**Resumo**

Diante de uma evolução contínua no desenvolvimento de novas tecnologias, garantir que um determinado sistema seja totalmente seguro torna-se quase impossível. Por isso é de extrema importância a busca por vulnerabilidades em Aplicações Web para que possam ser investigadas, exploradas a fim de corrigi-las ou amenizar seus efeitos no negócio de uma organização.

Testes de Penetração são métodos que visam encontrar e avaliar as brechas na estrutura de segurança de um sistema. Proteger informações de uma organização implica diretamente na continuidade, qualidade e integridade de seus serviços.

Fundado desde 1909 [5], o IFPE possui notável relevância como uma instituição pública destinada a oferecer serviços de peso para a sociedade. A instituição possui aplicações web que, dentre outros, abrigam dados essenciais para os cursos que ela oferece bem como para a sua administração financeira. Elas são utilizadas por professores, servidores e alunos nas atividades letivas, dessa forma representam um grande alvo para invasores e espiões mal intencionados. Ter os dados dessas aplicações acessados de forma indevida representa um grande risco para os serviços do IFPE podendo comprometer toda a sua atividade fim. Dessa maneira, os testes de intrusão podem promover a prevenção contra essas ameaças e contribuir de forma primordial para afirmar a existência relevante da instituição na sociedade.

Palavras-chave: Segurança da Informação, Pentest, busca por vulnerabilidades, testes de penetração, testes de intrusão.

**Introdução**

Dentre tantos elementos relevantes para os objetivos e negócio de uma organização, está a informação: um dos bens de maior valor que essa possui. De acordo com a norma NBR ISO/IEC 27002, o valor desse bem vai além das palavras escritas, números e imagens, abrange tudo que possa estar relacionado a ele. Por isso, cuidar da segurança de ativos de uma empresa deve ser uma preocupação séria. Em mundo cada vez mais interligado e envolvido com as aplicações web e outras tecnologias que promovem o compartilhamento de informações, é imprescindível a proteção contra riscos comprometedores do sigilo e da segurança da informação.

Entretanto, em meio às empresas, é notável, a existência de certa displicência no tratamento de dados sensíveis ao seu próprio negócio. Esse padrão acaba por facilitar o surgimento de brechas na segurança, permitindo que atacantes mal intencionados tenham acesso não autorizado a informações da empresa. Há um grande problema na ideia quanto ao conceito de segurança. Uma grande maioria das organizações se limita a proteger o espaço físico fazendo uso, por exemplo, de portas, câmeras e alarmes, mas desprezam atitudes como exposição de senhas, controle de acesso a informações sensíveis que entre outros, podem cair em domínio publico através de um acesso não autorizado.

Esse tipo de ação maliciosa tem consequências devastadoras para uma empresa ou para os prováveis clientes dela, caracterizados muitas vezes como os principais alvos em ações desse tipo. É fácil encontrar históricos recentes de organizações fortemente lesadas por ataques maliciosos à segurança. Em 2011, a Sony sofreu um grande ataque: mais de 70 milhões de dados de cartão de créditos de usuários da Playstation Network (PSN) foram acessados indevidamente[3]. Isso abalou a confiança da empresa, a qual, teve, inclusive, de responder penalmente pela falha de segurança[4]. Em 2014, houve um outro grande incidente com vazamentos de dados. Dessa vez a Apple, empresa do visionário Steve Jobs graças a uma brecha de segurança expôs fotos íntimas de um grande grupo de celebridades de Hollywood[1]. Essas imagens escandalizaram a empresa por terem se tornado de domínio publico ao cair na Internet.

A análise desses exemplos citados conduz à compreensão de que segurança da informação deve ser uma preocupação primordial para qualquer empresa. A maneira como essa segurança é tratada e as consequências disso contribuirão efetivamente para comprometer o futuro de uma organização. Dessa forma, é muito significante saber se o Instituto Federal de Pernambuco (IFPE), instituição que revela a sua grande importância na sociedade através da promoção educacional de profissão, ciência e tecnologia em todos os seus níveis e modalidades, possui algum sistema que, após submetido à testes de intrusão, apresente falhas na estrutura de segurança. Então, será possível buscar e identificar vulnerabilidades web pertinentes a esse sistema, que possam comprometer a integridade dos seus dados e serviços prestados.

**Problema de pesquisa**

**Hipótese do trabalho**

Referências

[1] João Kurtz. Apple investiga vazamento de fotos íntimas de celebridades no icloud.

<http://veja.abril.com.br/noticia/vida-digital/sony-e-alvo-de-acao-por-vazamento-de-dados-do-ps2/>, 2014.

[2] Josh Pauli. Introdução ao Web Hacking. Novatec, 2014.

[3] Geek Tech. Hacker do ps3 culpa arrogância da sony por vazamento de dados da psn.

http://www.relacionamentodigital.com/anal-o-que-e-seguranca-da-informacao, 2011.

[4] Veja. Sony é alvo de ação por vazamento de dados do ps3.

<http://veja.abril.com.br/noticia/vida-digital/sony-e-alvo-de-acao-por-vazamento-de-dados-do-ps2/>, 2011.

[5] Wikipédia. Instituto federal de pernambuco. <http://pt.wikipedia.org/wiki/Instituto_Federal_de_Pernambuco>, 2008.