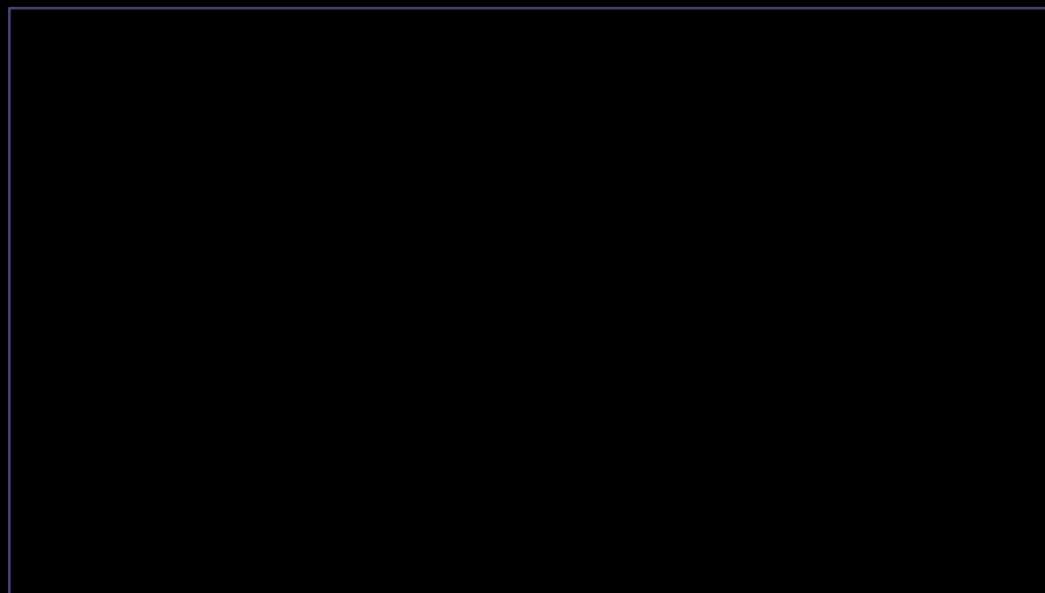




Prime

CCS-A

Ataques de Aplicativos



Escalonamento de Privilégios



Começa no usuário comum e vai até o nível de administrador.



Ataque em cadeia é chamado de **escalonamento de privilégios**.



Uma maneira de usar os privilégios é executar uma ação que roube o maior tipo de credencial possível.



Para se defender:

Evitar processos e serviços com privilégios elevados.

Cross-Site Scripting (XSS)

- ▶ Uma das metodologias mais famosas de ataque na web.



Ataque XSS não persistente – O script injetado não é persistido ou armazenado;



Ataque XX persistente – O script é armazenado no servidor web;



Ataque XSS baseado em DOM – O script é executado no navegador através do *Document Object Model* (DOM).

- ▶ Amplas consequências.

Para se defender



- ▶ Uso de bibliotecas anti-XSS para remover scripts das sequências de entrada.
- ▶ A validação de entrada evita que dados formados incorretamente entrem no sistema.

Ataques de Injeção

- ▶ Linguagem de Consulta Estruturada (SQL) - Envolve a manipulação de entrada.
- ▶ *Extensible Markup Language* (XML) e *Lightweight Directory Access Protocol* (LDAP) são executados do mesmo jeito.
- ▶ Como ocorre:



Acesso ao banco de dados.



Manipula a linha de comando.

SQL Injection

```
| Select count(*) from users_table where username = 'Adriano' and  
| password = 'senha'  
| 'or 1=1  
| Select count(*) from users_table where username = 'Adriano' and  
| password = ''or 1=1 --' |
```

Copiar

Colar

- ▶ Sanitizar (restringir caracteres como ; e --);
- ▶ Validar (entrada e restringir número de caracteres);
- ▶ Consultas parametrizadas (Analisa o parâmetro, e se for bom, envia para instruções SQL);

Biblioteca Dinâmica de Links (DLL)



Pedaço de código para adicionar funcionalidade a um programa por meio da inclusão de rotinas de biblioteca vinculadas em tempo de execução.



Injeção de DLL:

Adicionar uma DLL no diretório correto ou por meio de uma chave no registro.



Exemplo:

Microsoft Office ou qualquer outro programa que força o carregamento de uma DLL infectada.

Lightweight Directory Access Protocol (LDAP)

- ▶ Sistemas baseados em LDAP estão sujeitos a ataques de injeção.
- ▶ Hacker preenchendo um formulário da web que usa os dados para consultar um BD com uma chamada LDAP.
- ▶ Quando uma solicitação LDAP incorreta pode surgir:
 - ▶ Construção do LDAP com base na entrada do usuário.



Para se defender
Validação de entrada.

Linguagem de Marcação Extensível (XML)

- ▶ O XML pode ser adulterado via ataque de injeção.
- ▶ O objetivo do XML Injection é manipular um sistema baseado em XML.
- ▶ Vários alvos, por conta da onipresença do XML na web.
- ▶ Pode afetar:



Configurações;



Fluxos de dados;



Saídas de aplicativos.

Desreferência de Ponteiro / Objeto

- ▶ **Ponteiros** são ferramentas que os programadores usam para se referir a uma área da memória.
- ▶ Algumas linguagens de computador usam uma construção chamada de **ponteiro**.
- ▶ Desreferenciar um ponteiro = Alteração do significado do objeto para o conteúdo do local de memória.
- ▶ Quando um programador quer ler o conteúdo da memória, ele desreferencia o ponteiro.



Para se defender

Certifique-se de bloquear a execução de código não confiável ou injetado para que os hackers não possam ler essas áreas de memória.

Ataque de Passagem de Diretório

- ▶ Um invasor usa entradas especiais (../..) para contornar a estrutura da árvore de diretório do sistema de arquivos.
- ▶ Principais características:
 -  A entrada pode resultar na execução de código de forma não autorizada;
 -  São difíceis de detectar;
 -  Digitar ../.. várias vezes na URL para navegar através da estrutura de diretórios do servidor web.
- ▶ Para proteger contra ataques de travessia de diretório, inclua na lista negra caracteres comuns, como ../..

Buffer Overflow

- ▶ Tipo de ataque mais comum e mais utilizado.
- ▶ Um buffer é uma área de memória usada para armazenar informações enviadas a um aplicativo.
- ▶ Um estouro de buffer ocorre quando é enviado muitas informações para o aplicativo.
- ▶ Principais características:
 -  Substituído por dados maiores no buffer que a entrada do programa.
 -  Aproveita as restrições de espaço e desempenho e insere códigos maliciosos.
 -  Tiram proveito da não validação do comprimento das entradas.

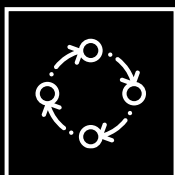
Condição de Corrida

- Condição que ocorre quando a saída de uma função depende da sequência ou tempo das entradas.
- Condição clássica: uma thread deve ser concluído em uma ordem específica antes que outra seja executada.
- Melhor forma de defesa: entender e gerenciar bloqueios.
- São definidas por janelas corrida (minimizando o tempo e sequenciando o objeto que é usado e libere-o novamente).
- Condições de corrida podem ser usadas para elevação de privilégios e ataques de negação de serviço.

Tempo de Verificação / Tempo de Uso



Sistemas diferentes podem interagir com o mesmo objeto ao mesmo tempo. Também é possível que eventos ocorram fora de sequência.



Problemas de sequência e loop infinito influenciam o projeto e a implementação das atividades de dados.



Entender essas condições é importante para os membros do time de desenvolvimento.



Ataque de Tempo de Verificação/Uso

Tira vantagem de uma separação entre o momento em que um programa verifica um valor e quando ele o utiliza.

Tratamento Inadequado de Erros

- ▶ Uma metodologia de ataque inclui forçar erros.
- ▶ Arquivo de log é uma fonte inestimável de informações.
- ▶ Erros típicos:



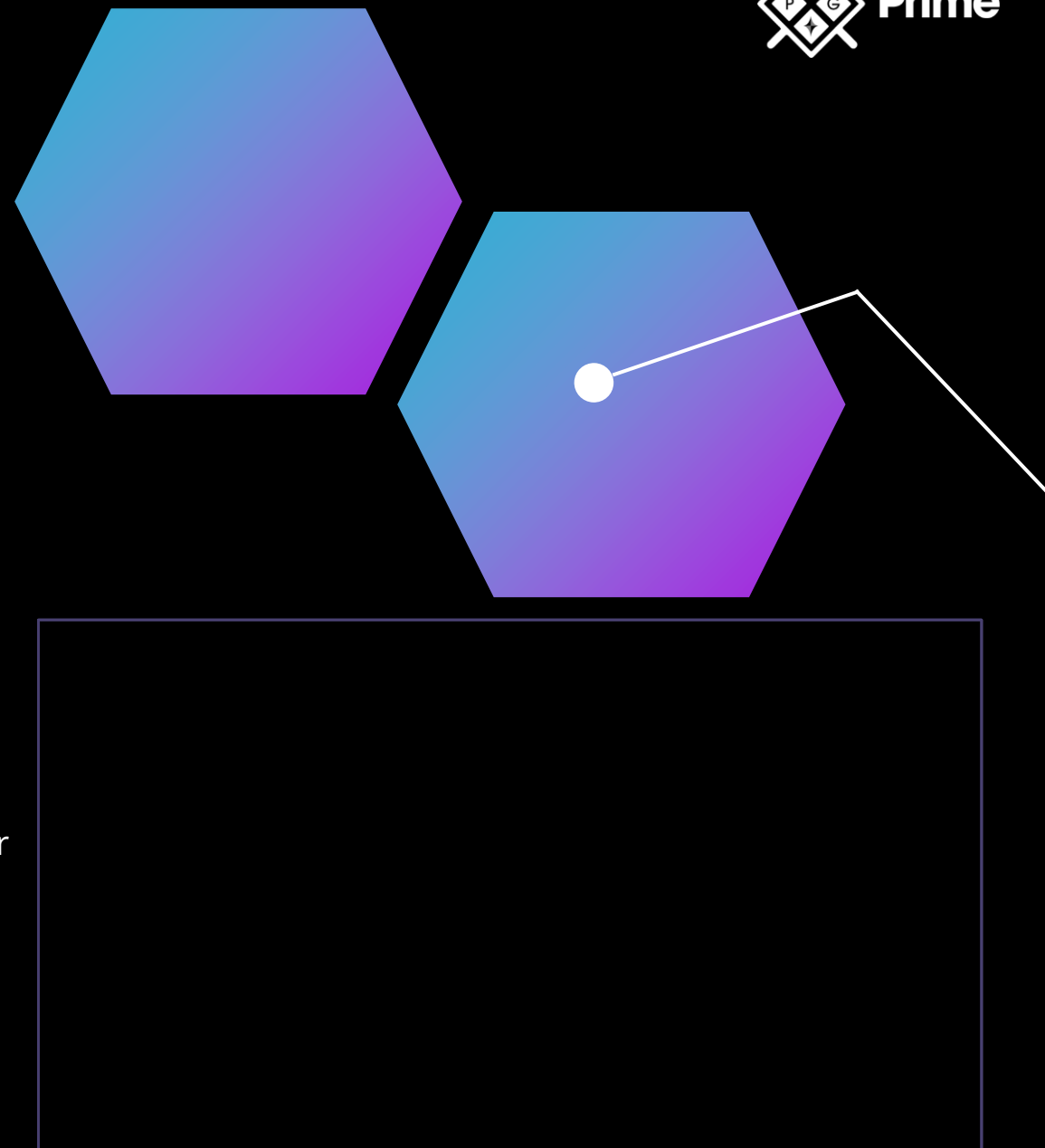
Transmitir informações do erro para o usuário.



Erros associados a instruções SQL podem revelar estruturas de dados e elementos de dados.



Erros em programas revelam números de linhas em que ocorreu uma exceção, o método que foi usado etc. Proteja com ACL.



Manipulação Inadequada de Entrada



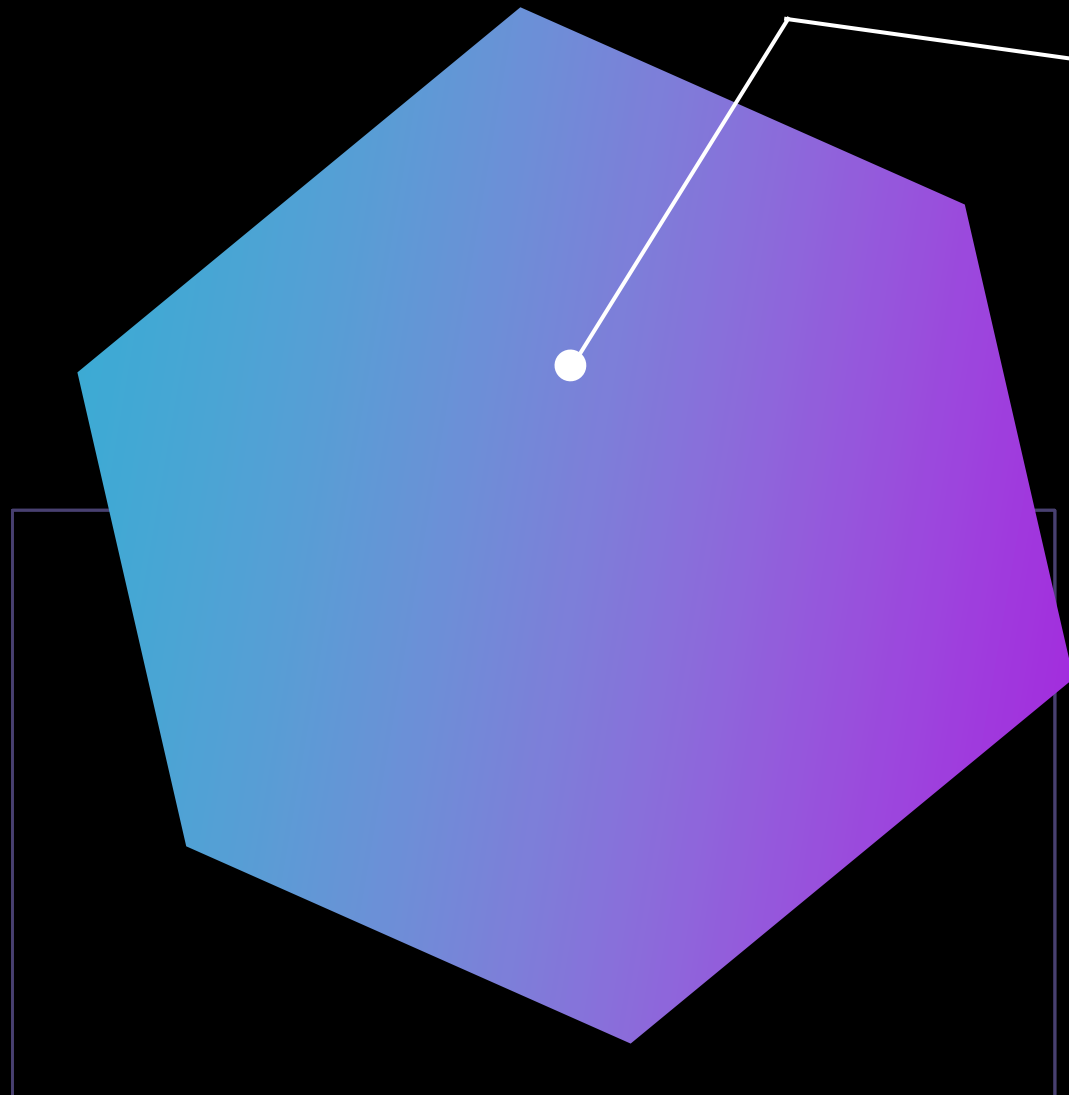
Verdadeira causa das vulnerabilidades de software.



Como evitar:

O ato de considerar todas as entradas hostis pode mitigar ataques com vulnerabilidades comuns.

- ▶ A validação de entrada é adequada para:
 - ▶ Buffer overflow;
 - ▶ Dependência de entradas não confiáveis;
 - ▶ Cross-Site Scripts (XSS);
 - ▶ Falsificação de solicitação entre sites (XSRF);
 - ▶ Passagem de diretório;
 - ▶ Cálculo incorreto do tamanho do buffer.
- ▶ A validação de entrada não é capaz de conter a maioria dos ataques de injeção.



OBRIGADO!

INDICADORES DE ATAQUES
DE APLICATIVOS