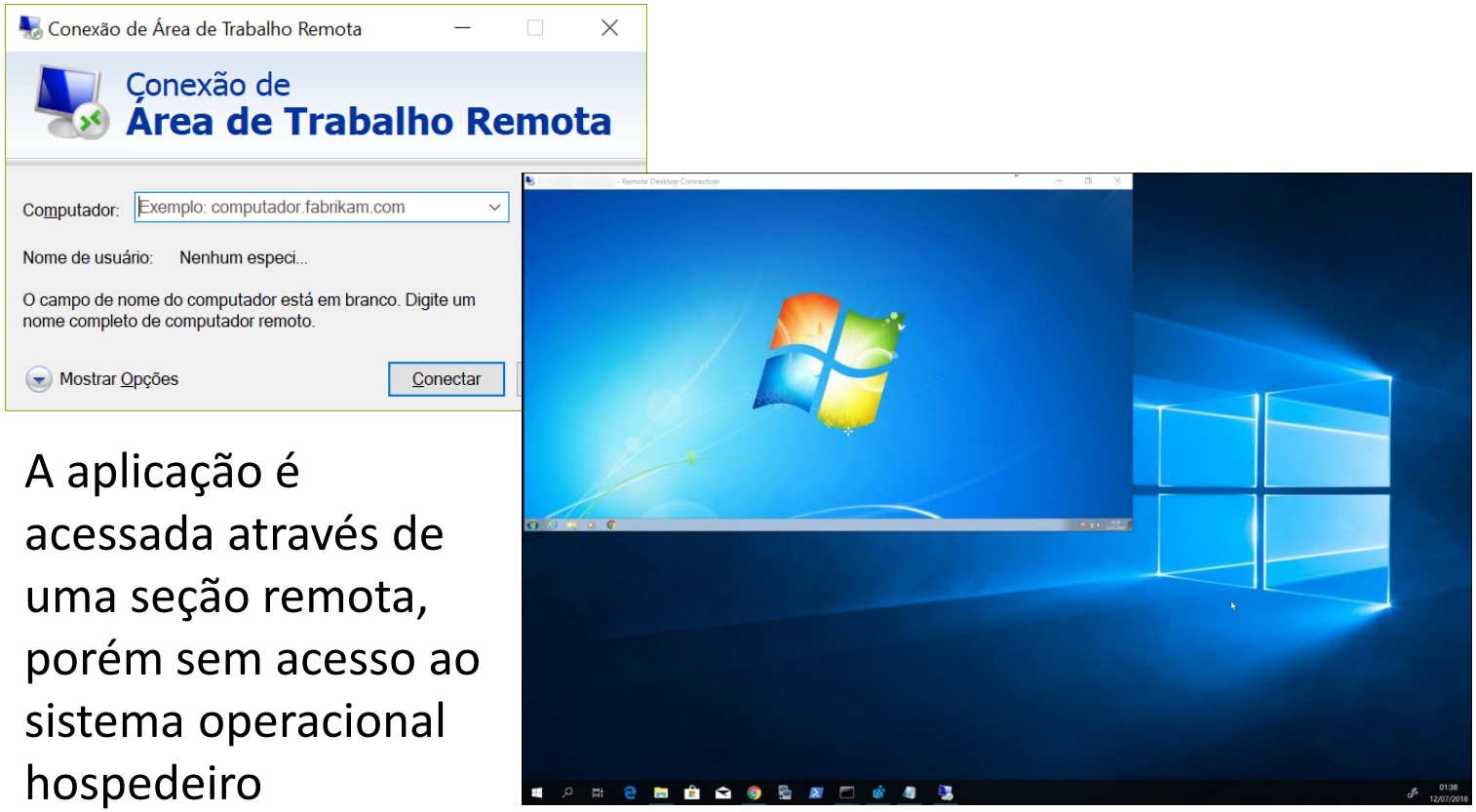
Injeção de comandos do sistema operacional (OS Command Injection)

CWE-78

FURB
UNIVERSIDADE DE BLUMENAU

Motivação



A aplicação é acessada através de uma seção remota, porém sem acesso ao sistema operacional hospedeiro

Exemplo 1

- Considerar que a aplicação possui uma funcionalidade que possibilita descompactar arquivos e que o nome do arquivo é fornecido pelo usuário
- Neste fragmento de código, a aplicação descompacta um arquivo, invocando uma aplicação externa

```
public void unpackFile(String fileName) {
    String commandLine = getUnzipApp() + " "  + " x -y " + "\"" + fileName + "\"";
    File defaultDir = new File((new File(arquivo)).getParent());
    Process p = Runtime.getRuntime().exec(commandLine, null, defaultDir);
    p.waitFor();
}
```

```
public String getUnzipApp() {
    if (Settings.getInstance().hasUnzipApp()) {
        return Settings.getInstance().unzipApp();
    } else {
        return "C:\\Program Files\\7-Zip\\7z.exe";
    }
}
```

Exemplo 1

- Um caso esperado, seria:

```
dados.zip
```

```
commandLine = "C:\\Program Files\\7-Zip\\7z.exe x -y \dados.zip \";
```

- Entretanto, o usuário poderia fornecer:

```
dados.zip & delete \. /s/q
```

- O caractere “&” é utilizado para separar comandos.

Definição Injeção de comandos do sistema operacional

- Ocorre quando alguma função da aplicação é executada através de comandos do sistema operacional ou por aplicações externas e sofrem influência da entrada do usuário.

- Nesta situação, quando a entrada de dados contém comandos especiais, é possível executar comandos diretamente do sistema operacional
  - Pode permitir a execução de comandos privilegiados (que o usuário não teria acesso, mas a aplicação possui)

- Também conhecido como *Shell injection*

Exemplo 2

- Neste fragmento, a aplicação busca listar o conteúdo do diretório **home** do usuário:

```
$userName = $_POST["user"];
$command = 'ls -l /home/' . $userName;
system($command);
```

- Um exemplo esperado do uso do comando:

```
ls -l /home/lucas
```

- Entretanto, o usuário poderia editar o parâmetro “user” para:

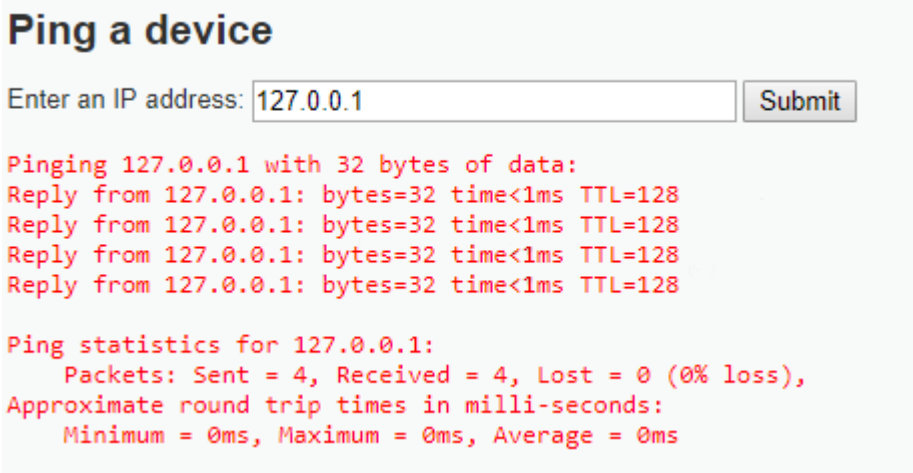
```
;rm -rf /
```

- Causando a execução de:

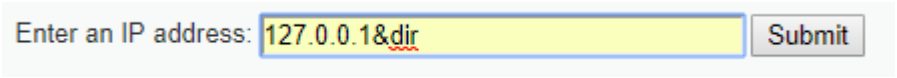
```
ls -l /home/;rm -rf /
```

Exemplo 3

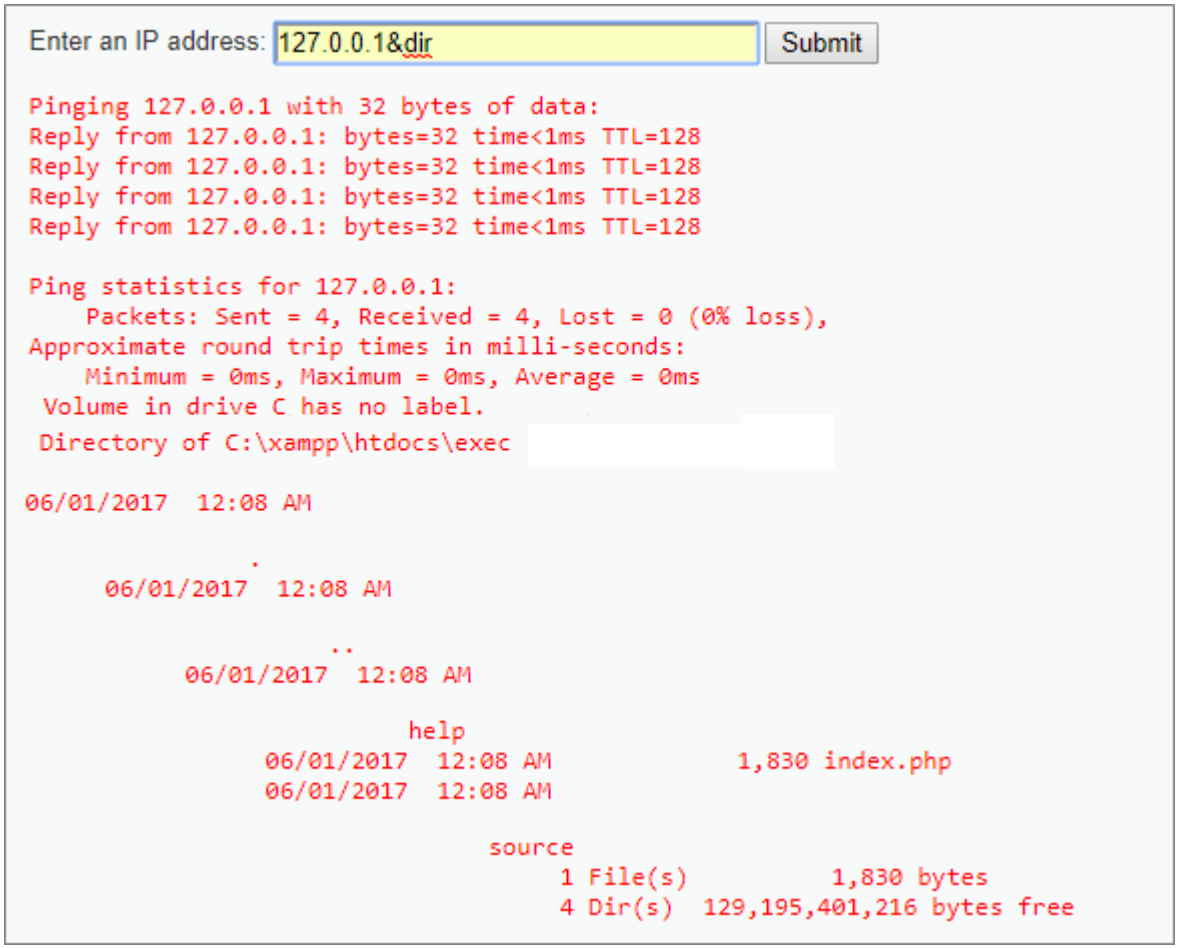
Esta aplicação permite conferir se um ponto TCP/IP está acessível:



A vulnerabilidade poderá ser explorada se a entrada contiver:



Exemplo 3


Enter an IP address: 127.0.0.1&dir
Submit
Pinging 127.0.0.1 with 32 bytes of data:
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128
Ping statistics for 127.0.0.1:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 0ms, Average = 0ms
Volume in drive C has no label.
Directory of C:\xampp\htdocs\exec
06/01/2017 12:08 AM
.
06/01/2017 12:08 AM
..
06/01/2017 12:08 AM
help
06/01/2017 12:08 AM
1,830 index.php
06/01/2017 12:08 AM
source
1 File(s)
1,830 bytes
4 Dir(s)
129,195,401,216 bytes free

Evitando Injeção de comandos do SO

- Implementar uma lista branca de caracteres aceitáveis
- Utilizar APIs da linguagem para interagir com o sistema operacional (e evitar chamadas de programas externos)