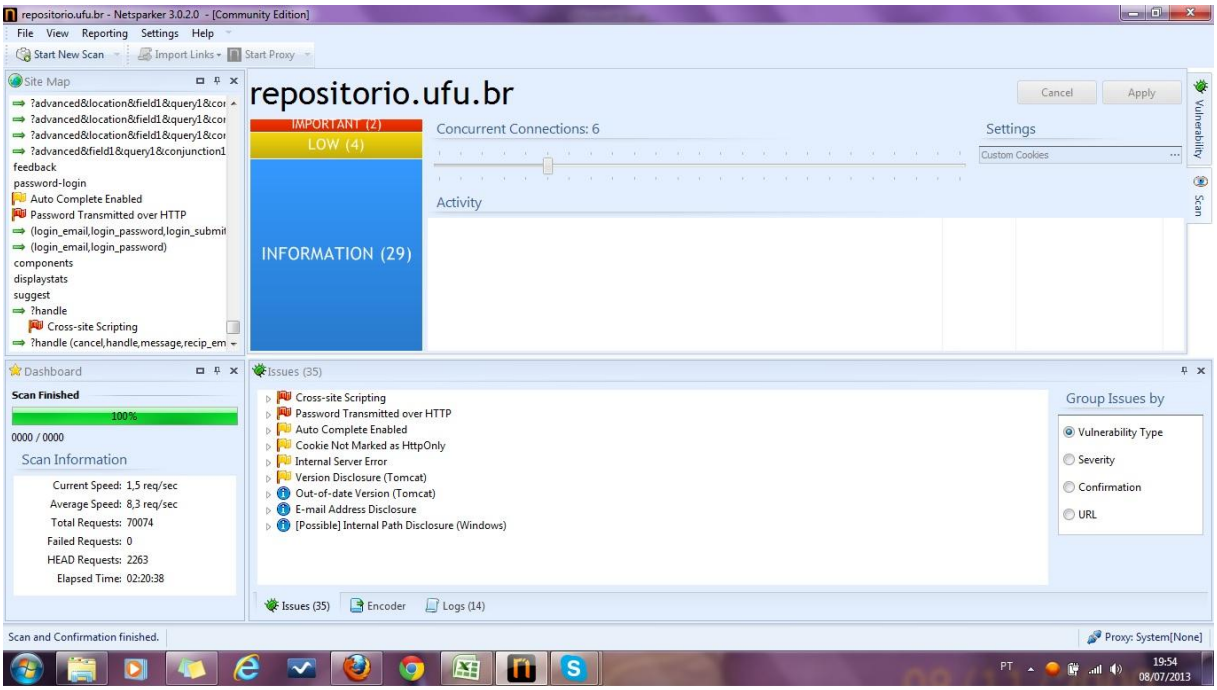

repositorio.bc.ufg.br - Netsparker 2.5.2.0 - [Community Edition]
File View Reporting Settings Help
Start New Scan
Import Links
Start Proxy
Site Map
repositorio.bc.ufg.br
Cancel
Apply
IMPORTANT (33)
MEDIUM (35)
INFORMATION (32)
Concurrent Connections: 6
Activity
Settings
Custom Cookies
Choose Security Tests
SQL Injection
Boolean SQL Injection
Blind SQL Injection
Cross-site Scripting
Command Injection
Blind Command Injection
Local File Inclusion
Remote File Inclusion
Remote Code Evaluation
HTTP Header Injection
Open Redirection
Dashboard
Scan Finished
100%
0312 / 2507
Scan Information
Current Speed: 7,9 req/sec
Average Speed: 21,3 req/sec
Total Requests: 74005
Failed Requests: 0
HEAD Requests: 2417
Elapsed Time: 00:57:47
Issues (103)
Cross-site Scripting
Password Transmitted over HTTP
HTTP Header Injection
Auto Complete Enabled
Internal Server Error
Version Disclosure (Tomcat)
Out-of-date Version (Tomcat)
E-mail Address Disclosure
[Possible] Internal Path Disclosure (Windows)
Group Issues by
Vulnerability Type
Severity
Confirmation
URL
Issues (103)
Encoder
Logs (13)
Scan and Confirmation finished.
Proxy: System[None]
PT
22:19
28/06/2013

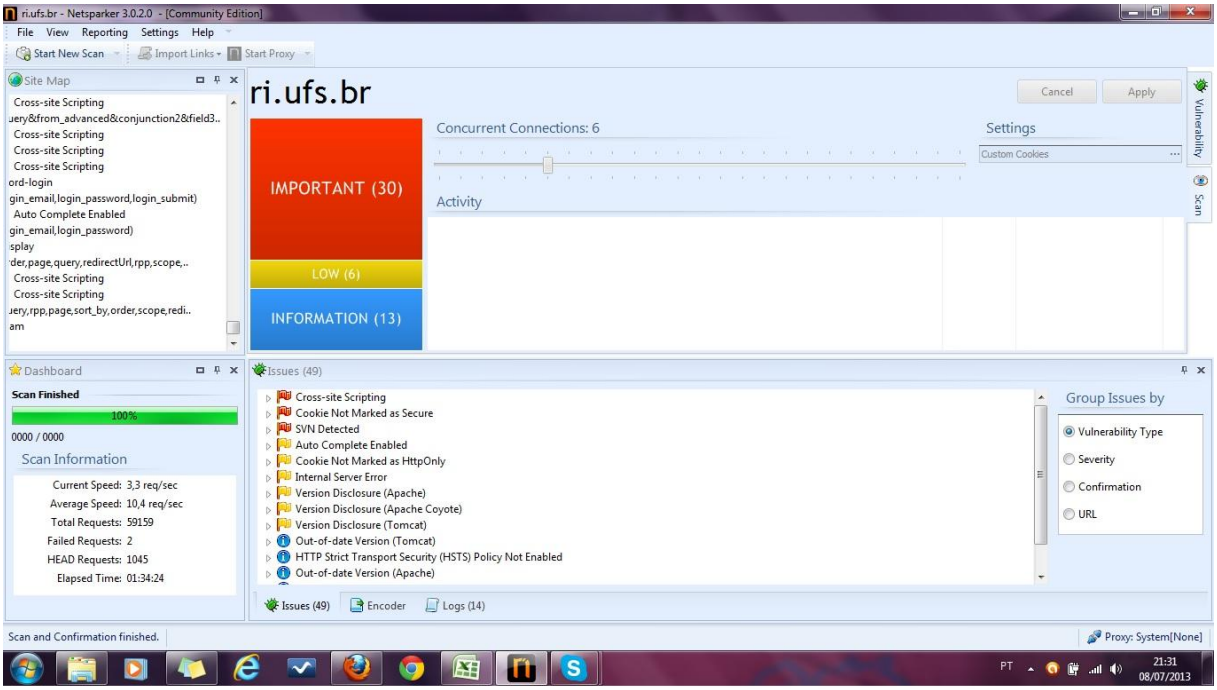

www.repositorio.ufop.br - Netsparker 2.5.2.0 - [Community Edition]
File View Reporting Settings Help
Start New Scan
Import Links
Start Proxy
Site Map
www.repositorio.ufop.br
Cancel
Apply
LOW (3)
INFORMATION (19)
Concurrent Connections: 6
Activity
Settings
Custom Cookies
Choose Security Tests
SQL Injection
Boolean SQL Injection
Blind SQL Injection
Cross-site Scripting
Command Injection
Blind Command Injection
Local File Inclusion
Remote File Inclusion
Remote Code Evaluation
HTTP Header Injection
Open Redirection
Dashboard
Scan Finished
100%
0376 / 2052
Scan Information
Current Speed: 4,0 req/sec
Average Speed: 11,7 req/sec
Total Requests: 62914
Failed Requests: 54
HEAD Requests: 1570
Elapsed Time: 01:29:27
Issues (23)
Password Transmitted over HTTP
Internal Server Error
Auto Complete Enabled
Version Disclosure (Apache Coyote)
E-mail Address Disclosure
[Possible] Internal Path Disclosure (Windows)
Group Issues by
Vulnerability Type
Severity
Confirmation
URL
Issues (23)
Encoder
Logs (14)
Scan and Confirmation finished.
Proxy: System[None]
PT
13:21
30/06/2013

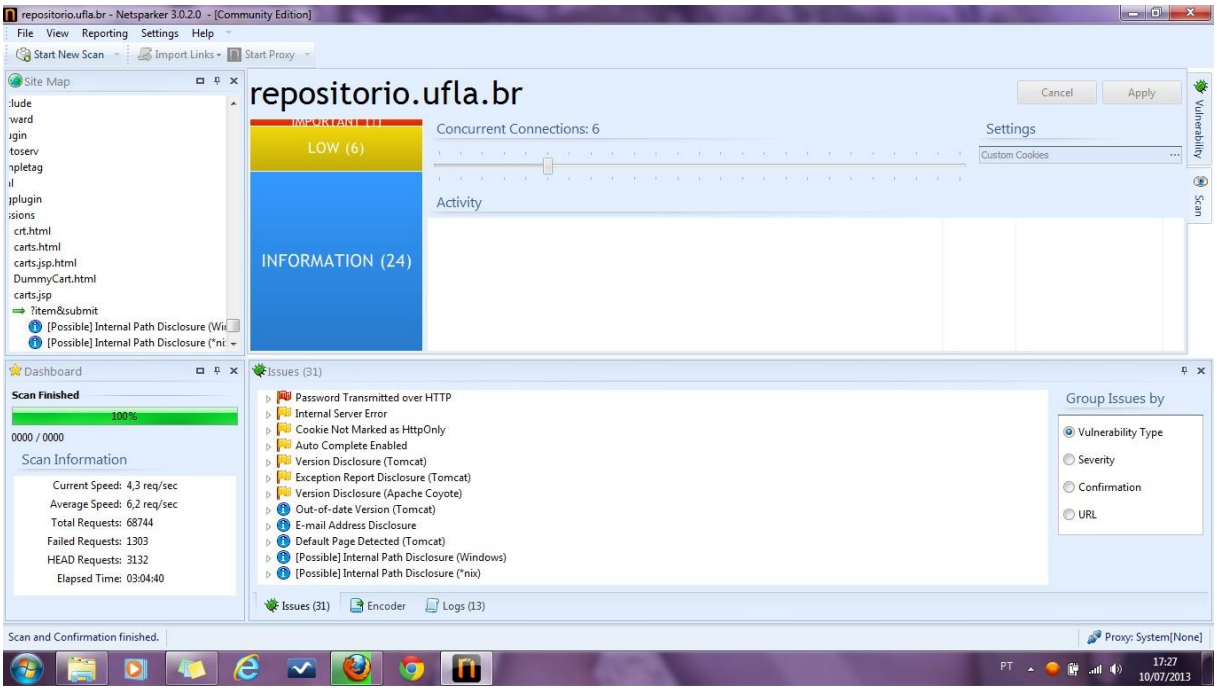

dspace.c3sl.ufpr.br - Netsparker 2.5.2.0 - [Community Edition]
File View Reporting Settings Help
Start New Scan
Import Links
Start Proxy
Site Map
dspace
361
362
172
171
170
169
126
browse
dspace
advanced-search
(conjunction2,conjunction3,field1,field2..
[Possible] Internal Path Disclosure (*ni
(num_search_field,results_per_page,field..
(num_search_field,results_per_page,field..
(num_search_field,results_per_page,query
dspace.c3sl.ufpr.br
Cancel
Apply
LOW (3)
INFORMATION (17)
Concurrent Connections: 6
Activity
Settings
Custom Cookies
Choose Security Tests
SQL Injection
Boolean SQL Injection
Blind SQL Injection
Cross-site Scripting
Command Injection
Blind Command Injection
Local File Inclusion
Remote File Inclusion
Remote Code Evaluation
HTTP Header Injection
Open Redirection
Vulnerability
Scan
Dashboard
Scan Finished
100%
0344 / 0926
Scan Information
Current Speed: 7,5 req/sec
Average Speed: 4,5 req/sec
Total Requests: 93440
Failed Requests: 171
HEAD Requests: 1527
Elapsed Time: 05:45:57
Issues (20)
Internal Server Error
Cookie Not Marked as HttpOnly
Version Disclosure (Apache Coyote)
E-mail Address Disclosure
[Possible] Internal Path Disclosure (Windows)
[Possible] Internal Path Disclosure (*nix)
Group Issues by
Vulnerability Type
Severity
Confirmation
URL
Issues (20)
Encoder
Logs (15)
Scan and Confirmation finished.
Proxy: System[None]
PT
20:50
30/06/2013

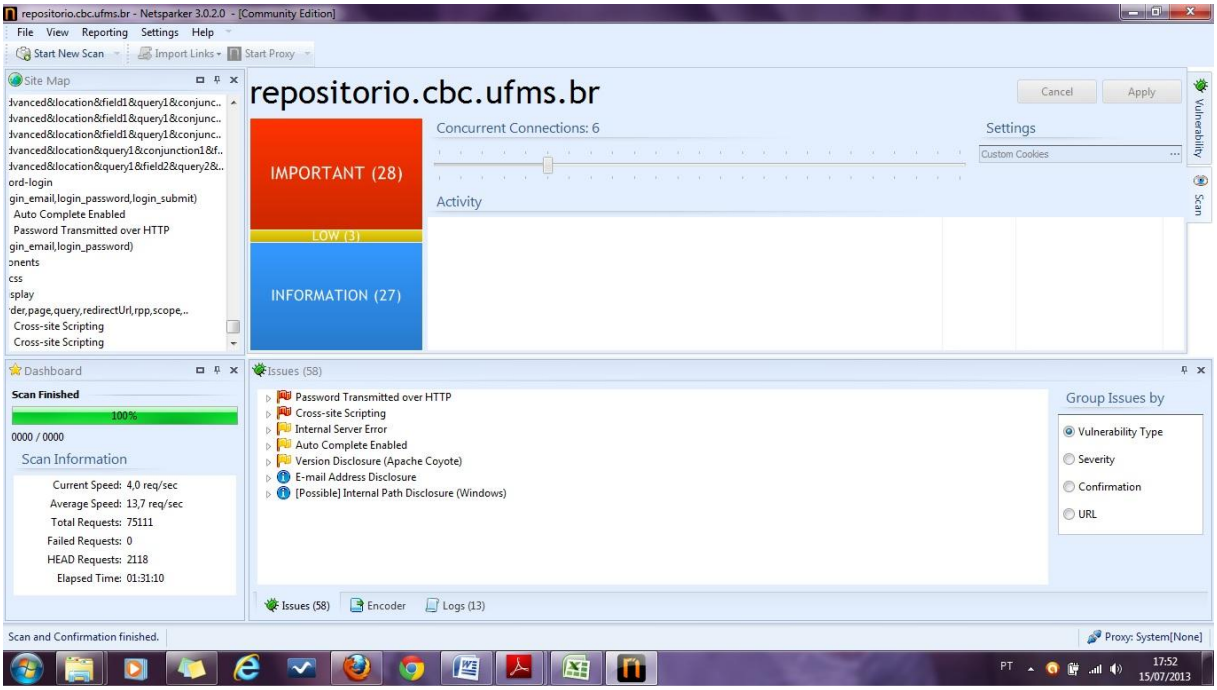

repositorio.furg.br - Netsparker 2.5.2.0 - [Community Edition]
File View Reporting Settings Help
Start New Scan
Import Links
Start Proxy
Site Map
[Possible] Internal Path Disclosure (Wi
browse
?submit_subscribe
488
?location&query&submit_search
[Possible] Internal Path Disclosure (Wi
?submit_subscribe
browse
513
?location&query&submit_search
[Possible] Internal Path Disclosure (Wi
?submit_subscribe
browse
514
?location&query&submit_search
[Possible] Internal Path Disclosure (Wi
repositorio.furg.br
Cancel
Apply
LOW (3)
INFORMATION (25)
Concurrent Connections: 6
Activity
Settings
Custom Cookies
Choose Security Tests
SQL Injection
Boolean SQL Injection
Blind SQL Injection
Cross-site Scripting
Command Injection
Blind Command Injection
Local File Inclusion
Remote File Inclusion
Remote Code Evaluation
HTTP Header Injection
Open Redirection
Vulnerability
Scan
Dashboard
Scan Finished
100%
0288 / 2319
Scan Information
Current Speed: 6,0 req/sec
Average Speed: 11,7 req/sec
Total Requests: 86756
Failed Requests: 0
HEAD Requests: 2136
Elapsed Time: 02:03:17
Issues (29)
Password Transmitted over HTTP
Internal Server Error
Auto Complete Enabled
Version Disclosure (Apache Coyote)
E-mail Address Disclosure
[Possible] Internal Path Disclosure (Windows)
Group Issues by
Vulnerability Type
Severity
Confirmation
URL
Issues (29)
Encoder
Logs (13)
Scan and Confirmation finished.
Proxy: System[None]
PT
20:26
01/07/2013

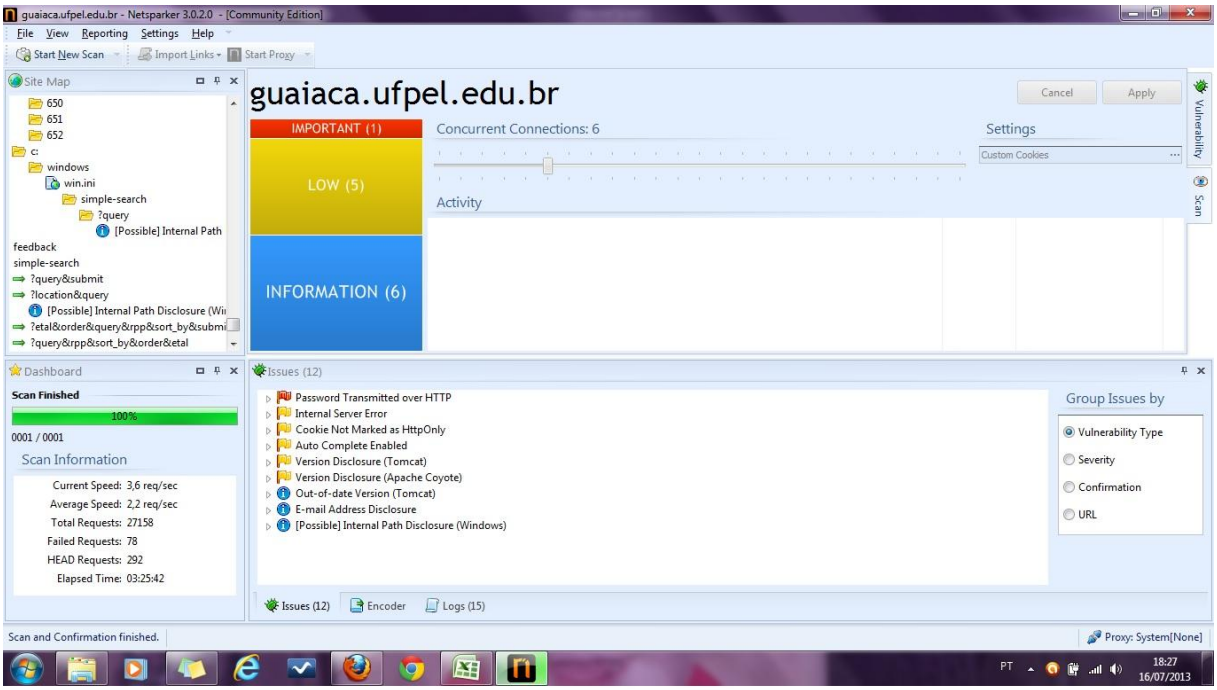

livresaber.sead.ufscar.br - Netsparker 3.0.2.0 - [Community Edition]
File View Reporting Settings Help
Start New Scan
Import Links
Start Proxy
Site Map
livresaber.sead.ufscar.br
Cancel
Apply
IMPORTANT (2)
LOW (5)
INFORMATION (29)
Concurrent Connections: 6
Settings
Custom Cookies
Activity
Vulnerability
Scan
Dashboard
Scan Finished
100%
0000 / 0000
Scan Information
Current Speed: 3,5 req/sec
Average Speed: 0,2 req/sec
Total Requests: 84775
Failed Requests: 48
HEAD Requests: 2430
Elapsed Time: 02:18:25
Issues (36)
Password Transmitted over HTTP
Cross-site Scripting
Internal Server Error
Cookie Not Marked as HttpOnly
Auto Complete Enabled
Version Disclosure (Tomcat)
Version Disclosure (Apache Coyote)
Out-of-date Version (Tomcat)
E-mail Address Disclosure
[Possible] Internal Path Disclosure (Windows)
[Possible] Internal Path Disclosure (*nix)
Group Issues by
Vulnerability Type
Severity
Confirmation
URL
Issues (36)
Encoder
Logs (14)
Scan and Confirmation finished.
Proxy: System[None]
PT
12:35
06/07/2013


repositorio.ufu.br - Netsparker 3.0.2.0 - [Community Edition]
File View Reporting Settings Help
Start New Scan
Import Links
Start Proxy
Site Map
repositorio.ufu.br
Cancel
Apply
IMPORTANT (2)
LOW (4)
INFORMATION (29)
Concurrent Connections: 6
Settings
Custom Cookies
Activity
Vulnerability
Scan
feedback
password-login
Auto Complete Enabled
Password Transmitted over HTTP
components
displaystats
suggest
Cross-site Scripting
Dashboard
Scan Finished
100%
0000 / 0000
Scan Information
Current Speed: 1,5 req/sec
Average Speed: 8,3 req/sec
Total Requests: 70074
Failed Requests: 0
HEAD Requests: 2263
Elapsed Time: 02:20:38
Issues (35)
Cross-site Scripting
Password Transmitted over HTTP
Auto Complete Enabled
Cookie Not Marked as HttpOnly
Internal Server Error
Version Disclosure (Tomcat)
Out-of-date Version (Tomcat)
E-mail Address Disclosure
[Possible] Internal Path Disclosure (Windows)
Group Issues by
Vulnerability Type
Severity
Confirmation
URL
Issues (35)
Encoder
Logs (14)
Scan and Confirmation finished.
Proxy: System[None]
PT
19:54
08/07/2013


ri.ufs.br - Netsparker 3.0.2.0 - [Community Edition]
File View Reporting Settings Help
Start New Scan
Import Links
Start Proxy
Site Map
Cross-site Scripting
Cross-site Scripting
Cross-site Scripting
Cross-site Scripting
Auto Complete Enabled
Cross-site Scripting
Cross-site Scripting
ri.ufs.br
Cancel
Apply
IMPORTANT (30)
LOW (6)
INFORMATION (13)
Concurrent Connections: 6
Settings
Custom Cookies
Activity
Vulnerability
Scan
Dashboard
Scan Finished
100%
0000 / 0000
Scan Information
Current Speed: 3,3 req/sec
Average Speed: 10,4 req/sec
Total Requests: 59159
Failed Requests: 2
HEAD Requests: 1045
Elapsed Time: 01:34:24
Issues (49)
Cross-site Scripting
Cookie Not Marked as Secure
SVN Detected
Auto Complete Enabled
Cookie Not Marked as HttpOnly
Internal Server Error
Version Disclosure (Apache)
Version Disclosure (Apache Coyote)
Version Disclosure (Tomcat)
Out-of-date Version (Tomcat)
HTTP Strict Transport Security (HSTS) Policy Not Enabled
Out-of-date Version (Apache)
Group Issues by
Vulnerability Type
Severity
Confirmation
URL
Issues (49)
Encoder
Logs (14)
Scan and Confirmation finished.
Proxy: System[None]
PT
21:31
08/07/2013


repositorio.ufla.br - Netsparker 3.0.2.0 - [Community Edition]
File View Reporting Settings Help
Start New Scan
Import Links
Start Proxy
Site Map
?item&submit
[Possible] Internal Path Disclosure (Wi
[Possible] Internal Path Disclosure (*ni
repositorio.ufla.br
Cancel
Apply
LOW (6)
INFORMATION (24)
Concurrent Connections: 6
Settings
Custom Cookies
Activity
Vulnerability
Scan
Dashboard
Scan Finished
100%
0000 / 0000
Scan Information
Current Speed: 4,3 req/sec
Average Speed: 6,2 req/sec
Total Requests: 68744
Failed Requests: 1303
HEAD Requests: 3132
Elapsed Time: 03:04:40
Issues (31)
Password Transmitted over HTTP
Internal Server Error
Cookie Not Marked as HttpOnly
Auto Complete Enabled
Version Disclosure (Tomcat)
Exception Report Disclosure (Tomcat)
Version Disclosure (Apache Coyote)
Out-of-date Version (Tomcat)
E-mail Address Disclosure
Default Page Detected (Tomcat)
[Possible] Internal Path Disclosure (Windows)
[Possible] Internal Path Disclosure (*nix)
Group Issues by
Vulnerability Type
Severity
Confirmation
URL
Issues (31)
Encoder
Logs (13)
Scan and Confirmation finished.
Proxy: System[None]
PT
17:27
10/07/2013


repositorio.cbc.ufms.br - Netsparker 3.0.2.0 - [Community Edition]
File View Reporting Settings Help
Start New Scan
Import Links
Start Proxy
Site Map
repositorio.cbc.ufms.br
Cancel
Apply
IMPORTANT (28)
LOW (3)
INFORMATION (27)
Concurrent Connections: 6
Settings
Custom Cookies
Activity
Vulnerability
Scan
Dashboard
Scan Finished
100%
0000 / 0000
Scan Information
Current Speed: 4,0 req/sec
Average Speed: 13,7 req/sec
Total Requests: 75111
Failed Requests: 0
HEAD Requests: 2118
Elapsed Time: 01:31:10
Issues (58)
Password Transmitted over HTTP
Cross-site Scripting
Internal Server Error
Auto Complete Enabled
Version Disclosure (Apache Coyote)
E-mail Address Disclosure
[Possible] Internal Path Disclosure (Windows)
Group Issues by
Vulnerability Type
Severity
Confirmation
URL
Issues (58)
Encoder
Logs (13)
Scan and Confirmation finished.
Proxy: System[None]
PT
17:52
15/07/2013


guaiaca.ufpel.edu.br - Netsparker 3.0.2.0 - [Community Edition]
File View Reporting Settings Help
Start New Scan
Import Links
Start Proxy
Site Map
guaiaca.ufpel.edu.br
Cancel
Apply
IMPORTANT (1)
LOW (5)
INFORMATION (6)
Concurrent Connections: 6
Settings
Custom Cookies
Activity
Vulnerability
Scan
Dashboard
Scan Finished
100%
0001 / 0001
Scan Information
Current Speed: 3,6 req/sec
Average Speed: 2,2 req/sec
Total Requests: 27158
Failed Requests: 78
HEAD Requests: 292
Elapsed Time: 03:25:42
Issues (12)
Password Transmitted over HTTP
Internal Server Error
Cookie Not Marked as HttpOnly
Auto Complete Enabled
Version Disclosure (Tomcat)
Version Disclosure (Apache Coyote)
Out-of-date Version (Tomcat)
E-mail Address Disclosure
[Possible] Internal Path Disclosure (Windows)
Group Issues by
Vulnerability Type
Severity
Confirmation
URL
Issues (12)
Encoder
Logs (15)
Scan and Confirmation finished.
Proxy: System[None]
PT
18:27
16/07/2013