Segurança em Sistemas de E-learning: uma Análise do Ambiente Tidia-Ae/Sakai

Eduardo H. Gomes [1,2], Edson P. Pimentel [1], João H. Kleinschmidt [1]
[1] Universidade Federal do ABC
[2] Instituto Federal de Educação Ciência e Tecnologia de São Paulo
{eduardo.gomes, edson.pimentel, joao.kleinschmidt}@ufabc.edu.br

Resumo

Com os avanços e popularização da Internet houve uma expansão da Educação a Distância através da Web e conseqüentemente um aumento no uso de sistemas de e-learning. Esses sistemas armazenam dados de estudantes, professores, conteúdos, avaliações e podem ser alvo de vários tipos de ataques de segurança. Em qualquer sistema o acesso a informações confidenciais é uma violação e no âmbito da educação isso não é diferente. Este artigo tem por objetivo apresentar um estudo sobre vulnerabilidades de segurança nos aspectos de confidencialidade e autenticação em sistemas de aprendizagem eletrônica baseada na web. Os experimentos foram realizados no ambiente Tidia-Ae/Sakai. Espera-se que a detecção de falhas de segurança encontrada e relatada nesse trabalho possa chamar a atenção dos desenvolvedores para esses aspectos no desenvolvimento de sistemas de e-learning.

Palavras chave:

E-learning, Scanner de vulnerabilidades, Segurança, Tidia-Ae, Sakai.

Abstract

The expansion of internet access was followed by a growth of distance education via Web and consequently an increased use of e-learning systems. These systems store data of students, teachers, content, assessments and may be vulnerable to various types of security attacks. In any system, non granted access to confidential information is a violation and in the Education field is no different. This article aims to present a study on security vulnerabilities in the aspects of confidentiality and authentication in e-learning systems based on the web. The experiments were performed in the environment Tidia-Ae/Sakai. It is expected that the detection of security flaws found and reported in this work can draw attention of the developers to those aspects in the development of e-learning systems.

Keywords:

E-learning, Vulnerability Scanner, Security, Tidia-Ae, Sakai.

Introdução

Segundo Moore [Moore, 1996] a integração da Web com as práticas antigas de EAD proporcionaram o surgimento do termo "Educação baseada na Web" (EBW). Com o crescimento no uso da internet, houve um aumento da demanda por cursos a distância e conseqüentemente surgiram várias plataformas no conceito de Sistemas Gerenciadores de Aprendizagem (designados de LMS - Learning Management Systems) que são muito bem sucedidos na educação em relação ao número de usuários, Devedzic [Devedzic, 2004].

É de suma importância que esses sistemas estejam alinhados a uma teoria pedagógica adequada aos objetivos de aprendizagem em questão. Além disso, busca-se melhorar as características técnicas nas ferramentas de criação, distribuição e gestão do conhecimento, visando um melhor grau de comunicação, trabalho colaborativo, acompanhamento do progresso do aluno, variedade nos métodos de avaliação, auto-avaliação e a estruturação dos conteúdos de aprendizagem conforme Crosetti [Crosetti, 2000].

Alguns autores consideram que a modalidade de e-learning é a próxima evolução da formação e uma estratégia fundamental para maximizar o capital humano na economia do conhecimento [PrimeLearning, 2001].

Dado que os sistemas de e-learning tem se tornado muito populares ao longo dos últimos anos e são acessados por uma ampla gama de usuários, a segurança é um requisito essencial pois esses sistemas podem se tornar alvo de vários tipos de ataque.

Por isso, a autenticação, não repúdio, a confidencialidade dos dados, integridade e outras questões de segurança são aspectos importantes a serem considerados no desenvolvimento desses sistemas, pois é de vital importância garantir a integridade tanto de avaliações e trabalhos desenvolvidos pelos alunos como a prevenção da falsificação dessas avaliações.

Com isso o objetivo desse artigo em particular é investigar possíveis vulnerabilidades de segurança em aspectos de confidencialidade e autenticação do ambiente Tidia-Ae / Sakai.

Este artigo está organizado da seguinte forma. Seção 2 apresenta os trabalhos relacionados com o presente trabalho. Seção 3fornece Informações básicas sobre o ambiente Tidia-Ae / Sakai. Seção 4 descreve brevemente a segurança em sistemas de E-learning e apresenta uma análise do problema. Seção 5 descreve o funcionamento dos Scanners de vulnerabilidades. Seção 6 é dedicada à parte experimental do presente trabalho onde os experimentos, a metodologia e os resultados são apresentados. Finalmente, a seção 7 propõe as soluções para as vulnerabilidades e apresenta algumas conclusões sobre este trabalho.

Conclusões

Neste trabalho questões de segurança relacionadas com o LMS Tidia-Ae / Sakai são estudadas. Dentre vários aspectos de segurança como a autenticação, a disponibilidade, confidencialidade e integridade, neste artigo optou-se por investigar ataques de confidencialidade e autenticação.

Além disso, este trabalho mostrou que uma instalação padrão de um servidor Tidia-Ae / Sakai é vulnerável a ataques. As principais vulnerabilidades encontradas foram: o ambiente permite a utilização de senhas fracas e ataques de adivinhação, permitindo o uso de técnicas de força bruta para adivinhação de nomes de usuários e senhas. A solução para essas vulnerabilidades seria uma política de senhas fortes, a utilização de Captcha nas telas de login e a implementação de mecanismos de bloqueio de acesso, ao se detectar múltiplas tentativas erradas de acesso ao ambiente em determinado tempo.

Outra vulnerabilidade encontrada foi o tráfego de dados na rede sem criptografia, ocasionada pela utilização do Protocolo HTTP durante a instalação, o que permite a utilização de analisadores de pacotes para revelar nomes de usuários e senhas. A solução para essa vulnerabilidade é a utilização de SSL (secure socket layer) que é a tecnologia padrão de segurança para o estabelecimento de uma conexão criptografada entre um servidor web e um navegador (HTTPS).

A vulnerabilidade de Cross Site Scripting (XSS) encontrada permite que um atacante envie códigos maliciosos para outro usuário. A proteção contra esse ataque é baseado no tratamento dos inputs do ambiente, filtrando variáveis de entrada de dados.

Outras vulnerabilidades estudadas neste artigo estão diretamente ligadas a uma errônea configuração do sistema ou utilização de serviços desatualizados que poderiam ser evitadas se houvesse uma documentação atualizada e de fácil entendimento.

A grande quantidade de publicações sobre a necessidade de segurança em sistemas de e-learning nos últimos anos já traz grande relevância à pesquisa acerca desse assunto. Com a chegada dessas novas aplicações ou tecnologias surge à necessidade de estudos específicos para a proteção dos dados e o desafio nesses sistemas de e-learning é pensar sempre no tripé segurança, desempenho e usabilidade.

Os resultados desse trabalho sugerem que as instituições e organizações mesmo investindo significativos recursos na implementação de sistemas de e-learning, o fazem com foco voltado a provisão de conteúdo, às vezes negligenciando as questões de segurança ou não as priorizando. Para criar ambientes de aprendizagem mais seguros e confiáveis, é essencial a remoção de todas as falhas de segurança em sistemas como o Tidia-Ae / Sakai.

Referências

[1] [Acunetix, 2011] Acunetix, Web Vulnerability Scanner, http://www.acunetix.com. Acessado em 28/03/2011.

[2] [Anantasec, 2011] Ananta Security. Web Vulnerability Scanners Evaluation, http://anantasec.blogspot.com. Acessado em 28/03/2011.

[3] [Appscan, 2001] Appscan – IBM, http://www-01.ibm.com/software/awdtools/appscan/#. Acessado em 28/03/2011.

[4] [Asha, 2008] S.Asha, C.Chellappan, Authentication of E-Learners Using Multimodal Biometric Technology. (2008). Biometrics and Security Technologies, 2008. ISBAST 2008. International Symposium on. DOI: 0.1109/ISBAST.2008.4547640.

[5] [Atutor, 2011] Atutor , http://www.atutor.ca. Acessado em 04/06/2011.

[6] [AulaNet, 2011] AulaNet, http://www.eduweb.com.br. Acessado em 04/06/2011.

[7] [Beder, 2005] Beder, D. M. ; Otsuka, J. L. ; Silva, C. G. DA ; Silva, A. C. DA; Talarico Neto, Americo; Oliveira, Alessandro ; Rocha, H. V. ; Ricarte, Ivan ; Silva, Júnia Coutinho Anacleto. (2005). The TIDIA-Ae Portfolio Tool: a case study of its development following a component-based layered architecture, II Workshop TIDIA FAPESP 2005, São Paulo.

[8] [Crosetti, 2000] Crosetti, B. d. B. (2000).Possibilidades educativas de las Webtools. Palma: Universitat de les Illes Balears.

[9] [CVE, 2011] Common Vulnerabilities and Exposures (CVE®), http://cve.mitre.org/about/index.html. Acessado em 17/04/2011.

[10] [Desira, 2009] Desira M. (2009). An Open Source Vulnerability Scanner for E-Commerce Web Applications, University of Malta.

[11] [Devedzic, 2004] Devedzic, V.; Simic, G.;Gasevic, D. (2004). Semantic Web and Intelligent Learning Management Systems. In: Proceedings of International Workshop on Applications of Semantic Web for E-Learning, Maceió, Brasil.

[12] [Gonçalves, 2007] Gonçalves, V. M. B. (2007). A Web Semântica no Contexto Educativo. Tese de doutorado. Porto: Universidade do Porto.

[13] [Gordon, 2006] L. Gordon, M. Loeb, W. Lucyshyn, R. Richardson. (2006). "Computer crime and security survey", Computer Security Institute.

[14] [Gualberto, 2009] Gualberto, T. M.; Abib, S ; Zorzo, S D. (2009). "INCA: A Security Service for Collaborative Learning Environments". International Conference on Education Technology and Computer (ICETC), IEEE Computer Society, 111-115.

[15] [Hernández, 2008] J. C. G. Hernández, M. A. L. Chávez, Moodle Security Vulnerabilities.(2008). 5th International Conference on Electrical Engineering Computing Science and Automatic Control.

[16] [Hoobienet, 2011] Hoobienet, http://www.hoobie.net/brutus/. Acessado em 28/03/2011.

[17] [Kumar, 2011] Kumar S., Dutta K. (2011). Investigation on security in LMS Moodle, International Journal of Information Technology and Knowledge Management.

[18] [Lin, 2004] N. Lin, L. Korba, G. Yee, T. Shih e H. Lin. (2004). Security and privacy technologies for distance education applications. Proc. of the 18th International Conference on Advanced Information Networking and Applications (AINA), IEEE Press, pp. 580-585, doi:10.1109/AINA.2004.1283972.

[19] [Lince-dc-Ufscar, 2010] Lince-dc-Ufscar. (2010). Avaliação do Projeto Tidia-Ae e suas Aplicações, projeto reuso de software fapesp. São Carlos, SP - Brasil.

[20] [Lotus, 2011] Lotus, http://www.lotus.com. Acessado em 04/06/2011.

[21] [Luvit, 2011] Luvit, http://www.grade.com. Acessado em 04/06/2011.

[22] [Madeira, 2007] J. Fonseca, M. Vieira, H. Madeira. (2007). "Testing and Comparing Web Vulnerability Scanning Tools for SQL Injection and XSS Attacks", 13° IEEE Pacific Rim Dependable Computing Conference (PRDC 2007), Melbourne, Victoria, Australia.

[23] [Moodle, 2011] Moodle, http://moodle.org. Acessado em 28/03/2011.

[24] [Moore, 1996] Moore, M. G., Kearsley, G. (1996). Distance Education: a systems view. Belmont (EUA): Wadsworth Publishing Company.

[25] [NTOSpider,2011] NTOSpider, NT OBJECTives, http://www.ntobjectives.com/ntospider. Acessado em 28/03/2011.

[26] [Pimentel, 2010] André P. Freire *, Flávia Linhalis, Sandro L. Bianchini, Renata P.M. Fortes, Maria da Graça C. Pimentel. (2010). Computers & Education, Vol. 54, No. 4. (16 May 2010), pp. 866-876. Revealing the whiteboard to blind students: An inclusive approach to provide mediation in synchronous e-learning activities.

[27] [PrimeLearning, 2001] PrimeLearning Inc., eLearning. (2001) A key strategy for maximizing human capital in the knowledge economy, W.R. Hambrecht & Co, http://www.astd.org.

[28] [Raitman, 2005] R. Raitman, L. Ngo e N. Augar. (2005). Security in the Online E-Learning Environment. Proc. of the 5th International Conference Advanced Learning Technologies (ICALT), IEEE Press, July 2005, pp. 702–706, doi=10.1109/ICALT.2005.236.

[29] [Sakai, 2011] Sakai Project, http://www.sakaiproject.org. Acessado em 28/03/2011.

[30] [Suto, 2010] Suto L. (2010) Analyzing the Accuracy and Time Costs of Web Application Security Scanners, San Francisco, February.

[31] [TelEduc, 2011] TelEduc, http://teleduc.nied.unicamp.br. Acessado em 04/06/2011.

[32] [Tidia-Ae, 2011] Tidia-Ae, http://tidia-ae.usp.br/download. Acessado em 28/03/2011.

[33] [WebCT, 2011] WebCT e Blackboard, http://www.blackboard.com. Acessado em 04/06/2011.

[34] [WebInspect, 2011] HP WebInspect, https://www.fortify.com. Acessado em 28/03/2011.

[35] [Wireshark, 2011] Wireshark, http://www.wireshark.org. Acessado em 04/07/2011 2011.