UNIVERSIDADE NOVE DE JULHO - UNINOVE

MBA EM GESTÃO DA TECNOLOGIA DA INFORMAÇÃO E INTERNET

Análise Teórica da Segurança no Uso da Linguagem PHP com Banco de Dados MySQL Aplicado ao Comércio Eletrônico

Leandro Marcos Bonafin

e-mail: leandro@bonafin.com.br

Artigo apresentado à Universidade Nove de Julho – UNINOVE, como requisito parcial para obtenção do grau de Especialista em Tecnologia da Informação e Internet, sob a orientação de José de Jesus Perez Alcazar.

SÃO PAULO

MAIO - 2014

SUMÁRIO

1 INTRODUÇÃO

O presente trabalho aborda sobre o referencial teórico acerca da segurança na execução de sistemas web com a linguagem PHP e banco de dados MySQL. A composição é fundamentada na captura conceitual sobre o tema segurança aplicado a dupla PHP e MySQL em sistemas de comercio eletrônico ou sites em geral.

A maior vantagem é o uso de PHP livre e gratuito com o banco de dados mais popular da internet, o MySQL, também grátis. O objetivo é mostrar de forma superficial os principais itens de segurança que devem ser observados na aplicabilidade desta solução tão popular e de baixíssimo custo.

Mais do que jogos e entretenimento a internet permite a utilização e sua flexibilidade, portabilidade e fácil comunicação para que sejam aproveitados por sistemas de informação da mais variada gama.

Neste ambiente, sistemas originalmente desenvolvidos sob a premissa cliente-servidor, estão sendo portados em parte, ou em sua totalidade para o ambiente internet.

No entanto, fora da camada de segurança na rede, os sistemas baseados na internet tem a necessidade de prever meios de se precaverem por si só de ataques dos mais variados tipos.

O aumento do comércio eletrônico com o advento e a disseminação do uso da internet, vem provocando uma necessidade de constante aumento da segurança.

É necessária a mudança de conceitos e premissas para o desenvolvimento rápido e seguro de sistemas baseados na internet. É neste ambiente adverso que se torna premente o estudo de técnicas de programação segura atingindo o escopo de programação dinâmica aliada a consulta de dados, visando eliminar estes problemas, ou, em pior situação, diminuir ao máximo o raio de um ataque virtual bem sucedido.

O objetivo deste artigo é, levantar de forma superficial as técnicas e possíveis soluções adotadas para evitar a invasão de hackers em sistemas dinâmicos vinculados a banco de dados ou sites de comercio eletrônico, comumente denominados lojas virtuais.

2 ANTECEDENTES HISTÓRICOS

2.1 A Linguagem de programação PHP

Foi em 1995 que surgiu a primeira versão do PHP, quando Rasmus Lerdorf criou para uso pessoal uma ferramenta chamada PHP/FI (Personal Home Page/Forms Interpreter), de acordo com Niederauer (2004).

Em 1994, para Sica (2007), Lerdorf, então membro da comunidade Apache, sentindo uma deficiência em produzir conteúdo dinâmico para a web, escreveu em linguagem Perl para funcionar como um CGI (Common Gateway Interface), o Personal Home Page. Devido sua grande propagação ele disponibilizou uma parte da documentação, dando origem ao PHP v.01. Posteriormente foi adicionado um sistema para interpretação de formulários, originando o PHP/FI. A partir disso, novos colaboradores foram aparecendo e uma grande evolução do PHP pode ser percebida.

Atualmente, de acordo com Sica (2007), o PHP encontra-se na versão 5, com a novidade no suporte para a programação orientada a objetos.

O PHP, segundo Niederauer (2004), é uma das linguagens mais utilizadas na web com mais de 10 milhões de sites. As estatísticas oficiais atualizadas até janeiro de 2013 calculadas pela Netcraft, disponíveis no site php.net, totalizam 244 milhões de sites que utilizam o PHP embutido em seus códigos.

O PHP é utilizado por mais de 24% dos servidores e é tido como a linguagem de criação de script do lado servidor mais popular da web.

O desenvolvimento de PHP é suportado de forma colaborativa por uma entusiasmada comunidade mundial de usuários bem capacitados e lotados de ideias que traduzem para à pratica.

Converse (2003) é fã do PHP e cita algumas razões para amá-lo. Dentre as quais o PHP é gratuito; é fácil; é incorporado ao HTML; é multiplataforma; é estável; é rápido; é aberto; não baseado em *tags*; trabalha bem com os outros; o PHP evolui; é popular e está crescendo; e não é proprietário.

Niederauer (2004) resume o PHP pelas seguintes características: é gratuito; embutido no HTML; baseado no servidor; e tem suporte a banco de dados (segundo o

autor esta é uma das principais características do PHP tornando-o popular); e tem portabilidade.

2.2 O Banco de Dados MySQL

O MySQL é alinguagem de banco de dados relacional. O MySQL foi criado na Suécia por suecos e um finlandês, os quais trabalhavam juntos desde a década de 1980. Na concepção do seu inventor, Andrew Taylor, a SQL significa “Structured Query Language”.

De acordo com o conceito definido por Converse (2003) o PHP é:

> “a língua franca, o latim medieval, os caracteres chineses no mundo de banco de dados relacional, um idioma muito comum que torna possível a todo mundo ser entendido através de um amplo espectro de diferença”.

Niederauer (2005) define MySQL com um SGBD – Sistema de Gerenciamento de Banco de Dados – relacional que utiliza a linguagem padrão SQL, e é largamente utilizada em aplicações para a internet, sendo a mais popular entre os bancos de dados com código fonte aberto.

O autor destaca que o MySQL é uma alternativa atrativa, mesmo possuindo uma tecnologia complexa de banco de dados, seu custo é bastante baixo. Tem como destaque suas características de velocidade, escalabilidade, confiabilidade e portabilidade; é um software livre; tem facilidade no manuseio; é compatível com diversas linguagens de programação como Delphi, Java, C, C++, C#, ASP entre outras; possui interfaces gráficas – MySQL *toolkit*.

Diante disso, o PHP e o MySQL formam uma excelente dupla para o desenvolvimento de paginas dinâmicas, independente do tamanho do projeto.

Hoje a versão atual do MySQL é a 5 e, de acordo com o site db-enginers.com, o SGBD está posicionado em 2º lugar no ranking de popularidade com score de 1309,1, atrás apenas do Oracle (1502,7), mas com vantagem frente ao SQL Server (1207,8).

Seu desenvolvimento e manutenção empregam aproximadamente 400 profissionais no mundo inteiro e mais de mil contribuintes testando o software. Em 2008

a MySQL AB – empresa desenvolvedora do MySQL – foi adquirida pela Sun. No ano seguinte a Oracle comprou a Sun, e atualmente o MySQL pertence a Oracle.

O site MySQL.com tem relatado no artigo ‘10 motivos para escolher o MySQL para aplicações web’ que:

> “o MySQL é utilizado por 9 dos 10 principais sites do mundo, assim como por milhares de aplicativos corporativos baseados na web. Para o Facebook, Twiter ou Wikipedia, você depende do MySQL. Quando você assiste a vídeos no YouTube, esta usando o MySQL. Toda vez que procura ingressos de eventos no site Ticketmaster, está usando MySQL”.

A Wikipedia relata que são empresas usuárias do MySQL a NASA, HP, Sony, Nokia, Google, Motorola, HP, Bradesco, entre outras.

2.3 O Comércio Eletrônico

A internet surgiu com a empresa ArpaNet na época da guerra fria. Tudo era muito diferente do que é hoje. Após a guerra fria a tecnologia dominada e guardada pelos americanos deixou de ser segredo e passou a ser utilizada por cientistas e universidades, de acordo com a afirmação de Mendes (2000).

No Brasil a internet definitivamente começou a se tornar conhecida em 1995, mesmo que as iniciativas remontam o ano de 1991 com o advento da Rede Nacional de Pesquisa – RNP, que era um sistema acadêmico ligado ao governo.

Após 20 anos o cenário é bem diferente. Hoje efetuamos compras e transações pela internet. Para entender a dimensão deste mundo é preciso conceituar algumas figuras.

Os formatos de comercio eletrônico se apresentam da seguinte forma, se acordo com Potter e Turban (2005), os mais comuns são:

- B2B – Bussines To Bussines: é a negociação eletrônica entre empresas e fornecedores e vice-versa;
- B2C – Bussines To Consumers: é a negociação eletrônica entre empresas e consumidores. Esta modalidade representa a virtualização da compra e venda. Como exemplo temos os conhecidos sites do Submarino, Americanas e companhias aéreas que vendem passagem on line (Tam, Gol, Azul, entre outras);

- C2B – Consumers To Bussines: é a negociação entre consumidores e empresas. É o reverso do B2C, ou também conhecido como leilão reverso. Os consumidores fazem a oferta para as empresas. No Brasil ainda não se percebe o uso desta modalidade;
- C2C – Consumers To Consumers: é a negociação entre consumidores. É uma modalidade muito comum na atualidade, porem de pequenos valores. No Brasil podemos citar como exemplo o MercadoLivre, BomNegócio, OLX, TodaOferta como principais atuantes.

Diante destas modalidades, a 28ª edição do relatório WebShoppers 2013 – divulgação que analisa a evolução do e-commerce, tendências, estimativas e comportamentos dos consumidores – relata que o comercio eletrônico brasileiro faturou R$ 28 bilhões em 2013, sendo 24% maior que o registrado no mesmo período de 2012. Em números de pedidos feitos via web o numero aumentou 20%,chegando a 35,5 milhões.

Frente a isso, o mercado brasileiro possui representatividade no contexto mundial. De acordo com o site e-commerce.org em 2012 o Brasil ocupava a 5ª posição em números de usuários de internet no mundo, com 45,6% da população conectada a web.

Nesta mesma edição o WebShoppers apurou que o estimulo para comprar online com maior frequência se dá por alguns motivos, a saber: 1) preços mais baratos, 82%; 2) frete grátis, 58%; 3) segurança e sigilo dos dados pessoais e financeiros, 37%, entre outros.

Logo, nota-se que o consumidor já avalia e dá importância para a gestão da segurança do site.

A em relação aos fatores que levam os consumidores a comprar em uma determinada loja, o relatório aponta a confiança na loja (17%) como o principal fator, seguido do preço (16%), do frete grátis (14%) e do prazo de entrega (13%). Por outro lado, a pesquisa revelou os fatores que os consumidores relevam para não comprar em uma loja, sendo a falta de confiança a principal causa, com 15%, seguindo do preço, 14%, prazo 13% e frete 12%. Ou seja, o consumidor está dando importância confiança da loja.

A legislação brasileira esta buscando trazer regulamentação especifica para esta modalidade peculiar de comercio. Existem diversos projetos de lei que tendem a regulamentar com maior precisão o comercio eletrônico e a proteção do consumidor em caso de fraudes comprovadas por falhas na segurança ou roubos de dados e informações. Entretanto, nada concreto existe que possa dar plena garantia ao usuário do comercio eletrônico brasileiro.

3 ASPECTOS DA SEGURANÇA

3.1 Política de Segurança e Monitoramento

O que é segurança? Segundo De Paula (2009) segurança é o estado, qualidade ou condição de seguro, condição daquele ou daquilo em que se pode confiar, certeza, firmeza, convicção.

A segurança da informação busca proteger os ativos de uma empresa ou individuo com base na preservação de três princípios básicos:

1. Integridade (sem alterações);
2. Confidencialidade (que a pessoa correta tenha o acesso);
3. Disponibilidade de informação (deve chegar apenas aos destinatários).

Em outras palavras, a segurança é uma atividade cujo propósito é proteger os ativos contra acessos não autorizados, evitar alterações indevidas que possam por em risco a disponibilidade da informação.

Faz-se necessária a criação de um processo de gestão da segurança para a implementação de controles de segurança eficazes. Este processo deve considerar a definição de políticas de segurança, procedimentos e gerenciamento dos riscos e ameaças.

Por questões estatísticas, as políticas superiores devem ser definidas em primeiro lugar, enquanto que procedimentos e outros documentos seguem como elementos táticos, como por exemplo, uma política de segurança para firewall, que se refere a controles de acesso e listas de roteamento de informações.

A organização deve implementar ainda, os regulamentos de segurança em conformidade com a legislação em vigor, os padrões que especificam o uso conforme de determinada tecnologia, os fundamentos ou princípios que levam em conta as diferentes plataformas existentes afim de garantir que a segurança seja implementada uniformemente em toda a organização, e os guias que se referem às metodologias para os sistemas de segurança.

As responsabilidades na execução das políticas de segurança devem estar relacionadas com o perfil de cada funcionário.

Em especial, os auditores de sistemas de informação são responsáveis pelo fornecimento de relatórios para a gerência superior sob a eficácia dos controles da segurança. Estes trabalhos são consolidados através de auditorias independentes e periódicas e confrontam se as políticas, padrões, guias e procedimentos são eficazes e estão em conformidade com os objetivos de segurança definidos para a instituição.

De modo geral a segurança no uso dos recursos de tecnologia de informação se dá por alguns conceitos básicos:

- Realização regular de backup dos dados;
- Manutenção de registro e controle das copias de segurança;
- Guarda em local externo, seguro e distinto daquele aonde se encontra a informação original;
- Utilização de políticas de senhas (senhas fortes, alterações periódicas);
- Utilização de criptografia no envio de dados com informações sensíveis;
- Utilização de conexão segura (criptografada) ao realizar transações via web.

Em paralelo, fechando o arco do raciocínio no universo de trabalho PHP & MySQL, da mesma forma é preciso tomar cuidado com alguns fatores que podem por em risco a segurança.

3.2 A Segurança do PHP e do MySQL

Na visão de Sica (2003), atualmente existem duas causas dos ataques via internet. A mais difícil de impedir é a que se baseia na engenharia social e a outra, de aspecto técnico, é a falha de programação.

Os ataques de engenharia social são os mais difíceis de serem banidos, justamente por não terem base em conceitos técnicos. São eles os principais: Hoax, Phising Scam (ou vírus social).

O que é um hoax? No conceito de VIMERCATE, trata-se de boatos recebidos por e-mail ou farsas compartilhados em redes sociais. Geralmente são mensagens dramáticas ou apelativas que acompanham imagens chocantes. Para se prevenir

disso, medidas simples podem ser adotadas, como um bom antivírus, não acreditar em qualquer coisa que receber por e-mail e se preferir faça denuncia do spam. Exemplos de hoax: “a Apple vai distribuir iPhone de graça”; “veja o rato encontrado dentro da garrafa de Coca-Cola”. Ou seja, são coisas que despertam a curiosidade da pessoa.

Phishing, phishing-scam ou phishing/scam, é classificada como um tipo de fraude em que um golpista tenta obter dados pessoais e financeiros de um usuário, pela utilização combinada de meios técnicos e engenharia social.

Estes ataques poderão ser reduzidos na medida que os usuários da internet se conscientizarem e passarem a adotar políticas de segurança e regras no uso dos seus próprios computadores pessoais.

Segundo Sena, os principais tipos de ataque no PHP são:

I. SQL Injection
II. PHP Injection
III. XSS – Cross-site Scripting
IV. CSRF – Cross-site Request Forgeryes

Sem dúvida, a popularização da internet trouxe mais conhecimento e ao mesmo tempo o surgimento dos ladrões de informações, os hackers (“do bem”) e os crackers (“do mal”).

A internet não é um ambiente seguro na concepção de Sica (2003). E o PHP não foge a regra, assim como em outras linguagens, a manutenção de um ambiente virtual 100% seguro é impossível no entendimento do autor. Tudo depende da programação e da configuração da segurança do servidor, aonde o interpretador fica instalado.

Os principais possíveis ataques ocorrem da seguinte forma.

O SQL Injection é uma injeção de uma instrução SQL através de parâmetros recebidos por um sistema.

Para Sena (apud Wikipedia), é:

> “um tipo de ameaça de segurança que se aproveita de falhas em sistemas que interagem com base de dados via SQL. A injeção SQL ocorre quando o atacante consegue inserir uma serie de instruções SQL dentro de uma consulta (query) através da manipulação de entradas de dados de uma aplicação.”

Na visão de Sica (2003):

> “a inserção de código SQL não previsto e de modo arbitrário, pode comprometer a funcionalidade do sistema como um todo e também da base de dados. Embora sua descoberta foi reportada a quase 15 anos, esta técnica de ataque ainda é um problema no que se refere a segurança.”

O PHP Injection é semelhante ao SQL Injection, no entanto este tipo de ataque resume-se em passar informações por query string (parâmetros da URL), comandos em PHP ou outros endereços de arquivos que serão interpretados e executados por seu script, na definição de Sena.

O XSS – Cross-site Scripting – é uma injeção de código HTML, CSS, ActiveX ou Javascript em uma pagina. O Javascript representa a maior ameaça por possibilitar o redirecionamento de usuários para outra pagina, modificar a pagina e ler o cookies.

Para Sica (2003), esta modalidade acontece quando uma aplicação aceita dados de usuários sem nenhum tratamento. Através deste tipo de ataque a segurança é comprometida e com isso se coletam dados de áreas restritas.

Na simplicidade de Sena, consiste em interpretar códigos HTML, Javascript, etc, em uma pagina web através de um formulário ou uma URL contendo o Javascript re-codificado para enganar o usuário. Sem muito conhecimento, um simples script em HTML, PHP e Javascript são suficientes para poder rapidamente roubar informações que ficam armazenadas em cookies, por exemplo.

O CSRF – Cross-site Request Forgeries (falsificação de solicitação entre sites) é um tipo de exploração maliciosa de um website pelo qual comandos não autorizados são transmitidos a um usuário que confia no website.

Para melhor entender o conceito, Sena (B26) explica que é um ataque forçando um usuário a executar ações indesejadas em uma aplicação web. Um ataque CSRF bem aplicado pode comprometer os dados e o funcionamento do usuário comum ou do administrador!

4 APLICABILIDADE TEÓRICA E PRÁTICAS

4.1 Boas Praticas

Para garantir, ou melhor, minimizar os impactos e consequências dos ataques aos sistemas, segundo a “Conferencia PHP”, é preciso ter em mente três regras básicas de segurança:

1. Filtrar e validar os dados de entradas;
2. Formatar (escapar) os dados de saída;
3. Nunca confiar nos usuários.

O SQL Injection pode ser evitado utilizando no PHP os comandos *mysql_real_scape_strings()* e Prepared Statement. Existe também uma ferramenta para testar a pagina, denominada SQL Inject Me.

Sica (2003) em sua experiência, sugere para a minimização das consequências do SQL Injection, a utilização do XML como interface do banco de dados antes de exibi-lo ao cliente. Resumidamente, a titulo de exemplo, o “Script1” faz a consulta no banco de dados e cria um XML, o qual é lido e exibido ao cliente por um “Script2”, limitando o acesso a base de dados pelo usuário.

O PHP Injection pode ser neutralizado configurando o PHP com os parâmetros *safe_mode* para “On” e o parâmetro allow_url_mode para “Off”.

Para impedir o ataque XSS Cross-site Scripting utilize no PHP os comandos *htmlspecialchars(), htmlentities(), strip_tags()* e *whitelist.* Existe uma ferramenta de diagnostico denominada XSS Me, um add-on da Mozilla, para aplicar no site.

Sena vê como solução ao CSRF – Cross-site Request Forgeryes – o gerenciamento de sessões autenticadas por tokens (hash) randômicos e utilizando este *token* num campo de formulário tipo hidden (invisível), que ao submeter o formulário ele faz a comparação do campo escondido com a variável da sessão.

O Email Injection, uma outra forma de invasão, pode ser bloqueado evitando-se o uso do comando *mail()* no PHP.

Outas ferramentas de diagnóstico podem ser utilizadas como o Skipfish, Acunetix, Zap, Arachni e Nessus. Todas são gratuitas e possuem objetivo de analisar as vulnerabilidades de segurança em aplicações web e servidores.

Alguns mecanismos de segurança podem ser adotados para evitar a violação dos dados e garantir a consistência e confiabilidade na recomendação de Azevedo.

Tais mecanismos podem ser físicos (portas, travas, cadeados) ou lógicos (criptografia, assinatura digital, controle de acesso, etc).

Em especial a criptografia é a técnica pela qual a informação pode ser transformada de sua forma original para outro legível, de maneira que possa ser conhecida apenas por seu destinatário, cita o autor.

Os objetivos da criptografia se resumem em:

1. Confidencialidade da mensagem. (só o destinatário consegue extrair o conteúdo);
2. Integridade da mensagem. (não haver alteração durante a transmissão);
3. Autenticação do remetente. (verificar que foi ele mesmo quem enviou) e;
4. Não repúdio. (não deveria ser possível ao emissor negar a autoria da mensagem

Dentre os tipos de criptografia destacam-se as mais comuns e indicadas: MD5, SHA e Hash.

Algumas falhas de PHP de acordo com Thiago Belem:

1. URL via GET: passar parâmetros pela RUL é um erro comum. Por exemplo um ID de um produto ou categoria. Ocorrem com frequência também a passagem da pagina via parâmetro de URL via GET (visível no browser) o ideal paea este caso é criar um array com as normas das paginas validas que podem ser incluídas.

4.2 Hospedagem Própria x Terceirizada

Nem sempre se tem domínio sobre as configurações. No caso do PHP, as vezes pode estar mal configurado. Existem vantagens e desvantagens.

A principal vantagem em ter hospedagem própria, é sem duvida a possibilidade de gerenciar as permissões e definir as configurações de acordo com sua política de segurança. Porém a desvantagem é o alto custo em manter um servidor dedicado com um administrador de banco de dados e link ativo com plano de contingencia (do link e do servidor).

A hospedagem terceirizada possui varias vantagens de acordo com Converse. Todo o tratamento dos mais variados aspectos ficará sob a responsabilidade do provedor de serviços da internet – ISP – como o hardware, atualizações de software, a segurança, os backups, ente outros. Em suma, a grande vantagem reside na economia de tempo.

A hospedagem de PHP em plataforma Linux, na visão do autor, tem uma boa relação custo-benefício, sendo ridiculamente barato.

Em contrapartida, os aspectos negativos da hospedagem em um ISP residem no controle. A centralização de configurações acaba limitando os recursos do PHP para profissionais experientes que tem a intenção de “querer” alguns recursos ativos para sua utilização.

Em resumo, diante dos prós e contras, a decisão deve ser baseada em “quanto mais simples foram as necessidades, mais possível e apropriada será optar na terceirização da hospedagem”.

Existe ainda a opção por auto-hospedagem, para os administradores de site pequenos e médios. As vantagens, neste caso residem no pleno controle da sua própria configuração e na rapidez na auto resolução de problemas técnicos.

Este método exige muito esforço técnico alem de poder sair mais caro.

A decisão entre hospedar ou terceirizar deve levar em conta alguns fatores como custo, dimensão e trafego do site, necessidades de hardware ou software, tipo de conteúdo e principalmente o desejo de controle.

5 CONCLUSÃO

É imensurável o reconhecimento do desenvolvimento da internet para o mundo atual. Esta invenção foi um progresso da humanidade.

Com a abordagem teórica do tema em foco, podemos predizer que esta modalidade de serviços via internet, avança a passos largos e é uma tendência real de futuro, aonde cada vez mais transações são realizadas sob esta plataforma.

Ressalta-se ainda ser de muita importância conhecer e entender as causas dos ataques virtuais para uma melhor definição das políticas de gestão da segurança, pilar essencial para que o negócio sobreviva e tenha sustentabilidade ao longo do tempo.

É prematuro dizer que são inseguros os sistemas que operam sob a plataforma online, baseados na web, ou menos seguros dos que rodam sob a camada de proteção da rede interna. A profunda e incessante preocupação no quesito segurança e seu sucesso neste ambiente os tornam tão seguros quanto a intranet.

Em acréscimo, verifica-se que o sucesso da dupla PHP & MySQL tem favorecido o aperfeiçoamento das técnicas de segurança, tendo em vista que milhares de colaboradores contribuem para que este projeto continue sendo acessível e disseminado seu conhecimento para novos seguidores.

Ainda, é de vital importância para a empresa, no momento da tomada de decisão, entender verdadeiramente a questão da hospedagem própria ou terceirizada, afim de obter uma elevada satisfação na aplicabilidade das tecnologias disponíveis a seu favor.

Embora as influências citadas definem, de certa forma, uma preocupação com a segurança, com frequência a comunidade colaborativa tem superado seus limites unindo forças para sanar tais deficiências e até proporcionar soluções de maior ângulo.

A amplitude do tema não permite detalhar com riqueza todos os pormenores que o assunto tecnicamente possui. Esta, portanto, é uma oportunidade que deve ser aproveitada em outra ocasião, afim de penetrar em cada aspecto que nos desperte maior atenção ou que seja de maior interesse para a finalidade que o estudo se dispõe.

6 REFERÊNCIAS

ATAIDES, Anderson Pereira. **Segurança com o MySQL.** Disponível em <http://andersonataides.tripod.com/artigos/mysqlseguro.pdf>. Acesso em 03.05.2014.

AZEVEDO. Arthur Henrique Ataíde de; CASTRO, Edkarla Andrade de; SERRÃO, Paulo Roberto de Lima. **Segurança em Banco de Dados.** Disponível em <http://pt.slideshare.net>. Acesso em 08.05.2014.

BLUM, Renato Opice; ELIAS, Paulo Sá. **Regulamentação do Comércio Eletrônico na América Latina.** Disponível em <http://ecommerceclass.com.br>. Acesso em 29.04.2014.

Cartilha de Segurança para a Internet. Disponível em <http://cartilha.cert.br>. Acesso em 14.05.2014

CONVERSE, Tim; PARK, Joyce. **PHP 4: A Bíblia. Tradução da** 2ª Ed. Original de Edson Furmankiewicz. Rio de Janeiro : Elsevier, 2003. 6ª reimpressão.

DB-ENGINES. **DB-Engines Ranking.** Disponível em <http://db-engines.com/en>. Acesso em 04.05.2014.

E-BIT. **Webshoppers 28ª Edição.** Disponível em <http://www.ebit.com.br/webshoppers>. Acesso em 05.05.2014.

Evolução da Internet e do e-commerce. Disponível em <http://www.e-commerce.org.br/stats.php>. Acesso em 07.05.2014.

FONSECA, Fernando. **Curso Básico de Segurança da Informação. Academia Latino Americana de Segurança da Informação: Módulo 1.** Disponível em <http://pt.slideshare.net>. Acesso em 01.05.2014.

Guia de Referência para a Segurança da Informação Usuário Final. Coordenação de Segurança da Informação. Disponível em <http://www.governoeletronico.gov.br>. Acesso em 01.05.2014.

MENDEZ, Marcos. **O Comércio Eletrônico no Brasil.** Disponível em <http://www2.ufpa.br/rcientifica/artigos_cientificos/ed_08/pdf/marcos_mendes3.pdf>. Acesso em 04.05.2014.

MySQL. **Top 10 Reasons to Choose MySQL for Next Generation Web Applications.** Disponível em <http://www.mysql.com>. Acesso em 04.05.2014.

NIEDERAUER, Juliano. **Desenvolvendo websites com PHP.** São Paulo : Novatec, 2004.

NIEDERAUER, Juliano. **Guia de Consulta Rápida Integrando PHP 5 com MySQL.** São Paulo : Novatec, 2005.

NIEDERAUER, Juliano. **Guia de Consulta Rápida PHP 5.** São Paulo : Novatec, 2004.

NIEDERAUER, Juliano. **PHP para quem conhece PHP.** São Paulo : Novatec, 2005.

PAULA, Anchises M.G de. **Segurança no Mundo da Internet. Ameaças Tendências e Proteção.** Disponível em <http://pt.slideshare.net>. Acesso em 01.05.2014.

PESSOA, Márcio. **Segurança em PHP; desenvolva programas PHP com alto nível de segurança e aprenda como manter os servidores web livres de ameaças.** São Paulo : Novatec, 2007.

PHP. **História do PHP.** Disponível em <http://www.php.net>.Acesso em 02.04.2014.

PHP**. PHP Usage Stats**. Disponível em <http://www.php.net>.Acesso em 02.04.2014.

POTTER, Richard; TURBAN, Efraim; RAINER, Kelly. **Administração de Tecnologia da Informação.** 3ª Ed. São Paulo : Campus, 2005.

Regulamentação do comércio eletrônico e a atualização do Código de Defesa do Consumidor. Disponível em <http://www.ecommercebrasil.com.br>. Acesso em 08.05.2014.

SANTOS, Rodrigo dos. **Segurança em aplicações PHP.** Disponível em <http://pt.slideshare.net>. Acesso em 01.05.2014.

SENA, Kilderson. **Segurança com PHP I – SQL Injection.** Disponível em <http://www.mxmasters.com.br>. Acesso em 03.05.2014.

SENA, Kilderson. **Segurança com PHP II – PHP Injection.** Disponível em <http://www.mxmasters.com.br>. Acesso em 03.05.2014.

SENA, Kilderson. **Segurança com PHP III – XSS.** Disponível em <http://www.mxmasters.com.br>. Acesso em 03.05.2014.

SENA, Kilderson. **Segurança com PHP VI – CSRF.** Disponível em <http://www.mxmasters.com.br>. Acesso em 03.05.2014.

SICA, Carlos; REAL, Petter Villa. **Programação Segura Utilizando PHP – fale a linguagem da internet.** Rio de Janeiro : Ciência Moderna : 2007.

VIMERCATE, Nicolly. **O que é hoax e como fugir das farsas da Internet.** Disponível em <http://www.techtudo.com.br>. Acesso em 03.05.2014.

WIKIPEDIA. **MySQL.** Disponivel em <http://pt.wikipedia.org>. Acesso em 04.05.2014.