PHP: detecção de falhas de programação que possibilitem injeção

FERNANDO, Rassion[1] (raisson.sb@gmail.com) ; **FERREIRA, Alcione**[2] (aferreira@uems.br); **CHASTEL, André**[3] (chastel@comp.uems.br);

[1] Discentes do curso de Sistemas de Informação da UEMS – Dourados

[2]Docente convocado do curso de Sistemas de Informação da UEMS – Dourados;

[3]Docente do curso de Sistemas de Informação da UEMS – Dourados;

A internet revolucionou o mundo comercial, tanto para compra, venda e transações em geral. A maneira com que o mercado vem evoluindo tecnologicamente vem obrigando, desde grande a pequenas empresas a se informatizarem. Isso muitas vezes pode trazer muitos riscos, pois com um investimento relativamente pequeno as empresas conseguem adquirir um home page, porém as vezes a falta de experiência e conhecimento de programadores fazem com que essas empresas se tornem vulnerareis diante a ataques virtuais, pois a fragilidade de seus sistemas acabam se tornando porta de entrada a atacantes mau intencionados. Segurança de servidores é um assunto muito importante quando se fala em segurança da informação, mais muitas vezes desconhecido por atuantes da área. Esse trabalho pretende tratar um pouco sobre esse assunto, tendo o arquivo de configuração do PHP como objeto de estudo, suas funções de segurança, e a criação de uma ferramenta que verifica códigos que possibilitem a alterações dessas funções que tem como objetivo manter um servidor com aplicação em PHP e seus arquivos seguros. O arquivo de configuração do PHP, o php.ini, é responsável pelas diretivas de configuração do servidor. Ele é lido quando o PHP é iniciado, ou quando o servidor web for inicializado para as versões de módulo de servidor. Através da função ini_set( ), é possível alterar os valores do php.ini durante a sua execução. Este trabalho tem como objetivo desenvolver uma técnica de prevenção de ataques a servidores de aplicação, verificando e impossibilitando que através do comando ini_set, sejam desabilitadas funções de segurança do PHP, descritas na lista de diretivas do php.ini como por exemplo disable_functions( ), função que permite desativar funções do modo de segurança, e funções do modo de segurança, como safe_mode_allowed_env_vars( ), que dá permissão ao usuário editar qualquer variável ambiente do sistema. Ameaças como Disfarce, onde um usuário finge ser outro para obter informações restritas, ou ataque a bibliotecas compartilhadas são exemplos de casos que poderão ser evitados caso seja tratado questões de segurança como essas citadas.

Palavras-Chave: Programação. Segurança. PHP.

Agradecimentos: Agradeço ao meu Orientador Profº Alcione Ferreira e ao meu Co-orientador Profº Msc. André Chastel pela dedicação em me acompanhar durante os estudos e desenvolvimento deste trabalho. Aos colegas de sala Eduardo, José e Flávio pelo companheirismo nos anos de faculdade.