Neutralização inadequada da saída para logs

CWE-117: Improper Output Neutralization for Logs

Neutralização inadequada da saída para logs

- Nesta vulnerabilidade, o software grava no log dados digitados pelo usuário. Como não é feita validação sobre a entrada de dados, o agente pode forjar entradas de log.

- No exemplo, uma aplicação web tenta ler um número inteiro da requisição. Se a entrada não for um número, uma mensagem de erro é acrescentada no arquivo de log:

```
String val = request.getParameter("val");
try {
    int value = Integer.parseInt(val);
} catch (NumberFormatException) {
    log.info("Falha ao analisar: " + val);
}
...
```

Neutralização inadequada da saída para logs

- Se o usuário submeter o texto “trinta e cinco”, é feita a seguinte chamada:

```
http://servidor.com/val=trinta%20e%20cinco
```

- Causando a geração do seguinte log no arquivo:

```
INFO: Falha ao analisar: trinta e cinco
```

- Um agente poderia fornecer a seguinte entrada

```
http://servidor.com/val=trinta%0aINFO:%20Usuario%20desconectado:
%20malfeitor
```

- Causando a seguinte saída:

```
INFO: Falha ao analisar: trinta
INFO: Usuario desconectado: malfeitor
```

Neutralização inadequada da saída para logs

- Uma defesa simples seria alterar todas as entradas contendo os caracteres \n e \r com outro símbolo, como:

```
message.replaceAll('\n', '_').replaceAll('\r', '_');
```

Uso excessivo de logs

CWE-779: Logging of Excessive Data

Uso excessivo de logs

- Ocorre quando uma aplicação possibilita a geração de logs em excesso, causando:
  - Dificuldade em processar o arquivo de log
  - Dificuldade em realizar análise dos arquivos de log
  - Falhas no sistema por falta de espaço no dispositivo de armazenamento

Uso excessivo de logs

- Como mitigar
  - Registrar apenas o que for essencial, que auxilia na depuração e correção de erros
  - Suprimir logs repetidos
  - Estabelecer um tamanho máximo para o arquivo de log.
    - Notificar o administrador do sistema caso o arquivo de log esteja atingindo um limite máximo.
    - Considerar também reduzir as funcionalidades que o usuário possa realizar, embora isso possa impossibilitar o acesso de usuários legítimos