OWASP
Open Web Application Security Project

A4: Referência Insegura e Direta a Objetos

Segurança de Aplicações

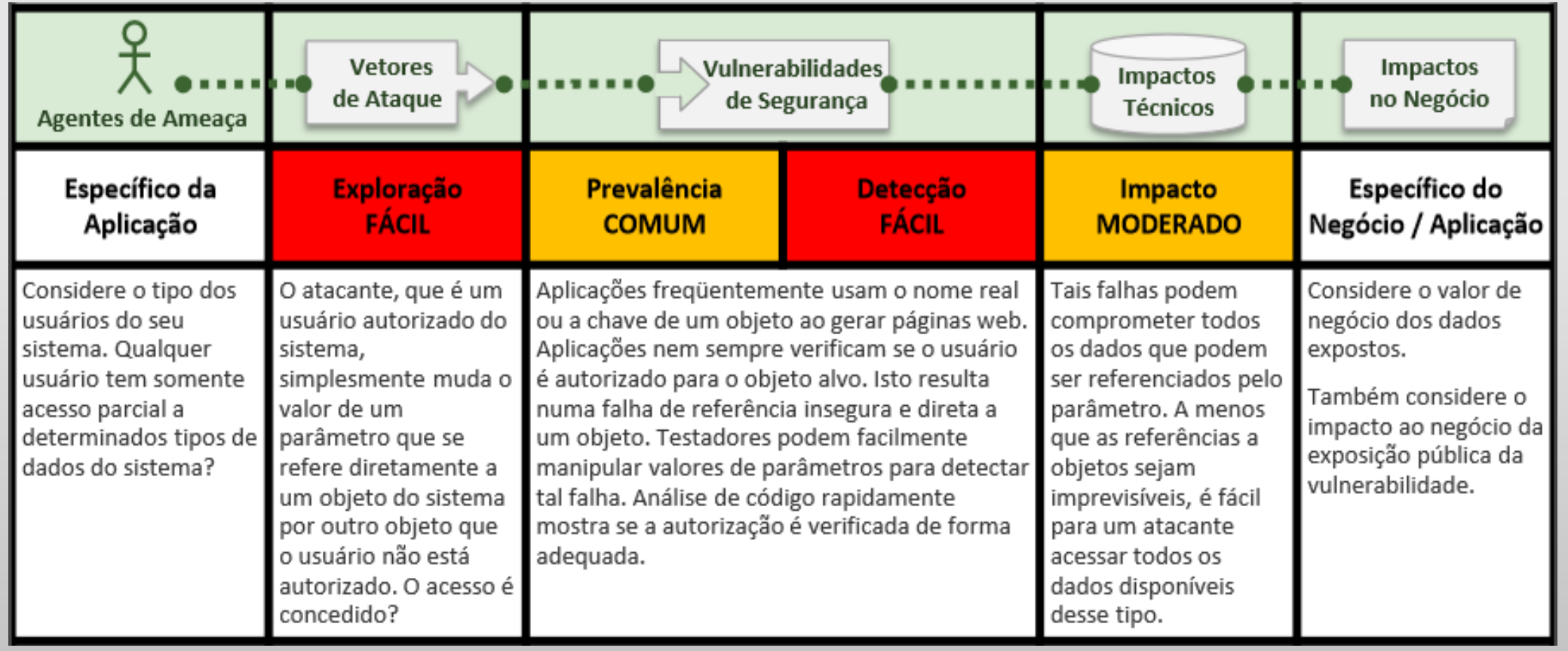
Felipe Ayres

A4: Referência Insegura e Direta a Objetos

Uma referência direta a um objeto ocorre quando um programador expõe uma referência para um objeto interno da implementação, como:

- Arquivo
- Diretório
- Chave de uma tabela no banco de dados
- URL
- Parâmetro de formulário

A4: Referência Insegura e Direta a Objetos



Específico da Aplicação	Exploração FÁCIL	Prevalência COMUM	Detecção FÁCIL	Impacto MODERADO	Específico do Negócio / Aplicação
Considere o tipo dos usuários do seu sistema. Qualquer usuário tem somente acesso parcial a determinados tipos de dados do sistema?	O atacante, que é um usuário autorizado do sistema, simplesmente muda o valor de um parâmetro que se refere diretamente a um objeto do sistema por outro objeto que o usuário não está autorizado. O acesso é concedido?	Aplicações freqüentemente usam o nome real ou a chave de um objeto ao gerar páginas web. Aplicações nem sempre verificam se o usuário é autorizado para o objeto alvo. Isto resulta numa falha de referência insegura e direta a um objeto. Testadores podem facilmente manipular valores de parâmetros para detectar tal falha. Análise de código rapidamente mostra se a autorização é verificada de forma adequada.		Tais falhas podem comprometer todos os dados que podem ser referenciados pelo parâmetro. A menos que as referências a objetos sejam imprevisíveis, é fácil para um atacante acessar todos os dados disponíveis desse tipo.	Considere o valor de negócio dos dados expostos. Também considere o impacto ao negócio da exposição pública da vulnerabilidade.

Estou vulnerável?

1. Para referências diretas a recursos restritos, a aplicação falha em verificar se o usuário está **autorizado** a acessar o exato recurso que ele requisitou?

2. Revisão de código da aplicação pode rapidamente verificar se qualquer abordagem é implementada com segurança.

Ferramentas automatizadas normalmente não procuram por essa falha, porque elas não podem reconhecer o que requer proteção ou o que é seguro ou inseguro.

Exemplo de Cenário de Ataque

A aplicação utiliza dados não verificados em uma chamada SQL que está acessando as informações de conta:

http://example.com/app/accountInfo?acct=**1**

```
String query = "SELECT * FROM accts WHERE account = ?";

PreparedStatement pstmt =
connection.prepareStatement(query , ... );

pstmt.setString( 1, request.getParameter("acct"));
```

O atacante simplesmente modifica o parâmetro 'acct' em seu navegador para enviar qualquer número de conta. Se não verificado adequadamente, o atacante pode acessar qualquer conta de usuário, em vez de somente a conta do cliente pretendido.

http://example.com/app/accountInfo?acct=**notmyacct**

Exemplo de Cenário de Ataque

Chave de uma tabela no banco de dados

URL gerada pela aplicação:

http://www.example.com/visualiza_info_conta.jsp?userId=**43510** ← acesso legítimo

URL adulterada:

http://www.example.com/visualiza_info_conta.jsp?userId=**54112** ← acesso indevido

Exemplo de Cenário de Ataque

Identificador de um Arquivo e Diretório

URL gerada pela aplicação:

http://www.example.com/downloadFile.do?filePath="**/var/lib/docs/file1.doc**“ ← acesso legítimo

URL adulterada:

http://www.example.com/downloadFile.do?filePath="**/var/lib/docs/file2.doc**“ ← acesso indevido

http://www.example.com/downloadFile.do?filePath="**/etc/shadow**" ← acesso indevido

Como faço para evitar?

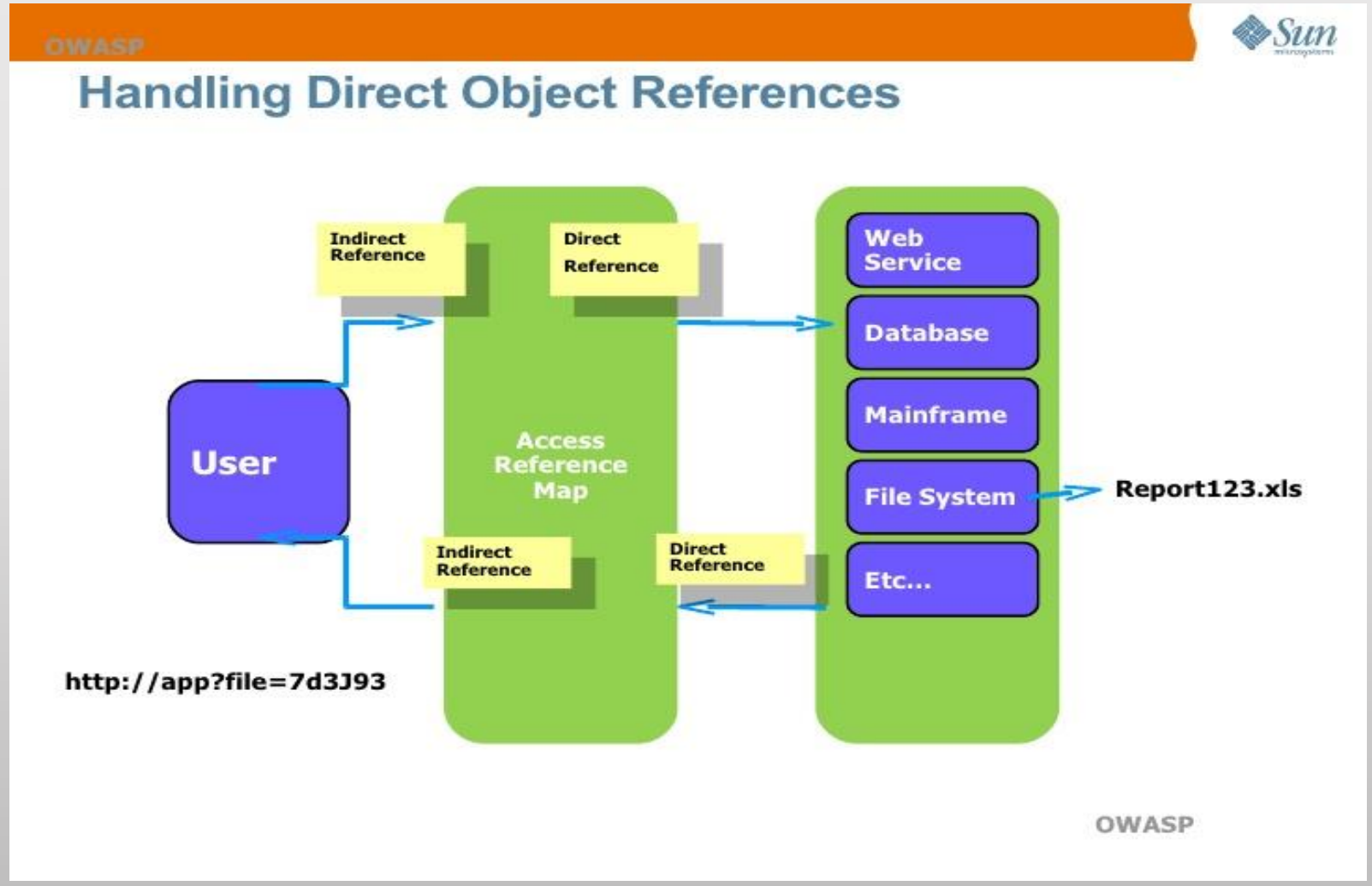
1. Utilize referências indiretas a objetos.

Uso de referência indiretas a objetos por usuário ou sessão. Isso impede que o atacante atinja diretamente os recursos não autorizados.

É usado para mapear referências diretas a objetos e mostrar referências indiretas, que são seguras para serem mostradas publicamente.

Mapa de Referência Indireta

Pode ser usado para ajudar a proteger nome de colunas de BD, nomes de arquivos, e qualquer outro tipo de referência direta.



Como faço para evitar?

2. Controle de Acesso

Verificar o acesso. Cada utilização de uma referência direta a objeto de uma origem não confiável deve incluir uma verificação de controle de acesso para garantir que o usuário está **autorizado** para o objeto requisitado.

Com falha de Referência Direta

```
int cartID = Integer.parseInt( request.getParameter( "cartID" ) );
String query = "SELECT * FROM table WHERE cartID=" + cartID;
```

Sem falha de Referência Direta

```
int cartID = Integer.parseInt( request.getParameter( "cartID" ) );
User user = (User)request.getSession().getAttribute( "user" );
String query = "SELECT * FROM table WHERE cartID=" + cartID + " AND
userID=" +
user.getID();
```

Casos conhecidos

Caso Real (ATO).

- No site da Australian Taxation Office's GST Start Up Assistance, um usuário modificou o ABN (identificador da empresa) que estava na URL.
  Resultado: O usuário se apossou de cerca de **17.000** registros de empresas cadastradas no sistema.

- Como eu usei o cartão de crédito do CEO do trampos.co para pagar minha assinatura Premium

Referências Diretas do Trabalho

http://www.fidelis.work/como-eu-usei-o-cartao-de-credito-do-ceo-do-trampos-co-para-pagar-minha-assinatura-premium/

http://pt.slideshare.net/lucams/referncia-insegura-direta-a-objeto

https://prezi.com/vgjmxevz9v5m/referencia-insegura-e-direta-a-objeto/

https://www.troyhunt.com/owasp-top-10-for-net-developers-part-4/

https://books.google.com.br/books?id=ndgRZ0notxgC&pg=PA142&lpg=PA142&dq=mapa+de+refer%C3%AAncia+indireta+aos+objetos&source=bl&ots=2dhD_fUquD&sig=byXr5VB6_XeP7b_-yc2Y7PUIqOA&hl=pt-BR&sa=X&ved=0ahUKEwj6vZnSxbnOAhUDEpAKHZZQAfQQ6AEIHDAA#v=onepage&q=mapa%20de%20refer%C3%AAncia%20indireta%20aos%20objetos&f=false