**7. Segurança**

O presente capítulo apresentará sugestões de segurança lógica e física para o Sistema de Camisetas Personalizadas.

**7.1. Mecanismos de segurança da Linguagem de Programação e SGDB**.

O termo captcha vêem do inglês “Completely Automated Public Turing test to tell Computers and Humans Apart” e pode ser traduzido como “público completamente automatizado para diferenciação entre computadores e humanos”. O captcha tem a função de impedir que pessoas utilizem ferramentas para acessar de forma abusiva paginas web ou interfaces de sistemas. Os captchas também são conhecidos com anti-robôs já que dependendo do nível de complexidade do captcha torna-se impossível ser interpretado automaticamente por um computador. O captcha é usado na maioria das vezes em telas de autenticação de sistemas corporativos, blogs, site de download entre outros. Tudo isso no intuito de restringir o acesso das informações somente a humanos.

A linguagem de programação PHP possui alguns métodos de criptografia entre eles os que mais se destacam são: o MD5, o SHA1 e o Base64.

MD5 é a sigla de Message-Digest Algorithm 5 foi desenvolvido em 1991 por Ronald Rivest, o MD5 é um algoritmo de hash de 128 bits. O MD5 é utilizado por software para proteger senhas, verificar a integridade de arquivos entre milhares de aplicações. Uma aplicação bem conhecida é o md5sum que consiste em criar uma string *hash* de um arquivo.

O SHA ou Algoritmo de Hash Seguro é uma família de algoritmos, o algoritmo mais usado desta família é o SHA1. O SHA1 é utilizado em uma gama de aplicações e protocolos de segurança. Os protocolos TLS, SSL e SSH são exemplos de protocolos que utilizam a criptografia do SHA1, mas mesmo sendo tão reconhecido o SHA1 possui algumas vulnerabilidades comprovadas da mesma forma que o MD5.

O base64 se comparado ao MD5 e ao SHA1 é o mais simples, este método de codificação de dados e voltado para a transferência de informações pela internet, o seu funcionamento é constituído de 64 caracteres que são “de A até Z”, “de a até z” e “de 0 a 9” e o mesmo pode ser facilmente descriptografado.

O recurso register\_globals do PHP oferece grande risco a integridade do sistema. O register\_globals possibilita a criação de variáveis do PHP a partir do envio da requisição ao servidor que hospeda a aplicação, por exemplo:

Acessando a http://dominio.com.br/index.php?function=kill com o register\_globals habilitado, automaticamente o PHP irá instanciar uma nova variável com o nome de “function” contendo o valor “kill”.

Este recurso do PHP já é considerado obsoleto já que não través benefício algum pelo contrario representa um grande risco de segurança e integridade do ambiente.

O SQL Injection é uma técnica de invasão de sistemas geralmente aplicada contra sistemas web, mas pode ser utilizada em qualquer linguagem de programação. O SQL Injection ocorre quando o atacando malicioso consegue inserir um fragmento de SQL ou ate mesmo uma instrução inteira dentro de uma consulta isso através das entradas de dados vulneráveis no sistema.

**7.2. Mecanismos de segurança e privacidade de dados.**

* Recomenda-se a utilização de um firewall para restringir os acessos ao servidor que o sistema estará instalado.
* Recomenda-se a utilização de um sistema operacional mais seguro. Como por exemplo: Linux.
* Recomenda-se que o servidor onde o sistema será instalado utilize um antivírus confiável e com rotina de atualização automática.
* Recomenda-se que as pessoas que irão manipular o servidor estejam devidamente credenciadas e autorizadas.

**7.3. Mecanismo de segurança de equipamentos e instalações.**

* Recomenda-se para assegurar à integridade física do ambiente onde será hospedado o Sistema de Camisetas Personalizadas a utilização de um controle de acesso à sala onde fica o servidor.
* Recomenda-se a utilização de no-breaks para impedir a interrupção do sistema.
* Recomenda-se a utilização de um sistema de prevenção e combate a incêndios.
* Recomenda-se a utilização de controle de temperatura na sala onde fica o servidor, assim como a utilização de climatizadores para evitar o superaquecimento do servidor.
* Recomenda-se a utilização de uma solução de backups passiva ou ativa para assegurar a recuperação de dados que eventualmente posam ser perdidos ou corrompidos.
* Recomenda-se atualização de links redundantes de conexão com a internet e com operadoras diferenciadas para garantir a disponibilização do sistema 24 horas por dia (24x7).