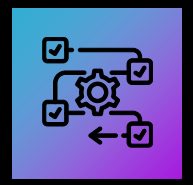
Prime

CCS-A

Ataques de Aplicativos

Ataques de Repetição



Repetição das condições que existiam na primeira vez em que a sequência de eventos ocorreu. Se era válido antes, pode ser novamente.

- Começa como um ataque de *sniffing* capturando o tráfego que se deseja reproduzir, então altera o tráfego e depois reproduz.
- Exemplos:

Receber o pagamento duas vezes;

Passar com sucesso em uma verificação de segurança em um evento de login.

Repetição da Sessão

"Sessão": conversa entre cliente e servidor. Estabelecido na conexão a um sistema web.

Repetição de sessão: Recriação da interação após sua ocorrência com o ID da sessão da vítima.

Como funciona:

- As transações sem estado não têm informações de onde o usuário veio ou para onde foi.
- No servidor: O invasor pode capturar o histórico de solicitações.
- No cliente: O invasor intercepta a conexão e usa o ID de sessão do cliente.

Estouro de Número Inteiro

- Uma condição de erro de programação quando armazenamos um valor numérico em uma variável muito pequena.
- Em alguns casos, o valor satura a variável quando resultado da operação aritmética excede o tamanho máximo do tipo inteiro atribuído.
- Características:
  - São facilmente testados;
  - Os analisadores de código podem apontar onde eles ocorrerão.
- Erros não podem aparecer no código de produção.

Falsificação de Solicitação (Request Forgery)

- Tipo de ataque em que um usuário realiza uma ação em nome de outro usuário ou inconscientemente.
- Características:
  - Ocorrem em navegadores, formulários ou entradas de usuário.
  - Ocorrem por descuidos do lado do cliente (clique em links e engenharia social);
  - Ocorrem por conta de problemas do lado do servidor.

Falsificação de Solicitação do Lado do Servidor

- Um invasor envia solicitações ao aplicativo do lado do servidor para fazer solicitações HTTP para um domínio da sua escolha.
- Características:

Exploram a relação de confiança entre servidor e alvo;

Inclui fazer o próprio servidor atacar outro na organização.

Falsificação de Solicitação Entre Sites (XSRF)

- Utilizam comportamentos não intencionais apropriados no uso definido, mas que são executados fora do uso autorizado.
- **Exemplo:**

Um banco que permita que você faça login e realize transações financeiras, mas não valide o token para cada transação.

- Técnicas de mitigação:

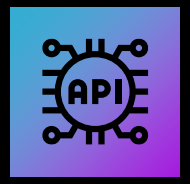
Limitar os tempos de autenticação;

Expiração de cookies;

Gerenciar elementos de uma página da Web, como a verificação de cabeçalho.

- Método mais forte: uso de tokens XSRF emitidos com antecedência.

Ataques de Interface de Programação de Aplicativos (API)



- Método “normal” de interação é por meio de comandos no servidor e apresentação no browser;
- Num aplicativo, por meio de uma API, o processamento é no próprio aplicativo.

As APIs são usadas para alimentar dados em um aplicativo e podem preocupar mais.

Este tipo de ataque ocorre quando a API faz chamadas para as funções e então é realizado ataques de injeção nessas funções.

Exaustão de Recursos

Estado em que um sistema não possui todos os recursos necessários para funcionar.

- A capacidade é definida pela quantidade necessária de:
  - Largura de banda - **TCP SYN Flood**;
  - Processamento;
  - Memória.
- As vulnerabilidades de esgotamento de recursos tendem a resultar em falhas no sistema.
- Em alguns casos, as interrupções param serviços essenciais.

Memory Leak / Vazamento de Memória

- Ocorre quando um programa não libera memória para outros processos usarem depois de concluído.
- O gerenciamento de memória abrange as ações utilizadas para controlar e coordenar a memória do computador.
- Vantagens das linguagens de programação mais recentes:
  - Fornecer gerenciamento automático de memória;
  - O gerenciamento automático torna erros menos propícios.

Remoção de Secure Sockets Layer (SSL)

- Ataque intermediário contra todos os SSL e versões anteriores de TLS.
- Características:

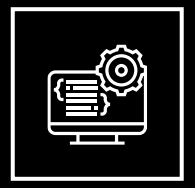
Realizado em qualquer lugar em que um ataque *man-in-the-middle* possa acontecer.

Intercepta a solicitação de conexão inicial para HTTPS, redirecionando-a para um site HTTP.

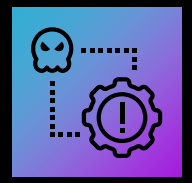
Funciona porque o início de um *handshake* SSL ou TLS é vulnerável. Use apenas TLS 1.2 ou 1.3

Manipulação de Drivers

Drivers são softwares que ficam entre o SO e um dispositivo periférico.



Drivers podem fazer parte do SO ou desenvolvidos por terceiros.



Manipulação de driver: ataque a um sistema por meio da alteração de drivers.

Shimming

- Processo de colocar uma camada de código entre o driver e o SO.
- Características:

Permite flexibilidade e portabilidade;

Fornece alterações entre versões de um SO sem modificar o código;

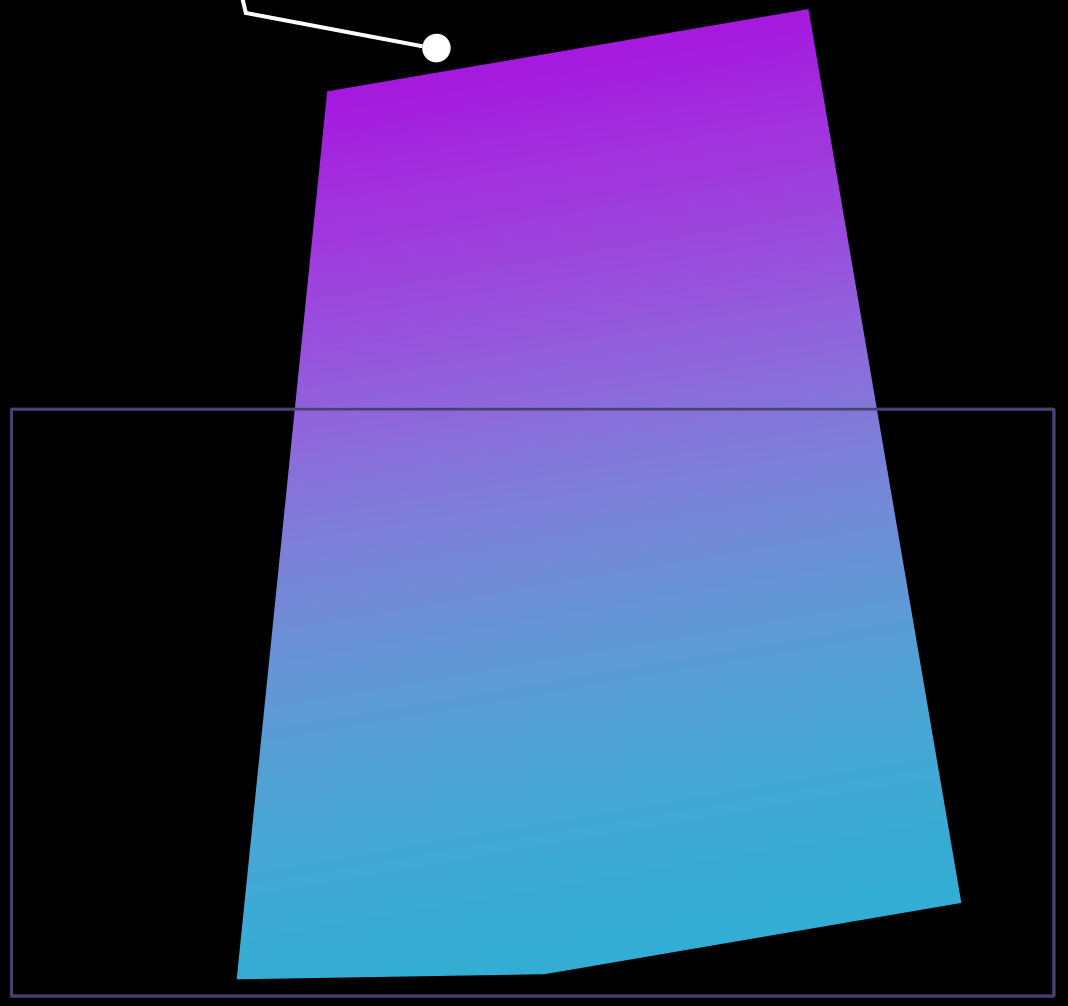
Representa um meio pelo qual um código malicioso pode mudar o comportamento de um driver.

Refatoração

- Processo de reestruturação do código de computador existente, sem alterar seu comportamento externo.
- Características:
  - Feito para melhorar atributos não funcionais do software.
  - Pode descobrir falhas de design que levam a vulnerabilidades.
  - Um meio pelo qual um invasor pode adicionar funcionalidade a um driver.
  - A refatoração de driver é quando um driver é substituído por um driver malicioso.

Pass the Hash

- Técnica de hacking em que o invasor captura o hash para autenticar um processo.
- Características:
  - Podem usar esse hash injetando-o em um processo no lugar da senha;
  - Um ataque altamente técnico;
  - O invasor não sabe a senha, mas pode usar um hash capturado e injetá-lo diretamente.



OBRIGADO!

OUTROS ATAQUES DE APLICATIVOS