Segurança de aplicações web e os dez anos do relatório OWASP Top Ten: o que mudou?

Alan Henrique Pardo de Carvalho[1]

Resumo:

Com a importância crescente da *Web* no cotidiano de pessoas e organizações, bem como a alta quantidade de incidentes de segurança, torna-se cada vez mais necessário aumentar a garantia de segurança da informação nesse ambiente. Nesse sentido, várias iniciativas são empreendidas para alertar desenvolvedores de *sites*, como a lista OWASP *Top Ten*, que traz desde 2003 as maiores vulnerabilidades encontradas em sites e as medidas para correção ou prevenção. Este trabalho mostra que mesmo com a publicação dessa lista, diversas dessas vulnerabilidades continuam a estar presentes, o que pode ter implicações na forma como as aplicações *web* são desenvolvidas. Ainda, são propostas ações que podem ser tomadas pela academia, empresas e profissionais parareverter esse quadro.

Palavras-chave: Segurança da informação; Desenvolvimento web; OWASP; Top Ten; vulnerabilidades.

Abstract:

With the growing importance of the Web in daily life of people and organizations, as well as the high amount of security incidents, it becomes increasingly necessary to raise the assurance of information security in this environment. In this sense, several initiatives are undertaken to alert developers of sites such as OWASP Top Ten list, which since 2003 brings major vulnerabilities found in sites and measures for correction or prevention. This work shows that even with the publication of this list, many of these vulnerabilities continue to be present, which may have implications in how web applications are developed. Still, are proposed actions that may be taken by academia, companies and professionals to reverse this situation.

Keywords: Informationsecurity; Web development; OWASP; Top Ten; vulnerabilities.

1Introdução

Como mostram Caiçara Junior e Paris (2007), a adoção de tecnologias de informação e comunicação, hoje em dia, especialmente representadas pelas aplicações *web*(*sites*) disponíveis na Internet, tem provocado profundas mudanças na forma como pessoas, organizações e governos se relacionam e como a informação pode ser obtida, levando a fenômenos de natureza social, econômica, cultural e política como o surgimento de novas formas de trabalho, as mudanças em processos organizacionais, as mobilizações organizadas por meio de redes sociais e o advento da urna eletrônica nos processos eleitorais brasileiros, para citar alguns exemplos.

[1] Mestre em Tecnologia pelo Centro Paula Souza. Coordenador de Curso e Docente na Faculdade de Tecnologia de São Caetano do Sul. E-mail: alancarv@gmail.com.

Sites como o Facebook e os serviços fornecidos pela Google estão entre os mais acessados por pessoas de todo o mundo, conectadas à *World Wide Web* (ou apenas *Web*), conceito desenvolvido no final da década de 1980 por Tim Berners-Lee no CERN, laboratório de pesquisas localizado na parte central da Europa e que, ao utilizar a infraestrutura da Internet para sua operacionalização, contribuiu significativamente para que mais de 2,7 bilhões de pessoas em 750 milhões de lares, segundo a União Internacional de Telecomunicações (ITU), estivessem usando a principal rede mundial em 2013 (ITU, 2013).

De acordo com o relatório mais recente do Comitê Gestor da Internet no Brasil (CETIC.br, 2013), no ano de 2012 a população com 10 anos de idade ou mais que acessavam a Internet chegou a 80,9 milhões de pessoas, em cerca de 40% dos mais de 61 milhões de domicílios brasileiros, o que representa aproximadamente 69% da população total do país. Para esse público, 73% das atividades desenvolvidas na Internet referem-se ao acesso a sites de relacionamento e 70% a envio e recebimento de *e-mail*, algo que é realizado principalmente via serviços de webmail como o Gmail, o Yahoo!Mail e outros.

Os serviços de governo eletrônico(*e-government*) têm sido acessados pelos brasileiros. Segundo o mesmo relatório, 65% dos usuários da Internet com 16 anos ou mais utilizaram algum serviço de governo eletrônico nos últimos 12 meses, como consultas ao CPF (Cadastro de Pessoas Físicas), busca de informações para emissão de documentos, obtenção de certidões, licenças e permissões, emissão de documentos diversos e o envio da declaração do Imposto de Renda Pessoa Física, entre outros serviços.

Os *sites* de comércio eletrônico (*e-commerce*) têm sido utilizados de forma crescente nos últimos anos. A consultoria E-bit, por meio de seu relatório Webshoppers 2014 (E-BIT, 2014) que traz informações obtidas junto a mais de 20 mil lojas virtuais, mostra que o comércio eletrônico brasileiro faturou R$ 28,8 bilhões em 2013, com um crescimento de 28% em relação a 2012, ultrapassando a previsão de crescimento que era de 25%. A quantidade de pedidos realizados via Internet foi de mais de 88 milhões, com crescimento de 32% em comparação com o ano anterior. A estimativa de crescimento para 2014 é de 20%, devendo o faturamento total chegar à casa dos R$ 34,6 bilhões.

Ainda de acordo com CETIC.br (2013), cerca de 98% das empresas utilizaram computadores nos últimos 12 meses e 97% das empresas acessaram a Internet nesse mesmo período. As principais atividades realizadas pelos funcionários dessas empresas foram enviar e receber *e-mail*, buscar informações sobre produtos e serviços, fazer pagamentos e consultas bancárias, realizar monitoramento de mercado e mensagens instantâneas.

E o relatório mostra que, das empresas que possuem acesso à Internet, 55% possuem um *website*, sendo as principais formas de utilização desses *sites* o fornecimento de informações institucionais sobre a empresa e a publicação de catálogos de produtos. Dos 38% das empresas que não possuem um *site*, pretendem desenvolvê-lo nos próximos 12 meses. Já sobre a presença em redes sociais, 36% das empresas com acesso à Internet tem um perfil próprio em alguma rede social, sendo as principais atividades desenvolvidas a publicação de notícias sobre a empresa, a interação com clientes, a publicação de notícias sobre temas relacionados à área de atuação da empresa e a publicação de conteúdo institucional da empresa.

Todo esse acesso a informações e possibilidades de comunicação *on-line*, para que seja bem sucedido e não se transforme em fator de preocupação ou mesmo prejuízos para pessoas e organizações, precisa ser baseado em níveis aceitáveis de segurança e essa tem sido uma preocupação constante de empresas, governos e instituições de ensino e pesquisa.

Apenas em 2013 foram registrados no Brasil mais de 352 mil incidentes de segurança (CERT.br, 2013) e os prejuízos causados por crimes cibernéticos podem ter chegado a mais de R$ 40 bilhões em 2012 (ITWEB, 2012), o que mostra a necessidade de investir em sistemas de proteção aos recursos de tecnologia da informação e comunicação, além da indispensável conscientização dos usuários, que estão sujeitos a serem vítimas de técnicas de engenharia social por parte de terceiros mal intencionados.Uma indicação disso é a pesquisa realizada pela consultoria PriceWaterhouseCoopers, que mostra que o investimento médio das empresas em Segurança da Informação cresceu de US$ 2,8 milhões em 2012 para US$ 4,3 milhões em 2013 (PWC, 2013).

2 A segurança de aplicações *web*

Estima-se que no ano de 2012 havia 634 milhões de *sites*da *WorldWide Web* (PINGDOM, 2013), como o notório Google, que nesse mesmo ano teve 1,2 trilhões de buscas realizadas, ou como o Facebook, com mais de um bilhão de usuários sendo que somente os brasileiros realizaram mais de 85 mil publicações mensais nas páginas dessa rede social. Ainda é digno de nota o fato do serviço de *webmail* Gmail ter tido, em 2012, 425 milhões de usuários ativos ao redor do mundo.

Seja o Google, o Facebook ou um *blog* pessoal, as aplicações *web* precisam operar sob requisitos básicos de Segurança da Informação, descritos por Harris (2013): a confidencialidade, que diz respeito à permissão de acesso aos dados e demais recursos apenas às pessoas para as quais tal acesso tiver sido concedido; a integridade, que está relacionada com a confiabilidade

dos dados armazenados ou transmitidos, pois não podem ser alterados sem autorização; e a disponibilidade, que é a capacidade do serviço (no caso, o *site*) de estar disponível para acesso quando necessário.

Alguns casos de tentativas de invasão a *sites*brasileiros foram amplamente divulgados pelos veículos de comunicação como em dezembro de 2012 (ESTADÃO, 2012), quando houve um ataque contra o *site* do instituto responsável pelas provas do ENEM (Exame Nacional do Ensino Médio). Em 2013, o *site* da Secretaria de Educação do Estado de São Paulo teve seu conteúdo modificado por invasores e cerca de quatro milhões de alunos foram afetados, além de 300 mil servidores, entre professores e funcionários da rede estadual de ensino (R7, 2013). No mesmo ano, o *site* oficial do governo brasileiro teve seu conteúdo deixado indisponível durante parte de um final de semana (EXAME.COM, 2013) e na mesma reportagem casos de invasão a *sites* do Exército e da Polícia Militar de São Paulo foram citados.

Esses e tantos outros casos de tentativas bem ou mal sucedidas de violação da confidencialidade, integridade e disponibilidade dos *sites* são objeto de atenção de grupos de profissionais voltados ao desenvolvimento e disseminação de recomendações, boas práticas e outros recursos que possam ser utilizados pelos desenvolvedores de *sites* e pelos responsáveis pela infraestrutura dos mesmos para que os níveis de garantia de Segurança da Informação possam ser incrementados. Na seção seguinte, um desses grupos será apresentado, assim como uma das iniciativas desenvolvidas por seus integrantes.

3 O OWASP

O *Open Web Application Security Project* (OWASP) ou, numa tradução livre, Projeto Aberto de Segurança para Aplicações *Web*, é uma organização sem fins lucrativos fundada em dezembro de 2001 com sede nos Estados Unidos cuja missão é promover iniciativas para que pessoas e organizações possam manter-se informados sobre os potenciais riscos de segurança de *software* (OWASP, 2014a).

Existem representações do OWASP em diversos países, chamadas "*chapters*" (capítulos) inclusive no Brasil que é o segundo país em quantidade de capítulos (19), atrás apenas dos EUA (89). A Índia, com grande relevância em quantidade de empresas e profissionais de Tecnologia da Informação, aparece como o terceiro país em quantidade de capítulos, num total de 17 representações (OWASP, 2014b).

A participação nas atividades do OWASP é livre e aberta a todos os interessados, assim como todos os documentos publicados no *site* da organização estão disponíveis para qualquer

pessoa sob uma licença de *software* aberto e livre (OWASP, 2014a). A organização se mantém com doações que podem ser feitas por qualquer pessoa no *site* e com o pagamento de anuidades de associados (OWASP, 2014b). Existem, atualmente, 2251 associados formalmente ao OWASP, mais da metade nos EUA (OWASP, 2014c).

Entre as atividades do OWASP para disseminar a cultura de segurança em aplicações estão a manutenção de uma lista eletrônica de troca de mensagens, organização de conferências, realização de palestras, publicação de livros e projetos diversos. Entre eles, o OWASP *Top Ten*, que será apresentado na sequência deste trabalho.

3.1 O OWASP Top Ten

O OWASP *Top Ten* é uma das iniciativas do OWASP no sentido de disseminação da cultura de segurança da informação junto aos profissionais de desenvolvimento de aplicações *web* (OWASP, 2007). Trata-se de um relatório que contém as principais vulnerabilidades encontradas em *sites* e que necessitam de correção imediata por parte dos desenvolvedores, pois não dependem necessariamente de medidas de segurança que possam ser implantadas nos servidores que dão o suporte necessário para que esses *sites* sejam acessados pelos visitantes.

Nesse caso, o *Top Ten* refere-se a falhas que podem ser – e são – exploradas ativamente por pessoas mal intencionadas e causar prejuízos, mas que podem ser corrigidas pelos programadores. A recomendação do OWASP é que, ainda na fase de desenvolvimento, as medidas de segurança sejam observadas pelos programadores das aplicações *web* como um padrão mínimo de maneira que esses *sites* não sejam colocados "em produção", ou seja, à disposição dos visitantes com tais vulnerabilidades.

A lista de vulnerabilidades é desenvolvida e atualizada a partir de consultas feitas junto a especialistas em Segurança da Informação e desenvolvimento de aplicações *web* de empresas e organizações de portes e ramos diversos, na esfera governamental ou privada, em vários países. A primeira versão do *Top Ten* foi publicada em 2003, houve algumas pequenas atualizações que geraram a edição de 2004 e houve edições em 2007, 2010 e 2013.

Na elaboração da lista foram levadas em consideração as experiências desenvolvidas com sucesso pelo SANS Institute, uma organização de pesquisa e educação em Segurança da Informação criada em 1989, e pelo FBI (*Federal Bureau ofInvestigation*), que publicaram uma lista de vulnerabilidades voltada a redes de computadores, além do trabalho do *Web Application Security XML Project*, elaborado pelo OASIS (*Organization for theAdvancementofStructuredInformation Standards*), uma organização sem fins lucrativos

voltada ao desenvolvimento de padrões abertos para tecnologias de informação e comunicação (OASIS, 2014), que serviu para definição das categorias de vulnerabilidades a serem descritas na OWASP *Top Ten*.

A seguir, serão descritas as vulnerabilidades mais frequentes (A1 até A10, em ordem decrescente de prevalência ou importância) em *sites*da WorldWide Web em cada uma das edições do *Top Ten*, de maneira que em seguida se possa ter um panorama de como essas falhas de *software* vem sendo (ou não) tratadas pelos profissionais de desenvolvimento de aplicações *web*. Nesse ponto cabe a observação de que a edição de 2003 não está disponível para acesso no *site* do OWASP. Assim, serão consideradas as edições a partir de 2004, que podem ser lidas por qualquer interessado.

4A evolução doOWASP*Top Ten*

Como descrito na seção anterior, o OWASP *Top Ten* é um relatório no qual consta uma lista de vulnerabilidades mais comuns em aplicações *web* (*sites*), decorrentes de falhas de programação que podem ser corrigidas pelos programadores e quedeveriam ser evitadas nas fases de desenvolvimento e teste dessas aplicações. Nesta seção serão apresentadas as várias edições dessa lista para que se tenha um panorama das vulnerabilidades mais presentes nos *sites*nosdez anosde *Top Ten*e estudadas pelo OWASP.

4.1 TopTen 2004

A primeira edição do OWASP *Top Tem* disponível para consulta é de 2004 e em sua introdução é mostrado que essa lista de vulnerabilidades "representa um amplo consenso a respeito de quais são as falhas mais críticas em aplicações *web*" (OWASP, 2013a).

Embora a discussão sobre cada uma das vulnerabilidades listadasnão faça parte do escopo deste trabalho, pode-se mencionar que algumas delas referem-se afalta de verificação (validação) nos dados fornecidos pelos visitantes dos *sites*, como em formulários por exemplo, ou a problemas relacionados ao processo de autenticação desses visitantes (identificação com *login* e senha), má definição de permissões de acesso a conteúdos dos *sites*, falta de controles para armazenamento de dados ou problemas de configuração de servidores, entre outros motivos (OWASP, 2013a).

O *Top Ten* 2004 contém, para cada uma dessas vulnerabilidades, as respectivas medidas que podem ser tomadas pelos programadores de *web sites* para efetuar as devidas correções nos códigos das aplicações e com isso diminuir o risco de exposição a tentativas de acesso indevido a dados ou mesmo interrupção dos serviços (*denialofservice*).

Embora o *Top Ten* 2003 não esteja disponível para acesso, é possível saber quais foram as mudanças em relação a essa edição de 2004, ilustradas na Tabela 1 a seguir.

Tabela 1 – Mudanças entre a edição 2003 e 2004 do OWASP *Top Ten*

***Top Ten* 2003**	***Top Ten* 2004**
A1 *UnvalidatedParameters*	A1 *Unvalidated Input*
A2 *Broken Access Control* A9 *Remote AdministrationFlaws*	A2 *Broken Access Control*
A3 *BrokenAccountandSession Management*	A3 *BrokenAccountandSession Management*
A4 *Cross Site Scripting (XSS) Flaws*	A4 *Cross Site Scripting (XSS) Flaws*
A5 *Buffer Overflows*	A5 *Buffer Overflows*
A6 *CommandInjectionFlaws*	A6 *InjectionFlaws*
A7 *ErrorHandlingProblems*	A7 *ImproperErrorHandling*
A8 *Insecure Use ofCryptography*	A8 *InsecureStorage*
	A9 *Denialof Service*
A10 *Web andApplication Server Misconfiguration*	A10 *InsecureConfiguration Management*

Fonte: OWASP (2006).

4.2 TopTen 2007

Três anos depois, o OWASP publicou uma nova lista com as vulnerabilidades mais encontradas em aplicações *web* e, além disso, buscou reforçar a necessidade de aplicação contínua das boas práticas de segurança em todas as fases do desenvolvimento de *sites*, já que Segurança da Informação não é algo que se faça (ou pense) uma única vez (*one-time event*).

A Tabela 2 a seguir mostra a evolução da lista em relação à sua edição anterior.

Tabela 2 – Mudanças entre a edição 2004 e 2007 do OWASP *Top Ten*

***Top Ten* 2004**	***Top Ten* 2007**
A4 *Cross Site Scripting (XSS)*	A1*Cross Site Scripting (XSS)*
A6 *InjectionFlaws*	A2*InjectionFlaws*
	A3 *Malicious File Execution*
A2 *Broken Access Control*	A4 *InsecureDirectObjectReference*
	A5 *Cross Site RequestForgery (CSRF)*
A7 *ImproperErrorHandling*	A6 *InformationLeakageandImproperErrorHandling*
A3 *BrokenAccountandSession Management*	A7*BrokenAccountandSession Management*
A8 *InsecureStorage*	A8 *InsecureCryptographicStorage*
	A9 *Insecure Communications*
A2 *Broken Access Control*	A10 *FailuretoRestrict URL Access*
A1 *Unvalidated Input*	
A5 *Buffer Overflows*	
A9 *Denialof Service*	
A10 *InsecureConfiguration Management*	Passou a fazer parte da A9 2007

Fonte: OWASP (2013f).

Ainda, os autores da lista reafirmaram a meta do OWASP de educar desenvolvedores, projetistas, arquitetos de *software* e organizações sobre as consequências das vulnerabilidades mais comuns encontradas nas aplicações *web*, sendo queo *Top Ten* é uma publicação que integra o conjunto de esforços para alcance dessa meta. (OWASP, 2013b).

A lista de vulnerabilidades elaborada nesta edição do*TopTen* foi baseada em um relatório de tendências em Segurança da Informação de 2006 publicado pela MITRE Corporation, organização que gerencia centros de pesquisa e desenvolvimento apoiados pelo governo dos EUA. A partir desse relatório foram identificadas as dez vulnerabilidades mais presentes e que deram origem ao *Top Ten* 2007.

4.3 TopTen 2010

A edição de 2010 do*TopTen* traz em suas linhas iniciais uma importante (e assustadora) constatação: a de que "*software* inseguro já está afetando negativamente nossas finanças, serviços de saúde, defesa, energia e outros recursos críticos de infraestrutura" (OWASP, 2013c).

Os autores continuam incentivando a adoção de práticas de segurança nas diversas fases do processo de desenvolvimento de aplicações *web* como uma das formas de diminuir a incidência de vulnerabilidades nos *sites* e consequente risco de ataques e prejuízos. Além disso, fazem referência a outros documentos publicados no site do OWASP, como o *OWASP Developer'sGuide* e o *Application Security Verification Standard*, que trazem importantes diretrizes que podem ser seguidas pelos desenvolvedores para aumento da garantia da segurança nos *sites*.

A Tabela 3 a seguir mostra a evolução da lista em relação à edição 2007.

Tabela 3 – Mudanças entre a edição 2007 e 2010 do OWASP *Top Ten*

***Top Ten* 2007**	***Top Ten* 2010**
A2*InjectionFlaws*	A1 *Injection*
A1*Cross Site Scripting (XSS)*	A2*Cross Site Scripting (XSS)*
A7*BrokenAccountandSession Management*	A3 *BrokenAccountandSession Management*
A4 *InsecureDirectObjectReference*	A4 *InsecureDirectObjectReference*
A5 *Cross Site RequestForgery (CSRF)*	A5 *Cross Site RequestForgery (CSRF)*
	A6 *Security Misconfiguration*
A8 *InsecureCryptographicStorage*	A7 *InsecureCryptographicStorage*
A10 *FailuretoRestrict URL Access*	A8 *FailuretoRestrict URL Access*
A9 *Insecure Communications*	A9 *InsufficientTransportLayerProtection*
	A10 *UnvalidatedRedirectsandForwards*
A3 *Malicious File Execution*	
A6 *InformationLeakageandImproperErrorHandling*	

Fonte: OWASP (2010a).

Além disso, foi introduzida uma metodologia de análise de riscos desenvolvida pelo OWASP para que os responsáveis pelo desenvolvimento de aplicações pudessem analisar o

impacto da exploração de cada uma das vulnerabilidades não apenas levando em conta os aspectos técnicos, mas como o negócio (*core business*) da organização pode ser afetado por um ataque bem sucedido.

4.4 *TopTen* 2013

A edição mais recente do *Top Ten* persiste no alerta quanto aos riscos decorrentes das vulnerabilidades em aplicações *web* que continuam existindo e deixa claro a necessidade dos desenvolvedores não mais tolerarem a presença das falhasrecorrentes, que podem ser facilmente evitadas ou corrigidas (OWASP, 2013d).

Nessa edição, pode-se ter acesso a mais detalhes relacionados à metodologia utilizada no desenvolvimento do documento. Foram consultadas sete companhias especializadas em segurança no desenvolvimento de aplicações, que em conjunto possuem dados sobre mais de 500 mil ocorrências de vulnerabilidades encontradas em diversasaplicações *web*. As dez vulnerabilidades foram selecionadas de acordo com critérios de prevalência, probabilidade de exploração (*exploitability*), facilidade de detecção (*detectability*) e impacto estimado no negócio (OWASP, 2013e).

A Tabela 4 a seguir ilustra as mudanças para a edição 2013 da lista.

Tabela 4 – Mudanças entre a edição 2010 e 2013 do OWASP *Top Ten*

***Top Ten* 2010**	***Top Ten* 2013**
A1 *Injection*	A1 *Injection*
A3 *BrokenAccountandSession Management*	A2*BrokenAccountandSession Management*
A2*Cross Site Scripting (XSS)*	A3*Cross Site Scripting (XSS)*
A4 *InsecureDirectObjectReference*	A4 *InsecureDirectObjectReference*
A6 *Security Misconfiguration*	A5*Security Misconfiguration*
A7 *InsecureCryptographicStorage* (juntou com A9)	A6 *Sensitive Data Exposure*
A8 *FailuretoRestrict URL Access*	A7 *MissingFunctionLevel Access Control*
A5 *Cross Site RequestForgery (CSRF)*	A8*Cross Site RequestForgery (CSRF)*
	A9 *UsingComponentswithKnownVulnerabilities*
A10 *UnvalidatedRedirectsandForwards*	A10 *UnvalidatedRedirectsandForwards*
A9 *InsufficientTransportLayerProtection*	Passou a fazer parte de A6 2013

Fonte: OWASP (2010b).

5Algumas reflexões e preocupações

Ao apreciar brevemente a evolução do OWASP *Top Ten* ao longo desses dez anos, observa-se que a despeito das vulnerabilidades poderem ser evitadas ou mesmo corrigidas pelos profissionais de desenvolvimento de aplicações *web* e, além disso, as diretrizes para tais correções constarem de todas as edições da lista, várias dessas vulnerabilidades permanecem presentes nos *sites*, mudando ou não de posição no que se refere à prevalência ou importância.

Isso pode ser observado na Tabela 5 a seguir.

Tabela 5 – Vulnerabilidades em cada edição da OWASP *Top Ten*

2003	2004	2007	2010	2013
A1	A1			
A2	A2	A4	A4	A4
		A10	A8	A7
A3	A3	A7	A3	A2
A4	A4	A1	A2	A3
A5	A5			
A6	A6	A2	A1	A1
A7	A7	A6		
A8	A8	A8	A7	A6
A9	A2			
A10	A10	A9	A9	A6
	A9			
		A3		
		A5	A5	A8
			A6	A5
			A10	A10
				A9

Fonte: Adaptado de OWASP (2006, 2013f, 2010a, 2010b).

O fato de várias dessas vulnerabilidades permanecerem na lista depois de uma década é preocupante, dada a incontestável importância das aplicações *web* para os diversos ramos de atividade e organizações de todos os portes, seja na esfera pública ou na privada.

Outro dado que pode trazer preocupações é o tempo decorrido desde a publicação da descoberta da vulnerabilidade até a correção da aplicação. Uma pesquisa da WhiteHat Security que analisou mais de 30 mil *sites* mostra que boa parte das correções são feitas em cerca de 200 dias, mas que podem chegar a mais de 700 dias (WHITEHAT SECURITY, 2014).

Apesar disso, 54% dos respondentes de uma pesquisa realizada pela PriceWaterhouseCoopers durante os meses de fevereiro a abril de 2013 junto a mais de 9.600 profissionais em 115 países declararam utilizar ferramentas de análise de código como uma das medidas de segurança em seus ambientes, mostrando algum movimento no sentido de aumento da garantia da segurança nas aplicações *web* (PWC, 2013).

Considerações finais

É certo que cada vez mais as aplicações *web*tem tido importância na vida de pessoas e organizações em todo o mundo conectado à *World Wide Web*. Assim, espera-se que tais aplicações sejam desenvolvidas e possam ser utilizadas com níveis aceitáveis de segurança, de maneira que o risco de eventuais prejuízos para as organizações que mantém essas aplicações e para seus usuários seja minimizado.

No entanto, como se pode observar ao longo deste trabalho, é possível inferir que as principais vulnerabilidades encontradas nessas aplicações não são resolvidas embora os meios para isso sejam divulgados por entidades como o OWASP e estejam disponíveis livremente para os profissionais responsáveis pelo desenvolvimento dessas aplicações, o que representa um contrassenso que precisa ser combatido.

Um possível caminho é a abordagem das boas práticas em Segurança da Informação no desenvolvimento de aplicações *web* nos cursos de graduação que abordam o tema, como o de Análise e Desenvolvimento de Sistemas, o de Sistemas de Informação, o de Sistemas para Internet e outros. Além disso, a disseminação dessas boas práticas em comunidades virtuais frequentadas por profissionais de desenvolvimento pode contribuir para a melhoria da qualidade das aplicações *web*. As conferências, simpósios, seminários e outros eventos voltados a profissionais e acadêmicos da área de desenvolvimento de aplicações são outros espaços nos quais a conscientização do uso de métodos e técnicas de desenvolvimento seguro de *software* podem ser praticadas.

Uma vez que existe uma contradição no fato de que o conhecimento necessário para a diminuição desse problema está disponível e que os desenvolvedores de aplicações *web* aparentemente não o aplica, dada a incidência recorrente dessas vulnerabilidades, sugere-se o desenvolvimento de um estudo no qual se possa saber o quanto esse conhecimento é ou não utilizado e, caso se constate que as medidas preconizadas pelo OWASP não estejam sendo amplamente adotadas, conhecer as razões que levam esses desenvolvedores a isso, o que pode trazer subsídios para outras ações no sentido da conscientização sobre Segurança da Informação nesse setor.

Referências

CAIÇARA JUNIOR, Cícero; PARIS, Wanderson Stael. **Informática, internet e aplicativos**. Curitiba: Ibpex, 2007.

CERT.br. **Estatísticas dos Incidentes Reportados ao CERT.br**. São Paulo: Centro de Estudos e Tratamento de Incidents de Segurança no Brasil, 2013. Disponível em <http://www.cert.br/stats/incidentes/>. Acesso em 17 abr. 2014.

CETIC.br. **TIC Domicílios e Empresas 2012 – Pesquisa sobre o uso das tecnologias de informação e comunicação no Brasil**. São Paulo: Comitê Gestor da Internet no Brasil, 2013. Disponível em <http://www.cetic.br/publicacoes/2012/tic-domicilios-2012.pdf>. Acesso em 17 abr. 2014.

E-BIT. **Relatório Webshoppers 2014 – 29ª edição**. São Paulo: E-bit, 2014. Disponível em <http://img.ebit.com.br/webshoppers/pdf/WebShoppers2014.pdf>. Acesso em 17 abr. 2014.

ESTADÃO. **Hackers tentam invadir site do Inep e prejudicam acesso a notas do Enem**. São Paulo: Grupo Estado, 2012. Disponível em <http://www.estadao.com.br/noticias/impresso,hackers-tentam-invadir-site-do-inep-e-prejudicam-acesso-a-notas-do-enem,978570,0.htm>. Acesso em 18 abr. 2014.

EXAME.COM. **Hackers derrubam site oficial do governo brasileiro**. São Paulo: Editora Abril, 2013. Disponível em <http://exame.abril.com.br/brasil/noticias/hackers-derrubam-site-oficial-do-governo-brasileiro>. Acessoem 18 abr. 2014.

HARRIS, Shon. **All In One CISSP Exame Guide, SixthEdition**. New York: McGraw-Hill, 2013.

ITU.**The World in 2013 – ICT Factsand Figures**.Geneva: InternationalTelecommunications Union, 2013. Disponível em <http://www.itu.int/en/ITU-D/Statistics/Documents/facts/ICTFactsFigures2013-e.pdf>. Acesso em 17 abr. 2014.

OASIS.**About Us**. Burlington: Organization for theAdvancementofStructuredInformation Standards, 2014. Disponível em <https://www.oasis-open.org/org>. Acesso em 16 abr. 2014.

OWASP.**2004 Updates OWASP Top Ten Project**. Bel Air: The Open Web Application Security Project, 2006. Disponível em <https://www.owasp.org/index.php/Updates_OWASP_Top_Ten_Project>. Acessoem 16 abr. 2014.

_____. **Introduction OWASP Top Ten 2004 Project**. Bel Air: The Open Web Application Security Project, 2007. Disponível em <https://www.owasp.org/index.php/Introduction_OWASP_Top_Ten_2004_Project>. Acessoem 16 abr. 2014.

_____. **MembershipDemographics as ofJanuary 2014**. Bel Air: The Open Web Application Security Project, 2014c. Disponível em <https://docs.google.com/a/owasp.org/spreadsheet/ccc?key=0Ag5ZloRZ0SmjdDcxdk5EbDVreEJ2dnRQTFE5Z0J1aGc#gid=0>. Acessoem 16 abr. 2014.

_____. **OWASP Chapter**. Bel Air: The Open Web Application Security Project, 2014b. Disponível em <https://www.owasp.org/index.php/OWASP_Chapter>. Acessoem 16 abr. 2014.

_____. **Top 10 2004**. Bel Air: The Open Web Application Security Project, 2013a. Disponível em <https://www.owasp.org/index.php/Top_10_2004>. Acesso em 16 abr. 2014.

_____. **Top 10 2007**. Bel Air: The Open Web Application Security Project, 2013b. Disponível em <https://www.owasp.org/index.php/Top_10_2007>. Acesso em 16 abr. 2014.

_____. **Top 10 2007-Methodology**. Bel Air: The Open Web Application Security Project, 2013f. Disponível em <https://www.owasp.org/index.php/Top_10_2007-Methodology>. Acessoem 16 abr. 2014.

_____. **Top 10 2010**. Bel Air: The Open Web Application Security Project, 2013c. Disponível em <https://www.owasp.org/index.php/Top_10_2010>. Acesso em 16 abr. 2014.

_____. **Top 10 2010-Introduction**. Bel Air: The Open Web Application Security Project, 2013e. Disponível em <https://www.owasp.org/index.php/Top_10_2013-Introduction>. Acessoem 16 abr. 2014.

_____. **Top 10 2010-Main**. Bel Air: The Open Web Application Security Project, 2010a. Disponível em <https://www.owasp.org/index.php/Top_10_2010-Main>. Acessoem 16 abr. 2014.

_____. **Top 10 2010-Release Notes**. Bel Air: The Open Web Application Security Project, 2010b. Disponível em <https://www.owasp.org/index.php/Top_10_2010-Release_Notes>. Acessoem 17 abr. 2014.

_____. **Top 10 2013**. Bel Air: The Open Web Application Security Project, 2013d. Disponível em <https://www.owasp.org/index.php/Top_10_2013>. Acesso em 16 abr. 2014.

_____.**Welcometo OWASP**. Bel Air: The Open Web Application Security Project, 2014a. Disponível em <https://www.owasp.org/index.php/Main_Page>. Acesso em 16 abr. 2014.

PINGDOM. **Internet 2012 in numbers**. Västeras: PingdomAB, 2013. Disponível em <http://royal.pingdom.com/2013/01/16/internet-2012-in-numbers/>. Acesso em 17 abr. 2014.

PWC.**The Global StateofInformation Security Survey 2014**.Londres: PriceWaterhouseCoopers, 2013. Disponível em <http://www.pwc.com/gx/en/consulting-services/information-security-survey/download.jhtml>. Acesso em 17 abr. 2014.

R7. **Invasão em site da Secretaria de Educação atingiu 4 milhões de alunos, diz governo**. São Paulo: Rádio e Televisão Record S.A., 2013. Disponível em <http://noticias. r7.com/sao-paulo/invasao-em-site-da-secretaria-de-educacao-atingiu-4-milhoes-de-alunos-diz-governo-13062013>. Acessoem 18 abr. 2014.

WHITEHAT SECURITY.**2014 Website Security Statistics Report**. Santa Clara: WhiteHat Security Inc, 2014. Disponível em <https://www.whitehatsec.com/resource/stats. html>. Acesso em 17 abr. 2014.