Aspectos de Segurança para o desenvolvimento de aplicações web

Evandro Menezes Gomes

Faculdade Área1/Devry Brasil – Coordenação de Pós-Graduação

Pós-Graduação em Segurança da Informação em Redes de Computadores

Caixa Postal 41.720-200 – Salvador – BA – Brasil
evandrofacs@gmail.com

RESUMO:

A popularidade da informação, portabilidade e fácil acesso providos pela plataforma Web têm popularizado seu uso no desenvolvimento de diversas aplicações. Porém, o crescente número de incidentes de segurança levanta preocupações quanto à sua seguridade.Entretanto, a realização de testes não são suficientes para garantir que o sistema tenha integridade e confiabilidade para corrigir falhas e negligências humanas. A maioria desses incidentes decorrem da falta de consideração de segurança durante o processo de desenvolvimento, nos últimos anos houve grandes avanços na popularização do uso da internet, além da possibilidade de efetuar transações com controle de acesso e de conhecimento de pessoas autorizadas. Este trabalho tem como objetivo propor práticas de segurança a serem aplicadas durante o processo de desenvolvimento de aplicações Web que minimizem os riscos, aumentando a qualidade e confiabilidade do produto final. Nele serão apresentados: conceitos de segurança da informação, as vulnerabilidades mais comuns existentes em software Web e algumas práticas que devem ser aplicadas durante o desenvolvimento.

Palavras chave: Informações, aplicações, internet, *segurança, TI*

1.Introdução

As organizações vêm procurando cada vez mais o uso de novas tecnologias de informação. Novas ferramentas alteram a base da competitividade e estratégias empresariais. As empresas, tanto a nível mundial como nacional, vem passando por mudanças nos últimos anos, as quais vêm estão fortemente relacionadas às empresas de TI. Os ambientes empresariais e as organizações dos vários setores vêm integrando as tendências da criação e utilização da internet. Nesse novo ambiente empresarial e por força das novas realidades do mercado, as empresas vem passando a criar e oferecer seus produtos e serviços amplamente apoiados em novas tecnologias do mercado. Assim, pela força da modernização nas organizações, todas as empresas vêm se esforçando para assimilação e utilização das tecnologias de informação que atendam as necessidades de segurança da informação em aplicações web.

2.Segurança das Informações na Plataforma Web

A utilização da internet e das aplicações web ocorrem através de navegadores. Dessa forma é importante reconhecer os tipos de conexões existentes e verificar a integridade e a confiabilidade das aplicações. A web traz inúmeras possibilidades de uso, porém para aproveitar cada uma delas de forma segura é importante que alguns cuidados sejam tomados.

A maioria dos acessos que através de aplicações web envolve o tráfego de informações sigilosas, da mesma forma que ocorre quando você acessa sites de pesquisa ou de notícias. Esses acessos são diferentes e geralmente realizados pelo protocolo HTTP, onde as informações trafegam em texto claro, ou seja, sem o uso de criptografia.

O protocolo HTTP, além de não oferecer criptografia, não garante que os dados não possam ser interceptados, coletados, modificados ou retransmitidos e nem que você esteja se comunicando exatamente com o site desejado. Por estas características, ele não é indicado para transmissões que envolvam informações sigilosas como senhas, números de cartões de crédito e dados bancários, devendo ser substituído pelo HTTPS, que oferece conexões seguras.

2.1. Riscos de Segurança em aplicações web

O principal alvo de ataques de Agentes Maliciosos (hackers ilegais e crackers), acontece devido à possibilidade de alcance rápido de altos ganhos, são as Aplicações web.

Ataques costumam ocorrer na Internet com diversos objetivos, assim como qualquer computador com acesso à Internet pode participar de um ataque, visando diferentes alvos e usando variadas técnicas. Qualquer serviço, computador ou rede que seja acessível via Internet pode ser alvo de um ataque. Os motivos que levam os atacantes a desferir esses ataques na Internet são bastante diversos, variando da simples diversão até a realização de ações criminosas.

Segundo o Instituto Gartner (2009), mais de 75% dos problemas com segurança em aplicações web são devidos a falhas exploráveis a partir das conexões web.

Abaixo relacionamos os principais Problemas e, níveis causado por hackers ilegais e crackers) , como por exemplo:

- Interrupção ou queda de desempenho do serviço;
- Acesso não autorizado a dados confidenciais e estratégicos;
- Roubo de informações cadastrais de Clientes;
- Fraudes e modificação de dados no fluxo das operações;
- Perdas financeiras diretas e indiretas;
- Prejuízos à imagem da marca da empresa;
- Perda da lealdade dos Clientes;
- Gastos extraordinários com incidentes de segurança.

2.2. Principais vulnerabilidades exploradas

A exploração de vulnerabilidades ocorre quando um atacante age em uma violação de segurança, acessando informações confidenciais, disparando ataques contra outros computadores ou tornando um serviço inacessível. Aplicações web buscam uma avaliação mais rigorosa e estão mais vulneráveis a esses ataques. Corrigir pontos vulneráveis ou pontos fracos que circulam em um setor que trabalha com a informação não acabará, mas reduzirá em muito os riscos em que ela estará envolvida. Logo estará evitando como também prevenindo a concretização de possíveis ameaças que podem:
explorar erros da aplicação Web;
explorar vulnerabilidades do servidor de aplicação Web;
explorar vulnerabilidades da linguagem de programação ou dos pacotes utilizados no desenvolvimento da aplicação Web;
invadir o servidor onde a aplicação Web está hospedada e alterar diretamente os arquivos que compõem o site;
furtar senhas de acesso à interface Web usada para administração remota.
Avaliar vulnerabilidades abrange analisar a existência de ameaças passíveis de exploração, a possibilidade de um mau uso do sistema ou de sua configuração incorreta e a possibilidade de falhas dos mecanismos de segurança.

2.2.1. Vulnerabilidades encontradas em aplicações web.

A melhor forma para verificar claramente dados não confiáveis é conferir ou apurar o código de forma rápida, usando ferramentas de análise de código que podem ajudar a encontrar fluxo de dados através da aplicação, também de XSS. Existem três tipos bem conhecidos de XSS: refletido, armazenado e inserção DOM. O XSS refletido é o de exploração mais fácil – uma página refletirá o dado fornecido pelo usuário como retorno direto a ele. Armazenado - Quando o atacante consegue inserir um XSS na aplicação e ele irá ser armazenado na base dados, inserção DOM é inserção do código HTML que faz referência ao script malicioso. Existem Ferramentas automatizadas que podem encontrar alguns problemas de XSS automaticamente. Portanto, uma cobertura completa exige uma combinação de revisão manual de código e teste de invasão, além das abordagens automatizadas. Tecnologias Web 2.0, como Ajax, podem tornar o XSS muito mais difícil de detectar via ferramentas automatizadas. Existe também (CSRF) Cross site request forgery não é um novo ataque, mas é simples e devastador.Um ataque CSRF força o navegador logado da vítima a enviar uma requisição para uma aplicação web vulnerável, que realiza a ação desejada em nome da vítima. Ainda vale ressaltar dos Ataques One-Click, Cross Site Reference Forgery, Hostile Linking e Automation Attack. O acrônimo XSRF é frequentemente utilizado. Ambos a OWASP e o MITRE padronizaram o uso do termo Cross Site Request Forgery e CSRF.

2.2.1.1. Falha de Injeção de Código.

As falhas de injeção ocorrem quando dados não confiáveis são enviados como parte de um comando ou consulta. O atacante usa falhas de SO (Sistema Operacional) e de LDAP, que podem manipular os dados para interpretar ou executar comandos indesejados ou permita o acesso a os dados não autorizados.

2.2.1.1.1. Medidas para evitar a falha de injeção.

Prevenção de falha de injeção é manter os dados não confiáveis separados dos comandos e consultas, a fim de evitar que os atacantes forneçam muitas dessas rotinas para fazer filtragens de dados o que é recomendada em aplicações que requeiram caracteres especiais em sua entradas Os dados parametrizados e lista branca podem ainda introduzir injeção por debaixo dos panos. As falhas de Injeção habilitam o atacante a criar, ler, atualizar ou apagar arbitrariamente qualquer dado disponível para a aplicação.

2.2.1.2. Quebra de autenticação e gerenciamento de sessão.

São criticas para a segurança na web autenticação e gerência de sessão apropriadas que envolvam falha na proteção de credenciais durante seu tempo de vida. Essas falhas estão ligadas á roubo de contas de usuários ou administradores, controlando e responsabilizando perfil, por causa de violações de privacidade e controle web. Muitos ambientes afetados são furos de gerência de sessão e autenticação, geralmente causados por falhas de autenticação como logout, recordação de dados de logon e atualizações de conta.

2.2.1.2.1. Medidas para evitar a Quebra de autenticação e gerenciamento de sessão.

A medida de autenticação protege as identidades das credenciais associadas a fim de verificar a autenticação, gerencia de sessão e funções secundárias. As abordagens automatizadas,que são ferramentas de localização de vulnerabilidade, têm dificuldade em esquemas de autenticação e de sessão personalizados, e isso pode evitar a autenticação de sessão.

2.3. Mecanismos de Segurança para o desenvolvimento seguro

Alguns cuidados precisam ser levados em consideração para garantir o desenvolvimento seguro em aplicações web, e a melhor maneira de desenvolver um software seguro é incorporar a segurança desde o início do desenvolvimento.
O desafio de se construir aplicações web menos suscetíveis à falhas de seguranças e um objetivo cada vez mais perseguido pelos desenvolvedores.
Além disso, a equipe do projeto deve conhecer as vulnerabilidades em diferentes ciclos de vida do desenvolvimento do software, para que estes possam ser removidos assim que possível.
A ISO (Organização Internacional para Padronização) define que mecanismos de segurança visam garantir que o sistema atende aos requisitos funcionais de segurança. Porem , as aplicações web somente e os sistemas a que ele se propõe não são suficientes para garantir os comportamentos imprevistos que poderão existir.

3. Requisitos de Segurança para o desenvolvimento seguro

Muitos desafios de se construção de aplicações menos suscetíveis a falhas de seguranças é objetivo cada vez mais constante de empresas que desenvolvem serviços online .
A Norma ISO/IEC 27002 (Organização Internacional para Padronização) tem como objetivo “iniciar, manter e estabelecer diretrizes e princípios gerais para melhorar a gestão de segurança da informação em uma organização.
Muitas organizações desenvolvem aplicações adotando requisitos visando a segurança dos softwares e a redução de custos de forma econômica.O que é necessário para a empresa testar a aplicação é particularmente útil para verificar e explorar se os mecanismos estão robustos, para encontrar possíveis falhas de programação ou venerabilidades no código fonte.
Algumas das atividades eficazes para a desenvolvimento seguro incluem:

• Práticas de Programação;
•Testar o retorno de funções;
•Documentar corretamente;
•Tratar as entradas de dados;
•Ter uma política de versão consistente;
•Usar bibliotecas confiáveis;
•Evitar arquivos temporários;
•Não armazenar senhas;
•Chaves criptográficas no código;
•Operar com o privilégio necessário.

3.1. Testes de segurança para desenvolvimento seguro

As aplicações web com segurança tem por finalidade garantir a integridade e confiabilidade dos sistemas online contra possíveis falhas que possam surgir durante a sua implementação. Uma garantia de segurança é obtida através de testes realizados e comprovados pelo cliente em laboratórios independentes. O objetivo é definir, conforme as normas realizadas, se os testes foram suficientes para demonstrar que as aplicações e os sistema funcionam conforme as especificações. Ainda convém lembrar que os testes serão definidos de acordo com a exigência estabelecida pelo cliente. É é bom lembrar das normas ISO/IEC 15408 information technology – Security techniques – Evaluation criteria for IT security(,) que tem por finalidade requisitos funcionais e não funcionais para o direcionamento dos testes a serem realizados, além de seguir alguns dos testes para um desenvolvimento seguro: Alvo de Avaliação (Target of Evaluation – TOE),Perfil de Proteção (Protection Profile – PP)Alvo de Segurança (Security Target – ST),Requisitos de Segurança Funcional (Security Functional Requirements – SFRs),Requisitos de Garantia de Segurança (Security Assurance Requirements – SARs),Nível de Garantia de Avaliação (Evaluation Assurance Level – EAL).

3.1.1. Testes de Segurança em aplicação web

Testar passou a fazer parte de um processo de engenharia responsável por 70% de um projeto bem sucedido . Os testes podem ocorrer em vários níveis onde a equipe de projeto os avalia por unidade, onde uma pequena parcela de funcionalidades tem sucesso. Para tudo que comprometia o sistema antes da década de 90, testes eram realizados no ciclo do desenvolvimento geralmente pelos próprios desenvolvedores, o que não acontece hoje. Com o passar do tempo, os teste eram realizados independentes, o que demandou melhorias, funcionamento e segurança, a fim de garantir os padrões e qualidade do produto final. O principal objeto era reduzir erros de programação e custos até a homologação do produto.

3.1.1. 1.Testes de Verificação para ambiente web

Em desenvolvimento de software as informações coletadas são importantes na fase do processo para garantir a qualidade das informações geradas. Ainda convém lembrar que a equipe de projeto está responsável pela coleta de informação que são:
Teste e Verificação de Requisitos;
Teste e Verificação da Modelagem Funcional;
Teste e Verificação da Modelagem Interna;
Teste e Verificação de Código.
Confirmar por testes, verificação de ,segurança e com provas objetivas que requisitos da aplicação e que o uso foram cumpridos.

3.1.1.1.1.Testes de Validação para ambiente web

Pretende mostrar que o software atende aos seus requisitos. Solicitado pelo cliente que deseja um teste bem implementado, refletem o uso esperado do software, o processo de avaliação do sistema e seus componentes, visando garantir a qualidade do produto final.Existem esforços no sentido de integrar os modelos de maturidade de teste com os modelos de maturidade da capacitação para software como o CMMI. Seguem padrões de teste e validação:

> Validação de Unidade: Garantir que as diversas unidades do software estão contempladas na totalidade de linhas de código;
> Validação de Integração: Garantir que os diversos componentes do software não apresentem erros quando integrados;
> Validação de Funcionalidade: Garantir que não existam diferenças entre os requisitos funcionais e o comportamento do software.(Edmar Fernando da Cruz, Euler Divino Rodrigues,Teixeira Leonardo, Maykon Parreira Rodrigues, Ricardo Brandão Gomes, Mundim ,1997,p.7).

4. Considerações Finais

Diante de todas estas diferenças e desafios, envolvendo várias áreas, desde o nível de negócio até o nível técnico, fica claro que aplicações web merecem uma atenção especial. Definir um processo de software para web certamente não é uma tarefa fácil. Na verdade, trata-se de uma composição de sub-processos, cada processo cobrindo questões particulares de cada área envolvida. A motivação deste trabalho foi justamente chamar a atenção para esta necessidade e prover um conjunto de requisitos que possa servir como passo inicial para uma iniciativa de definição de processo de software para sistemas web.
pode-se perceber através deste trabalho que o desenvolvimento e Aspectos de Segurança para o desenvolvimento de aplicações web , podem ser de grande valia para validar, detectar e, posteriormente, resolver problemas que antes necessitariam de um grande e complexo trabalho. Ainda, dada a quantidade de vulnerabilidades e surgimento de novas formas de tecnologia constantemente, faz-se necessário automatizar e criar ambientes cada vez mais seguros web.

5. Conclusão

Este artigo apresentou uma análise dos Aspectos de Segurança para o desenvolvimento de aplicações web, os conceitos sobre práticas da Segurança da Informação, foram analisados sob os requisitos básicos de segurança: autenticação, integridade e confidencialidade. Para cada um dos conceitos foram descritas suas vulnerabilidades conhecidas. Critérios foram abordadas neste artigo, pois isto pode implicar grandes custos, principalmente em redes corporativas, onde o número de funcionários e equipamentos pode ser elevado. A presente pesquisa objetivou apresentar importantes contribuições para o desenvolvimento e prática para aplicações web.

Algumas empresas de maneira geral vêm procurando identificar novas oportunidades de negócios, algumas procuram identificar oportunidades por meios de aplicação de tecnologia de forma direta em seus negócios, enquanto outras procuram meios de parcerias e serviços online.
Nele serão apresentados: conceitos de segurança da informação, as vulnerabilidades mais comuns existentes em software Web e algumas práticas que devem ser aplicadas durante o desenvolvimento.

6. Referência:

UTO, Nelson e MELO Sandro Pereira de. Vulnerabilidades em Aplicações web e mecanismo de proteção. http://www.owasp.org/ top 10 – 2013. Acesso em: 25/09/2015

CRUZ, Edmar Fernando da, TEIXEIRA, Euler Divino Rodrigues, RODRIGUES, Leonardo, Maykon Parreira, MUNDIM, Ricardo Brandão Gomes. TSDD - Teste de segurança durante o desenvolvimento http://profissionaisti.com.br/2009/02/seguranca-em-aplicacoes-web/ Acesso em: 25/09/2015.

WAGNER,Rosana,Alencar,Machado.
http://www.sirc.unifra.br/artigos2010/7.pdf Acesso em: 02/10/2015