

Desenvolvimento de uma Aplicação para Verificação de Segurança no Ambiente Moodle

Marcelo Kunz¹, Marco Antoni¹, Roberto Franciscatto², Evandro Preuss², Antonio R. Delepiane De Vit², Adriana Pereira²

¹Tecnologia em Sistemas para Internet – Colégio Agrícola de Frederico Westphalen (CAFW) - Universidade Federal de Santa Maria (UFSM)
98.400-000 – Frederico Westphalen – RS – Brasil

²Departamento Graduação, Pós-Graduação e Pesquisa – Colégio Agrícola de Frederico Westphalen (CAFW) - Universidade Federal de Santa Maria (UFSM)
98400-000 – Frederico Westphalen – RS – Brasil

marcelo.cafw@hotmail.com, marquinho9.10@gmail.com, {roberto, evandro, rodrigodevit}@cafw.ufsm.br, adriana.pereira@ufsm.br

Abstract. *This paper aims to address the context of information security in web applications and infrastructure, with a proposal to develop a tool to check security in a virtual learning environment Moodle. The prototype includes checking safety standards both in the application and in the services of the server. To develop such an application will be used scripting language for the Linux operating system, called Shell Script. Finally, are addressed in this article the results expected by the application of the prototype, its contribution and final considerations.*

Resumo. *O presente trabalho objetiva abordar o contexto da segurança da informação em aplicações web e sua infraestrutura, apresentando uma proposta de desenvolvimento de uma ferramenta para verificação de segurança no ambiente virtual de aprendizagem Moodle. O protótipo contempla a verificação de padrões de segurança tanto na aplicação quanto nos serviços do servidor. Para desenvolvimento de tal aplicação será utilizada a linguagem de criação de scripts para o sistema operacional Linux, denominada Shell Script. Por fim, são contemplados no presente artigo os resultados esperados pela aplicação do protótipo, sua contribuição e considerações finais.*

1. Introdução

Novas tecnologias voltadas à educação têm surgido com grande frequência, com o objetivo de complementar os estudos em sala de aula por parte dos alunos. Tais tecnologias procuram em sua essência promover o aprendizado de maneira constante além dos limites físicos de uma sala de aula. Neste cenário encontram-se as aplicações web (*e-learning*), *mobile learning* (*m-learning*), *ubíquo learning* (*u-learning*), entre outras, com o mesmo propósito (Valente, 2007).

Neste contexto, têm-se o surgimento dos AVA's (Ambientes Virtuais de Aprendizagem) que contemplam uma abordagem colaborativa, virtual e que tem o objetivo de auxiliar no processo de ensino e de aprendizagem de forma a permitir uma

integração entre tecnologia e ações de aprendizagem (Alves, 2005). Como exemplo de AVA, pode-se citar o Moodle, uma ferramenta de código livre, utilizada em mais de 150 países e que possui uma grande inserção nos ambientes escolares de aprendizado virtual (Moodle, 2012).

Um problema que surge com relação ao conteúdo que é disponibilizado de forma on-line é o fator segurança. Neste caso, as aplicações devem prover mecanismos de forma a assegurar que o usuário estará em um ambiente livre de ações que possam comprometer o bom funcionamento de suas atividades; porém, isto nem sempre é possível ou fácil de solucionar em um ambiente com cenários diversos (Martins & Reis, 2008).

Desta forma, ciente dos principais problemas de segurança relacionados a aplicações web, pretende-se através deste projeto desenvolver uma aplicação de verificação de segurança para o ambiente virtual de aprendizado Moodle. O presente trabalho está organizado da seguinte forma: na seção 2 será descrito sobre o contexto da segurança da informação de modo geral. Na seção 3 será apresentado como será desenvolvido o protótipo e as ferramentas que serão utilizadas. Na seção 4 são abordados os resultados esperados com a aplicação da ferramenta, e por fim na seção 5 as conclusões finais referentes ao respectivo trabalho.

2. Segurança da Informação

Ao analisar o cenário onde se encontra uma aplicação web, como é o caso dos ambientes virtuais de aprendizagem, percebe-se a necessidade de proteção tanto da aplicação web (que está disponível, muitas vezes possui um código fonte aberto e conhecido) quanto do servidor web que hospeda tal aplicação, sendo necessário neste caso, a análise dos principais serviços e configurações deste servidor.

2.1 As estruturas da segurança da informação

Quando abordamos o tema segurança da informação é importante considerar que o mesmo é composto por duas categorias principais: o controle de acesso físico (impedindo que pessoas não autorizadas tenham acesso físico à infraestrutura de um *datacenter*, por exemplo) e a parte lógica (implementada através de ferramentas existentes tais como: *firewall*, *honeypots*, criptografia, certificados digitais, protocolos de segurança, entre outros). Neste contexto entende-se que a segurança da informação, deve prover três itens essenciais (Laureano, 2012):

- Confidencialidade: limita o acesso à informação apenas por entidades autorizadas pelo dono da informação.
- Integridade: deve garantir que a informação manipulada esteja de acordo com os padrões estabelecidos pelo dono da mesma, impossibilitando a alteração ou exclusão desses dados por pessoas não autorizadas.
- Disponibilidade: a informação deve sempre estar disponível para todos aqueles que podem/devem ter acesso a ela.

2.2 Segurança em aplicações Web e Servidores

As aplicações web por estarem em um cenário de disponibilidade integral necessitam

de proteções para assegurar os requisitos citados na seção anterior. Sabe-se que em uma aplicação web, um atacante pode explorar diversos tipos de vulnerabilidades conhecidas e catalogadas, como: injeção de código (SQL injection), quebra de autenticação e gerenciamento de sessão, cross-site scripting (XSS), referência insegura a objetos, configuração incorreta de segurança, exposição de dados sensíveis, redirecionamentos e encaminhamentos inválidos, entre outros (OWASP, 2013).

Além de tais vulnerabilidades é preciso ter um cuidado especial quanto a infraestrutura que recebe um ambiente virtual de aprendizagem, no que diz respeito ao sistema operacional e configuração dos serviços básicos para deixar um AVA em perfeito funcionamento.

Quando se projeta uma estrutura (servidor e serviços) para receber o Moodle, é importante realizar várias verificações e ajustes na configuração do servidor, como por exemplo: manter o sistema operacional sempre atualizado, utilizar sempre as últimas versões estáveis de serviços básicos (interpretador de sites PHP, banco de dados MySQL e o servidor Web Apache), utilizar um firewall no servidor, desativar serviços e contas de usuários não utilizados, instalar detectores de rootkits, verificar as permissões em arquivos e pastas do Moodle, habilitar o suporte a SSL, além de uma política de senhas bem elaborada para usuários do ambiente (Moodle, 2012).

O grande desafio para um administrador de redes ou administrador de um AVA, está em fazer com que toda a aplicação, serviços e sistema operacional, funcione perfeitamente, com o maior nível de segurança possível. Diante de tal cenário faz-se necessário a utilização de uma ferramenta de segurança que faça uma verificação automática de segurança, considerando os principais requisitos de segurança presentes em um AVA, sua estrutura e forma de funcionamento.

3. Desenvolvimento do Protótipo

A ideia proposta neste trabalho é o desenvolvimento de uma aplicação de verificação de segurança voltada ao ambiente Moodle, onde seja verificado o servidor que hospeda a aplicação, os serviços básicos que dão suporte ao AVA, bem como a aplicação Moodle (quanto aos requisitos básicos de segurança proposto por seus desenvolvedores), como forma de promover um ambiente virtual de aprendizagem seguro.

Para a construção do protótipo, primeiramente foi realizada uma revisão acerca dos requisitos básicos de segurança envolvidos em aplicações web, servidores web e ambientes virtuais de aprendizagem. Em seguida, foi realizado um estudo das tecnologias de segurança para ambiente Linux e os principais requisitos de segurança indicados para a plataforma Moodle. O próximo passo será o desenvolvimento do protótipo que contemple a verificação dos requisitos usuais de segurança para o ambiente Moodle (verificação no servidor, quanto ao sistema operacional, serviços e aplicativos instalados, bem como, no ambiente virtual Moodle). Para este passo a ideia é a utilização da linguagem para criação de scripts, denominada Shell Script, oriunda dos sistemas Linux, que possui suporte a uma série de recursos, além de interfaces gráficas como o Zenity e o YAD, que permitem uma maior interação por parte do usuário.

Em seguida, será feita a análise detalhada da ferramenta de verificação de segurança (protótipo desenvolvido em Shell Script), através de testes em diferentes

cenários (versões diferentes do ambiente Moodle e diferentes distribuições Linux) e aplicação de questionários, como forma de obter informações sobre a ferramenta.

4. Resultados Esperados

Com o desenvolvimento deste trabalho, pretende-se em sua conclusão disponibilizar o software para uso em instituições, escolas, telecentros locais, com o intuito de fazer melhorias, corrigir eventuais problemas e obter respostas dos administradores/gestores do ambiente Moodle; propiciar a verificação de requisitos básicos de segurança, com o intuito de fornecer um maior nível de confiabilidade para o usuário; e proporcionar aos alunos de ambientes virtuais de aprendizagem como o Moodle, um ambiente interativo e integrativo de acesso a informação e ao conhecimento, com base na verificação de segurança sob diferentes aspectos (aplicação e servidor).

5. Considerações Finais

Diante de um cenário complexo, dinâmico e que necessita de disponibilidade e segurança pode-se perceber através deste trabalho que o desenvolvimento de uma ferramenta automática de segurança para o ambiente virtual de aprendizagem Moodle, pode ser de grande valia, para detectar e posteriormente resolver problemas que antes necessitariam de um grande e complexo trabalho de monitoramento manual. Ainda, dada a quantidade de vulnerabilidades e surgimento de novas tecnologias constantemente, faz-se necessário automatizar e criar ambientes cada vez mais seguros que propiciem o desenvolvimento das atividades educacionais de forma íntegra, hábil e ágil.

Referências

ALVES, L.; BRITO, M. (2005) O Ambiente Moodle como Apoio ao Ensino Presencial. Anais do 12º Congresso Internacional da Associação Brasileira de Educação a Distância – ABED

LAUREANO, M. Segurança da Informação. ISBN: 978-85-63687-50-0, páginas 152. Editora LT – Curitiba, 2012.

MARTINS, A.; REIS, F. (2008). A importância das Plataformas no Ensino à Distância. In Costa, Fernando. et al (Orgs.). Anais da Comunidade de aprendizagem Moodle. 2007. Portugal. Caldas Moodle 08. EDUCOM. Pp.36-38.

MOODLE. Site, 2012. Disponível em: <http://moodle.org>. Acesso em 03 de março de 2012.

OWASP. Project, 2013. Disponível em: https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project. Acesso em 10 de agosto de 2013.

VALENTE, L. & MOREIRA (2007). Moodle: moda, mania ou inovação na formação? – testemunhos do Centro de Competência da Universidade do Minho. In P. Dias et al (Orgs.). Anais da V Conferência, Challenges/Desafios 2007. Braga: Centro de Competência Nónio Séc. XXI.