CST0205-Ameaças, vulnerabilidades e ataques a Segurança Cibernética: Parte 5 - Ataques à aplicativos

Data do Post	@July 15, 2022 9:00 AM
Status	Done
Palavras-chave	Ameaças vulnerabilidades e ataques a Segurança Cibernética
Fonte	
Pronto	Preparado
IG post	☑
Publicado	☑

Post-Linkedin

Esse é o último artigo da série de cinco partes do tema "Ameaça, vulnerabilidades e ataques a Segurança Cibernética".

Usuários de tecnologias diariamente têm acesso a diversas aplicações mobile, ‘desktop’ ou WEB. Desde aqueles que os ajudam a serem pessoais mais produtivas, até aquelas que roubam mais tempo das pessoas. Todas essas aplicações também podem ser passíveis de ataques cibernéticos. Esse artigo traz uma visão holística desses tipos de ataques. Leia o artigo na íntegra.

Siga-me e veja outros posts no meu Instagram @idaleciosilvatech

Deixe o like para medirmos a repercussão do conteúdo.
Guarde para rever noutro momento.
Compartilha o conteúdo com os amigos e não só
Comente o que acha do conteúdo e da iniciativa e deixe sugestões.
Link do perfil no IG: https://www.instagram.com/idaleciosilvatech/
#cybersecurity #technology #linux #ataquescibernéticos #hacking #crimesvirtuais #despositivosmóveis #mobilidade #protection

Introdução

Existem muitas ameaças que podemos sofrer ao navegar na Internet. Existem muitos tipos de ataques, variedades de malware, técnicas que os hackers usam. Tudo isso pode nos afetar como usuários domésticos, colocar uma empresa em risco, bem como afetar páginas da web e aplicativos. Servidores de site pode sofrer vários tipos de ataques. Esse artigo explica quais são os principais que podem comprometer o bom funcionamento e a segurança.

Tipos de ataques a aplicativos

Cross-Site Scripting (XSS)

Cross-site scripting (XSS), ou scripts entre sites, é uma vulnerabilidade encontrada em aplicações web. O XSS permite que os criminosos injetem scripts nas páginas web visualizadas pelos usuários. Estes scripts podem conter código malicioso.

Cross-site scripting tem três participantes: o criminoso, a vítima e o website. O atacante não tem diretamente como alvo uma vítima. O criminoso explora vulnerabilidades dentro de um website ou aplicação web. Os criminosos injetam scripts do lado do cliente em páginas web visualizadas pelos usuários, as vítimas. O script malicioso passa inconscientemente para o navegador do usuário. Um script malicioso deste tipo pode aceder a quaisquer cookies, tokens de sessão ou outras informações confidenciais. Se os criminosos obtiverem o cookie de sessão da vítima, podem imitar esse usuário.

Injeção de código

Uma forma de armazenar dados num website é usar uma base de dados. Existem vários tipos diferentes de bases de dados, como uma base de dados SQL (Structured Query Language) ou uma base de dados XML (Extensible Markup Language). Ambos os ataques de injeção XML e SQL exploram vulnerabilidades no código do programa, como a não validação das consultas -as queries- à base de dados corretamente.

Injeção XML

Ao usar uma base de dados XML, uma injeção XML é um ataque que pode corromper os dados. Após o usuário fornecer a entrada, o sistema acede aos dados requeridos através de uma query. O problema ocorre quando o sistema não examina corretamente o pedido de entrada fornecido pelo usuário. Os criminosos podem manipular a query programando-a para atender às suas necessidades, podendo aceder às informações na base de dados.

Todos os dados confidenciais armazenados na base de dados ficam acessíveis aos criminosos e podem efetuar um qualquer número de alterações ao website. Um ataque de injeção XML ameaça a segurança do website.

Injeção SQL

O cibercriminoso explora uma vulnerabilidade inserindo uma instrução SQL maliciosa num campo de entrada. Mais uma vez, o sistema não filtra corretamente os caracteres na entrada do usuário numa instrução SQL. Os criminosos usam injeção SQL em websites ou em qualquer base de dados SQL.

Os criminosos podem falsificar uma identidade, modificar dados existentes, destruir dados ou tornarem-se administradores do servidor de base de dados.

Buffer Overflow

Esgotamento do Buffer ou transbordamento de dados (Buffer Overflow) ocorre quando os dados ultrapassam os limites de um buffer. As memórias intermédias são áreas da memória atribuídas a uma aplicação. Ao alterar dados para além dos limites de uma memória intermédia, a aplicação acede à memória atribuída a outros processos. Tal pode levar a uma falha do sistema, ao comprometimento de dados ou disponibilizar escalação de privilégios.

O CERT/CC da Universidade Carnegie Mellon estima que quase metade de todas os exploits de softwares são historicamente provenientes de alguma forma de buffer overflow. A classificação genérica buffer overflows inclui muitas variantes, como buffer overflows estáticos, erros de indexação, bugs no formato de strings, incompatibilidades de tamanho de buffer para Unicode e ANSI, e excesso do tamanho da pilha (heap size).

Execuções de código remoto

As vulnerabilidades permitem que um criminoso virtual execute código malicioso e assuma o controlo de um sistema com os privilégios do usuário que está a executar a aplicação. A execução remota de código permite que um criminoso execute um qualquer comando na máquina alvo do ataque.

Considere, por exemplo, o Metasploit. O Metasploit é uma ferramenta de desenvolvimento e execução de código de exploração contra um alvo remoto. Meterpreter é um módulo de exploração dentro do Metasploit que fornece funcionalidades avançadas. O Meterpreter permite que os criminosos escrevam as suas próprias extensões como um objeto partilhado. Os criminosos carregam e injetam estes ficheiros num processo em execução no destino. O Meterpreter carrega e executa todas as extensões da memória, para que eles nunca envolvam o disco rígido. Isto também significa que estes ficheiros voam sobre o radar da detecção de antivírus. O Meterpreter possui um módulo para controlar a webcam de um sistema remoto. Visto que um criminoso instale o Meterpreter no sistema da vítima, pode visualizar e captar as imagens da webcam da vítima.

Controles ActiveX e Java

Ao navegar na Web, algumas páginas podem não funcionar corretamente, a menos que o usuário instale um controlo ActiveX. Os controlos ActiveX fornecem a capacidade de um plugin para o Internet Explorer. Os controlos ActiveX são pedaços de software instalados pelos usuários para fornecer capacidades estendidas. São entidades terceiras que escrevem alguns controlos ActiveX, e que podem, portanto, ser maliciosos. Estes podem monitorizar os hábitos de navegação, instalar malware ou registar as teclas digitadas. Os controlos Active X também funcionam noutras aplicações da Microsoft.

O Java opera por um interpretador, a Máquina Virtual Java (JVM). A JVM ativa a funcionalidade do programa Java. A JVM coloca em caixas de proteção (sandboxes) ou isola o código não confiável do resto do sistema operativo. Existem

vulnerabilidades, que permitem que código não confiável contorne as restrições impostas pela sandbox. Há também vulnerabilidades na biblioteca de classes Java, que uma aplicação usa para a sua segurança. O Java é a segunda maior vulnerabilidade de segurança a par do plug-in Flash da Adobe.

Defesa contra ataques de aplicativo

A primeira linha de defesa contra um ataque de aplicação é escrever código sólido. Independentemente da linguagem utilizada, ou a fonte de entrada externa, a prática de programação prudente é tratar todas as entradas externas como uma função hostil. Valide todas as entradas como se fossem hostis.

Mantenha todo o software, incluindo sistemas operativos e aplicações actualizados, e não ignore os prompts de atualização. Nem todos os programas são atualizados automaticamente. No mínimo, selecione a opção de atualização manual. As atualizações manuais permitem que os usuários vejam exatamente as atualizações que ocorrem.

Como vimos, existem muitos ataques que podemos sofrer. Não importa se somos usuários domésticos ou uma grande organização. Além disso, qualquer dispositivo, sistema ou servidor pode ser atacado por um criminoso virtual. Isso significa que devemos tomar precauções e não cometer erros de qualquer espécie que nos comprometam.

Revisões de código pode ajudar a detectar código vulnerável no início da fase de desenvolvimento, scanners de código dinâmicos e estáticos podem fazer verificações automáticas de vulnerabilidade e programas de bônus de bug permitem que testadores éticos ou hackers encontrem bugs no site.
Use procedimentos armazenados com parâmetros que podem ser executados automaticamente. Um exemplo seria implementar CAPTCHA ou fazer com que os usuários respondam a perguntas. Isso garante que um formulário e uma solicitação sejam enviados por um ser humano e não por um bot.

Outro aspecto muito importante é usar um aplicação web firewall (WAF) para monitorar a rede e bloquear possíveis ataques. É uma medida de segurança que deve ser aplicada nos nossos servidores. Dessa forma, evitaremos a entrada de invasores que possam violar a nossa privacidade e segurança.

No entanto, lembre-se de que nenhum desses métodos pode substituir o outro. Isso significa que cada um adiciona o seu próprio valor à tabela e adiciona proteção contra determinados cenários de ataque. Nem todas as vulnerabilidades podem ser encontradas por revisões de código ou programas de bônus de bug, ou apenas por um firewall de aplicativo da web, pois nenhuma ferramenta é 100% segura. Tudo isso significa que devemos considerar uma combinação de todos esses métodos para proteger aplicativos e usuários da maneira mais eficiente possível.

Conclusão

Os ataques a sites e aplicativos são cada vez mais comuns e elaborados. Como podem causar grandes danos, é essencial saber de que forma identificá-los e, principalmente, evitá-los. Com ajuda especializada, o procedimento se torna simplificado.

Siga-me e veja outros posts no meu Instagram @idaleciosilvatech

Deixe o like para medirmos a repercussão do conteúdo.
Guarde para rever noutro momento.
Compartilha o conteúdo com os amigos e não só
Comente o que acha do conteúdo e da iniciativa e deixe sugestões.
Link do perfil no IG: https://www.instagram.com/idaleciosilvatech/
#cybersecurity #technology #linux #ataquescibernéticos #hacking #crimesvirtuais #despositivosmóveis #mobilidade #protection