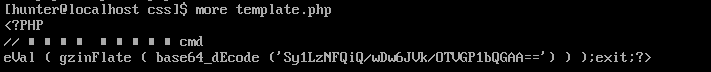
Lab 21:

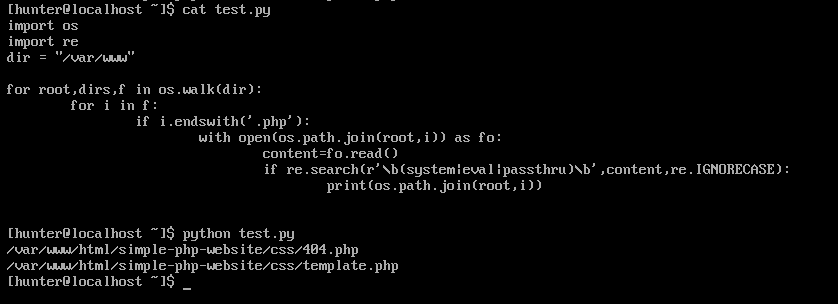
Backdoor PHP in CSS directory as 404.php:



Webshell in template.php:

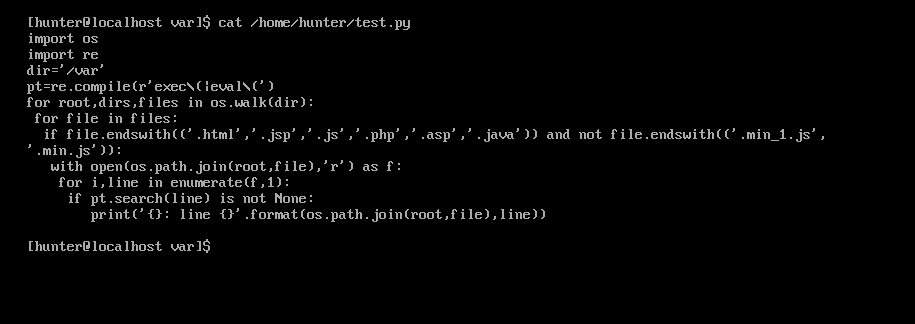


Simple script to scan:

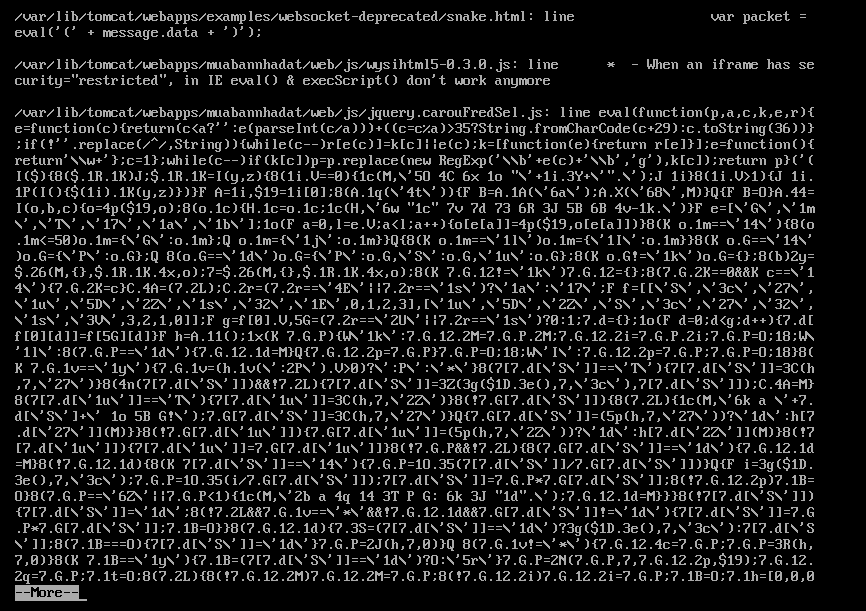


Lab 22:

Use simple python script:



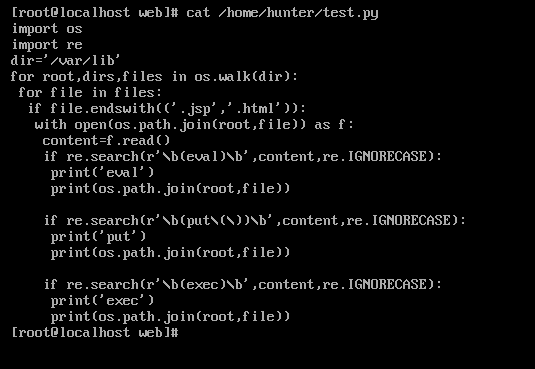
Run it and focus on some file has suspicious function:



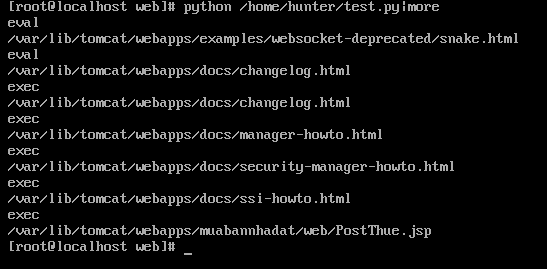
This file has obfuscaste sign and uses eval() function. Perhap, A webshell!

Lab 24:

Use simple python script:

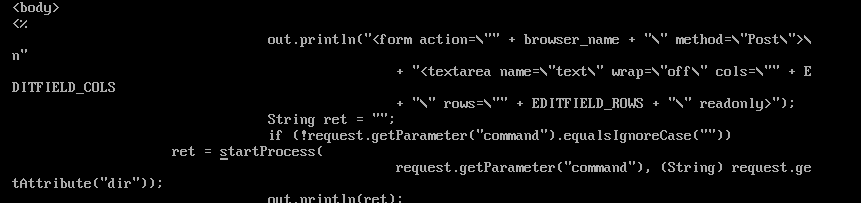


Have a list suspicious file using dangerous function:

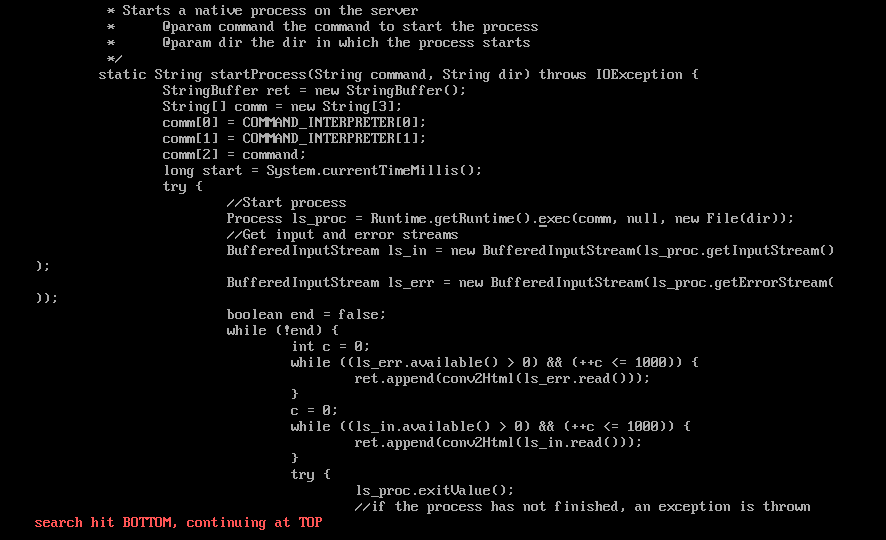


Let check them in a row:

Hmmm!



In PostThue.jsp has a command is pretty sus! Let check more detail about `startProcess()` function:



Kind of malicious funtion here, got them!