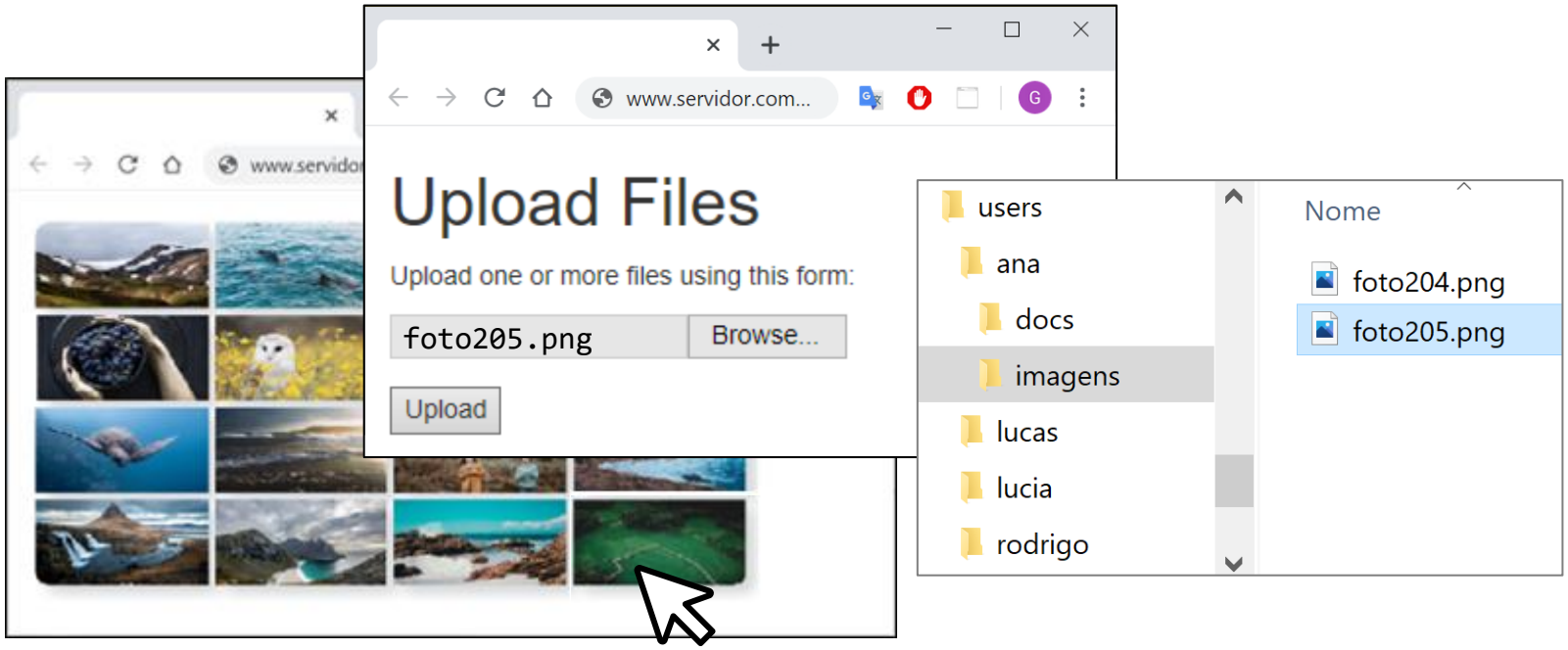
Caminho transversal
(*Path Traversal*)

CWE-35: Path Traversal

FURB
UNIVERSIDADE DE BLUMENAU

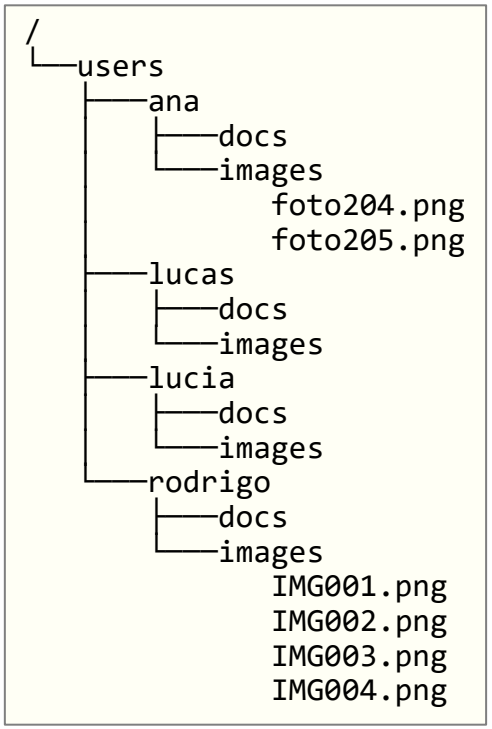
Motivação

Considerar um website que permite que o usuário envie arquivos (fotos, vídeos, etc)




```
http://www.servidor.com/imagens/foto205.png
```

Motivação



Para que o usuário “ana” faça o download de uma foto específica, acessa a seguinte URL:

```
http://www.servidor.com/imagens/filename=IMG001.png
```

Isto é, a aplicação define o nome do arquivo concatenando:

```
"/users/" + currentUser() + "/images/" + filename
```

Gerando portanto a string:

```
/users/ana/images/IMG001.png
```

Contudo, o usuário poderia invocar:

```
http://www.servidor.com/imagens/filename=../../rodrigo/images/IMG001.png
```

Que levaria a aplicação a acessar:

```
/users/evandro/images/../../rodrigo/images/IMG001.png
```

Caminho transversal

- A possibilidade de utilizar um caminho relativo para acessar um arquivo além do diretório esperado é chamado de **Caminho transversal** (*Path traversal* ou *Directory traversal*).

- Ocorre quando um software permite que o usuário informe o nome de um arquivo para leitura de um diretório específico (restrito), porém o software não restringe caracteres especiais no nome do arquivo, permitindo que o arquivo seja lido de outro local.

Definição

- Ao utilizar alguns elementos especiais, como “..” ou “/”, agentes podem acessar arquivos de locais diferentes do esperado pelo fabricante do software.

- A sequencia “../” é interpretada como o diretório pai do diretório atual, e o uso deste termo permite acessar um caminho relativo.

Como evitar

Caminho transversal

- Efetuar o “saneamento” da entrada. O saneamento consiste em simplesmente suprimir a sequência de caracteres indesejadas. Por exemplo:

```
http://www.servidor.com/images/filename=../../marta/images/IMG001.png
```

- Suprimindo as ocorrências de “../”, ficaria:

```
http://www.servidor.com/images/filename=marta/images/IMG001.png
```

- Contudo, considerar que o agente poderia fornecer:

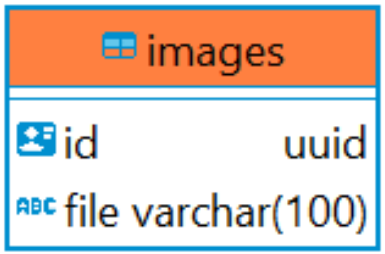
```
http://www.servidor.com/images/filename=..../marta/images/IMG001.png
```

Como evitar

Caminho transversal

- Validar a entrada contra uma lista branca, para aceitar somente caracteres de uma lista de permissões rigorosa, limitando assim os caracteres que podem ser utilizados como nome de arquivo.

- Ao invés de trabalhar com nomes de arquivos ou caminhos, atribuir códigos para cada arquivo. Estes arquivos são mapeados para o arquivo correspondente



	id	file
1	93d9ca36-5dc0-4ef3-bf23-10085b60c263	FOTO1.JPG
2	8972150c-e65c-4654-80f4-2252f661b1e0	VERAO2018.PNG
3	2e601b5e-318f-4b2c-b4e9-8cf83119db62	2018_05_02-NIVER.JPG

http://www.servidor.com/imagens/fileid=2e601b5e-318f-4b2c-b4e9-8cf83119db62