DOI: 10.5748/9788599693124-13CONTECSI/RF-4145

COUNTERMEASURES TO RISKS THAT ARE EXPOSED TO THE WEB APPLICATION VULNERABILITIES: A LITERATURE REVIEW

Cleberton Carvalho Soares (Faculdade Estácio de Sergipe, Sergipe,Brasil) cleberton.soares@estacio.br
Paulo Caetano da Silva (Universidade Salvador, Bahia,Brasil) paulo.caetano@prof.unifacs.br

Information is an influential variable in corporate environment, potentially rich and fundamental for strategic planning. Among the technologies related to software engineering, web applications currently add, nowadays, most of architected and built software products; however, web is a communication environment that imposes several risks to the information that is manipulated and exchanged on it. Especially for secret or confidential information,is recommended to know the risks that it is exposed to, related countermeasures to protect,and efforts that must be done to propose alternatives to improve the processes of software engineering to encourage appropriate use of information protection. This article aims to present a literature review on countermeasures to solve or mitigate security risks that exposes web applications to multiple vulnerabilities. This work is hoped to serve as a support for software engineering professionals to can deploy web applications with higher level of information security.

Keywords: Web Applications, Security Risks, Information Security.

CONTRA MEDIDAS A RISCOS QUE EXPÕEM AS APLICAÇÕES WEB A VULNERABILIDADES: UMA REVISÃO DA LITERATURA

A informação é uma variável influente no ambiente corporativo, potencialmente rica e fundamental para o planejamento estratégico. Dentre as tecnologias relativas a engenharia de software, as aplicações web, atualmente,agregam a maioria dos produtos de softwares arquitetados e construídos; porém, a web é um ambiente de comunicação que impõe vários riscos à informação que por ela é manipulada e intercambiada. Principalmente para informações confidenciais e sigilosas, convém saber quais os riscos e quais as contra medidas que servem de proteção para a informação, e empreender esforços para propor alternativas para melhoria nos processos da engenharia de software para que estimulem uma utilização adequada de proteção à informação. Este artigo apresenta uma revisão da literatura sobre contra medidas para dirimir ou mitigar riscos de segurança que expõem as aplicações web a diversas vulnerabilidades. Espera-se que este trabalho sirva de apoio para que profissionais de engenharia de software possam implementar aplicações web com níveis mais elevados de segurança da informação.

Palavras-chave: Aplicações Web, Riscos de Segurança, Segurança da Informação.

1. INTRODUÇÃO

O risco é um problema potencial que pode ou não ocorrer, com características particulares para cada sistema, mesmo que estes sistemas sejam similares. Para eliminar ou mitigar o risco é essencial dedicar-se à análise daqueles que são considerados comuns, certos ou óbvios, já que por serem conhecidos, têm maior chance de serem eliminados. Porém, convém dar maior ênfase àqueles que promovem impacto negativo de maiores proporções, seja na esfera da tecnologia ou do negócio. Encontrar soluções para combater riscos continua a ser um importante problema de pesquisa (SHAR, 2012:1).

Encontra-se na literatura, com maior destaque a da área de administração, ênfase sobre o nível de relevância da informação para as organizações. A informação é uma variável influente no ambiente corporativo, potencialmente rica e fundamental para o planejamento estratégico. Qualquer ferramenta tecnológica que interaja ou infira com a informação, em qualquer etapa do seu ciclo de vida, precisa utilizar-se de mecanismos que priorize o nível de segurança da informação adequado ao negócio (BEAL, 2005).

O uso e desenvolvimento de tecnologias da informação são fomentados pelos sistemas de informações, os quais definem novos paradigmas para a produção, gestão e intercâmbio dos produtos de informação. Esses sistemas, segundo a norma ABNT 27002 (2013), são expostos a diversos riscos a partir de ameaças à segurança da informação, incluindo fraudes eletrônicas, espionagem, sabotagem, vandalismo, roubo. A evolução do comércio e dos negócios eletrônicos, por exemplo, tonaram a privacidade uma grande preocupação da sociedade da informação.

Dentre as tecnologias relativas a engenharia de software, as aplicações web atualmente agregam a maioria dos produtos de softwares arquitetados e construídos, porém, a web é um lugar em que encontramos a maioria dos intrusos, espionando e tentando fazer uso indevido da informação (TANENBAUM; WETHERALL, 2011), além de ser considerada por Sêmola (2005) uma infraestrutura sem gestão. É neste contexto tecnológico de comunicação que ocorre o intercâmbio de informações por meio de aplicações web. Portanto, as ameaças presentes na Internet expõem as informações, em seu ciclo de vida, a diversos riscos de segurança da informação, portanto, torna-se imprescindível identificá-los para dirimi-los ou mitigá-los.

No âmbito da comunicação através da Internet, encontra-se vasta literatura alusiva a implementação de proteção para informação com uso dos protocolos de comunicação (e.g. VPN, SSL/TLS, IPSec, IPv6) que subsidiam proteção ao ambiente de trânsito da informação, ou seja, nas camadas de rede e transporte do modelo OSI (SILVA, 2012). Contudo, não somente a utilização de protocolos de redes de computadores seguros é suficiente para atender a demanda de segurança da informação para a Internet e para as aplicações web; se assim o fosse, problemas alusivos ao roubo e alteração de informações como, por exemplo, senhas de cartão de crédito ou de *internet banking* que transitam pela Internet não seriam tão recorrentes, além de tantos outros tipos de ataques mencionados por pesquisas recentes, conforme podemos observar em BORGOHAIN; KUMAR; SANYAL (2015).

Este artigo está organizado da seguinte forma: a Seção 2 discute-se os principais riscos de segurança em aplicações web. Na Seção 3 é apresentada a revisão da literatura; e na Seção 4 são feitas recomendações a partir do que foi encontrado nos trabalhos e a conclusão do artigo.

2. PRINCIPAIS RISCOS DE SEGURANÇA EM APLICAÇÕES WEB

A diversidade oriunda das estratégias para empreender ataques às aplicações web e das vulnerabilidades de segurança criam as possibilidades de se obter êxito em obter e/ou alterar as informações confidenciais sigilosas sem a devida autorização. As possiblidades formam rotas. Todas as rotas buscam comprometer o funcionamento das aplicações web, seja através de impactos técnicos (e.g. parada no banco de dados), ou propiciar um impacto no negócio da empresa, comprometendo sua credibilidade diante do mercado. E exatamente a exploração destas rotas que formam os riscos.

Muitas instituições internacionais visam apoiar o desenvolvimento de sistemas com atenção às questões de segurança para a aplicação, oferecendo publicações a respeito da implementação de segurança para o produto de software, suporte técnico e treinamentos, dentre outras atividades, e.g. (i) a CWE (Common Weakness Enumeration); (ii) o Institute SANS ; (iii) a Common Vulnerabilities and Exposures (CVE); (iv) a SAFECode ; (v) o Web Application Security Consortium (WASC); e (vi) a Open Web Application Security Project (OWASP) .

Dentre as organizações que emitem normas sobre segurança da informação, podemos destacar a ISO (International Organization for Standardization), a BSi (British Standards) e a AS/NZS (Australian/New Zealand Standard). No Brasil, a ABNT (Associação Brasileiras de Normas Técnicas) é a responsável pela recomendação de padrões técnicos em diversas áreas e também é um membro da ISO. Dentre outras recomendações, a ABNT dispõe de um conjunto de normas para implantação de um sistema gestor de segurança da informação.

A identificação de riscos para as aplicações web foi um dos desafios a serem transpostos neste trabalho, para isso foi realizada uma pesquisa que permitiu a escolha do periódico da OWASP denominado de OWASP Top 10. Esse periódico, cuja publicação tem aceitação acadêmica (XIAOLI et al, 2009; ALBREIKI et al; CARVALHO, 2014), tem uma base de dados que envolve informações de milhares de organizações em todo o mundo e cujo foco é nos riscos inerentes às tecnologias web. O periódico OWASP Top 10 já está na quinta publicação ao longo de dez anos, sendo a OWASP Top 10 2013 a mais atual edição.

Dentre os objetivos da OWASP na publicação do periódico está o de apoiar as empresas que desenvolvem aplicativas web, apresentando os dez riscos mais críticos encontrados em aplicações web, através de uma análise quantitativa. A análise quantitativa leva em consideração a verificação de quantas aplicações web pesquisadas apresentadas um determinado risco, dentre todas que estão disponíveis para serem analisadas.

Por tratar especificamente dos riscos sobre as aplicações web; pela aceitação acadêmica; e pela relevante base de dados para a elaboração do periódico, os riscos identificados pelo periódico da OWASP são admitidos como referência para transpor o desafio de identificação dos riscos para a elaboração da revisão da literatura proposta neste artigo.

Com base no periódico OWASP Top 10 2013, a negligência ou imperícia dos profissionais da engenharia de software em relação à segurança informação expõem as aplicações web aos riscos listados na Tabela 1, a qual também detalha sobre as consequências que podem ocorrer caso o ataque à aplicação web tenha sucesso, além de classificar respectivamente o impacto de cada um dos riscos relacionados.

Apesar do esforço empreendido pela OWASP na publicação do seu periódico, constata-se a partir da comparação entre as versões disponíveis do OWASP Top 10, que os riscos são praticamente os mesmos, com pouca variação na quantidade de aplicações web vulneráveis e na ocorrência de novos riscos. Portanto, tornar-se uma motivação saber por que analistas de sistemas e programadores mantêm seus produtos de softwares vulneráveis a riscos conhecidos? E por que as empresas permitem manipular ou intercambiar suas informações confidenciais sigilosas, em ambiente tão inóspito como a Internet, sem níveis elevados de segurança para a informação?

Tabela 1 - Riscos mais críticas encontrados em aplicações web

RISCOS	CONSEQUÊNCIAS	Impactos ao Negócio
Injeção de código	Manipulação nos dados pode fazer com que o interpretador execute comandos indesejados ou permita o acesso a dados não autorizados por meio dos objetos identificados.	Severo
Quebra de Autenticação e Gerenciamento de Sessão	Assumir a identidade de usuários, principalmente maiores privilégios (administrador, por exemplo), sem autenticar-se ou para má implementação da aplicação.	Severo
Cross-Site Scripting (XSS)	Assumir sessões do usuário, alterar informação ou redirecionar o usuário para sites com dados maliciosos.	Moderado
Referência Insegura e Direta e Objetos	Manipular estas referências para expor e explorar o objeto referenciado, inclusive tornando-o público.	Moderado
Configuração Incorreta de Segurança	Aplicação web com baixo nível de segurança, com estrutura baseada em legado com várias lacunas de segurança da informação.	Moderado
Exposição de Dados Sensíveis	Roubar ou modificar dados desprotegidos com o propósito de realizar fraudes, e.g. em cartões de crédito, roubo de identidade, ou outros crimes.	Severo
Falta de Função para Controle de Nível de Acesso	Forjar as requisições, com o propósito de acessar a funcionalidade sem autorização adequada.	Moderado
Cross-Site Request Forgery (CSRF)	Forjar requisição HTTP, incluindo o cookie da sessão da vítima e qualquer outra informação de autenticação incluída na sessão.	Moderado
Utilização de Componentes Vulneráveis Conhecidos	Aplicação sensível a uma gama de possíveis ataques já conhecidos contando com uma sessão com elevados privilégios, visto que não foram aplicadas as contramedidas de segurança.	Moderado
Redirecionamentos e Encaminhados Inválidos	Redirecionar as vítimas para sites de “phishing” ou “malware”, ou usar encaminhamentos para acessar páginas não autorizadas.	Moderado

Fonte: OWASP Top 10 2013

3. REVISÃO DA LITERATURA

Para a revisão da literatura, a questão de pesquisa que norteou a atividade de busca por trabalhos correlatos foi:

- Há literatura disponível que discuta sobre como dirimir ou mitigar os riscos apresentados pelo periódico da OWASP em aplicações web, com uso de uma abordagem técnica?

Os critérios definidos para a seleção dos artigos identificados na revisão da literatura são os seguintes:

- Trabalhos aceitos e publicados em periódicos, os quais foram publicados a partir da primeira edição do OWASP Top 10;
- Contramedidas de segurança aos riscos vinculados restritamente a aplicações web.

No intuito de definir quais são os riscos mais relevantes para serem mitigados foram considerados:

- Os três primeiros riscos definidos pelo periódico da OWASP, os quais são mais encontrados em aplicações web; e
- Todos os riscos cuja classificação relacionada ao impacto nos negócios ou tecnologia tenha a classificação como “Severo”.

Com base no critério de relevância, foram identificados quatro riscos, os quais formam a base para seleção e classificação dos artigos que serão discutidos a seguir.

3.1. Cross-Site Scripting (XSS)

Foi possível identificar na revisão da literatura que a discussão sobre como os desenvolvedores e analistas de sistemas lidam com a questão da segurança da informação é um tema já abordado, inclusive no que se refere aos produtos de software baseados em tecnologias web. CONRY-MURRAY (2006), esclarece sobre formas de ataques do XSS e sugere a necessidade de desenvolvedores de aplicações web realizarem capacitação, pois não apresentam habilidades para implementar contramedidas eficazes, além de destacar também sobre a necessidade de realização de testes de vulnerabilidades antes do atacante, ou seja, o que denota inobservância a processos estabelecidos da engenharia de software (testes dos sistemas).

Semelhantemente, LAWTON (2007) discute riscos de segurança vinculados com a natureza interativa e colaborativa da Web 2.0, e.g. o XSS e CSR (Cross-Site Request Forgery). É sugerido que os programadores desenvolvam as aplicações web usando técnicas de programação que tenham foco nas questões de segurança. O autor destaca que a popularização da web impõe desafios ainda maiores para qualquer aplicação que a utilize como meio de comunicação.

JOVANOVIC et al. (2010) ressalta que aplicações web têm se tornado um dos canais de comunicação mais importantes entre vários tipos de prestadores de serviços e clientes na Internet, porém, com possuem grande vulnerabilidade a ataques do tipo XSS e Injeção de Código (SQL). Como contramedida, os autores apresentam uma ferramenta denominada de “Pixy”, que serve para detectar vulnerabilidades por meio de análise de fluxo de dados.

SOOD & ENBODY (2011), discutem sobre a situação adversa relacionada a iniciativas dos bancos para proteção das transações dos seus clientes ao XSS e CSRF, por que eles são vetores de ataque que permitem o roubo de uma seção estabelecida entre cliente e servidor em intercâmbio de informações. Como contramedida de segurança da informação proposta, é apresentado o resultado de avaliação de segurança declarativa, a qual propõe melhorias ao protocolo HTTP para controlar o estado do browser e proteger a seção do usuário (cliente). SAIEDIAN & BROYLE (2011), rechaçam a premissa que o modelo SOP (Same-Origin Policy)[1] é eficiente contramedida ao XSS, ao contrário, segundo os autores, o SOP propicia um aumento nas vulnerabilidades.

BRADBURY (2012) discute que parte dos problemas relacionados ao XSS, apesar de ser uma vulnerabilidade bem compreendida, é proveniente da pouca conscientização sobre segurança da informação pelos desenvolvedores; e que há uma tendência de se aumentar a fragilidade dos sistemas com a evolução e inovação tecnológica, pois repercutem no surgimento de vulnerabilidades a partir do mesmo agente de ameaça. SHAR & TAN (2012) apresentam várias contramedidas de combate aos riscos do XSS, mas ressaltam que há continuidade das vulnerabilidades nas aplicações web pela falta de familiaridade dos desenvolvedores na compreensão do problema e na limitação de implementar os mecanismos de contramedidas.

FRAIWAN et al. (2012) apresentam uma técnica para identificação de dados maliciosos, a partir de características comuns nos malwares, a fim de que seja possível à aplicação web identificar ataques de XSS, por exemplo, a partir de listas de características comuns criadas a partir da coleta e armazenamento desses dados caracterizadores. Em trabalho mais atual alusivos ao XSS, DAS et al. (2015) discutem sobre vulnerabilidades oriundas do XSS, bem como práticas atuais de contramedidas de segurança da informação. Os autores apresentam como contramedida uma proposta a partir da criação de listas com características coletadas a partir da análise da forma de exploração do XSS. Por se tratar de uma solução estática, semelhante a assinaturas de site maliciosos presentes nos *firewalls*, requer que as listas sejam geridas periodicamente, sob pena de que a desatualização promova a vulnerabilidade da aplicação web, a partir de inovações na estratégia ou no método de ataque.

3.2. Injeção de Código

GARY & ZHENDONG (2007) esclarecem que a Injeção de Código é um tipo identificado como comum de ataques às aplicações web, que promove a execução de consultas não autorizadas, por exemplo, em banco de dados. Os autores fazem críticas quantos aos modelos propostos para prevenir, de maneira estática e dinâmica, o risco da Infeção de Código. Como alternativa de resolução, apresenta uma proposta baseada em uma política denominada de "conversadora", a fim de avaliar se o código a ser executado após o intercâmbio entre cliente e servidor estão com algum ataque de Injeção de Código.

HALFOND et al (2008) discutem sobre a problemática da evolução do cenário das aplicações web, que por consequência se tornaram alvos de ataques de segurança. HALFOND et al (2008) apresentam uma ferramenta denominada Web Application SQL-injection Preventer (WASP), a qual atua no conceito que os autores definem como sintaxe-aware. Mais recentemente, LEE et al (2012) apresenta um método de detecção ao ataque a partir da injeção, através da análise estática e dinâmica combinada, conforme GARY &

[1] https://www.w3.org/Security/wiki/Same_Origin_Policy

ZHENDONG (2007), em que é removido o valor do atributo no momento da execução da consulta SQL, utilizando uma comparação a parâmetros pré-determinados.

DORAI & KANNAN (2011) empreendem uma abordagem menos tecnicista sobre a Injeção de Código, e ressaltam a necessidade em observar a seguridade do banco de dados. Os autores discutem sobre a importância dos desenvolvedores web e outros profissionais na área da tecnologia da informação erradicarem as vulnerabilidades a partir do agente de injeção. Porém, não faz uso de nenhuma norma da gestão da segurança da informação.

De igual modo, CHO (2015) especifica que usuários mal-intencionados podem roubar o conteúdo do banco de dados, aproveitando-se de erros cometidos por programadores. Como estratégia para mitigar a Injeção de Código, propõe a criação de um ambiente web de avaliação na divulgação de informações de uma aplicação web, a fim de apoiar tanto o emissor como o receptor. Contudo, notamos uma deficiência nas especificações que permitissem uma caracterização da referida aplicação web de validação, e dos requisitos para sua implementação.

3.3. Cross-Site Request Forgery (CSRF)

LARKIN (2007) cita que tem ocorrido aperfeiçoamentos com este método de ataque. O autor sugere a necessidade de desenvolvedores de aplicações web realizarem capacitações, e que deve ser observado a realização de testes de vulnerabilidades antes do atacante. Nesta mesma ênfase, MAO et al. (2009) mencionam sobre a necessidade de contramedidas de segurança da informação contra o CSRF, em especial, para aplicações web com viés financeiro. Para tanto, propõem uma inspeção nos tokens de autenticação, a fim de avaliar se as requisições são legítimas através de uma técnica que foi denominada de Browser-Enforced Authenticity Protection (BEAP).

Vinculado à relação da aplicação web com protocolos redes, ROCCHETTO et al. (2014) fazem menção a posição de destaque do CSRF no relatório OWASP Top 10, e enfatizam que desenvolvedores devem atuar em contramedidas de segurança da informação. Apesar da existência de muitos recursos de proteção contra o CSRF, existem vulnerabilidades mais complexas que contribuem para o atacante alcançar seu objetivo. A proposta de contramedida feita no artigo é apresentar como deve ser especificada uma aplicação web, a fim de que seja mais fácil a identificação de sua exposição a ataques CSRF.

A dificuldade em identificar a ocorrência do CSRF ou de um conteúdo autorizado é discutida por RYCK et al (2011), os quais destacam que a implementação de contramedidas de segurança costuma apresentar dificuldade com relação ao controle de acesso, quando existe a dependência de autenticações em diversas aplicações para permissão da operação. O artigo apresenta uma proposta de tratar os servidores das aplicações web com base em indicadores que apontem a atividade não-maliciosa, assim como TELIKICHERLA et al (2014) que apresentam uma proposta de uma política de como aplicações web podem acessar dados no servidor de maneira mais segura.

3.4. Exposição de Dados Sensíveis

GRITZALIS et al (1999) propõem observar questões de segurança alusiva a Internet, principalmente para intercâmbio de dados vinculados à saúde das pessoas. A partir do pressuposto que a segurança se refere a um conjunto de medidas, que podem ser

classificadas como processual, lógico e físico, e que visam a prevenção, a detecção, a indicação, e correção de certos tipos de má utilização do sistema, tanto acidental como deliberado, o artigo utiliza uma arquitetura composta por certificados digitais e criptografia para propor uma boa prática para desenvolvimento de aplicações web para a área médica.

HAMANN et al (2001) apresentam uma proposta para alcançar níveis mais elevados de segurança da informação através de mecanismo de autenticação através do uso de *smarts card*. ANANE et al (2008) destacam sobre a relevância da criptografia para evitar o acesso não autorizado e garantir a integridade dos dados. Identifica-se que o artigo não apresenta menção às normas de segurança da informação, porém apresenta um esquema de fragmentação que envolve proteger apenas o dado que é confidencial, e não todo o texto como rotineiramente são implementados nos sistemas computacionais. Entende-se que esta é uma proposta relevante, principalmente para a busca de soluções eficientes, neste caso, relacionada ao custo de processamento.

Ainda relacionado aos mecanismos da segurança da informação, KANSO et al (2012) destacam o papel fundamental para aplicações web das funções de *hash* no âmbito da integridade da informação. Através das simulações, mostram que a função de *hash* não representa impacto considerável no custo de processamento e atende aos requisitos para proteção dos dados confidenciais.

SAKHARE (2015) cita sobre estratégias que as empresas estão usando para solucionar o problema da segurança em aplicações web. Ressaltam que deve ser entendido como uma questão crítica de pesquisa, uma vez que as aplicações web estão cada vez mais sendo utilizadas nas rotinas de negócios das empresas. O autor disponibiliza um ambiente de teste e validação para aplicações web, contudo, não apresenta quais os riscos estão sendo testados, nem deixa claro como identificaram tais riscos ou qual o método de gestão de riscos foi utilizado.

4. RECOMENDAÇÕES E CONCLUSÃO

Inicialmente, a partir da revisão da literatura, permitiu-se identificar que há publicações vinculadas aos riscos citados pelo periódico OWASP Top 10 2013, e que foram publicados a partir do ano de 2005, porém, com maior quantitativo entre os anos de 2008 a 2012.

Dentre os trabalhos identificados, percebe-se preponderância de trabalhos sobre o Cross-Site Scripting (XSS), com mais de um terço da produção com abordagem para este risco. O Cross-Site Request Forgery (CSRF) recebeu a atenção na proposição de contramedidas de segurança em 25% dos trabalhos identificados. Os demais trabalhos identificados referem-se aos riscos “Exposição de Dados Sensíveis” e “Injeção de Código”, com cinco publicações alusivas a cada um dos temas, representando em torno de 20% do total dos trabalhos catalogados.

Na Tabela 2 é apresentado um resumo quantitativo a respeito do resultado obtido com a revisão da literatura realizada, coerente com os critérios dispostos na Seção 3. Os valores numéricos foram apurados correlacionando os principais riscos às aplicações web ao ano de publicação dos trabalhos catalogados.

Tabela 2 – Resumo Quantitativo de Trabalhos Correlatos

Agente de Ameaça	ANO DE PUBLICAÇÃO					Total
	2003	2004	2005 a 2007	2008 a 2012	A partir de 2013	
Cross-Site Scripting (XSS)	-	-	02	06	01	09
Cross-Site Request Forgery (CSRF)	-	-	01	03	02	06
Exposição de Dados Sensíveis	02			02	01	05
Injeção de Código	-	-	01	02	02	05

Fonte: Autores deste trabalho.

Segundo os trabalhos identificados pode-se inferir que profissionais da engenharia de software podem ser responsabilizados pela ineficiente proteção às aplicações web, mediante a manutenção dos mesmos riscos. Contudo, convém identificar se a problemática está na negligência ou imperícia dos profissionais da engenharia de software no desenvolvimento de aplicações web; bem como, se as equipes formadas por esses profissionais são alertadas e capacitadas sobre a necessidade da segurança da informação nos seus produtos de software, em especial, àquelas que utilizam a web como meio de intercâmbio de dados. É preciso destacar que a informação é o elemento a ser protegido, em razão do seu valor para as empresas em geral.

Também a partir da análise dos trabalhos catalogados na revisão da literatura, percebe-se que há preponderância da abordagem técnica na exposição das contramedidas de segurança para as aplicações web. Convém a utilização de uma abordagem conceitual para elucidar aos desenvolvedores sobre os riscos que envolvem as aplicações web, e também para apresentar as contramedidas de proteção à informação. Foram identificados poucos trabalhos que enfatizam sobre, por exemplo, a gestão da segurança da informação nessa revisão da literatura (DAS et al; 2015; SHAR & TAN, 2012; DORAI & KANNAN, 2011; HAMANN et al, 2001). É fato que mediante e inovação tecnológica, as abordagens conceituais tendem a ter maior perenidade, ou seja, mantêm-se válida mesmo com mudanças em linguagens ou paradigmas de programação - e mesmo não se pode afirmar com abordagens técnicas, as quais são mais dependentes e específicas das tecnologias.

Finalmente, não foi encontrada nessa revisão da literatura nenhuma pesquisa que fez menção alusiva à engenharia de software, no sentido de alertar, por exemplo, para que as empresas definam um processo de desenvolvimento de sistemas que contemple atividades para instituir, capacitar, validar e avaliar a implementação de suas aplicações web, contemplando os mecanismos de segurança da informação. Entende-se que essa pode ser uma contramedida eficiente para combater o que podemos considerar o maior dos riscos: a imperícia ou negligência.

5. REFERÊNCIAS

ABNT 27002. Associação Brasileira de Normas Técnicas. ABNT NBR ISO/IEC 27002:2013. Código de Prática para a Gestão da Segurança da Informação. 2013.

ALBREIKI, H.H.; MAHMOUD, Q.H., Evaluation of static analysis tools for software security. Innovations in Information Technology (INNOVATIONS), 2014 10th International Conference on , vol., no., pp.93,98, 9-11 Nov. 2014

ANANE, R; DHILLON, S; BORDBAR, B. Stateless data concealment for distributed systems. Journal of Computer & System Sciences. 74, 2, 243-254, Mar. 2008. ISSN: 00220000.

BEAL, Adriana. Segurança da Informação: princípios e melhores práticas para a proteção dos ativos de informação nas organizações – São Paulo: Atlas, 2005.

BOJINOV, H; BURSZTEIN, E; BONEH, D. The Emergence of Cross Channel Scripting. Communications of the ACM. 53, 8, 105-113, Aug. 2010. ISSN: 00010782.

BORGOHAIN, T; KUMAR, U; SANYAL, S. Survey of Security and Privacy Issues of Internet of Things. International Journal of Advanced Networking & Applications. 6, 4, 2372-2378, Jan. 2015. ISSN: 09750290.

BRADBURY, D. The dangers of badly formed websites. Computer Fraud & Security. 2012, 1, 12-14, Jan. 2012. ISSN: 13613723.

CHO, Y; PAN, J. Design and Implementation of Website Information Disclosure Assessment System. PLoS ONE. 10, 3, 1-29, Mar. 2015. ISSN: 19326203.

CONRY-MURRAY, A. XSS Vulnerabilities Abound. Network Computing. 17, 16, 16, Aug. 31, 2006. ISSN: 10464468.

DAS, D; SHARMA, U; BHATTACHARYYA, DK. Detection of Cross-Site Scripting Attack under Multiple Scenarios. Computer Journal. 58, 4, 808-822, Apr. 2015. ISSN: 00104620.

DORAI, R; KANNAN, V. SQL Injection-Database Attack Revolution and Prevention. Journal of International Commercial Law & Technology. 6, 4, 224-231, Oct. 2011. ISSN: 19018401.

FRAIWAN, M; et al. Analysis and Identification of Malicious JavaScript Code. Information Security Journal: A Global Perspective. 21, 1, 1-11, Feb. 2012. ISSN: 19393555.

GARY, WASSERMANN; ZHENDONG, SU. 2007. Sound and precise analysis of web applications for injection vulnerabilities. In Proceedings of the 28th ACM SIGPLAN Conference on Programming Language Design and Implementation (PLDI '07). ACM, New York, NY, USA, 32-41. DOI=10.1145/1250734.1250739 http://doi.acm.org/10.1145/1250734.1250739.

GRITZALIS, S; et al. Developing secure Web-based medical applications. Medical Informatics & the Internet in Medicine. 24, 1, 75-90, Mar. 1999. ISSN: 14639238.
HALFOND, WJ; ORSO, A; MANOLIOS, P. WASP: Protecting Web Applications Using Positive Tainting and Syntax-Aware Evaluation. IEEE Transactions on Software Engineering. 34, 1, 65-81, Jan. 2008. ISSN: 00985589.

HAMANN, E; et al. Securing e-business applications using smart cards. IBM Systems Journal. 40, 3, 635, June 2001. ISSN: 00188670.

JOVANOVIC, N; KRUEGEL, C; KIRDA, E. Static analysis for detecting taint-style vulnerabilities in web applications. Journal of Computer Security. 18, 5, 861-907, Aug. 2010. ISSN: 0926227X.

KANSO, A; YAHYAOUI, H; ALMULLA, M. Keyed hash function based on a chaotic map. Information Sciences. 186, 1, 249-264, Mar. 2012. ISSN: 00200255.

KHAN Muhammad U. A.; ZULKERNINE, Mohammad. Quantifying Security in Secure Software Development Phases. Annual IEEE International Computer Software and Applications Conference, 2008, pp. 905-960.

LARKIN, E. Don't Let Bad Guys Pose as You. PC World. 25, 4, 36, Apr. 2007. ISSN: 07378939.

LAWTON, G. Web 2.0 Creates Security Challenges. Computer. 40, 10, 13-16, Oct. 2007. ISSN: 00189162.

LEE, I; et al. A novel method for SQL injection attack detection based on removing SQL query attribute values. Mathematical & Computer Modelling. 55, 1/2, 58-68, Jan. 2012. ISSN: 08957177.

MAO, Ziqing; et al. Defeating Cross-Site Request Forgery Attacks with Browser-Enforced Authenticity Protection. Financial Cryptography and Data Security Lecture Notes in Computer Science Volume 5628, 2009, pp 238-255.

OWASP Top 10 2013. OWASP Top Ten Project. http://owasptop10.googlecode.com/files/OWASP%20Top%2010%20-%202013.pdf

PRESSMAN. Engenharia de Software – Uma Abordagem Profissional. 7ª Edição. Porto Alegre: AMGH, 2011.

ROCCHETTO, Marco; et al. Model-Based Detection of CSRF. ICT Systems Security and Privacy Protection IFIP Advances in Information and Communication Technology Volume 428, 2014, pp 30-43.

RYCK, Philippe De; et al. Automatic and Precise Client-Side Protection against CSRF Attacks. Computer Security – ESORICS 2011 Lecture Notes in Computer Science Volume 6879, 2011, pp 100-116.

SAIEDIAN, H; BROYLE, D. Security Vulnerabilities in the Same-Origin Policy: Implications and Alternatives. Computer. 44, 9, 29-36, Sept. 2011. ISSN: 00189162.

SÊMOLA, Marcos. Gestão da Segurança da Informação – Uma visão executiva. Rio de Janeiro: Elsevier, 2003.

SHAR, L K. TAN, H B K. Predicting Common Web Application Vulnerabilities from Input Validation and Sanitization Code Patterns. in Proceedings 27th IEEE/ACM International Conference on Automated Software Engineering (ASE 2012),September 2012, pp. 310-313.

SOOD, A; ENBODY, R. n. Computer Fraud & Security. 2011, 7, 11-16, July 2011. ISSN: 13613723.

TANENBAUM, Andrew S. WETHERALL, David J. Redes de Computadores. 5ª Edição. Pearson. 2011.

TELIKICHERLA, K. C; et al. CORP: A Browser Policy to Mitigate Web Infiltration Attacks. Information Systems Security Lecture Notes in Computer Science Volume 8880, 2014, pp 277-297.

Wasukar, Amit R; Usman, Mohammad; Sakhare, Neha. Vulnerability Management In Web Application. International Journal For Research In Emerging Science And Technology. Volume-2, Special Issue-1, March-2015.

XIAOLI, Lin; ZAVARSKY, P.; RUHL, R.; LINDSKOG, D., Threat Modeling for CSRF Attacks," Computational Science and Engineering, 2009. CSE '09. International Conference on , vol.3, no., pp.486,491, 29-31 Aug. 2009 doi: 10.1109/CSE.2009.372