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 encontradas e relatadas nesse trabalho possam chamar a atenção dos desenvolvedores para esses aspectos no desenvolvimento de sistemas de e-learning.

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.

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

Área temática – Seguridad de la Información.

1.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.

2. Trabalhos relacionados

Nos parágrafos abaixo apresentamos alguns trabalhos relacionados à segurança em ambientes de e-learning que possuem uma intersecção com o trabalho apresentado neste artigo, tornando possível identificar contribuições a serem feitas no Tidia-Ae / Sakai ou mesmo em outros ambientes de e-learning como a implementação de mecânismos de identificação que não sejam apenas através do método usuário e senha.

A contribuição do trabalho de [Hernández, 2008] foi de apresentar um modelo UML dos serviços de segurança do Moodle, que também é um LMS open-source, afim de reduzir a curva de aprendizagem de sua arquitetura possibilitando que desenvolvedores implementem serviços

sempre pensando em segurança. O trabalho também mostrou que o Moodle é vulneravel a alguns tipos de ataque de segurança.

Visando atender altos níveis de confidencialidade e privacidade em ambientes de aprendizagem colaborativa, o trabalho de [Gualberto, 2009] chamado de INCA (Integridade, não repúdio de confidencialidade e autenticidade) propõe um serviço complementar que é fornecido através de Web Services e fornece uma infra estrutura de chave pública. O trabalho apresentou um estudo de caso na ferramenta de chat do Sakai e demonstrou uma contribuição significativa com a segurança do ambiente.

No trabalho apresentado por [Asha, 2008] os autores propõe um sistema de autenticação dinâmica utilizando biometria multimodal a fim de evitar que outra pessoa tente utilizar o sistema após a sessão de login.

3. O ambiente Tidia-Ae / Sakai

O projeto Tidia-Ae (Tecnologias da Informação no Desenvolvimento da Internet Avançada - Aprendizado Eletrônico) que teve seu início em setembro de 2004 e foi financiado pela FAPESP (Fundação de Apoio à Pesquisa do Estado de São Paulo) com o objetivo principal de estimular a pesquisa na área de Tecnologia da Informação aplicada à Educação a Distância em projetos relacionados a redes de computadores de alta velocidade, ou internet avançada, Pimentel [Pimentel, 2010].

Especificamente, o Tidia-Ae tem como objetivo a pesquisa e desenvolvimento de ferramentas de suporte e apoio ao ensino e aprendizagem que possam ser reutilizadas, ou seja, a criação de um sistema flexível para que se consiga "montá-lo" a partir de um conjunto dessas ferramentas e satisfazer diferentes cenários de aprendizagem conforme Beder [Beder, 2005]. O projeto em sua primeira fase envolveu mais de 150 pesquisadores e 20 laboratórios de Universidades de São Paulo.

Na segunda fase do projeto que teve seu início em maio de 2007, optou-se por iniciar uma parceria com o projeto Sakai, que veremos mais adiante, e adotou-se seu framework para o desenvolvimento de ferramentas de e-learning.

O projeto Sakai [Sakai, 2011] é um LMS open-source produto da parceria das universidades de Stanford, Michigan, Indiana, MIT e Berkeley baseado na tecnologia Java.

O Sakai teve seu inicio em 2004 e é uma ferramenta de colaboração integrada e ambiente de aprendizagem, pode ser usado para uma variedade de finalidades, tais como ensino, pesquisa, aprendizado etc. No Sakai as aplicações são inseridas no sistema sem que este precise de qualquer configuração, fazendo uma analogia, é um conceito similar aos plugins [Lince-dc-Ufscar, 2010].

Dentre muitas de suas ferramentas como demonstra [Lince-dc-Ufscar, 2010] destaca-se:

Ferramenta	Descrição
Annoucements	Avisos importantes.
Resources	Armazenamento e organização de materiais.
Email Archive	Acesso a emails enviados aos participantes.
Wiki	Criação e edição colaborativa de conteúdo Web.
Blog	Ferramenta de posts em formato de blogue.
Calendar	Organização de prazos e atividades.
News	Criação e exibição de notícias via RSS.
Syllabus	Sumário de disciplinas.
Assigments	Criação e avaliação de atividades.
Gradebook	Cálculo, apresentação e armazenamento de notas.
Tests & Quizzes	Criação e organização de testes online.
Sitestats	Geração de relatório de atividades dos participantes.

Tabela 1 - Ferramentas do Ambiente Sakai

4. Segurança em Sistemas de E-learning

A maioria das pesquisas em sistemas de e-learning, tem seu interesse voltado à provisão de conteúdo para os usuários e não ponderam sobre requisitos de segurança no desenvolvimento das ferramentas [Gualberto, 2009]. Devido à arquitetura aberta desses sistemas, essa negligência em questões de segurança pode muitas vezes deixar os sistemas de gerenciamento de aprendizagem vulneráveis a ataques maliciosos. Conforme demonstrou Raitman [Raitman, 2005] em sua pesquisa, a segurança tem um papel essencial em sistemas de e-learning que é prover uma sessão fim-a-fim com segurança entre alunos e professores com a instituição educacional.

Outra abordagem da segurança foi apresentada por lin [Lin, 2004] que em seu artigo pesquisou o ponto de vista do aprendiz e demonstrou que a segurança em LMS's tem a missão de construir um sentimento de segurança para que se consiga obter interação e colaboração dentro desses ambientes. Por isso, aspectos como autenticação, confidencialidade, disponibilidade, integridade e não repúdio devem ser sempre considerados no desenvolvimento desses ambientes. Recentemente a necessidade de segurança em sistemas de e-learning tem sido destaque em muitas literaturas.

A confidencialidade garante que a informação somente pode ser acessada por pessoas explicitamente autorizadas, é a proteção de sistemas de informação para impedir que pessoas não autorizadas tenham acesso ao mesmo. Raitman [Raitman, 2005] cita que em ambientes de e-learning os alunos necessitam da garantia de que seus trabalhos submetidos pela rede sejam mantidos em sigilo e apenas o tutor tenha acesso ao mesmo. Neste artigo o foco é voltado na exploração de vulnerabilidades para acessos não autorizados com ênfase no mecanismo de autenticação a usuários e senhas.

O Tidia-Ae/Sakai utiliza login e senha do usuário para o acesso ao ambiente de maneira imediata e fácil à informação. Isso é importante para a distribuição on-line dos conteúdos, pois os usuários estão dispersos ao redor do mundo. Esse método é o mais simples para a autenticação de identidade e acesso.

Em ataques de Confidencialidade o principal objetivo do atacante é o acesso a dados e recursos confidenciais e não a alteração dos dados. Entre as vulnerabilidades mais comuns estão o armazenamento e tráfego dos dados sem criptografia, referência insegura de objetos, que podem ser imagens, códigos ou chaves primárias como parâmetros de url ou de formulários, vazamento de informações sigilosas sobre sua lógica, configuração e detalhes internos, tratamento de erros impróprio, permitindo divulgação intencional de informações confidenciais.

Ataques de autenticação são geralmente implementados na página de login, mas podem ter como alvo páginas de alterações de senha, esqueci minha senha, lembrar minha senha, atualização de contas e outras funções relacionadas e podem estar sujeitas a ataques automáticos de ferramentas de força bruta. No caso do LMS Tidia-Ae, como demonstrado adiante, um atacante pode abrir várias conexões simultâneas e efetuar várias tentativas de conexão sem ser detectado.

5. Scanner de vulnerabilidades em aplicações web

Para testar o ambiente Tidia-Ae / Sakai foi utilizado um scanner de vulnerabilidades de segurança. Segundo Desira [Desira, 2009], um scanner de vulnerabilidade é um processo automatizado, que após inicial configuração não necessita de interação humana. Basicamente envolve 3 passos: Configuração, "fingerprint" ou "crawling" e escaneamento. Em cada uma dessas etapas, as seguintes funções são executadas:

Configuração
Onde se define o endereço da aplicação web através da URL (Uniform Resource Locator) e onde também se configuram os parâmetros para quais tipos de ataques será feito o teste de penetração.

"Fingerprint" ou "Crawling"
Nesta etapa é feito o mapeamento dos serviços utilizados e produz-se um mapa da estrutura interna da aplicação.

Scanner
Abre cada link encontrado a partir da página principal e efetua testes de penetração repetidas vezes para todos os tipos de vulnerabilidades até que todos os links sejam testados.

Para testar vulnerabilidades em aplicações web, existem duas abordagens principais encontradas na literatura: "white box" e "black box" conforme Madeira [Madeira, 2007] demonstra em seu trabalho. Na abordagem "white box" é necessário analisar todo o código fonte exaustivamente, para isso é necessário ter acesso a toda documentação do sistema. Existem ferramentas que podem auxiliar essa tarefa e podem ser encontradas em [Madeira, 2007]. Neste método devido sua complexidade, várias vulnerabilidades podem não ser encontradas, nessas situações a melhor

abordagem seria a “black box”.

Neste trabalho foi utilizada a abordagem “black box”, onde o Tidia-Ae / Sakai foi testado por fora e não se conhecia os módulos internos da aplicação. Utilizando-se de técnicas “fuzzy” sobre requisições do protocolo HTTP em tarefas repetidas centenas ou até milhares de vezes para cada tipo de vulnerabilidade conhecida, essa técnica é chamada de teste de penetração e é uma das mais utilizadas para avaliar efetivamente a segurança de sistemas web [Gordon, 2006].

Existem vários tipos de scanners de vulnerabilidades web comerciais no mercado como: WebInspect – HP [WebInspect, 2011], Acunetix Web Vulnerability Scanner – Acunetix [Acunetix, 2011], Appscan – IBM [Appscan, 2001], NTOSpider - NT OBJECTives [NTOSpider, 2011] e outros. Tendo como base as pesquisas de Suto [Suto, 2010] e Anantasec [Anantasec, 2011] que analisam em seus trabalhos a qualidade desses scanners optou-se nesse artigo pela ferramenta Acunetix Web Vulnerability Scanner, pois em ambos os trabalhos foi classificada como um bom scanner.

Cada scanner tem seus próprios métodos e diferentes tipos de ataques, para essa pesquisa foi utilizada a configuração “default” no Acunetix Web Vulnerability Scanner e que é encontrada na maioria dos outros scanners para testar as vulnerabilidades mais comuns em sistemas web, [Suto, 2010], que são:

- Authentication Bypass ou Brute forcing
- SQL Injection / Blind SQL Injection
- Cross Site Scripting / Persistent Cross Site Scripting
- Command Injection
- XPath Injection
- SOAP/AJAX Attacks
- CSRF / HTTP Response Splitting
- Arbitrary File Upload attacks
- Remote File Include (PHP Code Injection)
- Application Errors

6. Resultados

Para a descoberta das vulnerabilidades do LMS Tidia-ae utilizou-se a versão 2.0 rodando no framework Sakai 2.5. O sistema operacional utilizado para a instalação do Tidia-ae foi o Windows XP com service Pack 4 virtualizado através do Software Vmware. O scanner de vulnerabilidades Acunetix foi instalado na máquina física cujo sistema Operacional era Windows 7 com service Pack 1. O LMS Tidia-ae foi instalado conforme documentação existente e nenhuma configuração adicional foi feita após sua implementação.

Após configurar o endereço do sistema representado localmente pela URL: http://localhost:8080/portal, o escaneamento durou onze minutos e vinte e um segundos e gerou uma distribuição de alertas como mostrado na figura 1 onde foram encontradas três vulnerabilidades de grau severo de comprometimento do sistema. Permitindo que um usuário malicioso explorando essas vulnerabilidades possa comprometer a database ou pichar o website

(deface). Seis vulnerabilidades de grau médio e vinte e uma de grau baixo.

Figura 1. Mapa de distribuição de alertas de vulnerabilidades encontradas pelo scanner.

Além das vulnerabilidades encontradas, a ferramenta também efetuou o mapeamento dos serviços utilizados e produziu um mapa da estrutura interna da aplicação como mostrado na figura 2.

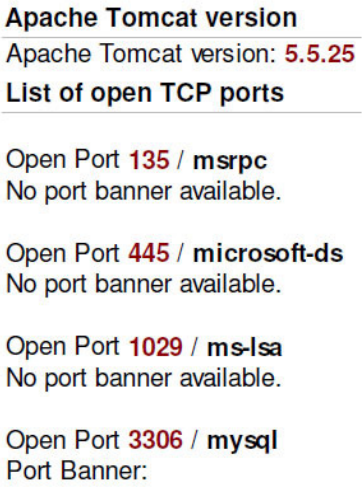

Figura 2. Mapeamento dos serviços utilizados pela estrutura interna do servidor e suas respectivas portas.

Dentre as três de grau de severidade alto, duas são do tipo autenticação e classificadas como "Weak Password", ou seja, o sistema permite a utilização de "senhas fracas" e o scanner utilizando um ataque de força bruta simples com um dicionário padrão de nomes, senhas e variações foi capaz de adivinhar as credenciais de administrador para acesso ao sistema, as duas URL's responsáveis pela autenticação são mostradas na tabela 2. O usuário e senha descobertos pelo scanner são criados automaticamente durante a instalação.

Vulnerabilidade do tipo Weak Password
/portal/relogin /portal/xlogin Usuário: admin , Senha: admin **REQUEST** POST /portal/relogin HTTP/1.1 Content-Length: 31 Content-Type: application/x-www-form-urlencoded

Host: localhost:8080
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.0)
eid=admin&pw=admin&submit=Login

RESPONSE
HTTP/1.1 302 Moved Temporarily
Server: Apache-Coyote/1.1
Set-Cookie: JSESSIONID=8ac9dd3d-6581-4c90-9fa5-826a418ed9ef.localhost;
Path=/
Location: http://localhost:8080/portal
Content-Length: 0
Date: Mon, 28 Mar 2011 00:31:00 GMT

Tabela 2 – Usuário admin e senha admin expostos pelo scanner

A terceira vulnerabilidade de grau de severidade alto se trata de um ataque de integridade do tipo "Cross Site Scripting" ou "XSS", [Kumar, 2011].

Essa vulnerabilidade permite a um atacante enviar códigos maliciosos (geralmente na forma de código Javascript) para outro usuário.

Como através do navegador não é possível saber se o script deve ser confiável ou não, ele irá executar o script no contexto do usuário permitindo a execução de funções e eventos como mostrado na tabela 3 onde o Scanner inseriu na URL /portal/help/main o evento Javascript "OnMouseOver" contendo a função "Prompt" permitindo ao atacante modificar o conteúdo da página apresentada ao usuário, provocando um "Deface", representado pela figura 3.

Através desse ataque também é possível que o invasor acesse cookies ou tokens de sessão armazenados no navegador do cliente. Com isso, o atacante pode personificar o usuário verdadeiro.

Vulnerabilidade do tipo Cross Site Scripting ou "XSS"

/portal/help/main

GET
/portal/help/main?help=%22%20**onmouseover**%3d**prompt**%28995006%29
%20bad%3d%22 HTTP/1.1
Cookie: JSESSIONID=B99067F7AE1E6440EA1D3F1ADA480B6D;
JSESSIONID=49D05A08825CA5837A091A56F81DA807;
JSESSIONID=5d515401-2e1b-4f99-85cb-

Tabela 3 – Evento Javascript inserido na URL

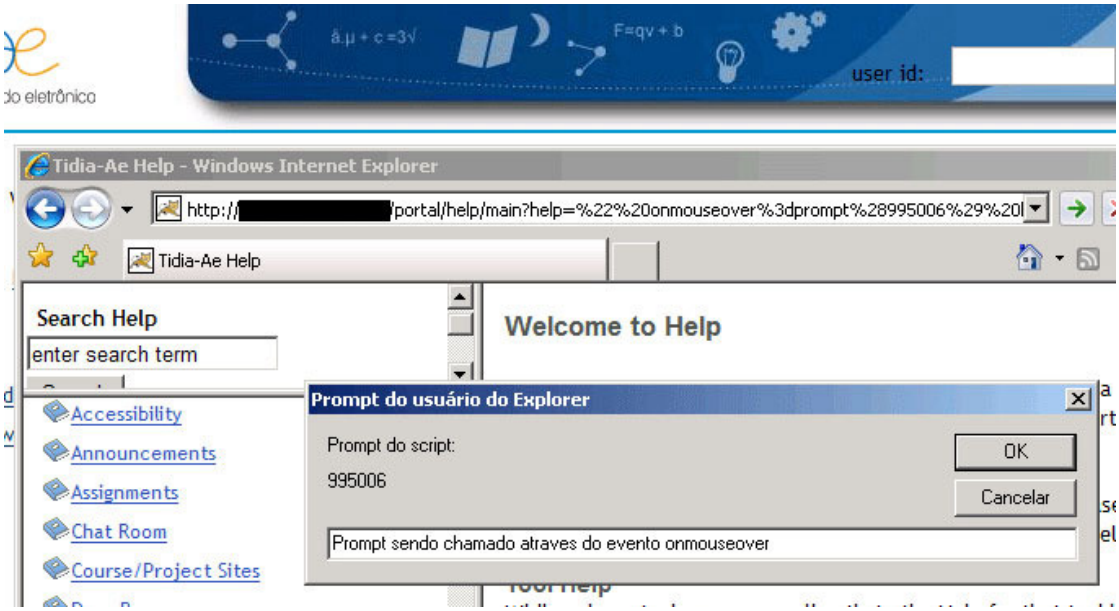

Figura. 3. Janela do tipo prompt foi evocada através do evento OnMouseOver.

Outra vulnerabilidade de grau de severidade alto foi encontrada no Tidia-Ae / Sakai quando se monitorou um segmento de rede utilizando a ferramenta de análise de pacotes conhecida como "Wireshark" [Wireshark, 2011], cuja função principal é analisar o fluxo de pacotes de rede para remontagem, decodificação, coleta de tráfego e estatísticas de protocolo.

Por default a instalação do Tidia-Ae / Sakai utiliza o protocolo HTTP para trafegar os dados, ou seja, os dados trafegam sem nenhum tipo de criptografia pela rede, com isso o Wireshark foi capaz de revelar o nome do usuário e senha dos usuários que se utilizavam do ambiente, essa falha é conhecida como "password reveal", aqui mostrado na figura 4.

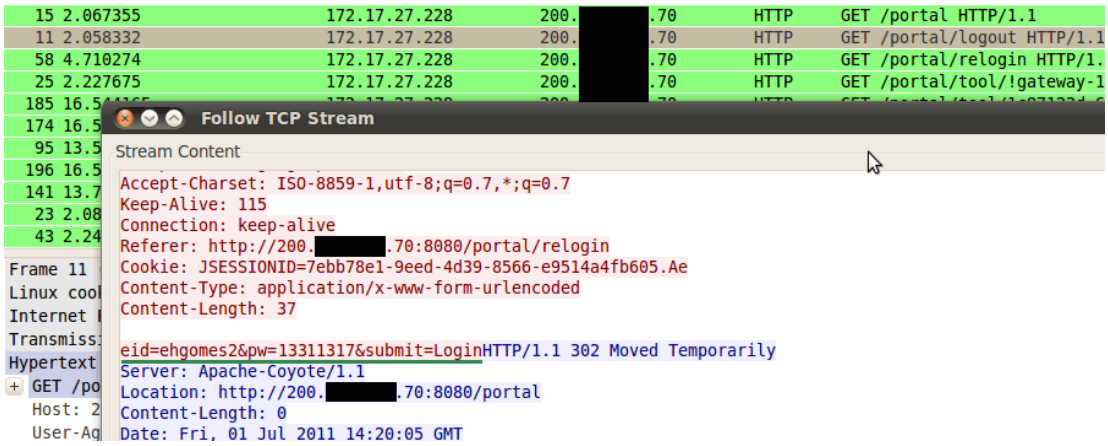

Figura. 4. eid=ehgomes2 e pw=13311317 – usuário e senha respectivamente.

Das seis vulnerabilidades de grau de severidade médio, todas as seis são do tipo de confidencialidade.

Duas delas apresentam vazamento de informações através de mensagens de erros conforme tabela 4 que posteriormente foram identificadas como falso positivo já que se tratava das páginas de documentação do Tomcat.

Tipo	Impacto
Error message on page	*/tomcat-docs/manager-howto.html* **Falso positivo**
Error message on page	*/tomcat-docs/printer/manager-howto.html* **Falso positivo**

Tabela 4- Vazamento de informações

As outras quatro vulnerabilidades estão diretamente ligadas à configuração do sistema, mas especificamente na utilização do servidor Apache Tomcat 5.5.25 que possui vulnerabilidades conhecidas e mostradas na tabela 5.

Tipo	Impacto
Tomcat Authentication Bypass	*Tomcat pode ignorar a autenticação e um atacante pode obter acesso não autorizado a arquivos e diretórios.*
Tomcat WAR File Directory Traversal	*Tomcat pode falhar ao higienizar entrada de dados, o que permite um atacante apagar ou sobrescrever arquivos no servidor web.*
Tomcat version older than 5.5.26	*Session hi-jacking CVE-2007-5333* *Elevated privileges CVE-2007-5342* *Information disclosure CVE-2007-5461* *Data integrity CVE-2007-6286*
Tomcat version older than 5.5.27	*Cross-site scripting CVE-2008-1232* *Cross-site scripting CVE-2008-1947* *Information disclosure CVE-2008-2370*

Tabela 5 - Vulnerabilidade de erro de Configuração

Para maiores detalhes sobre os erros da tabela 5, consultar a base Common Vulnerabilities and Exposures [CVE, 2011].

Das vinte e uma vulnerabilidades de grau de severidade baixo, sete confirmaram-se como falsos positivos, doze delas estão dividas entre duas vulnerabilidades de cookies de sessão conforme mostrado na tabela 6.

Tipo	Impacto
Session Cookie without HttpOnly flag set	*A flag HTTPOnly instrui o browser que o cookie só pode ser acessado pelo servidor e não por scripts do lado do cliente.*
Session Cookie without Secure flag set	*A flag secure instrui o browser que o cookie só pode ser acessado através de um canal seguro SSL.*

Tabela 6 - Vulnerabilidade de Cookie de Sessão: "JSESSIONID"

As últimas duas de baixo grau de severidade são do tipo “password-guessing attack”, ou ataque de adivinhação de senha, uma ameaça comum para desenvolvedores de sistemas web. Esse ataque de força bruta é uma tentativa de descobrir uma senha sistematicamente, tentando todas as combinações possíveis de letras, números e símbolos até descobrir a combinação correta.

As páginas mostradas na tabela 7 não possuem nenhuma proteção contra ataques de adivinhação de senha. Permitindo que um invasor possa tentar descobrir uma senha fraca.

Tipo	URL’s
Password guessing attack	*/portal/relogin* */portal/xlogin*

Tabela 7 - Vulnerabilidade de Autenticação

Em sistemas web é recomendada a implementação de algum tipo de bloqueio de conta após um determinado número de tentativas de senha incorreta. O scanner Acunetix testou dez credenciais inválidas e nenhum bloqueio de conta foi detectado.

Para reforçar empiricamente a pesquisa, uma nova tentativa de descoberta de senha foi efetuada utilizando-se o software Brutus [Hoobienet, 2011] com 40 conexões simultâneas e intervalos de 10 segundos entre as tentativas. Mais uma vez nada foi detectado.

7. 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

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

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

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

[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.

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

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

[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.

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

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

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

[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.

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

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

[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.

[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.

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

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

[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.

[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.

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

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

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

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

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

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

[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.

[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.

[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.

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

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

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

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

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

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

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