XVIII ENCONTRO NACIONAL DE PESQUISA EM CIÊNCIA DA INFORMAÇÃO – ENANCIB 2017

GT-8 – Informação e Tecnologia

SITES DOS MUNICÍPIOS DA PARAÍBA: ANÁLISE DE VULNERABILIDADES COMPUTACIONAIS

Alnio Suamy de Sena (Universidade Federal da Paraíba-UFPB)

Wagner Junqueira de Araújo (Universidade Federal da Paraíba-UFPB)

SITES OF PARAÍBA MUNICIPALITIES: ANALYSIS OF COMPUTATIONAL VULNERABILITIES

Modalidade da Apresentação: Comunicação Oral

RESUMO: O governo eletrônico pode ser caracterizado pela utilização das Tecnologias de Informação e Comunicação pela administração pública, como ferramenta de apoio aos processos de Governo e para entrega de produtos e serviços à sociedade. Contudo as plataformas digitais estão sujeitas a diferentes tipos ameaças eletrônicas, tais ameaças exploram vulnerabilidades no ambiente organizacional e computacional e colocam os ativos de informação em constante risco. Essa pesquisa teve como objetivo analisar possíveis vulnerabilidades computacionais existentes em sites de governo eletrônico dos municípios do Estado da Paraíba. Foram considerados como população da pesquisa os 50 municípios que representam maior participação para a composição do Produto Interno Bruto do Estado da Paraíba (83,4%), deste conjunto foi possível analisar os sites de 40 cidades. A pesquisa se caracterizou como descritiva, com abordagem quantitativa. Para a coleta dos dados, foi utilizado o Nestparker, um software para testes de penetração que tem como função identificar vulnerabilidades em aplicações *Web*. Como resultado, foram encontradas 822 vulnerabilidades, das quais 15% são Críticas e 15% de Alta Criticidade e 10% foram classificadas como de Média Criticidade. Tais vulnerabilidades tem o potencial de permitir que elementos mal-intencionados causem impactos negativos relevantes à continuidade dos serviços oferecidos nestes sites. Além de identificar as vulnerabilidades foi efetuado analises para indicar como corrigir cada um dos problemas encontrados, o que permite aos gestores públicos tomarem ações que visem minimizar falhas de segurança, bem como no desenvolvimento de uma política de segurança da informação.

Palavras-Chave: Tecnologia da informação e comunicação; Governo Eletrônico; Gestão da segurança da informação; Análise de vulnerabilidades.

ABSTRACT: The E-government can be described like the use of Information and Communication Technologies by the public administration, as a tool to support Government processes and deliver products and services to society. However digital platforms are subject to different types of cyber threats. These threats exploit vulnerabilities in the organizational and computational environment and put information assets at constant risk. This research goal was identified computational vulnerabilities in e-government sites in the Paraíba municipalities. Was considered as population of the survey the 50 municipalities that represent the largest share of the Gross Domestic Product of the State of Paraíba (83.4%), from this set it was possible to analyze the 40 sites. It is a descriptive research, with a quantitative approach. To data collect was used Nestparker, a software for penetration testing. As a result, 822 vulnerabilities were found, of which 15% are critical and 15% high critical, and 10% were classified as medium. Such vulnerabilities have the potential to allow hackers to provoke significantly impact the continuity of the services offered by these sites. Besides identifying the vulnerabilities, a study was carried out an analysis for each problem and proposing actions to correct each of the problems identified. This permit public managers to take actions aimed at minimizing security breaches, as well as making it possible to create tactics for developing an information security policy.

Keywords: Information and communication technology; Electronic Government; Information security management; Vulnerability analysis.

1 INTRODUÇÃO

Os avanços nas Tecnologias de Informação e Comunicação (TIC) permitiram o desenvolvimento de diversas aplicações, tais como o comércio eletrônico (*e-commerce*), a aprendizagem eletrônica (*e-learning*) e o governo eletrônico (*e-government*) (GUPTA; DASGUPTA; GUPTA, 2008). Sendo objeto de estudo dessa pesquisa, o governo eletrônico pode ser caracterizado como o uso e a aplicação das TIC, pela administração pública, com o intuito de racionalizar e integrar fluxos de trabalho e processos, conduzindo de maneira eficiente as informações e os serviços sob sua responsabilidade e atendendo às demandas da sociedade (UNITED NATIONS, 2014).

O desenvolvimento das TIC provoca alterações na dinâmica do governo com a sociedade, melhorando a organização do setor público, facilitando a comunicação com a sociedade, proporcionando outras maneiras de desenvolver a economia (FREIRE; STABILE, 2013) e se transformando em um instrumento de desenvolvimento sustentável (UNITED NATIONS, 2014).

Apesar de se utilizar das TIC, o governo eletrônico deve ser mais que o simples acesso à Internet, pois segundo a *Organization for Economic Cooperation and Development* (OECD, 2003), a prestação de serviços on-line ou a automação das rotinas de trabalho, deve ser encarada como uma iniciativa que busque o redesenho das estruturas burocráticas da administração pública a fim de que essa atinja os objetivos do papel do Estado (KENNEDY; COUGHLAN; KELLEHER, 2012), devendo envolver: i) mudanças nos fundamentos de funcionamento do governo e sua estrutura burocrática; ii) interação direta com os cidadãos, empresas, fornecedores e clientes internos do governo e iii) a busca pela contínua eficiência da administração pública em atender as demandas da sociedade (DAMIAN; MERLO, 2013).

O Banco Mundial (2015) destaca como principais vantagens da implementação do governo eletrônico: a redução dos custos das atividades, pois o atendimento eletrônico tem custos bastante reduzidos quando comparados ao atendimento presencial; a promoção do desenvolvimento econômico, pois simplifica as relações entre governo e setores produtivos; a melhoria da transparência, pois ao tornar as informações acessíveis de maneira fácil e rápida, possibilita a fiscalização por parte da sociedade; a melhoria na prestação de serviços, pois serviços on-line possibilitam a redução da burocracia e o aumento na qualidade dos serviços em tempo, conteúdo e acessibilidade.

De acordo com o *Government Accountability Office* (GAO, 2015), o avanço das TIC fez crescer a dependência do Governo Federal pela utilização de sistemas informatizados para realizar operações, processar, manter e relatar informações essenciais onde o governo eletrônico encontra na Internet seu principal canal de divulgação e comunicação com a sociedade. Conforme Mandarino Junior e Canongia (2010), a preocupação tanto com os conteúdos quanto com o tipo de uso, e a respectiva segurança da Internet, crescem em igual medida aos desenvolvimentos tecnológicos.

A Internet, por proporcionar conectividade em tempo real, expandiu fortemente o volume transacionado de informações disponíveis, mas ao mesmo tempo fez crescer a preocupação com o tráfego de informações que circulam por meio eletrônico e sua adequada segurança (CARVALHO, 2011). A preocupação com a segurança da informação é essencial para prevenir a perda de recursos, o uso não autorizado ou inadequado, a divulgação ou alteração de informações confidenciais e a interrupção das atividades das organizações (GAO, 2015).

As vulnerabilidades presentes nos sistemas de informação ou sites Web representam uma falha na concepção de um processo ou programa e essa fragilidade cria um ambiente propício a ser explorada por ameaças e/ou atacantes. O número de ataques virtuais contra governos e organizações comerciais continua a crescer em frequência e gravidade (PONEMON, 2015) e mostram uma tendência no aumento de ataques cada vez mais sofisticados e prejudiciais, pois na falta de programas e políticas adequadas de segurança, os governos têm experimentado um grande número de incidentes que envolvem perda de dados, roubos e invasões. O Centro de Tratamento de Incidentes de Segurança de Redes de Computadores da Administração Pública Federal (CTIR.Gov, 2016), responsável pela notificação e tratamento de incidentes da Administração Pública Federal, relatou mais de 5.000 incidentes ocorridos apenas no primeiro semestre de 2016.

Os órgãos governamentais não estão suficientemente protegidos para impedir as ameaças cibernéticas, pois conforme apontado pelo Tribunal de Contas da União (TCU) (BRASIL, 2014), o nível de adoção das práticas de segurança da informação, de forma geral, ainda está distante de um cenário satisfatório para a Administração Pública Federal (APF). O levantamento do TCU, apurou que 87% das organizações da Administração Pública Federal disponibilizam algum tipo de serviço por meio da Internet, o relatório também destacou que

61% das organizações da APF não apresentam capacidade adequada de governança e gestão de TI.

Dessa maneira, essa pesquisa propõe-se a responder a seguinte questão de pesquisa: Quais as possíveis vulnerabilidades computacionais existentes em sites de governo eletrônico dos municípios do Estado da Paraíba?

Tanto o Governo eletrônico como a gestão da segurança da informação são temas de estudo da Ciência da Informação. O Governo eletrônico é estudado por diferentes abordagens, como canal de disseminação da informação, democratização da informação, socialização da informação, controle do estado, satisfação dos usuários e até pela qualidade dos serviços oferecidos. No trabalho desenvolvido, o objetivo foi analisar possíveis vulnerabilidades computacionais existentes em sites de governo eletrônico dos municípios do Estado da Paraíba sob a ótica da gestão da segurança da informação e quando possível, fornecer subsídios para corrigir as vulnerabilidades e minimizar os riscos.

2 METODOLOGIA, DESENVOLVIMENTO E ANÁLISE

Para responder a essa questão foi escolhida uma amostra intencional. Segundo o Instituto Brasileiro de Geografia e Estatística (IBGE, 2016), a Paraíba possui 223 municípios. Como amostra foram considerados os 50 municípios que representam maior participação para a composição do Produto Interno Bruto do Estado da Paraíba – PIB (83,4%). Deste conjunto foi possível analisar os sites de 40 municípios. Em 10 municípios não foi possível aplicar os testes por instabilidades dos sites ou problemas de conexão de rede.

Cabe esclarecer que para fins desta pesquisa “sites de governo eletrônico” referem-se às páginas eletrônicas localizadas na Internet nas quais os governos dos municípios mostram sua “identidade, seus propósitos, suas realizações e possibilitam a concentração e disponibilização de serviços e informações, o que facilita a realização de negócios e o acesso à identificação das necessidades dos cidadãos” (PINHO, 2008, p. 473), podem possuir estruturas informacionais e computacionais mais simples ou mais complexas.

Esta pesquisa foi defendida em nível de mestrado no Programa de Pós-graduação nas Organizações Aprendentes - PPGOA da Universidade Federal da Paraíba. Em seu texto completo, a pesquisa aborda as características do governo eletrônico, suas vantagens e desafios, discute os conceitos de segurança da informação e sua importância para a adequada proteção dos sistemas e informações, descreve as vulnerabilidades identificadas e

propõe soluções para minimizar cada uma delas. Neste artigo estas discussões são breves, pois o texto está focado na apresentação dos resultados apurados na pesquisa.

Como instrumento para a coleta de dados foi utilizado o *software* Netsparker, que é um *scanner* de vulnerabilidades. Um *scanner* de vulnerabilidades é um sistema computacional que usa "[...] métodos automatizados para identificar vulnerabilidades em elementos e sistemas de rede" em que cada "um dos ativos pertencentes ao escopo da varredura é testado contra uma série de fraquezas conhecidas para a plataforma específica" (UTO, 2013, p. 37). A coleta de dados foi implementada entre março de junho de 2017, sendo necessárias mais de 300 horas de processamento para identificar as vulnerablidades da amostra. Foram utilizados 4 computadores tipo *workstation* do Laboratório de Tecnologias Intelectuais – LTI e um *laptop* para a realização desta tarefa.

O *scanner* utiliza-se de um banco de dados de vulnerabilidades já conhecidas. Este banco de dados é elaborado e atualizado com os dados de diferentes organizações: *Open Web Application Security Project* (OWASP), *Payment Card Industry* (PCI), *Common Weakness Enumeration* (CWE), *Web Application Security Consortium* (WASC) e *Common Attack Pattern Enumeration and Classification* (CAPEC). A organização OWASP, por exemplo, faz um levantamento trienal sobre as vulnerabilidades encontradas em aplicações Web. O Quadro 1 apresenta as 10 vulnerabilidades mais críticas em aplicações Web identificadas pela OWASP no relatório de 2013.

Quadro 1: Vulnerabilidades (OWASP).

POSIÇÃO	VULNERABILIDADE
1	*Injection*
2	*Broken Authentication and Session Management*
3	*Cross-Site Scripting (XSS)*
4	*Insecure Direct Object References*
5	*Security Misconfiguration*
6	*Sensitive Data Exposure*
7	*Missing Function Level Access Control*
8	*Cross-Site Request Forgery (CSRF)*
9	*Using Known Vulnerable Components*
10	*Unvalidated Redirects and Forwards*

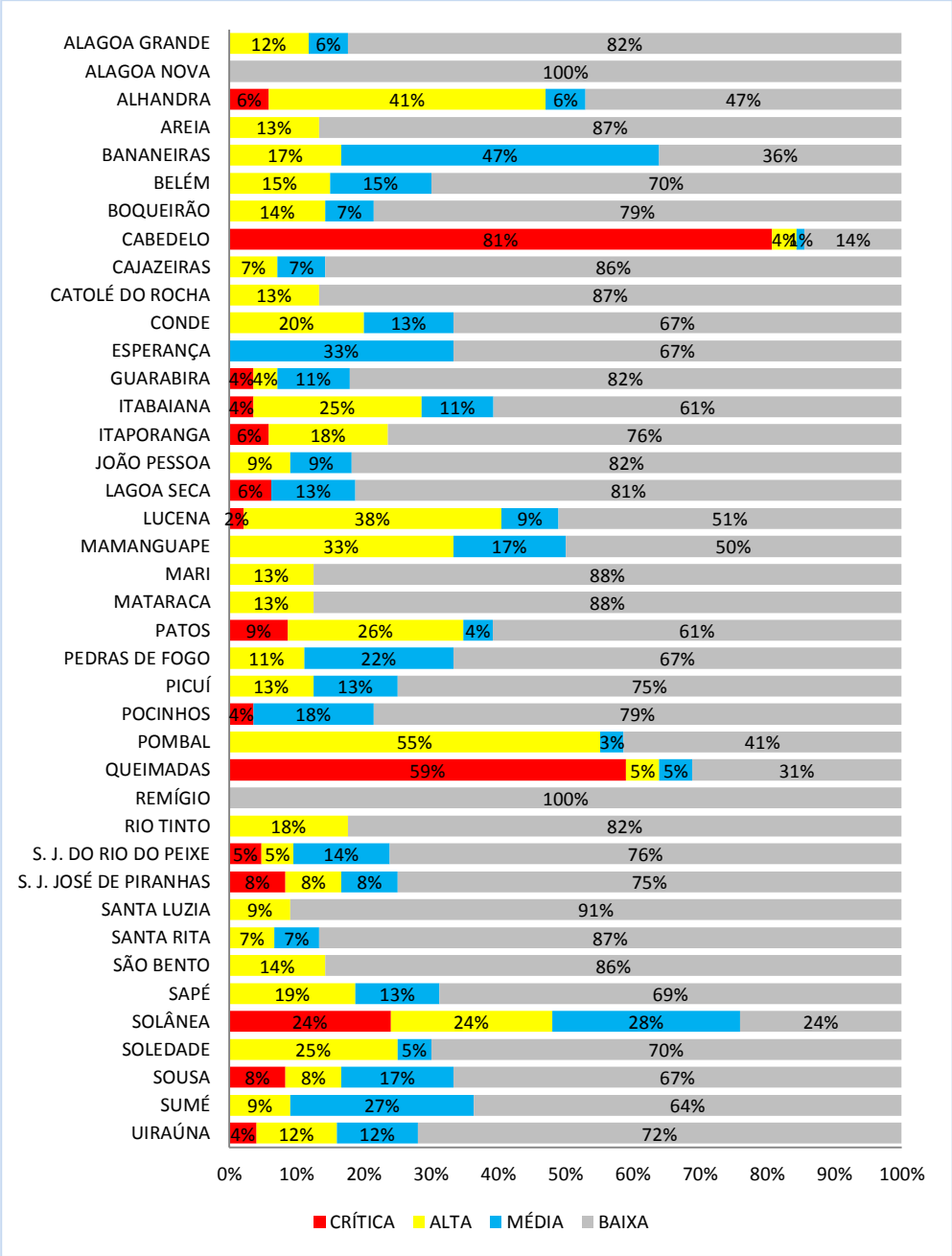
Fonte: Elaborado pelos autores com base nos dados da OWASP (2017).

Os graus de criticidade foram organizados em cinco níveis, sendo eles: i) Crítico, ii) Alta Criticidade, iii) Média Criticidade, iv) Baixa Criticidade e v) Alerta, sendo o nível Crítico o de maior risco. Quanto mais alto o nível de classificação de criticidade da vulnerabilidade detectada maior é a facilidade de acesso indevido aos sites de governo eletrônico.

3 RESULTADOS E DISCUSSÃO

No total foram identificadas 822 vulnerabilidades, das quais 15% são Críticas e 15% de Alta Criticidade e 10% foram classificadas como de Média Criticidade. O gráfico 1 apresenta um panorama geral das vulnerabilidades por níveis de criticidade para cada um dos sites analisados.

Gráfico 1: Vulnerabilidades por cidades.



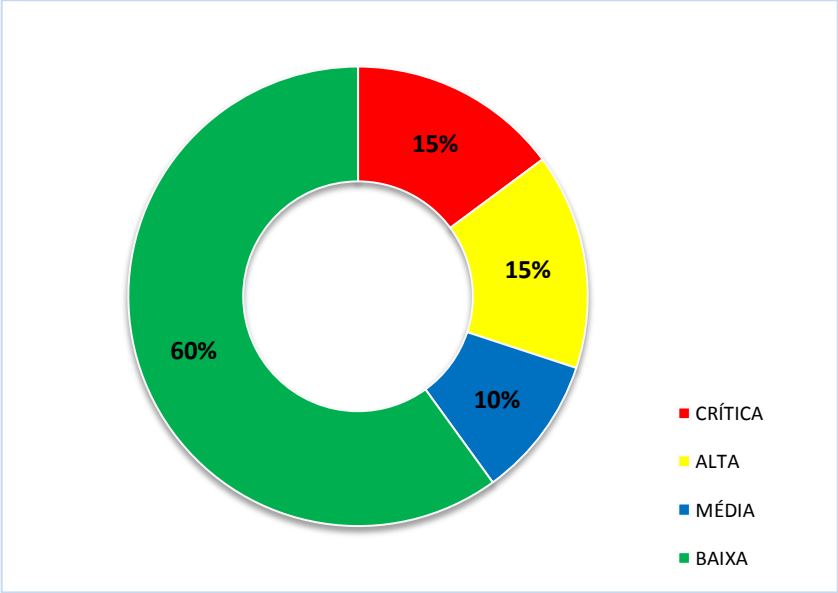
Fonte: Dados da pesquisa (2017).

Observa-se que algumas cidades apresentaram um alto percentual de vulnerabilidades Críticas e de Alta Criticidade, como: Alhandra (47%), Patos (35%), Cabedelo

(85%), Lucena (40%), Pombal (55%), Solânea (48%) e Queimadas (64%). Em comparação com relatório de ameaças do iBLISS (2016), que apresenta dados de organizações privadas no Brasil, observa-se que em média a soma das vulnerabilidades Críticas e de Alta Criticidade encontradas em setores privados do país correspondem a 20%, ou seja, alguns municípios desta amostra possuem um percentual de vulnerabilidades muito maior que a média do setor privado.

O Gráfico 2 resume o percentual de vulnerabilidade por nível de criticidade encontradas nos municípios participantes amostra. Ressalta-se que em 100% dos sites analisados foi identificado algum tipo de vulnerabilidade.

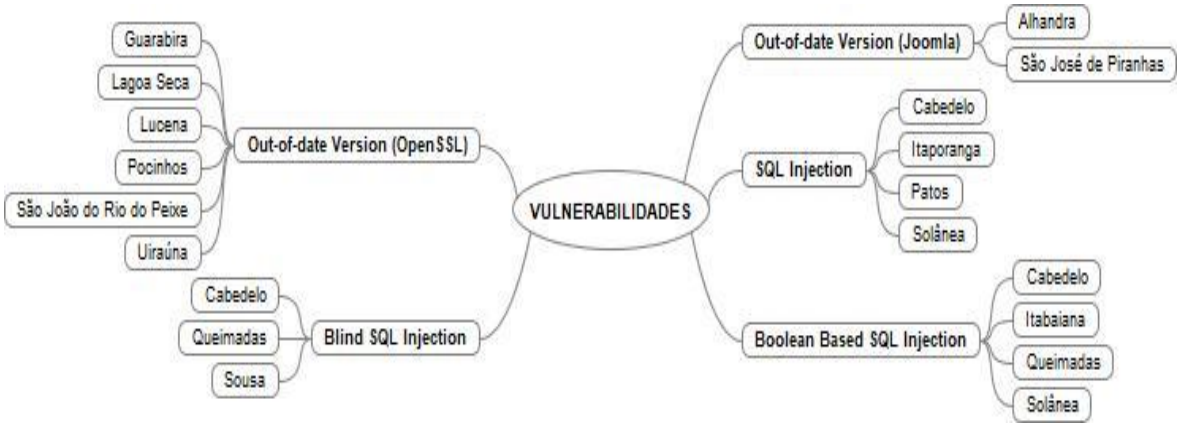
Gráfico 2: Percentual de vulnerabilidades por nível de criticidade.



Fonte: Dados da pesquisa (2017).

As vulnerabilidades Críticas são vulnerabilidades cuja exploração pode levar ao comprometimento em larga escala da infraestrutura de TI. “São brechas facilmente exploradas, pois o hacker não precisa de nenhuma credencial especial e nem precisa persuadir um usuário. Esse tipo de falha precisa ser remediado o mais rápido possível.” (IBLISS, 2016, p. 4). A figura 1 apresenta as vulnerabilidades Críticas associadas aos sites das cidades.

Figura 1: Vulnerabilidades críticas *versus* cidades.



Fonte: Dados da pesquisa (2017).

Conforme a proposta do trabalho, cada vulnerabilidade identificada foi estudada na literatura especializada, sendo descrito seu impacto e as medidas para corrigir e minimizar os riscos expostos. Nos tópicos 3.1 a 3.3 são detaladas as vulnerabilidades classificadas como críticas e as medidas para sua correção.

3.1 Vulnerabilidade - *Out-of-date Version (Joomla)*

O *Joomla* é um sistema de gerenciamento de conteúdo de código aberto para a publicação de conteúdo da Web. O Netsparker identificou que alguns sites pesquisados estão usando o código *Joomla* e detectou que o mesmo encontra-se desatualizado.

A desatualização desse código apresenta várias vulnerabilidades que podem ser exploradas por atacantes. Entre as vulnerabilidades encontradas em virtude da desatualização do *Joomla*, destacam-se:

a. ***Joomla CSRF Vulnerability***: Permite que atacantes remotos sequestrem a autenticação de vítimas não especificadas para pedidos que carregam o código via vetores desconhecidos. CSRF é um ataque que engana a vítima para enviar uma solicitação maliciosa. Ele herda a identidade e privilégios da vítima para desempenhar uma função indesejada em nome da vítima.

b. ***Joomla SQL Injection Vulnerability:*** permite que um usuário remoto não autorizado obtenha privilégios de administrador sequestrando a sessão de administrador. Após a exploração da vulnerabilidade, o invasor pode obter o controle total do site e executar ataques adicionais.

c. ***Joomla Sensitive Information Disclosure:*** Um invasor pode obter informações confidenciais ou ignorar certas restrições de segurança e executar ações não autorizadas.
d. ***Joomla! Multiple XSS Vulnerabilities:*** Essa vulnerabilidade refere-se ao ataque de injeção de código do lado do cliente, em que um invasor pode executar *scripts* maliciosos. O invasor explora uma vulnerabilidade dentro de um site ou aplicativo da Web que a vítima visita, usando essencialmente o site vulnerável como veículo para entregar um *script* malicioso ao navegador da vítima.

A solução para a corrigir essa vulnerabilidade consiste na atualização da plataforma de gerenciamento de conteúdo *Joomla* para a sua versão mais recente. As cidades que apresentaram essa vulnerabilidade foram: Alhandra e São José de Piranhas. Essa vulnerabilidade é classificada como critica pelas organizações OWASP (2013), PCI (2016) e CAPEC (2017).

3.2 *Out-of-date Version (OpenSSL)*

O *OpenSSL* é um código aberto do padrão *Secure Socket Layer* (SSL) usado em inúmeros servidores Web. O SSL é um protocolo que ao invés de transmitir os pacotes em texto simples, legível por humanos, ele permite que as informações sejam criptografadas utilizando algoritmos, ou seja, as informações deverão ser lidas apenas pelo usuário a quem se destina a mensagem, não sendo possível que durante o tráfego da informação, usuários não autorizados tenham acesso aos dados. O Netsparker identificou que alguns sites pesquisados estão usando o *OpenSSL* e detectou que o mesmo encontra-se desatualizado.

A desatualização desse código apresenta várias vulnerabilidades que podem ser exploradas por atacantes. Entre essas vulnerabilidades, destacam-se:

a. ***OpenSSL Denial of Service Vulnerability:*** Esse tipo de ataque tem como objetivo a negação de serviço (DoS), ou seja, um invasor tenta impedir que usuários legítimos acessem informações ou serviços. Quando você digita um URL para um determinado site no seu navegador, você está enviando uma solicitação para o servidor do computador desse site para exibir a página. O servidor só pode processar um certo número de requisições ao mesmo tempo, portanto, se um invasor sobrecarregar o servidor com solicitações excessivas, ele não poderá

processar as solicitações legítimas. Esta é uma "negação de serviço", porque impede o acesso ao site.

b. ***OpenSSL TLS Heartbeart Read Overrun Vulnerability:*** Essa vulnerabilidade permite que informações protegidas sejam roubadas da comunicação criptografada SSL / TLS, ou seja, um invasor é capaz de acessar dados previamente alocados na memória e que pode incluir desde *cookies* de sessão à chaves privadas (que são usadas para a segurança da comunicação entre dois computadores).

c. ***OpenSSL Information Disclosure Vulnerability:*** Ao atacar um servidor que usa uma versão vulnerável do *OpenSSL*, um invasor remoto não autenticado pode recuperar informações confidenciais, como senhas secretas. Ao levantar essas informações, um invasor pode decriptar, falsificar ou executar ataques *man-in-the-middle* no tráfego de rede que de outra forma estariam protegidos pelo *OpenSSL*.

A solução para a correção dessa vulnerabilidade consiste na atualização do código *OpenSSL* para a sua versão mais recente. Essa vulnerabilidade está classificada como crítica em conformidade com as organizações OWASP (2013), PCI (2016) e CAPEC (2017).

3.3 *SQL Injection / Blind SQL Injection / Boolean Based SQL Injection*

Estas são três vulnerabilidades Críticas baseadas na linguagem SQL, a diferença entre cada uma das vulnerabilidades é a técnica utilizada para a sua exploração. Nesse caso específico, a correção da vulnerabilidade será a mesma para as três vulnerabilidades Críticas encontradas.

O SQL é uma linguagem de programação projetada para gerenciar dados armazenados em um Sistema de Gerenciamento de Banco de Dados Relacional (RDBMS), portanto SQL pode ser usado para acessar, modificar e excluir dados.

A *SQL Injection* é uma técnica de ataque baseada na manipulação do código SQL que visa comprometer a segurança da base de dados por meio de comandos inseridos nos campos de formulários ou URL. Um ataque bem-sucedido permite o acesso aos dados confidenciais dos usuários registrados no banco de dados do sistema/aplicação, ou seja, através de uma manipulação forçada do código SQL é possível que um atacante consiga

acesso ao sistema se fazendo passar por um usuário real. É possível também que o atacante manipule ou até destrua os dados presentes no banco de dados, impossibilitando que usuários antes cadastrados, tenham o devido acesso.

O OWASP (2013) alerta que SQL *Injections* podem resultar em perda ou corrupção de dados, falta de responsabilização ou negação de acesso. Algumas vezes esta ação pode levar ao comprometimento completo do servidor. Essa vulnerabilidade está classificada como critica pelas organizações OWASP (2013), PCI (2016), CWE (2017), WASC (2017) e CAPEC (2017).

A *Blind SQL Injection* se assemelha à SQL *Injection*, a única diferença é a forma como os dados são recuperados do banco de dados. Quando o site é configurado para mostrar mensagens de erro genéricas (erro padrão HTTP 500 ou 404) e o banco de dados não fornece dados para a página da Web, o invasor rouba os dados enviando ao banco de dados com uma série de perguntas verdadeiras ou falsas. É possível também que o atacante manipule ou até destrua os dados presentes no banco de dados, impossibilitando que usuários antes cadastrados tenham o devido acesso.

A técnica de exploração booleana é muito útil quando o testador encontra uma situação de *Blind SQL Injection* na qual nada é conhecido sobre o resultado de uma operação. Esse comportamento pode ocorrer nos casos em que o programador criou uma página de erro personalizada que não revela nada na estrutura da consulta ou no banco de dados (a página não retorna um erro SQL, ela retorna um erro padrão HTTP 500 ou 404, ou ainda realiza o redirecionamento). Usando métodos de inferência, é possível evitar este obstáculo e assim obter êxito na recuperação dos valores de alguns campos desejados. Este método consiste em realizar uma série de consultas booleanas contra o servidor, observando as respostas e finalmente deduzindo o significado de tais respostas.

Aqui também a manipulação dos códigos SQL em um ataque, caso bem-sucedido, permite ao atacante o acesso ao banco de dados do site onde, terá acesso aos dados confidenciais dos usuários, podendo alterá-los ou excluí-los.

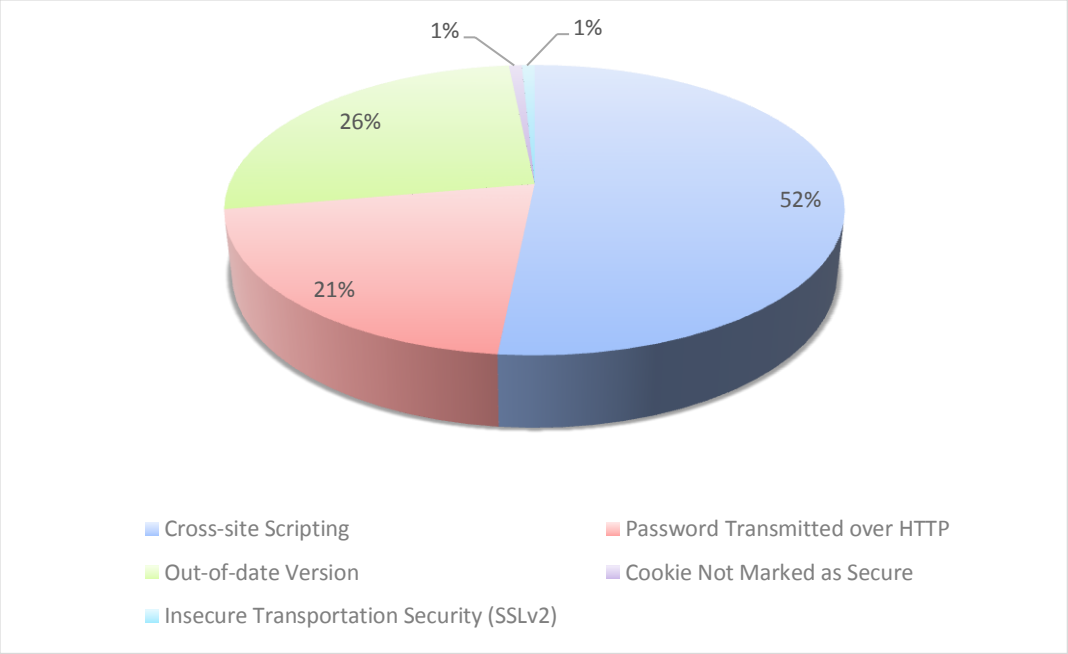
Conforme o OWASP (2013), a solução para a correção das três vulnerabilidades baseadas no código SQL consiste em:

- Utilizar uma interface segura que evite o uso do interpretador inteiramente ou forneça uma interface parametrizada.

- Caso uma interface parametrizada não esteja disponível, deve-se filtrar cuidadosamente os caracteres especiais utilizando a sintaxe para esse interpretador.
- Utilizar uma “lista branca" ou validação de entrada positiva também é recomendado, mas não é uma defesa completa, já que muitas aplicações requerem caracteres especiais em suas entradas.

O gráfico 3 apresenta os percentuais por tipos de vulnerabilidades de Alta Criticidade, possibilitando uma perspectiva mais ampla dos problemas levantados neste trabalho.

Gráfico 3: Tipo de vulnerabilidades de Alta Criticidade.



Fonte: Dados da pesquisa (2017).

A vulnerabilidade *Cross-site Scripting* é a que apresenta maior incidência (52%) entre as vulnerabilidades de Alta Criticidade e está inserida entre as dez vulnerabilidades mais críticas às aplicações Web segundo o relatório da OWASP (2013).

O *Cross-site Scripting* (XSS) refere-se ao ataque de injeção de código do lado do cliente, em que um invasor pode executar *scripts* maliciosos em um site ou aplicativo Web. Ao executar o XSS, um atacante não tem como alvo uma vítima diretamente. Em vez disso, o invasor explora vulnerabilidades dentro de sites ou aplicativo da Web que a vítima visita, usando essencialmente o site vulnerável como veículo para entregar *scripts* maliciosos

ao navegador da vítima. O navegador do usuário final entende que o *script* veio de uma fonte confiável, o que permite a esse *script* mal-intencionado acessar todos os *cookies*, *tokens* de sessão ou outras informações confidenciais retidos pelo navegador (OWASP, 2016).

Destaca-se também a vulnerabilidade *Out of date Version* (desatualização), que é responsável por 26% das vulnerabilidades de Alta Criticidade, o que evidencia uma dificuldade em gerir eficientemente as atualizações de softwares. O relatório do iBLISS (2016) destacou que as desatualizações de software correspondem a 32% das falhas de segurança do setor privado.

4 CONSIDERAÇÕES

A Internet tornou-se um importante meio para interações e busca de informações. Contudo é um espaço repleto de ameaças, o que eleva a necessidade de cuidados em relação à segurança da informação. Os sites de governo eletrônico, ao oferecerem serviços pela Internet ficam expostos a estas ameaças que podem criar problemas para a segurança e a confiança dos cidadãos.

Nesse contexto, essa pesquisa permitiu identificar as vulnerabilidades eletrônicas a que estão sujeitos os sites de governo eletrônico dos municípios do Estado da Paraíba. Dos 50 municípios delimitados para compor a população dessa pesquisa, em 10 não foi possível executar o *scanner* de vulnerabilidade em razão de não haver resposta do servidor (computador) responsável por hospedar o site de governo eletrônico do município ou por instabilidade de conexão da rede.

Em todos os municípios, os sites analisados apresentaram vulnerabilidades que variaram de Baixa à Média Criticidade, e não necessitam de correção tão imediata. Já vulnerabilidades Críticas e de Alta Criticidade, necessitam de remediação urgente dada sua capacidade de interromper a continuidade do serviço e comprometer a confidencialidade, integridade e disponibilidade da informação.

Foram encontradas 822 vulnerabilidades, 30% dessas são Críticas e de Alta Criticidade, o que indica fragilidade, por parte da Administração Pública, no gerenciamento e controle da segurança da informação. Essas falhas têm o potencial de causar danos significativos à capacidade dos municípios prestarem serviços aos seus usuários.

Observando a alta taxa de vulnerabilidades Críticas e de Alta Criticidade, pode se inferir a inexistência, ou pelo menos, a ineficiência de uma política de segurança da informação que tenha como um de seus objetivos. O monitoramento constante de ameaças eletrônicas a fim de procurar reduzir os impactos negativos de uma possível exploração dessas vulnerabilidades.

Os danos decorrentes da exploração de vulnerabilidades Críticas e de Alta Criticidade permitem o roubo de senhas e de dados sigilosos, acesso remoto, alterações de conteúdo, controle da administração de servidores (computadores), exclusão de dados, etc. Dessa forma, essa pesquisa contribuiu para a identificação desse tipo de vulnerabilidade, evidenciando suas possíveis consequências.

Cabe ressaltar que duas vulnerabilidades identificadas nessa pesquisa e recorrentes na maioria dos municípios analisados foram as *Out-of-Date-Version* (desatualização de *software*) e *Password Transmitted over* HTTP (senha transmitida pelo HTTP). O que reforça a percepção da falta de uma política básica de segurança da informação e evidencia a fragilidade na questão da segurança da informação em portais de governo eletrônico, pois são duas vulnerabilidades de fácil correção.

A desatualização de *software* é facilmente resolvida com um simples cronograma de verificação das possíveis atualizações que são disponibilizadas pelos desenvolvedores. A transmissão não autorizada de senhas pelo HTTP é resolvida alterando o modo de conexão para HTTPS, o que assegura que as informações transmitidas serão criptografadas, aumentando significativamente a segurança dos dados.

A interação e integração entre governo e usuários levam à necessidade de retenção de dados destes usuários, logo isto passa a ser um ponto crucial na administração de um sistema de governo eletrônico, pois a responsabilidade por garantir a segurança dessas informações torna-se um desafio para os gestores.

Antes da implantação de um sistema de governo eletrônico os municípios deveriam ter como prioridade a segurança da aplicação, eliminando ou pelo menos diminuindo possíveis falhas. Conforme demonstrado na análise dos dados dessa pesquisa, essa prioridade não foi percebida, pois 95% municípios da amostra, apresentaram vulnerabilidades com o potencial de prejudicar a continuidade dos serviços e/ou expor os dados de seus usuários.

Infere-se desse dado que existe a necessidade de monitoramento constante por parte dos gestores desses sistemas na busca de identificar e sanar vulnerabilidades e no aperfeiçoamento da segurança. Alerta-se para o fato de que nos sites identificados com vulnerabilidade baixas, não necessariamente significa que estes estão bem gerenciados ou foram construídos de forma segura, o mais provável é que sejam simples páginas estáticas que não oferecem serviços transacionais à população. Como esta pesquisa foi quantitativa e não qualitativa, com foco na segurança da informação, o conteúdo dos sites não foi avaliado, portanto trata-se apenas de uma hipótese. Validar ou refutar esta hipótese pode ser objeto de outros estudos.

O relatório apresentado pelo TCU (2014) identificou que 61% das organizações da Administração Pública Federal não apresentam capacidade adequada de Governança e Gestão de TI, ou seja, não conseguem gerir de forma eficaz seus sistemas de informação. Os dados levantados neste artigo sugerem que a Administração Pública Municipal no Estado da Paraíba também apresenta problemas neste mesmo segmento.

As ameaças eletrônicas estão em constante desenvolvimento e sempre em busca de vulnerabilidades que permitam o acesso às informações sigilosas. Observamos que os sites estudados nessa pesquisa não estão suficientemente protegidos para evitar consistentemente essas ameaças.

Por fim, é imprescindível a adoção de uma política de segurança que acompanhe e monitore cada etapa de implantação dos sistemas de governo eletrônico e permita minimizar as vulnerabilidades decorrentes de falhas de programação e sua possível exploração. Este trabalho traz um alerta aos gestores dos sites analisados, pois independente do nível de criticidade das vulnerabilidades identificadas, todos os participantes da amostra apresentaram algum tipo de falha em seus sites. Os administradores públicos devem considerar o uso de ferramentas de detecção de vulnerabilidades para ajudar a examinar e desenvolver planos que solucionem os problemas em curto e longo prazo.

REFERÊNCIAS

BANCO MUNDIAL. **e-Goverment**. 2015. Disponível em: <http://www.worldbank.org/en/topic/ict/brief/e-government.> Acesso em: 13 jul. 2016.

BRASIL. Tribunal de Contas da União. **Acórdão nº 3.117/2014.** 2014. Plenário. Relator: Ministro Augusto Sherman Cavalcanti. Sessão de 12/11/2014. Disponível em:

<http://portal.tcu.gov.br/lumis/portal/file/fileDownload.jsp?fileId=8A8182A14D78C1F1014D794C57073235>. Acesso em: 25 out. 2016.

CARVALHO, Paulo Sérgio Melo. Conferência de abertura: o setor cibernético nas forças armadas brasileiras. In: BARROS, Otávio Santana Rego; GOMES, Ulisses Mesquita (Org.). **Desafios estratégicos para segurança e defesa cibernética**. Brasília: 2011. p. 13-34. Disponível em: <http://livroaberto.ibict.br/bitstream/1/612/2/Desafios%20estrat%C3%A9gicos%20para%20seguran%C3%A7a%20e%20defesa%20cibern%C3%A9tica.pdf >. Acesso em: 14 out. 2016.

CENTRO DE TRATAMENTO DE INCIDENTES DE SEGURANÇA DE REDES DE COMPUTADORES DA ADMINISTRAÇÃO PÚBLICA FEDERAL. **Estatísticas de incidentes de rede na APF**: 1° trimestre. 2016. Disponível em: <http://www.ctir.gov.br/arquivos/estatisticas/2016/Estatisticas_CTIR_Gov_1o_Trimestre_2016.pdf>. Acesso em: 15 out. 2016.

COMMON ATTACK PATTERN ENUMERATION AND CLASSIFICATION – CAPEC. 2017. Disponível em: <https://capec.mitre.org/>. Acesso em: 13 abr. 2017.

COMMON WEAKNESS ENUMERATION - CWE. Cross-site Scripting. Disponível em: <https://cwe.mitre.org/data/definitions/79.html>. Acesso em: 13 abr. 2017.

DAMIAN, Ieda Pelógia Martins; MERLO, Edgard Monforte. Uma análise dos sites de governos eletrônicos no Brasil sob a ótica dos usuários dos serviços e sua satisfação. **Revista de Administração Pública**, v. 47, n. 4, p. 877-900, 2013.

FREIRE, Felipe Ribeiro; STABILE, Max. As novas tecnologias e a participação eletrônica: entre promessas e desafios. In: BARBOSA, Alexandre F. (Coord.). **Pesquisa sobre o uso das tecnologias da informação e comunicação no setor público brasileiro:** TIC governo eletrônico 2013. São Paulo: 2014. p. 47-56. Disponível em: <http://cetic.br/media/docs/publicacoes/2/TIC_eGOV_2013_LIVRO_ELETRONICO.pdf>. Acesso em: 25 ago. 2016.

GOVERNMENT ACCOUNTABILITY OFFICE - GAO. **Information Security:** federal agencies need to better protect sensitive data. [S.l.: s.n], 2015. Disponível em: <http://www.gao.gov/assets/680/673678.pdf>. Acesso em: 16 out. 2016.

GUPTA, Babita; DASGUPTA, Subhasish; GUPTA, Atul. Adoption of ICT in a government organization in a developing country: An empirical study. **Journal of Strategic Information Systems**, v. 17, p. 140-154, 2008.

IBLISS. **Relatório de Ameaças de 2016**. Disponível em: <https://www.ibliss.com.br/relatorio-de-ameacas-2016/>. Acesso em: 05 mar. 2017.

INSTITUTO BRASILEIRO DE GEOGRAFIA E ESTATÍSTICA - IBGE. Disponível em: <http://cidades.ibge.gov.br/download/mapa_e_municipios.php?lang=&uf=pb>. Acesso em 27 de out. 2016.

KENNEDY, Aileen; COUGHLAN, Joseph P.; KELLEHER, Carol. Business process change in e-government projects: the case of the Irish land registry.**Technology Enabled Transformation of the Public Sector:** Advances in E-Government: Advances in E-Government. 2012.

MANDARINO JÚNIOR, Raphael; CANONGIA, Cláudia. **Segurança cibernética no Brasil:** livro verde. Gabinete de Segurança Institucional (GSI), Brasília, DF, 2010.

OPEN WEB APPLICATION SECURITY PROJECT – OWASP. **Owasp Top 10-2013**: the ten most critical web application security risks. 2013. Disponível em: <http://www.lulu.com/shop/owasp-foundation/owasp-top-10-2013/paperback/product-21241952.html>. Acesso em: 26 de out. 2016.

ORGANIZATION FOR ECONOMIC COOPERATION AND DEVELOPMENT - OECD. **The case of E-government**: Excerpts from the OECD Report "The E-Government Imperative". Paris: OECD, 2003. Disponível em: <https://www.oecd.org/gov/budgeting/43496369.pdf>. Acesso em 23 de jun. 2016.

PAYMENT CARD INDUSTRY – PCI. **The Prioritized Approach to Pursue PCI DSS Compliance, 2016.** Disponível em: <https://www.pcisecuritystandards.org/documents/Prioritized-Approach-for-PCI_DSS-v3_2.pdf?agreement=true&time=1493141839795>. Acesso em: 13 abr. 2017.

PINHO, José Antônio Gomes. Investigando portais de governo eletrônico de estados no Brasil: muita tecnologia, pouca democracia. **Revista de Administração Pública**, v. 42, n. 3, p. 471-493, 2008.

PONEMON INSTITUTE. **2015 Cost of Cyber Crime Study:** Global. [S.l.: s.n], 2015. Disponível em: <https://ssl.www8.hp.com/ww/en/secure/pdf/4aa6-1889ptl.pdf>. Acesso em: 16 out. 2016.

UNITED NATIONS. E-Government Survey 2014: E-Government for the future we want. **United Nations Department of economic and social affairs**, 2014. Disponível em: <https://publicadministration.un.org/egovkb/Portals/egovkb/Documents/un/2014-Survey/E-Gov_Complete_Survey-2014.pdf>. Acesso em: 15 jul. 2016.

UTO, Nelson. **Teste de invasão de aplicações web.** Rio de Janeiro, RJ, 2013, Disponível em: <https://esr.rnp.br/livro/seg9#p/20>. Acesso em: 25 de out. 2016.

WEB APPLICATION SECURITY CONSORTIUM – WASC.
Disponível em: <http://www.webappsec.org/>. Acesso em: 13 abr. 2017.