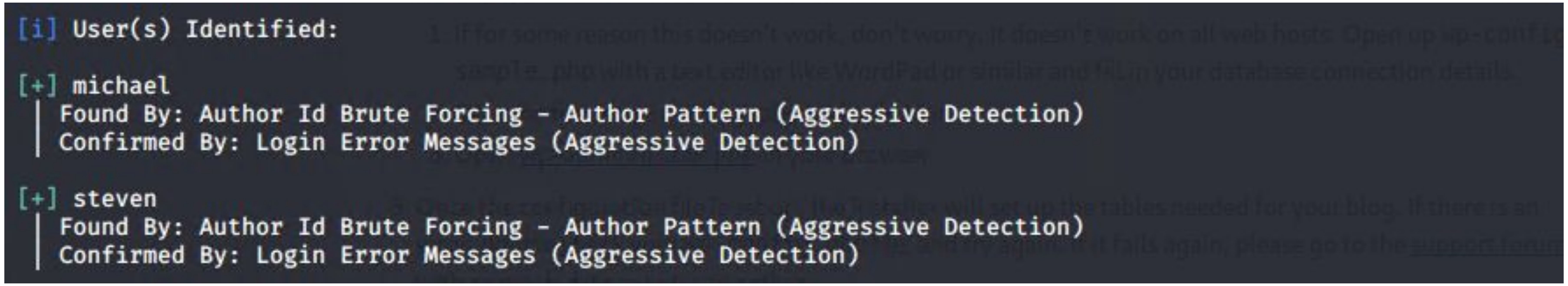
Exploitation: Open Port 22 SSH and Weak Passwords

Summarize the following:

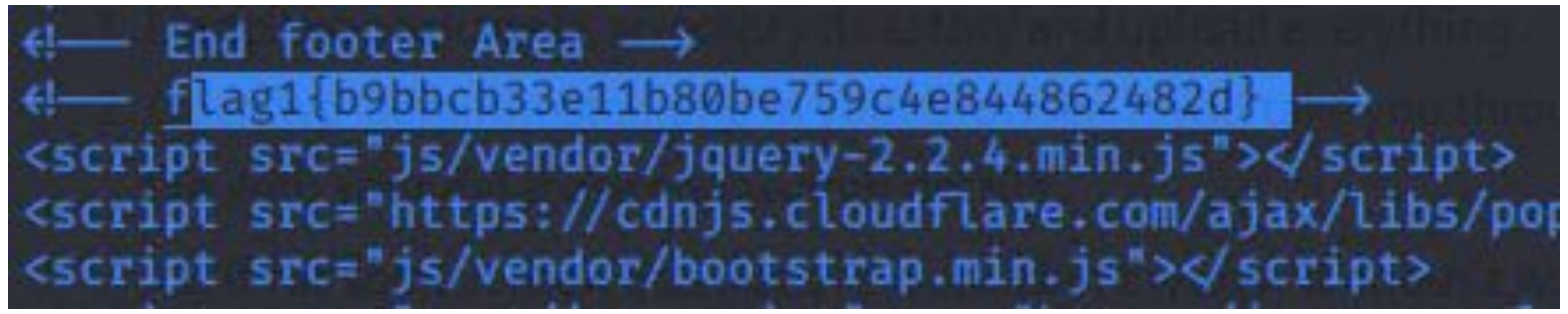
- How did you exploit the vulnerability?
  - We used wpscan to find the users and guessed the weak password in order to SSH into the system.
- What did the exploit achieve?
  - The exploit granted us user shell access for Michael’s account. We explored the files to find flags 1 and 2



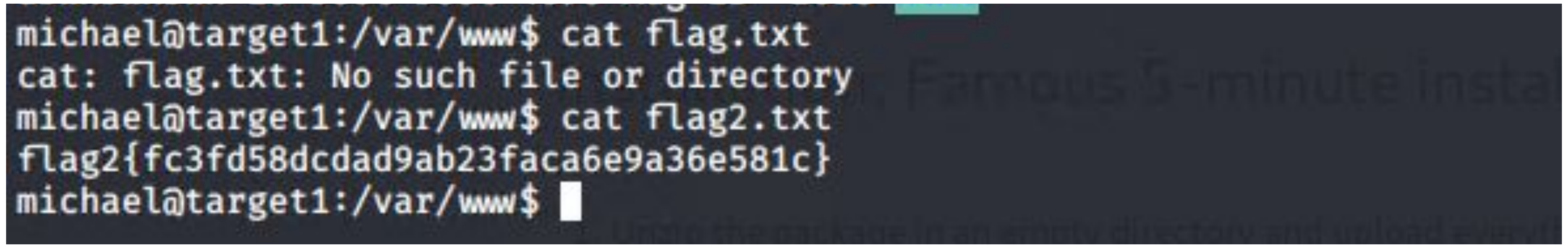
```
[i] User(s) Identified:

[+] michael
 | Found By: Author Id Brute Forcing - Author Pattern (Aggressive Detection)
 | Confirmed By: Login Error Messages (Aggressive Detection)

[+] steven
 | Found By: Author Id Brute Forcing - Author Pattern (Aggressive Detection)
 | Confirmed By: Login Error Messages (Aggressive Detection)
```



```
<!-- End footer Area -->
<!-- flag1{b9bbcb33e11b80be759c4e844862482d} -->
<script src="js/vendor/jquery-2.2.4.min.js"></script>
<script src="https://cdnjs.cloudflare.com/ajax/libs/pop
<script src="js/vendor/bootstrap.min.js"></script>
```



```
michael@target1:/var/www$ cat flag.txt
cat: flag.txt: No such file or directory
michael@target1:/var/www$ cat flag2.txt
flag2{fc3fd58dcdad9ab23faca6e9a36e581c}
michael@target1:/var/www$ █
```