T10 OWASP Top 10 Riscos de Segurança em Aplicações – 2017

A1 – Injeção

As falhas de Injeção, tais como injeção de SQL, de SO (Sistema Operacional) e de LDAP, ocorrem quando dados não fiáveis são enviados para um interpretador como parte de um comando ou consulta. Os dados manipulados pelo atacante podem iludir o interpretador para que este execute comandos indesejados ou permita o acesso a dados não autorizados.

A2 – Quebra de Autenticação e Gestão de Sessão

As funções da aplicação relacionadas com autenticação e gestão de sessão geralmente são implementadas de forma incorreta, permitindo que os atacantes comprometam senhas, chaves e tokens de sessão ou, ainda, explorem outra falha da implementação para assumir a identidade de outros usuários.

A3 – Cross Site Scripting (XSS)

Falhas XSS ocorrem sempre que uma aplicação recebe dados não fiáveis e os envia ao navegador sem validação ou filtro adequados. XSS permite aos atacantes executarem scripts no navegador da vítima que podem “sequestrar” sessões do usuário, desfigurar sites, ou redirecionar o usuário para sites maliciosos.

A4 – Controle de acesso quebrado

As restrições no que podem fazer os utilizadores autenticados não são corretamente aplicadas. Os atacantes podem utilizar estas fraquezas para obter acesso em funções e dados não autorizados, tais como aceder informações de outros utilizadores, ver ficheiros sensíveis, modificar os dados dos utilizadores, modificar os direitos de acesso, etc.

A5 - Configuração Incorreta de Segurança

Uma boa segurança exige a definição de uma configuração segura e implementada na aplicação, frameworks, servidor de aplicação, servidor web, banco de dados e plataforma. Todas essas configurações devem ser definidas, implementadas e mantidas, já que geralmente a configuração padrão é insegura. Adicionalmente, o software deve ser mantido atualizado.

A6 – Exposição de Dados Sensíveis

Muitas aplicações web e APIs não protegem devidamente os dados sensíveis, tais como dados fiscais, de saúde e informações pessoais. Os atacantes podem roubar ou modificar esses dados desprotegidos com o propósito de realizar fraudes de cartões de crédito, roubo de identidade, ou outros crimes. Os dados sensíveis merecem proteção extra como criptografia no armazenamento ou em trânsito, bem como precauções especiais quando comunicados pelo navegador.

A7 – Proteção insuficiente contra ataques

A maioria das aplicações e APIs faltam de capacidade para detectar, prevenir e reagir contra ataques manuais ou automatizados. A proteção contra ataques vai mais longe que simplesmente validar dados dos utilizadores e necessita deteção automática, registar os eventos, reagir e também bloquear tentativas de exploração. Os donos das aplicações tem também precisa de instalar correções rapidamente para se proteger de estes ataques.

A8 – Cross-Site Request Forgery (CSRF)

Um ataque CSRF força a vítima que possui uma sessão ativa em um navegador a enviar uma solicitação HTTP forjada, incluindo o cookie da sessão da vítima e qualquer outra informação de autenticação incluída na sessão, a uma aplicação web vulnerável. Esta falha permite ao atacante forçar o navegador da vítima a criar pedidos que a aplicação vulnerável aceite como pedidos legítimas realizadas pela vítima.

A9 – Utilização de Componentes Vulneráveis Conhecidos

Componentes, tais como bibliotecas, frameworks, e outros módulos de software quase sempre são executados com os privilégios da aplicação. Se um componente vulnerável é explorado, um ataque pode causar sérias perdas de dados ou o comprometimento do servidor. As aplicações e APIs que utilizam componentes com vulnerabilidades conhecidas podem minar as suas defesas e permitir uma gama de possíveis ataques e impactos.

A10 – APIs desprotegidas

As aplicações modernas geralmente oferecem clientes avançados e APIs, tais como JavaScript no navegador e nas aplicações mobiles, e que usam uma API especifica (SOAP/XML, REST/JSON, RPC, GWT, etc.). Essas APIs geralmente não são protegidas e contem muitas vulnerabilidades.